



BANCA D'ITALIA
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Analisi e studi

La normativa in tema di prevenzione del riciclaggio:
autorità, regole e controlli

a cura di Giovanni Castaldi e Claudio Clemente

febbraio 2023

numero

20



BANCA D'ITALIA
EUROSISTEMA



Unità di Informazione Finanziaria per l'Italia

Quaderni dell'antiriciclaggio

Analisi e studi

La normativa in tema di prevenzione
del riciclaggio: autorità, regole e controlli

Numero 20 - Febbraio 2023

La serie Quaderni dell'antiriciclaggio ha la finalità di presentare dati statistici, studi e documentazione su aspetti rilevanti per i compiti istituzionali dell'Unità d'Informazione Finanziaria per l'Italia.

La serie si articola in due collane: la collana Dati statistici presenta, con periodicità semestrale, statistiche sulle segnalazioni ricevute e informazioni sintetiche sull'operatività dell'Unità; la collana Analisi e studi comprende contributi sulle tematiche e sui metodi in materia di contrasto al riciclaggio e al finanziamento del terrorismo.

La collana Analisi e studi comprende lavori realizzati all'interno della UIF, talvolta in collaborazione con altri settori della Banca d'Italia o con Istituzioni esterne. I lavori pubblicati riflettono esclusivamente le opinioni degli autori, senza impegnare la responsabilità delle Istituzioni di appartenenza.

Comitato editoriale:

ALFREDO TIDU, GIOVANNI CASTALDI, MARCO LIPPI, PAOLO PINOTTI

Il Quaderno è stato curato da:

GIOVANNI CASTALDI E CLAUDIO CLEMENTE

I curatori ringraziano sentitamente tutti gli autori che hanno contribuito a celebrare con questo volume i primi quindici anni di attività della Unità di Informazione Finanziaria per l'Italia.

Un ringraziamento particolare a Luca Crisculo che ha inoltre curato, con pazienza e professionalità, la revisione del testo.

Le opinioni espresse dagli Autori non impegnano in alcun modo l'Istituto di appartenenza.

I contributi sono aggiornati alla data del 31 dicembre 2022.

© Banca d'Italia, 2023

Unità di Informazione Finanziaria per l'Italia

Direttore responsabile

Claudio Clemente

Per la pubblicazione cartacea:

autorizzazione del Tribunale di Roma n. 1942013 del 30 luglio 2013

Per la pubblicazione telematica:

autorizzazione del Tribunale di Roma n. 1932013 del 30 luglio 2013

ISSN 2283-3498 (stampa)

ISSN 2283-6977 (online)

Tutti i diritti riservati.

È consentita la riproduzione a fini didattici e non commerciali, a condizione che venga citata la fonte.

Stampa a cura della Divisione Editoria e stampa della Banca d'Italia

Indice

Premessa	7
CAPITOLO 1 - Prevenzione e repressione del riciclaggio (a cura di G. Castaldi)	11
1. Il contrasto del riciclaggio nel contesto internazionale (P. Costanzo)	11
2. L'evoluzione della disciplina internazionale (P. Costanzo e M. Siani)	23
3. Il riciclaggio nella prospettiva penale ed in quella amministrativa (F. Di Vizio)	37
4. Il finanziamento del terrorismo (F. Di Vizio)	50
CAPITOLO 2 - Autorità (a cura di C. Clemente)	56
1. Ministro e Ministero dell'Economia (I. Borrello e V. Tusini Cottafavi)	56
2. Il Comitato di Sicurezza Finanziaria (I. Borrello e V. Tusini Cottafavi)	58
3. Unità di informazione finanziaria per l'Italia (C. Clemente e I. Borrello)	63
4. Le Autorità di vigilanza di settore (R. Cervone)	74
5. La Direzione Nazionale Antimafia e Antiterrorismo (DNAA) (I. Borrello)	77
6. Amministrazioni e organismi interessati (S. Pace)	82
7. Organi investigativi: NSPV e DIA (W. Negrini)	85
8. I rapporti della UIF con le altre Autorità (A.M.A. Carriero e R. Circosta)	89
9. L'AMLA (Anti-Money Laundering Authority europea) (P. Costanzo)	96
CAPITOLO 3 - Adeguata verifica, profilazione, conservazione (a cura di G. Castaldi)	105
1. Analisi, valutazione e mitigazione del rischio (W. Negrini e L. La Rocca)	105
2. Profilazione del rischio del cliente (F. Berghella)	108
3. Adeguata verifica della clientela (I. Cosenza e I. Cesarotto)	111
4. Titolare effettivo (R. Circosta)	118
5. Misure di adeguata verifica della clientela (M. Colonnello)	123
6. Esecuzione degli obblighi di adeguata verifica da parte di terzi (M. Foppiani)	126
7. L'astensione (R. Tiberi)	130
8. Gli obblighi di conservazione (P. Bianchi)	133
CAPITOLO 4 - Segnalazione di operazioni sospette (a cura di D. Muratti)	138
Premessa (D. Muratti e A. Tidu)	138
1. La segnalazione di operazioni sospette (D. Muratti)	139
2. L'emersione del sospetto e le procedure di segnalazione (A. Monaco)	142
3. Il modello segnaletico (R. Marzano)	144
4. Indicatori e schemi di anomalia (L. La Rocca)	146
5. Selezione automatica delle operazioni sospette (F. Berghella)	150
6. Approfondimento delle segnalazioni (F. Fiorini, E. Prizio, G. Paoni e D. Colombo)	153
7. Sospensione delle operazioni sospette (B. Bastioni)	158
8. Tutela della riservatezza e divieto di comunicazione (D. Muratti)	164
9. Il flusso di ritorno (I. Longhi)	169

CAPITOLO 5 - I presidi organizzativi (a cura di R. Cercone)	173
Premessa (A. Marrone e F. Lelli)	173
1. Organi societari: compiti e responsabilità (A. Marrone e F. Lelli)	174
2. La funzione antiriciclaggio, il responsabile delle segnalazioni di operazioni sospette e la funzione di revisione interna (A. Marrone e F. Lelli)	175
3. Gli assetti organizzativi antiriciclaggio nei gruppi bancari e finanziari (A. Marrone e F. Lelli)	178
4. Il punto di contatto centrale (D. Muschella)	180
5. L'esercizio di autovalutazione (F. Lelli)	183
6. Aspetti evolutivi: gli Orientamenti EBA sulle politiche e le procedure relative alla gestione della conformità e al ruolo del responsabile antiriciclaggio (A. Marrone)	184
CAPITOLO 6 - Gli altri obblighi (a cura di A.M.A. Carriero)	186
Premessa (A.M.A. Carriero)	186
1. Le comunicazioni oggettive (C. Bentivogli e K. Bucaioni)	187
2. Segnalazione dei dati aggregati e analisi strategica (M. Gara e S. Iezzi)	194
3. Limitazioni all'uso del contante, degli assegni e di altri valori (A. Baldassarre)	198
4. Le informative delle FIU estere (D. Bartolozzi)	204
5. I movimenti transfrontalieri di contante: obblighi dichiarativi previsti dal D.lgs. 195/2008, evoluzione normativa e stato dell'arte (A. Cuzzocrea)	208
6. Le dichiarazioni di operazioni in oro: la legge 17 gennaio 2000, n. 7 (F. Di Natale e R. Coppola)	214
7. Whistleblowing (M. Siani)	217
8. Le comunicazioni della Pubblica amministrazione (R. Lo Santo e I. Cosenza)	220
CAPITOLO 7 - La prevenzione e il contrasto del finanziamento del terrorismo e dell'attività dei paesi che minacciano la pace e la sicurezza internazionale (a cura di G. Ilacqua)	224
Premessa (A. Cassetta e L. Baron)	224
1. Il quadro normativo internazionale (A. Cassetta e L. Baron)	225
2. La normativa nazionale (A. Cassetta e L. Baron)	226
3. Il finanziamento del terrorismo: tratti caratteristici del fenomeno (A. Cassetta e L. Baron)	228
4. Gli indicatori di anomalia e le comunicazioni della UIF (A. Cassetta e L. Baron)	231
5. Le segnalazioni di operazioni sospette (A. Cassetta e L. Baron)	233
6. Le sanzioni finanziarie "mirate" (D. Bartolozzi)	235
7. Le sanzioni dell'UE in risposta all'invasione russa dell'Ucraina (C. Greco e M. Soscia)	241
8. La proliferazione armi di distruzione di massa (D. Bartolozzi)	244
CAPITOLO 8 - Le disposizioni sanzionatorie penali e amministrative (a cura di V. Tusini Cottafavi)	247
1. Principi ed evoluzione del quadro sanzionatorio (V. Tusini Cottafavi)	247
2. Le violazioni antiriciclaggio rilevanti dal punto di vista del diritto penale (L. Criscuolo e A. Cuzzocrea)	250

3. Le sanzioni amministrative per violazioni degli obblighi antiriciclaggio (<i>A. Cuzzocrea e L. La Rocca</i>)	256
4. Le competenze e le procedure sanzionatorie per le violazioni degli obblighi antiriciclaggio (<i>A.M.A. Carriero e L. La Rocca</i>)	264
APPENDICE - Gli altri operatori (a cura di L. Criscuolo)	269
Premessa (<i>L. Criscuolo</i>).....	269
1. Imprese e intermediari assicurativi (<i>E. Gatti e D. Blanco</i>).....	269
2. Società fiduciarie (<i>A. Cuzzocrea</i>)	272
3. Revisori legali e società di revisione legale (<i>C. Di Biase</i>)	276
4. Collaboratori esterni, soggetti convenzionati e agenti (<i>C. Oriolo</i>).....	280
5. Professionisti (<i>S. Pace</i>).....	284
6. Operatori del settore del gioco (<i>A. Cassetta e L. Baron</i>)	288
7. Operatori in valute virtuali (<i>L. La Rocca</i>)	292
8. Operatori in oro (<i>A. Cuzzocrea</i>)	296
9. Società di recupero crediti (<i>C. Carrella e A. Greco</i>)	298
10. Operatori non finanziari gestori del contante (<i>C. Ciccolo e F. D'Urso</i>).....	301
11. Case d'asta e antiquari (<i>C. Oriolo</i>)	304

Premessa

Nei paesi eticamente evoluti la prevenzione del riciclaggio e del finanziamento del terrorismo è entrata da tempo a far parte dei principali obiettivi della legislazione nazionale che, per suo tramite, si propone anche il contrasto dei reati che del riciclaggio costituiscono il presupposto.

In attuazione delle cinque direttive antiriciclaggio, che hanno recepito e reso vincolanti in ambito europeo i principi ispiratori delle raccomandazioni del Gruppo di Azione Finanziaria Internazionale (GAFI), lo Stato italiano ha iniziato a legiferare in materia fin dal 1991 e, a far tempo dal 2008, ha affidato all'Unità di informazione finanziaria per l'Italia (UIF) il delicato compito di ricevere e analizzare le segnalazioni di operazioni sospette provenienti dai destinatari dei relativi obblighi.

La riforma del 2007, con la costituzione della UIF, ha impresso un forte impulso alla collaborazione attiva degli intermediari bancari e finanziari e di altre categorie di operatori obbligati: le segnalazioni sono progressivamente passate da poco più di 12.500 nel 2007 a oltre 155.000 nel 2022, un livello di 12 volte superiore a quello iniziale e con un numero di soggetti segnalati cresciuto in maniera più che proporzionale, grazie alla maggiore quantità di articolate informazioni richieste ai segnalanti.

La crescita della consapevolezza degli operatori e della capacità delle Autorità di intercettare comportamenti illeciti hanno consentito al sistema antiriciclaggio nazionale di ottenere risultati anche di eccezionale rilievo: situazioni irregolari consolidate nel tempo e nuove modalità di riciclaggio sono venute alla luce grazie alle informazioni contenute nelle segnalazioni. Il sistema ha pertanto conquistato la fiducia dei cittadini e delle istituzioni ed è ora riconosciuto a livello internazionale come un'eccellenza italiana.

Gli importanti risultati raggiunti sono dovuti anche alle caratteristiche dell'apparato istituzionale definito dalla regolamentazione che, in linea con i principi internazionali e con la disciplina europea, ha attribuito l'analisi finanziaria a una Financial Intelligence Unit (FIU) nazionale che, essendo collocata presso la Banca d'Italia, garantisce il possesso dei requisiti fondamentali di indipendenza, autonomia gestionale e capacità tecnica. Gli approfondimenti investigativi sono stati invece affidati a organismi specializzati nei settori della criminalità finanziaria, di quella organizzata e del terrorismo, quali il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e la Direzione Investigativa Antimafia.

Ulteriori elementi di forza sono costituiti dalle regole della collaborazione tra autorità che, sia pure perfettibili in termini di ampiezza e di utilizzo delle basi dati disponibili all'indagine finanziaria, hanno consentito l'integrazione dell'attività di contrasto e l'affermarsi di prassi operative caratterizzate da immediatezza ed efficacia. Ne costituisce un importante indicatore di successo l'incremento che si è registrato nella collaborazione tra la UIF e l'Autorità Giudiziaria, alimentato dalla crescente consapevolezza delle opportunità offerte dall'approfondimento delle operazioni sospette segnalate e dalle relazioni con la capillare rete internazionale delle FIU.

I presidi antiriciclaggio e la collaborazione delle autorità aiutano le indagini: ormai gli accertamenti bancari e finanziari fanno parte dell'ordinaria "cassetta degli attrezzi" degli investigatori per gran parte dei reati, anche per quelli di natura non finanziaria. In questo ambito un fondamentale elemento di crescita nelle informazioni disponibili è stato costituito dall'inserimento, in occasione del recepimento della quarta direttiva europea antiriciclaggio, della Direzione Nazionale Antimafia e Antiterrorismo (DNA) tra le autorità del sistema di prevenzione e dallo sviluppo delle relazioni che si sono instaurate con la UIF. Con la DNA sono stati avviati incroci sistematici delle rispettive basi dati, che hanno apportato un contributo determinante alla valorizzazione delle segnalazioni di operazioni sospette collegate in particolare alla criminalità organizzata e hanno supportato l'attività di impulso della Direzione Nazionale.

La collaudata funzionalità dei meccanismi adottati per la prevenzione del riciclaggio ne ha determinato una progressiva estensione al contrasto al finanziamento del terrorismo e dei programmi di proliferazione di armi di distruzione di massa e alle operazioni connesse con le attività delle imprese produttrici di mine anti-persona e di munizioni a grappolo. Il riconoscimento dell'utilità delle

informazioni fornite dal sistema e dei relativi approfondimenti finanziari hanno indotto a prevedere un loro utilizzo anche per fronteggiare reati diversi dal riciclaggio e a promuovere la collaborazione con altre istituzioni pubbliche nell'ambito, in particolare, della prevenzione e contrasto della corruzione e dell'evasione fiscale.

Ebbene, a quindici anni dalla istituzione dell'Unità, questo volume vuole celebrare il primo periodo di vita della nuova autorità attraverso una analisi delle regole e delle prassi operative che caratterizzano il funzionamento del sistema di antiriciclaggio, rilevandone pregi e difetti alla vigilia dell'imminente riforma della disciplina europea, destinata a rafforzare in modo significativo l'armonizzazione delle norme nazionali e a modificare radicalmente l'apparato istituzionale europeo per la prevenzione del riciclaggio e del finanziamento del terrorismo.

Si tratta di una ulteriore evoluzione del sistema di prevenzione che ha visto, nel corso degli oltre trenta anni di vigenza della relativa regolamentazione, la graduale e progressiva estensione della platea dei destinatari degli obblighi antiriciclaggio: dagli intermediari bancari e finanziari alle diverse tipologie di professionisti, agli operatori del settore dei giochi e alle altre molteplici categorie di soggetti che svolgono attività suscettibili di essere strumentalizzate a fini di riciclaggio o di finanziamento del terrorismo anche nelle forme più innovative come, da ultimo, quelle adottate dagli operatori in valute virtuali.

Poteri normativi e di controllo su alcune categorie di destinatari sono attribuiti alle rispettive Autorità pubbliche di vigilanza; per altre categorie, analoghe prerogative sono assegnate ad Organismi di autoregolamentazione, espressione degli stessi soggetti destinatari degli obblighi; altre categorie sono invece assoggettate alle disposizioni del decreto antiriciclaggio senza mediazioni interpretative e senza organi di supervisione specificamente dedicati alla verifica del rispetto delle regole.

Si tratta, quindi, di una vastissima platea di soggetti obbligati, non tutti dotati di autorità o organismi di riferimento e caratterizzati da peculiarità operative estremamente eterogenee che li espongono a rischi di utilizzo a fini di riciclaggio anche significativamente differenti quanto a modalità e intensità. Tali circostanze enfatizzano il ruolo e le responsabilità delle FIU, che devono essere necessariamente dotate di competenze professionali aggiornate e a carattere trasversale, idonee alla comprensione delle diverse tipologie di attività e a consentire anche l'individuazione, con finalità preventive, di modelli comportamentali e indicatori di rischio di riciclaggio che possono caratterizzare ciascuna di esse.

Nel nostro paese le caratteristiche della UIF e il dialogo tra autorità e destinatari degli obblighi hanno consentito di innescare un circolo virtuoso che ha accresciuto la capacità di individuare specifiche aree di esposizione ai rischi di riciclaggio e ha promosso un efficace sfruttamento del patrimonio informativo in possesso degli operatori in virtù delle relazioni con la clientela.

La strategia che la UIF ha inteso perseguire per onorare il ruolo attribuitole dall'ordinamento è stata quella di accrescere la consapevolezza delle diverse categorie di operatori sul contributo che ciascuna di esse può e deve dare al funzionamento del sistema. Nel contempo è stato perseguito l'obiettivo di affinare le proprie capacità di analisi; di accrescere le dimensioni, la tipologia e la riservatezza delle informazioni disponibili e gli scambi con le altre autorità; di migliorare le capacità di intelligence; di promuovere il rafforzamento della riservatezza delle informazioni a tutela dei segnalanti e dei segnalati e a garanzia del funzionamento del sistema.

Sul fronte dei rapporti con i soggetti obbligati si è inteso razionalizzare il processo di invio delle segnalazioni, integrandolo con quelli dell'analisi finanziaria della UIF e della disseminazione agli organi investigativi per garantirne affidabilità, velocità ed efficacia. Sostanziali avanzamenti nella quantità e nella qualità degli approfondimenti e dell'attività di collaborazione sono stati ottenuti con l'introduzione di una innovativa piattaforma per la raccolta e la gestione delle segnalazioni (RADAR), con il completamento del *data warehouse*, che integra le basi dati utilizzate per le analisi, e con la realizzazione di un sistema dedicato alla gestione informatica degli scambi con gli Organi investigativi, che è stato poi esteso all'Autorità giudiziaria e alle FIU estere.

L'efficacia dell'attività della UIF è stata confermata anche nella Mutual Evaluation effettuata dal GAFI nel 2015. Le analisi operative e strategiche dell'Unità sono state valutate favorevolmente e in grado di fornire valore aggiunto nell'avvio delle indagini per riciclaggio, reati presupposto e finanziamento del terrorismo. Riscontri positivi sono stati espressi anche sull'assetto istituzionale dell'Unità, che è stata giudicata in grado di svolgere le proprie funzioni con piena autonomia e indipendenza nonché di compiere tutti i processi decisionali senza alcuna interferenza esterna. Un esito positivo è giunto anche dal *follow-up* del 2019 relativamente alla conformità della normativa agli standard del GAFI.

Nella prospettiva di migliorare le capacità degli operatori di individuare le anomalie da considerare sospette e migliorare la qualità delle relative segnalazioni, l'Unità ha diffuso modelli e schemi rappresentativi di comportamenti anomali collegati a differenti tipologie di illeciti, indicatori di anomalia per singole categorie di operatori e comunicazioni relative a fenomeni emergenti con un approccio proattivo inteso a individuare per tempo i nuovi rischi.

Sono stati anche progressivamente introdotti presidi ulteriori alla segnalazione di operazioni sospette: dal 2019 è operativo il meccanismo delle comunicazioni oggettive delle operazioni in contante di importo rilevante; inoltre, un crescente numero di scambi di informazioni con le autorità estere ha fatto seguito alla consapevolezza della dimensione internazionale del riciclaggio.

Nel tempo si è sviluppato un notevole miglioramento della collaborazione attiva. Permangono comunque disomogeneità qualitative e quantitative anche fra operatori di grandi dimensioni. Nei comparti non finanziari l'apporto all'azione di prevenzione mantiene un ampio potenziale ancora inespresso. In un contesto nel quale operatori privati sono chiamati a svolgere onerose funzioni di pubblico interesse, una nota stonata è rappresentata dal trattamento normativo riservato agli uffici della pubblica amministrazione: questi, infatti, dopo essere stati assoggettati per primi, insieme agli intermediari bancari, a tutti gli obblighi previsti dalla normativa di prevenzione, sono stati poi, in un primo tempo, esclusi dagli adempimenti di adeguata verifica e conservazione dei dati e, successivamente, sottratti dalla disciplina generale, con un ingiustificato ridimensionamento delle attività assoggettate a comunicazione di dati e informazioni relativi a operazioni sospette.

Parallelamente all'estendersi dei soggetti sottoposti agli adempimenti antiriciclaggio è stata rafforzata anche l'efficacia delle misure di prevenzione. La semplice identificazione del cliente, prescritta in origine dalla regolamentazione, si è evoluta in un complesso processo di "*adeguata verifica*", volto conoscere e seguire nel tempo sia il profilo economico e le vicende soggettive delle controparti contrattuali sia le caratteristiche oggettive dell'operatività posta in essere. Ciò consente di attribuire ai singoli clienti un profilo personale di rischio, al quale commisurare – in applicazione del criterio del *risk based approach* – il livello di approfondimento e l'estensione delle misure antiriciclaggio. Questa conoscenza approfondita della clientela, oltre a costituire un presupposto indispensabile per una proficua collaborazione con le Autorità competenti, contribuisce anche, più in generale, alla gestione sana e prudente dell'attività dei singoli soggetti obbligati, mitigando i rischi legali e reputazionali legati al possibile coinvolgimento in attività di riciclaggio e di finanziamento del terrorismo.

Non sempre tuttavia la persona che assume la qualifica formale di cliente corrisponde al reale titolare dell'interesse economico connesso all'esecuzione dell'operazione o allo svolgimento del rapporto. A fronte di queste difficoltà, le norme comunitarie e nazionali di settore, nell'intento di rafforzare i presidi antiriciclaggio, hanno anzitutto stabilito criteri per la individuazione della titolarità effettiva dei clienti costituiti in forma di società di capitali e di altre entità giuridiche. Recenti disposizioni comunitarie, ancora in corso di applicazione nel nostro ordinamento, hanno poi prescritto ai singoli Stati membri di istituire appositi registri dei titolari effettivi – collegati a livello europeo - ai quali le società ed altri enti giuridici individuati a livello nazionale sono obbligati a comunicare l'identità dei propri titolari effettivi nonché ulteriori dati e informazioni sul loro conto.

Si tratta di un sistema che presenta, peraltro, diverse criticità. Gli oneri di costituzione e funzionamento sono destinati a ricadere sia sulle società e gli enti tenuti alla individuazione e comunicazione ai registri nazionali dei propri titolari effettivi sia sugli intermediari e gli altri soggetti

obbligati ad effettuare l'adeguata verifica. Questi ultimi, poi, anche accedendo a pagamento alla consultazione dei registri, non sono per questo esonerati dal verificare comunque l'affidabilità delle informazioni registrate.

Siamo ora a un punto di svolta. Il 20 luglio 2021 la Commissione europea ha pubblicato un "Pacchetto Antiriciclaggio" con proposte legislative per una riforma complessiva del sistema normativo e dell'apparato istituzionale europeo per la prevenzione del riciclaggio e del finanziamento del terrorismo. Le quattro proposte che formano l'AML Package consistono in tre regolamenti e in una sesta direttiva.

La riforma risponde a due distinte esigenze da molto tempo sottolineate con determinazione dalla UIF nelle diverse sedi europee. Andava innanzitutto superato l'approccio basato sull'armonizzazione minima, che ha costantemente ispirato le direttive antiriciclaggio emanate in questi trenta anni, senza cambiamento di linea neppure nelle ultime tre succedutesi a intervalli sempre più ravvicinati a partire dal 2007. Occorreva poi assicurare omogeneità di applicazione delle norme da parte delle autorità di controllo dei singoli paesi e accrescere la collaborazione tra le FIU europee, garanzia ineludibile per fronteggiare, in un mercato fortemente interconnesso, i rischi collegati alla dimensione sovranazionale del riciclaggio. Omogeneità delle norme e del livello dei relativi presidi costituiscono un indispensabile presupposto per evitare possibili infiltrazioni di capitali di origine illecita nel sistema finanziario europeo per il tramite di Stati con regolamentazioni non adeguate e, nel contempo, per assicurare un terreno competitivo, non alterato a scapito degli operatori assoggettati ad oneri più elevati di conformità da parte di paesi più rigorosi nel fronteggiare i rischi di riciclaggio.

La scelta di istituire un'Autorità europea antiriciclaggio (*Anti-Money Laundering Authority* - AMLA), quale agenzia europea con compiti sovranazionali diversificati nei comparti della supervisione antiriciclaggio e dell'attività delle FIU, consolida l'apparato antiriciclaggio come sistema organico con caratteristiche di completezza e separatezza rispetto a comparti pure collegati (quali quello del Meccanismo di Vigilanza Unico (SSM) e quello delle indagini penali, nel quale operano Europol, Eurojust e la Procura europea-EPPO).

L'AMLA si profilerà con caratteristiche peculiari nel panorama delle agenzie dell'Unione. Nella sua unitarietà soggettiva, sancita dalla personalità giuridica, essa svolgerà due funzioni distinte e separate, ma complementari, dotate di autonoma rilevanza e reciproca indipendenza sia sul piano operativo sia quello regolamentare. L'AMLA, infatti, agirà, in conformità a distinti statuti normativi e separati contesti istituzionali, quale Supervisore antiriciclaggio europeo e quale Meccanismo sovranazionale di supporto e coordinamento delle FIU.

Anche se manca ancora qualche tempo all'avvio concreto dell'operatività dell'AMLA, occorre tenersi pronti e rendersi disponibili al cambiamento, evitando o contenendo approcci "al ribasso". Già nella fase di costruzione e avvio dell'AMLA sarà importante svolgere un ruolo proattivo, formulare anzitutto proposte sulle procedure, sui metodi e sugli strumenti tecnici necessari per le attività di supervisione e di coordinamento delle FIU.

Si apre dunque una nuova stagione. L'auspicio è che la prossima disciplina, fondata sullo strumento del regolamento di diretta applicazione negli ordinamenti nazionali, si collochi su livelli elevati di presidio e che le esigenze di mediazione tra i regimi in vigore nei diversi stati non finisca per condurre ad una riduzione dell'efficacia del sistema nel suo complesso. Occorre, semmai, puntare a una semplificazione degli adempimenti formali per rendere meno oneroso il sistema e presidiare con maggiore efficacia il reale rispetto delle regole che consentono di individuare le anomalie da intercettare. Occorre, per operatori ed autorità, un approccio non burocratico focalizzato sul mero adempimento di obblighi, ma basato sulla comprensione della finalità dei presidi: solo così il sistema potrà mantenere e rafforzare, anche nella prevenzione e repressione di reati diversi dal riciclaggio, la sua utilità ormai generalmente riconosciuta.

Giovanni Castaldi e Claudio Clemente

CAPITOLO 1

Prevenzione e repressione del riciclaggio

(a cura di G. Castaldi)

1. Il contrasto del riciclaggio nel contesto internazionale (P. Costanzo)

Le attività di riciclaggio si caratterizzano per l'articolazione in più atti o operazioni, estesi nella durata e nello spazio. La condotta complessiva comprende la realizzazione di reati suscettibili di generare proventi, l'acquisizione delle relative disponibilità illecite, il compimento su di esse di una serie potenzialmente assai ampia di atti di occultamento, trasferimento, trasformazione. Si tratta di un'attività organizzata, che attinge a una serie estesa di reati presupposto (a seconda del "comparto" in cui opera l'organizzazione) e si riverbera, a valle, in complesse operazioni di "ripulitura" attraverso molteplici passaggi (nei luoghi fisici, nella titolarità giuridica, nella natura delle disponibilità).

Traendo vantaggio dalla diversità dei presidi nazionali e dalla diversa intensità dei controlli, ai criminali conviene distribuire le fasi "produttive" (illeciti generatori di proventi), le operazioni di collocamento e trasformazione, l'imputazione e l'intestazione dei beni in diversi luoghi, scegliendo di volta in volta le giurisdizioni più "ospitali".

L'attitudine transnazionale del riciclaggio si presta dunque a forme di arbitraggio, sia da parte della criminalità sia – duole constatarlo - da parte degli ordinamenti nazionali, coinvolti in meccanismi nocivi di "concorrenza" per mantenere il massimo grado di attrattività di capitali, collocando al minimo la soglia dei controlli preventivi e dell'*enforcement*¹. Meccanismi di correzione degli incentivi "al ribasso" e ancor più di sanzione, sono difficili da introdurre per la mancanza di un livello sovranazionale di Autorità e di *governance*. Nell'arco di oltre trent'anni sono stati compiuti ad ogni modo passi importanti per la costruzione di un sistema antiriciclaggio internazionale credibile e capace di incidere sul comportamento di Stati sovrani². Esso si basa su un quadro dettagliato di standard e sull'azione di molteplici organismi.

1.1. Gli organismi internazionali

Le caratteristiche transfrontaliere del riciclaggio rendono impossibili forme efficaci di prevenzione e di contrasto da parte di singoli Stati. Gli ordinamenti più rigorosi possono essere spiazzati da pratiche di arbitraggio, con la conseguenza di aumentare i costi interni connessi all'applicazione dei presidi e "dirottare" il riciclaggio verso sistemi meno rigorosi.

La consapevolezza del rilievo del riciclaggio è maturata in corrispondenza dell'aumento significativo delle disponibilità illecite prodotte, nel corso degli anni Ottanta del secolo scorso, soprattutto per l'apertura di vasti mercati internazionali per il traffico di stupefacenti, il relativo consumo "di massa" e l'affermarsi di organizzazioni criminali capaci di operare su tali mercati con efficienza, causando danni devastanti al tessuto sociale, all'economia e anche all'assetto democratico di alcuni paesi. Il riversamento nell'economia e nel sistema finanziario di masse enormi di capitali illeciti per il necessario riciclaggio (all'epoca non ancora riconosciuto come fattispecie autonoma rispetto ai delitti-presupposto di cui costituiva il postfatto) iniziava a provocare effetti destabilizzanti sotto vari profili: alterazione della concorrenza, con l'occupazione o l'impossessamento criminale di imprese e filiere produttive; instabilità nel settore bancario e finanziario, per la mobilità e volatilità dei capitali criminali, per le interferenze nella *governance* (e nell'allocazione del credito), per i molteplici rischi connessi, non ben conosciuti né presidiati (e a volte consapevolmente accettati).

Il riciclaggio inizia a trovare riconoscimento nelle fonti internazionali che, dalla fine degli anni '80, estendono il contrasto di reati "gravi" nella fase a valle di produzione e utilizzo dei proventi. L'importanza

¹ Paesi poveri di risorse possono puntare sull'offerta di servizi finanziari o societari a non residenti per attrarre capitali esteri; giurisdizioni economicamente più solide e sottoposte a vincoli sovranazionali diretti possono invece inserire incentivi a capitali esteri a discapito dei controlli in mix complessi di politica economica.

² I mezzi di persuasione si basano su meccanismi coercitivi e su fattori reputazionali. Si tratta di una combinazione di strumenti non pienamente efficace per modificare verso la prevenzione e il contrasto il potente sistema di incentivi distorto.

crescente del fenomeno e la sua dannosità sollevano l'attenzione di organismi internazionali a competenza generale e inducono all'istituzione di nuovi organismi dedicati. Il "campo" della prevenzione e del contrasto al riciclaggio si specializza e acquista una propria fisionomia; nasce e si sviluppa un settore multidisciplinare e complesso, ricco di collegamenti con vari altri, da quello penale a quelli bancario e finanziario, a quello fiscale.

La "Raccomandazione" del Comitato dei Ministri del Consiglio d'Europa R 80/10 del 27 giugno 1980 getta le prime basi per i presidi di prevenzione nel settore finanziario introducendo, sia pure in forma non vincolante, misure di identificazione, conservazione documentale, collaborazione attiva per la rilevazione di fatti illeciti. La Convenzione di Vienna delle Nazioni Unite del 1998 contro il traffico di stupefacenti introduce un'inedita fattispecie penale di riciclaggio, che costituisce a tutt'oggi il modello di incriminazione³ per gli aspetti che concernono la condotta⁴.

Il Consiglio d'Europa, seguendo un approccio più "generalista" per raccogliere in un unico strumento antiriciclaggio gli aspetti di attualità, adotta l'8 novembre 1990 la Convenzione di Strasburgo "*on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime*". Essa si distingue per l'ampio ambito dei reati presupposto: devono rientrarvi tutti gli illeciti che generano profitti. La Convenzione di Strasburgo è stata poi sostituita dalla Convenzione di Varsavia del Consiglio d'Europa del 16 maggio 2005, recante una disciplina più estesa e aggiornata sul versante del contrasto e su quello della prevenzione.

1.1.1. Il Gruppo di Azione Finanziaria Internazionale (GAFI)

Il "Financial Action Task Force" è riconosciuto come l'organismo di riferimento nel sistema antiriciclaggio internazionale. Ad esso è attribuita la responsabilità di formulare standard globali, ai quali si allineano sia altri enti internazionali sia gli Stati nazionali, ed è assegnato il ruolo di verificarne la corretta ed efficace applicazione.

Il GAFI fu istituito dai paesi G7 in occasione del Summit di Parigi del 14 luglio 1989 con lo scopo di accentrare in una sede intergovernativa le iniziative necessarie allo sviluppo di un organico sistema antiriciclaggio, sul piano penale, della prevenzione nei settori esposti dell'economia, della collaborazione tra Autorità a livello nazionale e internazionale. I 16 membri iniziali comprendevano, oltre ai paesi G7 e alla Commissione europea, Australia, Austria, Belgio, Lussemburgo, Olanda, Spagna, Svezia, Svizzera. Il nuovo Organismo era costituito nella forma di una "task force" priva di soggettività giuridica, con carattere provvisorio e proroghe biennali. Il Segretariato, incardinato presso l'OCSE, forniva supporto alla Plenaria degli Stati membri, unico organo competente ad assumere decisioni (sulla base di "consenso", ovvero di una sostanziale unanimità).

Negli oltre trent'anni dalla sua istituzione, il GAFI ha attraversato significativi cambiamenti nella membership, nell'organizzazione e nella *governance*, tutti orientati a rimarcare la stabilità e l'indipendenza e a rafforzare la capacità operativa (soprattutto per lo svolgimento sistematico di "cicli" quanto più possibile ravvicinati di valutazioni nei confronti dei Paesi membri), pur senza scalfire l'originaria impostazione inter-governativa basata sul "consenso" per le decisioni.

Il 12 aprile del 2019 i Governi degli Stati membri hanno approvato una significativa revisione del mandato del GAFI e hanno trasformato l'Organizzazione da temporanea a permanente. La Parte III del "Mandato", dedicata all'organizzazione, individua gli organi interni, precisandone i compiti: la Plenaria⁵, il Presidente e il Vice Presidente, un Comitato di Indirizzo ("Steering Committee"), il Segretariato. La durata della Presidenza, assunta a turno dagli Stati membri, è stata prolungata da uno a due anni, a beneficio della continuità operativa e strategica. Il Presidente è coadiuvato da un Comitato di Indirizzo con compiti di consulenza composto, a rotazione, da rappresentanti dei Paesi membri.

Nel sistema "consensuale" per le determinazioni della Plenaria, il Presidente non è dotato di particolari poteri decisionali. Egli esercita un'influenza determinante, definendo le priorità da perseguire nel corso del proprio mandato (comunque sottoposte alla Plenaria), convocando le riunioni e proponendone l'agenda, rapportandosi ai Governi nazionali e ai vertici di altri organismi internazionali. Il Presidente è affiancato da un Vice Presidente, a sua volta con mandato biennale; questi ha lo status di "Presidente designato", ovvero è destinato a subentrare nella carica per il successivo mandato.

³ Forte impulso alle iniziative internazionali proveniva dalla coeva esperienza degli Stati Uniti, alle prese con potenti organizzazioni criminali attive nel settore degli stupefacenti; il reato di riciclaggio fu introdotto negli USA nel 1986.

⁴ L'ambito dei reati presupposto, che nell'art. 3 della Convenzione è limitato a quelli in materia di droga, è stato in seguito ampiamente esteso in altre fonti.

⁵ Affiancata da cinque Gruppi di Lavoro: *Evaluation and Compliance* (ECG); *Policy Development* (PDG); *Risks, Trends and Methods* (RTMG); *Global Network Coordination* (GNCG); *International Cooperation Review* (ICRG).

Sono ammessi a partecipare alle attività del GAFI soggetti appartenenti a tre categorie: “membri”; “membri associati”; “istituzioni finanziarie internazionali”. La qualifica di “membro” spetta agli Stati ammessi a far parte del Gruppo. La compagine si è estesa notevolmente negli anni: dagli iniziali 16 fondatori nel 1989 si è arrivati agli attuali 39. Per quanto relativamente ampia, la *membership* non è dunque globale: essa è contenuta entro limiti idonei a contemperare le esigenze di partecipazione e rappresentatività con la necessità di mantenere meccanismi di *governance* e decisionali efficienti. I membri vengono ammessi tenendo conto di fattori di distribuzione geografica, di dimensione delle economie nazionali, geo-politici.

Emerge dunque un'apparente discrasia tra la portata globale delle attività del GAFI e la compagine circoscritta dei suoi membri. In realtà, il GAFI è al centro di una rete globale (*FATF Global Network*) di cui fanno parte molteplici organismi internazionali di carattere regionale, che sviluppano nelle aree geografiche di competenza le politiche e i progetti definiti centralmente e rappresentano i propri membri negli organi centrali. I nove *FATF-Style Regional Bodies* – FSRBs⁶, composti dai paesi delle rispettive aree geografiche, possiedono lo status di *Associate Member*, cui accede il diritto/dovere di partecipare alle attività del GAFI nella Plenaria e nei Gruppi di Lavoro.

Il Global network del GAFI comprende 205 giurisdizioni e assume così una dimensione effettivamente globale che rende ragione del mandato “universale” dell'Organizzazione. Questa, in effetti, va intesa come un “sistema” unitario articolato in un corpo centrale (Plenaria con i suoi organi, Segretariato) e in una rete di organizzazioni regionali che partecipano alle attività comuni esprimendo il punto di vista delle rispettive membership, elaborato negli organi degli FSRB⁷.

Ciascun FSRB è organizzato in assemblee plenarie e gruppi di lavoro, secondo una struttura che replica quella dell'organismo centrale⁸. Gli FSRB sono “delegati” a svolgere le *Mutual Evaluation* dei paesi delle rispettive regioni, in un'ottica di decentramento, in conformità alla “Universal Methodology” appositamente elaborata per fornire criteri comuni ed evitare scostamenti. I risultati delle valutazioni, dopo la preliminare approvazione dell'FSRB, sono sottoposti alla Plenaria “centrale” per la rilevazione di eventuali incongruenze e per una complessiva verifica (*Quality and Consistency Review*). La Plenaria e, dunque, gli Stati che vi partecipano come membri a pieno titolo, assicurano l'unitarietà e la coerenza dell'interpretazione degli standard e dei metodi di lavoro, dei quali (la Plenaria) è custode esclusiva.

Il campo d'azione degli FSRB comprende, in più, solo poche altre funzioni, relative in particolare alla ricognizione di tipologie di riciclaggio e finanziamento del terrorismo di rilievo locale e all'individuazione di questioni interpretative, ugualmente emerse nella regione, da sottoporre agli organi centrali. Gli FSRB non svolgono attività di elaborazione di policy, standard o linee-guida, appannaggio esclusivo degli organi centrali del GAFI.

Il mandato, pur restando ancorato alla “protezione del sistema finanziario e dell'economia in generale”, nonché all'integrità e alla sicurezza di questi, è stato negli anni esteso nel novero delle minacce da fronteggiare e delle finalità da perseguire. Nel 1989 l'attenzione era esclusivamente rivolta al riciclaggio; nel 2001, con l'accresciuta consapevolezza dei rischi globali posti dal terrorismo dopo l'attacco alle Torri Gemelle, si aggiunse la finalità di prevenire e contrastarne il finanziamento. Il mandato fu esteso poi al contrasto del finanziamento della proliferazione di armi di distruzione di massa⁹.

Il riciclaggio, il finanziamento del terrorismo e il finanziamento della proliferazione di armi di distruzione di massa sono evidentemente fenomeni eterogenei¹⁰, tuttavia accomunati dal ricorso a strumenti e operatori dell'economia legale e, in particolare, del sistema finanziario, per l'acquisizione, il

⁶ Si tratta di: Asia/Pacific Group on Money Laundering (APG); Caribbean Financial Action Task Force (CFATF); Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL); Eurasian Group (EAG); Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG); Financial Action Task Force of Latin America (GAFILAT); Inter Governmental Action Group against Money Laundering in West Africa (GIABA); Middle East and North Africa Financial Action Task Force (MENAFATF); Task Force on Money Laundering in Central Africa (GABAC).

⁷ La configurazione complessiva del GAFI quale “network” si realizza dunque a un costo: quello di differenziare lo status e il ruolo dei Paesi, alcuni (una minoranza) membri diretti e altri (la grande maggioranza) coinvolti in maniera indiretta e collettiva per mezzo degli FSRB.

⁸ Con alcune differenze dipendenti dai diversi rispettivi mandati e dal mantenimento a livello centrale di alcune competenze riguardanti, ad esempio, l'elaborazione di standard e policy (PDG), la valutazione dei Paesi “a rischio” (ICRG) e naturalmente il coordinamento della rete globale (GNCG).

⁹ Ciò avvenne in coincidenza con lo sviluppo di un sistema di “sanzioni finanziarie” internazionali nei confronti dell'Iran e della Corea del Nord, fondato su risoluzioni delle Nazioni Unite e, in Europa, su regolamenti dell'Unione.

¹⁰ Ad esempio, mentre il riciclaggio ha per oggetto disponibilità di origine illegale e consiste in un processo di occultamento o trasformazione di tali disponibilità per conferire loro parvenza di liceità, il finanziamento del terrorismo può realizzarsi con denaro legale, spesso in piccoli importi, e all'opposto l'illegalità risiede nella sua destinazione o utilizzo. Per altro verso, mentre il riciclaggio e il finanziamento del terrorismo configurano reati posti in essere da individui o gruppi organizzati, programmi di “proliferazione” sono appannaggio di apparati governativi e, assieme al relativo finanziamento, non sempre integrano fattispecie di reato.

trasferimento e l'utilizzo di fondi. La comune connotazione economico-finanziaria e l'esigenza di policy e misure di prevenzione e contrasto su tale piano spiegano il coinvolgimento del GAFI e l'estensione del suo mandato.

Le attività svolte dal GAFI per il perseguimento del proprio composito mandato, da ultimo ribadite e precisate nel richiamato documento del 2019, si articolano su diversi fronti. L'Organizzazione è riconosciuta quale responsabile globale per lo sviluppo di standard per la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo e della proliferazione. Le Quaranta Raccomandazioni costituiscono il riferimento in queste materie per gli ordinamenti nazionali e per gli altri organismi internazionali¹¹. Alle caratteristiche di universalità ed esclusività degli standard corrisponde tuttavia la natura non formalmente vincolante di questi. Gli Stati non sono formalmente "obbligati" ad attenersi alle Raccomandazioni del GAFI; queste non esprimono "regole" in senso stretto e dipendono, per la loro effettiva applicazione, da specifici meccanismi di *enforcement*.

Pur in assenza di "sanzioni" in senso stretto, le violazioni e gli scostamenti comportano rischi e costi di natura economica, reputazionale e politica. L'incentivo alla corretta applicazione degli standard deriva dunque da una valutazione di "convenienza" nella quale vengono soppesati i vantaggi conseguibili attraverso il disallineamento (maggiore afflusso di capitali esteri verso particolari settori dell'economia o della finanza; riduzione dei costi di *compliance*) e le conseguenze delle verifiche (maggiore difficoltà nell'accesso di operatori economici nazionali, sottoposti a due diligence più intensa in altri paesi, a mercati esteri, sino a possibili effetti di "de-risking" con esclusioni generalizzate; effetti economici negativi di altre contromisure). L'efficacia degli standard del GAFI e, in ultima istanza, del sistema internazionale antiriciclaggio nel suo complesso, dipendono in misura cruciale dalla capacità di orientare opportunamente gli incentivi, definendo meccanismi dissuasivi rispetto a condotte opportunistiche.

L'attuazione degli standard forma oggetto di estesi programmi di verifica e valutazione. Il GAFI svolge mutual evaluation dei Paesi membri, così denominate per la natura di *peer reviews*, condotte in maniera reciproca per ciascun paese da esperti di altri paesi. Agli esperti nazionali, coadiuvati dal Segretariato, spettano le verifiche, le analisi e le conclusioni; queste sono rimesse alla Plenaria, ovvero agli Stati membri, senza l'intervento di un organo terzo valutatore o decisore¹². Le valutazioni si svolgono in cicli successivi, con l'obiettivo di realizzare interventi non troppo distanti nel tempo per ciascun paese.

Le verifiche si svolgono su due versanti: quello della *Technical Compliance*, nel quale si determina la conformità delle regole nazionali agli standard, e quello della "Effectiveness", rivolto a misurare il grado di efficacia delle misure poste in essere e dell'azione delle Autorità. Sebbene naturalmente collegate, le verifiche sulla *compliance* e sull'efficacia sono in rapporto di reciproca indipendenza: è possibile, ad esempio, che sistemi relativamente conformi agli standard sul piano della regolamentazione si rivelino non in ugual misura efficaci alla luce dei risultati ottenuti; ovvero, all'opposto, che la capacità di ottenere risultati in concreto sia superiore al livello di conformità regolamentare.

I risultati sono espressi in giudizi analitici e si riflettono in rating assegnati, secondo precisi criteri di giudizio, a ciascun aspetto del sistema antiriciclaggio. I rating consentono una visione sintetica dell'esito e facilitano le comparazioni tra diversi paesi. I Rapporti di valutazione esprimono anche "raccomandazioni" sulle iniziative da intraprendere per risolvere le criticità individuate. Il livello dei rating determina le caratteristiche delle verifiche di "follow-up", sia nella periodicità (due anni, un anno, più volte nell'anno) sia nella profondità e intensità (ad esempio, con riguardo alle misure correttive).

Assieme alle mutual evaluation, il GAFI svolge ulteriori verifiche, non nella forma di *peer review*, nei confronti di qualsiasi paese, anche non appartenente al Global Network, con l'obiettivo di individuare "Paesi caratterizzati da alto rischio, non cooperativi ovvero con carenze strategiche".

¹¹ Il sistema degli standard per il contrasto del riciclaggio e del finanziamento del terrorismo e della proliferazione, definito nelle Quaranta Raccomandazioni e nelle Note Interpretative che ne costituiscono parte integrante, è completato da un esteso corpo di documenti con linee guida e best practice.

¹² Tali caratteristiche di "mutualità" delle valutazioni non vengono meno quando il loro svolgimento viene affidato ad Istituzioni Finanziarie Internazionali riconosciute quali "assessing body": in particolare, il Fondo Monetario Internazionale e la Banca Mondiale possono effettuare valutazioni "antiriciclaggio", in osservanza della Metodologia del GAFI, consegnando le relative conclusioni al GAFI per la discussione e l'approvazione secondo le ordinarie procedure.

Il programma è preordinato alla assunzione di iniziative, in raccordo con i paesi interessati, per porre rimedio alle criticità individuate, ma anche alla definizione di “contromisure” per proteggere l’integrità del sistema finanziario internazionale e di quelli dei singoli Stati.

L’azione di verifica esercita una notevole efficacia dissuasiva, in grado di contenere approcci opportunistici e, in caso di disallineamenti rilevanti, programmare e realizzare interventi correttivi. Le misure che il GAFI può adottare fanno leva su aspetti reputazionali ed economici. Sul primo profilo, anzitutto, i paesi ad alto rischio vengono inseriti in due liste pubbliche, differenziate in base alla gravità dei rilievi e accompagnate da “Public Statement”, che precisano le carenze e le contromisure da applicare. Le due liste e i relativi Statement vengono aggiornati ad ogni sessione plenaria (tre volte l’anno).

La pubblicazione delle liste è accompagnata da misure da applicare per il contenimento dei rischi, riconducibili a due generi. Alcune sono orientate a proteggere gli Stati, e i soggetti al loro interno, dai rischi che promanano dai paesi listati; consistono nell’applicazione di presidi rafforzati di verifica adeguata nei confronti di controparti dei paesi colpiti. Nei casi più gravi possono innescarsi fenomeni di “de-risking”, con effetti indesiderati di esclusione finanziaria. L’escalation dalla sanzione reputazionale al danno economico attraverso l’applicazione di presidi di verifica rafforzata è rapida e diretta, favorita dalla portata globale degli interventi. L’effetto dissuasivo non è inferiore a quello di sanzioni di tipo coercitivo¹³.

A quest’ultima categoria può essere ricondotto il secondo tipo di misure che il GAFI può imporre nei confronti dei paesi listati. Queste consistono, in una chiave “offensiva” diversa da quella difensiva propria dei presidi richiamati prima, nel divieto per i Paesi membri di rendere disponibili a soggetti provenienti dai paesi listati disponibilità di qualsiasi tipo o servizi. Tali forme di “embargo”, differenziate per tenere conto del contesto e colpire selettivamente, vengono di solito realizzate attraverso un’azione concertata tra governi nazionali e organismi internazionali e trovano riflesso in Risoluzioni dell’ONU.

L’individuazione e l’analisi di minacce di riciclaggio e finanziamento di terrorismo e proliferazione fornisce indirizzo e supporto alle altre funzioni del GAFI (specie quelle di elaborazione di policy e standard). L’analisi di “trends” e “methods” criminali in continua evoluzione, e la ricognizione dei presidi e delle loro debolezze costituiscono il presupposto per l’aggiornamento degli standard, orientano le policy elaborate attraverso linee guida, forniscono indicazioni alle Autorità nazionali sui rischi e le priorità. Dallo studio delle “tipologie” di riciclaggio e finanziamento di terrorismo e proliferazione prendono le mosse le iniziative regolamentari e le attività di indirizzo, da cui a loro volta dipendono le procedure di valutazione della *compliance* e dell’efficacia¹⁴.

Questa dinamica funzionale del GAFI può essere illustrata con due esempi. Nel 2014 il GAFI rivolse attenzione allo sviluppo delle valute virtuali e alle forme del loro utilizzo in attività economiche illecite. Una prima analisi su caratteristiche di strumenti, tipologie di impiego e rischi fu pubblicata nel giugno 2014¹⁵. A questa iniziativa esplorativa seguirono delle “linee guida” nel 2015¹⁶. Nel 2018 e nel 2019 furono elaborati standard dedicati, con modifiche alle Raccomandazioni e alle Note Interpretative. La ricognizione di rischi e metodi di uso illegale delle valute virtuali proseguì nel 2020 e nel 2021, con un programma dedicato¹⁷; questi approfondimenti hanno a loro volta informato l’aggiornamento delle linee guida (2019 e 2021) e l’elaborazione di chiarimenti sui presidi per le “stablecoin”¹⁸. Con riguardo alla titolarità effettiva, istituito da tempo consolidato negli standard, è stata ravvisata la necessità di rafforzare i requisiti di “trasparenza” (Raccomandazioni 24 e 25). La revisione poggia su uno studio “orizzontale” sull’applicazione delle misure di trasparenza e sui relativi controlli a livello nazionale e sull’analisi di tipologie aggiornate di attività criminali che si avvalgono di schemi di titolarità effettiva indiretta per occultare il possesso o il trasferimento di beni¹⁹.

¹³ Il rapporto tra i Paesi listati e quelli rimossi dalla lista (80 i primi, 60 i secondi al 2020) fornisce una misura dell’efficacia del meccanismo.

¹⁴ Le complesse attività e procedure di analisi delle tipologie sono coordinate da un Gruppo di Lavoro permanente (Risk, Trends and Methods Group). Tra i rapporti recenti, in aggiunta a quelli citati di seguito, possono essere ricordati i seguenti: *Ethnically or Racially Motivated Terrorism Financing; Money Laundering from Environmental Crimes; Trade-Based Money Laundering: Risk Indicators; Covid 19 – Related Money Laundering and Terrorism Financing Risks*.

¹⁵ Cfr. FATF, *Virtual currencies: key definitions and potential AML/CFT risks*, 2014.

¹⁶ Cfr. FATF, *Guidance for a risk-based approach to virtual currencies*, 2015.

¹⁷ Cfr. FATF, *Virtual asset red flag indicators of money laundering and terrorist financing: 12-month review on Virtual Assets and Virtual Asset Service Providers*, in due edizioni.

¹⁸ FATF, *Report to the G20 on the so called stablecoins*, 2020.

¹⁹ Cfr. FATF, *Report on concealment of beneficial ownership*, 2018, elaborato con il Gruppo Egmont.

1.1.2. Il Gruppo Egmont delle Financial Intelligence Unit

L'Egmont Group²⁰ fu istituito nel 1995 quale organismo globale delle FIU. Esso consiste in un "network" di Autorità nazionali; diversamente dal GAFI, non è un'organizzazione inter-governativa. Il Gruppo Egmont persegue obiettivi di taglio operativo, nelle materie delle FIU, volti in primo luogo a rafforzare la collaborazione e i compiti di analisi²¹.

Le attività principali consistono nell'elaborazione di linee-guida per l'uniforme applicazione degli standard internazionali, nello svolgimento di verifiche per l'individuazione di criticità e di misure correttive, nella gestione di un'infrastruttura informatica globale per gli scambi di informazioni, nel monitoraggio di tipologie di riciclaggio e finanziamento del terrorismo (frequentemente in collaborazione con il GAFI). I lavori sono distribuiti tra quattro gruppi di lavoro tematici²²; i rapporti conclusivi sono sottoposti ai Capi delle FIU per le decisioni e l'adozione.

Dalla natura non governativa e dall'assenza di una base fondante nel diritto internazionale discendono la natura "informale" del Gruppo Egmont e la portata non strettamente vincolante delle indicazioni e degli indirizzi espressi. Come nel caso del GAFI, tuttavia, la dimensione globale dell'Organizzazione, il riferimento ad essa in fonti internazionali, la diretta connessione con le attività di altri organismi conferiscono elevato peso e autorevolezza a iniziative e decisioni. Anche in questo caso, le implicazioni reputazionali dello scostamento dagli standard sull'attività e la collaborazione delle FIU sancito dalle verifiche, ovvero la non appartenenza di una FIU al Gruppo (o peggio la sua sospensione o espulsione) si rivelano particolarmente significative, si propagano rapidamente attraverso il sistema delle valutazioni e delle "sanzioni" del GAFI e non tardano a riverberarsi sul Paese interessato nel suo complesso.

La membership nel Gruppo Egmont costituisce il risultato di una procedura di valutazione nella quale viene riscontrata la sussistenza dei requisiti propri della FIU secondo le regole internazionali. Viene anche verificata la capacità di operare con efficacia, sia nello svolgimento delle attività domestiche (ricezione di segnalazioni, analisi, disseminazione) sia nella collaborazione internazionale. L'ammissione al Gruppo equivale dunque a un riconoscimento della FIU e della sua conformità agli standard.

La compagine del Gruppo Egmont, formata da 167 FIU, assume respiro globale. Nonostante l'ampiezza, il modello organizzativo è sostanzialmente accentrato, con alcuni temperamenti.

Il principale organo decisionale è l'assemblea dei Capi delle FIU, cui partecipano tutti i membri; ad essa spettano, ad esempio, le decisioni sull'ammissione di membri, valutazioni e provvedimenti relativi a FIU appartenenti all'Organizzazione, adozione di standard, di policy e di rapporti su progetti tematici. Per la discussione di argomenti non riservati l'assemblea si riunisce in una configurazione "plenaria" ancora più ampia, con la partecipazione di membri osservatori²³.

Come per il GAFI, le decisioni sono assunte per consenso, non a maggioranza. Le difficoltà di funzionamento connesse all'ampiezza della membership e al metodo del consenso vengono attenuate, nel sistema di *governance*, attraverso due meccanismi. Al "Comitato Egmont" (*Egmont Committee*), organo esecutivo, sono attribuite dalla "Charter" del Gruppo estese deleghe decisionali e di proposta. I Capi delle FIU si limitano spesso alla ratifica o presa d'atto delle soluzioni elaborate dal Comitato.

Il sostanziale "travaso" di poteri dai Capi delle FIU al Comitato determina un assetto e una ripartizione di attribuzioni tra i due organi che non appare equilibrata, con il Comitato in una posizione di organo di gestione e indirizzo. È una circostanza da considerare criticamente anche alla luce della composizione del Comitato, che non rappresenta i Capi delle FIU e non ne esprime gli orientamenti. Ne fanno parte infatti i responsabili degli altri organi del Gruppo Egmont: il Chair (che lo presiede), i Vice Chair, il Segretario Esecutivo, i Chair dei Gruppi di Lavoro, i Rappresentanti Regionali (unici membri del Comitato portatori del punto di vista della membership, per linee "geografiche"), il Rappresentante della FIU che ospita la rete "ESW".

²⁰ L'Organizzazione prende nome dall'edificio di Bruxelles ove si tenne la riunione fondativa, il Palais d'Egmont. La FIU italiana divenne parte dell'Organizzazione immediatamente dopo, nel 1996.

²¹ Il perimetro delle materie regolate dal Gruppo Egmont è determinato dalle Raccomandazioni 29 e 40 e dalle connesse Note Interpretative, riguardanti rispettivamente le attività, l'organizzazione e i poteri delle FIU e la collaborazione internazionale tra queste. Rilevano anche, per il Gruppo Egmont, le Raccomandazioni sulla rilevazione e segnalazione di operazioni sospette (20 e 21, per gli intermediari finanziari; 23, per gli operatori non finanziari).

²² Information Exchange (IEWG); Membership, Support and Compliance (MSCWG); Policy and Procedures (PPWG); Technical Assistance and Training (TATWG).

²³ Tra questi figurano il GAFI, i connessi Organismi Regionali, la Commissione europea, Interpol, Europol, la World Customs Organization, il Fondo Monetario Internazionale, la Banca Mondiale, l'OSCE, lo United Nations Office on Drugs and Crime (UNODC).

Le complessità organizzative e decisionali connesse con la struttura accentrata sono temperate dalla presenza di “Gruppi Regionali”²⁴ tra cui le FIU si distribuiscono su base geografica. Diversamente dal sistema del Network del GAFI, effettivamente decentrato, nel quale gli Organismi Regionali sono soggetti separati, i Gruppi Regionali del Gruppo Egmont non sono strutture a sé stanti, dotate di propria organizzazione e di un mandato autonomo. Essi consistono in gruppi di lavoro interni e agiscono quali sedi di coordinamento e condivisione, prive di poteri decisionali, per canalizzare informazioni e decisioni da e verso gli organi centrali (Comitato, Gruppi di Lavoro). I Gruppi Regionali hanno anche il compito di monitorare gli sviluppi legislativi e operativi che interessano le FIU.

L’elaborazione di istruzioni e linee-guida si radica sulla definizione di “FIU”, coniata dal Gruppo Egmont e ripresa e specificata in tutte le fonti internazionali antiriciclaggio. Nel 1995, immediatamente dopo la sua istituzione, il Gruppo si confrontò con la necessità di individuare e sintetizzare i tratti caratteristici essenziali di una “FIU” per coniarne una definizione universalmente applicabile, in grado di tenere insieme approcci nazionali diversificati e di mantenere un nucleo comune di elementi essenziali, originali e qualificanti. Il risultato fu il seguente: *A central, national agency responsible for receiving (and, as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to counter money laundering and terrorism financing*²⁵.

Senza la possibilità di svolgere un esame puntuale dei diversi elementi espressi nella definizione²⁶, è importante rimarcare la caratteristica di essere al tempo stesso generale, in grado di comprendere caratteristiche e funzioni tipiche, e capace di far risaltare la “specialità” della nuova figura di Autorità. Il risultato è ottenuto soprattutto ponendo al centro le funzioni specialistiche della ricezione, dell’analisi e della disseminazione di segnalazioni di operazioni sospette.

La definizione di “FIU” del Gruppo Egmont è stata recepita in tutte le successive fonti internazionali in materia. Essa è stata aggiornata dalle Raccomandazioni del GAFI, nella rivisitazione di questi del 2012, e dallo stesso Gruppo Egmont, nel 2013. In Europa, la definizione di “FIU”, implicita nella prima direttiva antiriciclaggio del 1991, è stata introdotta in termini espliciti dalla seconda direttiva del 2001 e aggiornata dalla quarta direttiva del 2015²⁷.

I *Principles for Information Exchange between Financial Intelligence Units* e le *Operational Guidance for FIU Activities* (2013) esprimono numerose indicazioni sulle attività e sulla collaborazione delle FIU. Vengono precisati dettagli su caratteristiche e finalità dei compiti di ricezione, analisi e disseminazione²⁸, sull’esercizio di poteri informativi, su contenuti e modalità degli scambi di informazioni (richieste, informative)²⁹. Inoltre, la Raccomandazione 29 del GAFI, insieme alla relativa Nota Interpretativa, è indicata nella *Charter* del Gruppo Egmont quale parte integrante delle regole applicabili alle FIU membri dell’Organizzazione.

Tale sorta di “rinvio ricettizio” conferisce rilevanza diretta alle regole del GAFI, indirizzate agli Stati membri, per le FIU appartenenti al Gruppo Egmont, con l’effetto di completare il quadro dei “Principles” e delle “Operational Guidance” e di integrare le Raccomandazioni nell’“ordinamento settoriale” definito per le FIU. È su questo impianto di previsioni, nel quale

²⁴ Ve ne sono otto: Americas; Asia and Pacific; East and Southern Africa; Eurasia; Europe I; Europe II; Middle East and Northern Africa; West and Central Africa.

²⁵ Il riferimento al finanziamento del terrorismo è stato aggiunto nella revisione della definizione effettuata nel 2004.

²⁶ Cfr. P. Costanzo e R. Righetti, *La collaborazione internazionale in materia di antiriciclaggio: l’“Unità di Informazione Finanziaria” nella disciplina comunitaria e in quella domestica*, in Cass. Penale, 2002, 11, pp. 3569 ss. In base alla definizione, la “FIU” si colloca a fianco, con tratti distinti, di altre autorità con compiti “antiriciclaggio”: organi di polizia e giudiziari, che svolgono indagini, e autorità di supervisione, incaricate dei controlli sul rispetto degli obblighi.

²⁷ Per tenere conto degli affinamenti introdotti dal GAFI e dal Gruppo Egmont (art. 32, comma 3).

²⁸ Le previsioni sull’“analisi”, distinta in “operativa” e “strategica”, sono particolarmente importanti per definire una nozione comune, sia pure necessariamente generica, di tale concetto particolarmente sfuggente e diversamente inteso, “cifra” qualificante del ruolo delle FIU quale distinto da quello svolto dagli Organi investigativi sui medesimi fatti di riciclaggio o finanziamento del terrorismo.

²⁹ Di particolare importanza è il riferimento al dovere, per la FIU che riceve una richiesta di informazioni, di attivare tutti i poteri di cui dispone per lo svolgimento dei propri compiti domestici al fine di acquisire i dati utili per fornire l’assistenza richiesta. Le richieste di collaborazione internazionale sono in tutto equiparate alle segnalazioni di operazioni sospette domestiche quale presupposto per l’esercizio dei poteri informativi disponibili.

rientrano sia gli standard del GAFI sia le indicazioni attuative elaborate dal Gruppo Egmont, che si basano le verifiche da questo svolte nei confronti delle FIU.

Le valutazioni sulla conformità alle previsioni internazionali non si rivolgono ai paesi e al loro sistema antiriciclaggio. Esse riguardano le FIU, in coerenza con la natura non governativa del Gruppo Egmont, e attengono alle caratteristiche e alle attività di queste. Cionondimeno, in virtù dell'elevata capacità di "convincimento" delle analisi e dalle decisioni del Gruppo Egmont, i risultati delle verifiche si traducono in un potente stimolo alla realizzazione delle necessarie riforme da parte dei paesi interessati.

Diversamente dal GAFI, l'attività di valutazione del Gruppo Egmont non viene svolta "a tappeto". Gli interventi sono effettuati in maniera selettiva e sono indotti dal verificarsi di alcuni presupposti determinati. La causa più frequente di attivazione è l'esito negativo di Mutual Evaluation o di altre valutazioni svolte dal GAFI e da altri organismi internazionali, con l'assegnazione di rating insufficienti nei comparti che riguardano la FIU. Frequenti sono anche i casi di valutazioni avviate dal Gruppo Egmont a motivo di cambiamenti normativi o istituzionali nel sistema antiriciclaggio nazionale che investono la FIU e che appaiono suscettibili di alterarne le caratteristiche, le funzioni o i poteri.

Diversamente dalle Mutual Evaluation del GAFI, le verifiche del Gruppo Egmont non esprimono rating ai quali conseguono commisurate procedure di follow-up. In presenza di criticità, alle verifiche seguono procedure di supporto o di sanzione; le sanzioni principali riguardano lo status di membership: consistono, a seconda della gravità, nella sospensione e nell'espulsione. Incisiva è anche la sanzione della sospensione o dell'interruzione del collegamento della FIU dalla rete di comunicazione globale *Egmont Secure Web* impiegata per gli scambi di informazioni. Tale misura determina l'impossibilità di attivare la collaborazione internazionale, con gravi conseguenze operative³⁰. In casi di disallineamenti meno gravi ovvero di carenze operative le sanzioni sono accompagnate o sostituite da interventi di assistenza. In questi casi vengono definiti, congiuntamente con la FIU interessata, "piani d'azione" che individuano obiettivi, misure da adottare, tempi di completamento.

Il Gruppo Egmont gestisce e sviluppa la rete informatica globale per lo scambio di informazioni tra le FIU (*Egmont Secure Web* – ESW). Si tratta di un'infrastruttura di importanza fondamentale; essa consente la condivisione sicura di informazioni riservate, necessarie per la rilevazione e l'analisi di attività di riciclaggio o di finanziamento del terrorismo.

Tra le principali attività del Gruppo Egmont figura lo sviluppo di "policy" e linee-guida per le FIU e l'approfondimento di tipologie di riciclaggio. Il Gruppo, privo della capacità di formulare indirizzi "vincolanti", opera in stretto contatto con il GAFI per l'elaborazione di *policy* nelle materie di competenza³¹. La produzione del Gruppo Egmont in tema di tipologie è intensa; la parte riservata degli approfondimenti viene condivisa esclusivamente tra le FIU, i risultati complessivi su prassi e schemi operativi vengono pubblicati e in molti casi confluiscono nei lavori del GAFI.

1.2. L'attività dell'Unione europea. L'Unione come "regolatore" e "valutatore" antiriciclaggio

L'Unione europea presenta un ordinamento sovranazionale compiuto e fondato su una consolidata base giuridica³² che, nelle materie di competenza, attribuisce sovranità alle regole e alle decisioni adottate dagli organi europei, comprimendo quella degli Stati membri. L'Unione opera nel comparto dell'antiriciclaggio esercitando i propri poteri e prerogative in termini analoghi a quanto avviene negli altri settori di competenza.

Un vero e proprio ordinamento europeo antiriciclaggio ha preso forma nel corso degli anni, sviluppandosi in molteplici direzioni. Sul piano regolamentare, l'assetto è definito in primo luogo attraverso direttive, dalla prima del 1991 alla quinta del 2018. Su questo "tronco" principale si innestano

³⁰ Conseguenze si producono anche per le altre FIU, a loro volta impossibilitate a ottenere informazioni dalla controparte sospesa dalla connessione alla rete.

³¹ Ad esempio, il Gruppo Egmont ha collaborato con il GAFI per linee-guida sulla rilevazione e segnalazione di operazioni sospette nell'ambito di gruppi (soffermandosi su necessità e limiti dei flussi informativi interni), sulla cooperazione inter-istituzionale tra FIU e altre autorità nazionali, in particolare con gli Organi investigativi.

³² Naturalmente, l'ordinamento sovranazionale dell'Unione comprende gli Stati membri ai quali si indirizzano le regole e le policy europee antiriciclaggio. In questa prospettiva, l'Unione europea consiste in un'Istituzione con competenza territoriale di scala regionale, geograficamente limitata, anche in ciò distinguendosi dal GAFI e dal Gruppo Egmont entrambi enti di carattere globale (l'uno intergovernativo, l'altro di natura "tecnica").

regolamenti³³ e direttive su materie specifiche per le quali è sufficiente un livello minimo di armonizzazione³⁴ o rivolte ad aspetti di rilievo penale³⁵.

L'applicazione della procedura di infrazione conferisce alle regole europee antiriciclaggio una valenza diversa da quella propria degli standard del GAFI. Tuttavia, il meccanismo europeo di infrazione e le connesse attività di monitoraggio e di verifica si applicano per qualsiasi materia, non sono specificamente mirate alla *compliance* antiriciclaggio e difettano di una "metodologia" dedicata in grado di isolare e individuare carenze tecniche con sufficiente penetrazione e granularità. Diversamente dalle *Mutual Evaluation* del GAFI, le verifiche della Commissione consistono nel riscontro della presenza o assenza, negli ordinamenti nazionali, di disposizioni corrispondenti a quelle europee da recepire o applicare senza, in prima battuta, un esame delle previsioni nazionali volto a valutarne l'adeguatezza.

Le verifiche svolte nella procedura di infrazione non si estendono alla considerazione degli effetti e dell'efficacia di regole e misure messe in campo. Si tratta di un'altra importante differenza dalle valutazioni del GAFI nelle quali, oltre alla *technical compliance*, viene posto sotto esame il livello di efficacia nella concreta applicazione. Anche nelle conseguenze delle valutazioni sussistono naturalmente importanti differenze. Violazioni riscontrate in procedure europee di infrazione possono condurre all'irrogazione, da parte della Corte di Giustizia, di sanzioni autoritative, con carattere "punitivo".

La capacità dissuasiva di tali sanzioni resta da verificare nel settore antiriciclaggio. La complessità della procedura di infrazione e la "concorrenza" in essa di iniziative molteplici nelle più svariate materie ha sinora precluso un'azione sistematica di individuazione di carenze antiriciclaggio da parte degli Stati membri e di relativo *enforcement*³⁶.

1.2.1. Individuazione di Paesi terzi ad "alto rischio"

Elevata efficacia va ascritta alle iniziative europee per l'individuazione di Paesi terzi ad "alto rischio" nella prospettiva del riciclaggio e del finanziamento del terrorismo, inclusi in una lista pubblica che ne segnala le criticità.

Tale efficacia è determinata da fattori analoghi a quelli richiamati per le liste del GAFI: alle giurisdizioni "colpite" viene inferto un sensibile danno reputazionale che si traduce in maggiori costi e difficoltà nell'accesso ai mercati europei (specie bancari e finanziari) sino a generare effetti di de-risking. L'ambito non comprende gli Stati membri dell'Unione per i quali, sottoposti alle comuni regole europee, vale una presunzione di allineamento a tali regole. In ciò il sistema europeo si discosta da quello del GAFI nel quale, come si è visto, la ricognizione di paesi con carenze strategiche si estende ai propri membri.

Il sistema europeo di selezione e pubblicazione di liste "nere" di Paesi terzi è dettagliatamente regolato nella quarta direttiva, sul punto modificata e ampliata dalla quinta³⁷.

L'art. 9 affida alla Commissione l'identificazione di "Paesi terzi con carenze strategiche nei rispettivi regimi nazionali di AML/CFT", precisando che deve trattarsi di paesi che, a causa di tali carenze, "pongono minacce significative al sistema finanziario dell'Unione". La Commissione ha pubblicato il primo atto delegato con la lista di Paesi terzi ad alto rischio nel luglio 2016³⁸. Esso è stato più volte integrato, soprattutto per tenere conto dell'evoluzione delle analoghe liste del GAFI.

La direttiva ancora la valutazione a un ambito ampio e "tipizzato" di materie³⁹. Per conferire oggettività, trasparenza e prevedibilità alle valutazioni, la Commissione ha elaborato e pubblicato una complessa "Metodologia"⁴⁰ che descrive criteri e procedure.

³³ Ad esempio, in tema di dichiarazione del trasferimento fisico di contante e altri valori (Regolamenti (CE) n. 1889/2005 e (UE) 2018/1672) e di tracciabilità di bonifici e rimesse di fondi (Regolamenti (CE) n. 1781/2006 e (UE) 2015/847).

³⁴ Ad esempio, la direttiva (UE) 2019/1153 sull'utilizzo di informazioni "finanziarie" a supporto di indagini e procedimenti penali.

³⁵ Ad esempio, le direttive (UE) 2018/1673 e (UE) 2017/541, sulle fattispecie penali di riciclaggio e finanziamento del terrorismo.

³⁶ Possono essere ad ogni modo ricordate le procedure avviate nei confronti di alcuni Paesi per ritardi o inadempienze nel recepimento della quarta direttiva (UE) 2015/849. Analoghe iniziative sono state assunte in relazione all'inadeguato recepimento delle Direttive (UE) 2017/541 sul reato di terrorismo (procedura n. 2021/2180), UE 2018/1673 sul reato di riciclaggio (procedura n. 2021/0055) e (UE) 2019/1153 sull'uso dell'intelligence finanziaria (procedura 2021/0447).

³⁷ Sino al 2015 l'approccio dell'Unione ai rischi provenienti dall'esterno era fondato su un criterio di segno opposto. Anziché rivolgersi a Stati terzi con significative carenze per la compilazione di una lista "nera", venivano individuate in una lista "bianca" le giurisdizioni con sistemi antiriciclaggio "equivalenti" a quello europeo nei cui confronti veniva consentita l'applicazione di procedure di verifica in forma semplificata.

³⁸ Regolamento delegato (UE) 2016/1675 del 14 luglio 2016. La lista europea consolidata è consultabile sul [sito Internet della Commissione Europea](#).

³⁹ Le aree da esaminare comprendono: le fattispecie penali di riciclaggio e finanziamento del terrorismo; i presidi di adeguata verifica, conservazione delle informazioni e segnalazione di operazioni sospette; i poteri e le procedure delle autorità antiriciclaggio; il grado di efficacia che il sistema nel suo complesso è in grado di esprimere.

⁴⁰ Cfr. *Revised EU Methodology for Identifying High Risk Third Countries under Directive (EU) 2015/849*, 2020.

La Metodologia si sofferma sul ruolo degli organi europei, sui rapporti con l'analogo esercizio del GAFI, sul "contraddittorio" con i Paesi terzi valutati; delinea quindi una procedura articolata in otto "step" e una fase di "follow up"; individua le fonti informative da impiegare, i criteri per determinare l'esistenza di carenze in ciascun comparto e la rispettiva significatività. La controversa dialettica su obiettivi e portata della lista nera europea si è assestata su una linea di omologazione al GAFI⁴¹.

Gli effetti di rigore derivanti dall'inclusione nella lista nera europea sono analoghi a quelli delle corrispondenti contromisure del GAFI, ma più intensi ed estesi. L'art. 18(a) della direttiva antiriciclaggio richiede anzitutto ai soggetti obbligati degli Stati membri di applicare misure di verifica rafforzata in relazione a rapporti continuativi e transazioni che riguardano Paesi terzi listati⁴². In un approccio di armonizzazione massima che esclude diversificazioni nazionali, tali misure vengono tassativamente elencate in dettagliati doveri di "due diligence"⁴³. Inoltre, le Autorità competenti devono applicare specifiche verifiche e limitazioni nell'autorizzare lo stabilimento di filiali o succursali nell'Unione ovvero in paesi listati da parte di soggetti obbligati, rispettivamente, nell'Unione o in paesi ad alto rischio. Misure rafforzate sono anche previste per i rapporti di corrispondenza e la loro possibile interruzione. Per effetto della pedissequa aderenza alle determinazioni del GAFI (non scerve da influenze politiche), le contromisure europee confermano e amplificano gli effetti di queste più che definire un sistema commisurato ai rischi specifici per l'Unione.

1.2.2. Il "Comitato in materia di prevenzione del riciclaggio e del finanziamento del terrorismo"

Il *Committee on the Prevention of Money Laundering and Terrorist Financing* (CPMLTF), da ultimo previsto e regolato dalla quinta direttiva⁴⁴, fu introdotto dalla prima direttiva nel 1991 e successivamente più volte rivisto nella sua veste formale⁴⁵. Tratto costante è sempre stato quello di fornire supporto alla Commissione europea (che lo presiede) nello svolgimento dei compiti a questa attribuiti dalle direttive e dalle altre fonti antiriciclaggio⁴⁶. Le competenze del Comitato, inizialmente circoscritte alla predisposizione del periodico rapporto della Commissione sull'applicazione delle regole antiriciclaggio da parte degli Stati membri, si sono considerevolmente estese.

Il Comitato è composto da rappresentanti degli Stati membri di livello "governativo". Il ruolo di ausilio e consulenza alla Commissione è ben distinto da quello svolto dagli Stati membri in seno al Consiglio. Si tratta, in effetti, di una struttura riconducibile al sistema della "Comitologia" (*Comitology*), in passato impiegato per la compartecipazione di Commissione e Stati membri nella regolamentazione attuativa in materia bancaria e finanziaria.

Attraverso il Comitato esperti degli Stati membri partecipano alla predisposizione del *Supra-National Risk Assessment*⁴⁷, all'elaborazione della metodologia di valutazione dei Paesi terzi ad alto rischio e alle relative verifiche⁴⁸. Nel Comitato la Commissione e gli Stati membri si confrontano e si coordinano per la partecipazione alle attività del GAFI, nell'intento di formare posizioni condivise su temi di interesse europeo. Attraverso il Comitato, inoltre, la Commissione riceve dagli Stati membri informazioni e

⁴¹ La Commissione europea si è trovata condizionata da due vincoli contrapposti. Gli Stati membri hanno insistito per mantenere un completo allineamento della lista europea a quella del GAFI, con il duplice intento di contenere l'esposizione politica e di limitare i fattori di complicazione (e di costo) per la compliance derivanti dalla necessità di applicare liste non uniformi. Il Parlamento europeo ha invece ribadito la necessità di orientare la valutazione verso giurisdizioni dalle quali promanano rischi per il Mercato Interno, evitando il semplice "recepimento" delle conclusioni del GAFI e compilando un'autonoma lista europea.

⁴² Si noti che la portata dell'obbligo va oltre i casi di provenienza del cliente o della controparte da Paesi a rischio. Il primo comma dell'art. 18 attribuisce infatti rilievo a qualsiasi collegamento, ad esempio l'origine, la destinazione o la collocazione di fondi, disponibilità o rapporti.

⁴³ Tra cui l'acquisizione di ampie informazioni sui soggetti coinvolti, sull'origine delle disponibilità, sugli scopi perseguiti, l'applicazione di misure aggiuntive di monitoraggio, il coinvolgimento dei vertici aziendali nelle decisioni.

⁴⁴ Cfr. art. 1, n. 40, con il quale viene introdotto l'art. 64-bis della quarta direttiva: "La Commissione è assistita dal comitato in materia di prevenzione del riciclaggio e del finanziamento del terrorismo («Comitato») di cui all'articolo 23 del regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio".

⁴⁵ Esso è configurato dal citato art. 64-bis come "un comitato ai sensi del regolamento (UE) n. 182/2011" recante, quest'ultimo, "le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione".

⁴⁶ Cfr. ad esempio i riferimenti al Comitato nel regolamento (UE) 2015/847 sulle informazioni che devono accompagnare i trasferimenti di fondi (art. 23).

⁴⁷ La valutazione sovranazionale dei rischi mira a individuare e "misurare" minacce e vulnerabilità relative a fattori esterni che si riverberano sull'Unione ovvero che scaturiscono da dinamiche "cross-border" non agevolmente rilevabili dagli Stati membri attraverso gli esercizi nazionali di valutazione dei rischi (art. 6 della direttiva).

⁴⁸ In virtù della competenza del Consiglio nel procedimento di adozione degli atti delegati della Commissione che definiscono e aggiornano la lista "nera", il ruolo del CPMLTF in questa materia consiste nel raccordo tra Commissione e Consiglio, più che in una vera e propria assistenza di natura tecnica nelle valutazioni, per la quale mancherebbe la necessaria neutralità.

valutazioni per il rapporto periodico sul recepimento della direttiva antiriciclaggio, da presentare al Parlamento e al Consiglio⁴⁹.

1.2.3. La “Piattaforma” delle FIU dell’Unione europea

La *EU FIUs’ Platform* è stata istituita nel 2006 dalla Commissione quale comitato tecnico composto da rappresentanti delle FIU per fornire supporto alla Commissione stessa e consentire il confronto e il coordinamento tra le FIU dei Paesi membri. L’iniziativa seguiva l’adozione della terza direttiva che, nel 2005, segnò una marcata estensione dell’ambito e della complessità del sistema antiriciclaggio europeo, a sua volta conseguente alla riforma degli standard del GAFI del 2002. Il nuovo sistema, informato all’approccio basato sul rischio, comporta la necessità di valutazioni, spesso prive di diretti riferimenti in precedenti esperienze, con un accresciuto ruolo delle Autorità nazionali e della Commissione.

Al contempo, con la terza direttiva le regole europee su caratteristiche, poteri, attività e collaborazione delle FIU vengono ampliate in un sistema complesso e tuttavia non armonizzato che, proprio per queste caratteristiche, rende necessario un impegno di coordinamento e l’elaborazione di indicazioni uniformi per l’attuazione, specie per mantenere e sviluppare forme efficaci di collaborazione. Anche a queste esigenze la Piattaforma è chiamata a rispondere. Essa arricchisce il sistema degli organi di “policy” nel comparto, affiancandosi come gruppo composto da Autorità specializzate al preesistente CPMLTF, espressione di organi governativi.

Con l’istituzione della Piattaforma viene anche posto rimedio, sia pure parziale, a un’asimmetria macroscopica tra il sistema europeo antiriciclaggio e quello, per molti versi connesso, della regolamentazione e della supervisione bancaria e finanziaria⁵⁰.

La Piattaforma delle FIU è stata formalmente riconosciuta dalla quarta direttiva, nel 2015. Nell’art. 51, sulla descrizione dei compiti, e in altre disposizioni della stessa direttiva, vengono specificate le due richiamate esigenze di supporto alla Commissione e di coordinamento tra le FIU.

La Piattaforma è chiamata ad “agevolare la cooperazione tra FIU”, approfondire “questioni in materia di attuazione” della direttiva di rilievo per le FIU ovvero per i soggetti segnalanti⁵¹; compiti specifici richiamati dall’art. 51 riguardano⁵²: l’“individuazione di operazioni sospette con carattere transfrontaliero”⁵³, la “standardizzazione dei formati delle segnalazioni”, da impiegare nella rete FIU.NET, l’“analisi congiunta dei casi di carattere transfrontaliero”⁵⁴. Inoltre, la Piattaforma ha il compito di contribuire alla “identificazione delle tendenze e dei fattori rilevanti per la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo a livello sia nazionale che sovranazionale”.

Dall’art. 51 emerge dunque l’abbozzo di un disegno di coordinamento sovranazionale per la rilevazione e l’analisi di attività di riciclaggio e finanziamento del terrorismo di rilievo *cross-border*. Vengono delineate tre fasi: l’individuazione di casi significativi, sulla base di criteri di selezione comuni; lo scambio “automatico” (obbligatorio, non su richiesta né spontaneo) delle relative informazioni tra le FIU interessate, in formati uniformi attraverso FIU.NET; l’analisi congiunta dei fenomeni individuati.

⁴⁹ Con il rapporto la Commissione dà conto dell’adeguatezza delle misure antiriciclaggio nazionali sulla base dei rischi, della capacità delle autorità competenti di operare e collaborare efficacemente, del funzionamento della collaborazione internazionale (art. 65, specificato e ampliato dalla quinta direttiva).

⁵⁰ Il sistema bancario e finanziario era da tempo articolato in distinti livelli di elaborazione e coordinamento politico e tecnico, secondo i canoni della Procedura “Lamfalussy”. La materia è stata integralmente rivisitata con l’istituzione del *Single Supervisory Mechanism*, con l’accentramento di compiti presso una nuova Autorità sovranazionale e un sistema di ripartizione di interventi e di coordinamento tra il piano europeo e quello nazionale.

⁵¹ Rientrano in questo ambito, ad esempio, aspetti attuativi della rilevazione e segnalazione di operazioni sospette.

⁵² I compiti e le attività individuati per la Piattaforma nell’art. 51 della quarta direttiva costituiscono il nucleo attorno al quale sono state elaborate le competenze dell’AMLA quale “Meccanismo” delle FIU nelle proposte legislative dell’AML Package.

⁵³ Il riferimento è alle segnalazioni “che riguardano un altro Stato membro”, da trasmettere “prontamente alla FIU di tale Stato membro” (art. 53).

⁵⁴ L’istituto delle “analisi congiunte” costituisce un’importante novità introdotta dalla quarta direttiva, al pari della nozione di “segnalazione cross-border” e del connesso obbligo di scambio automatico tra le FIU. Si tratta di una forma di collaborazione, sperimentata nella prassi dei rapporti tra le FIU, nella quale queste non si limitano a scambiare informazioni per le rispettive analisi ma condividono l’analisi stessa svolgendo l’esame congiunto delle informazioni per una ricostruzione condivisa di attività sospette che attraversano i rispettivi Paesi.

Questi tre elementi di un efficace sistema sovranazionale si trovano ora alla base del nuovo sistema delineato nell'AML Package. Questo, in particolare, conferma e amplia l'istituto della segnalazione *cross-border*, definisce una procedura per la selezione di casi rilevanti da sottoporre ad analisi congiunta, individua le principali fasi di quest'ultima attribuendo ruoli e responsabilità all'AMLA e alle FIU.

La Piattaforma delle FIU ha perseguito il proprio mandato attraverso numerosi progetti e attività. All'indomani dell'adozione della quarta direttiva, essa ha svolto un'articolata ricognizione delle carenze regolamentari e operative e delle aree di maggiore scostamento tra le soluzioni nazionali sulle caratteristiche delle FIU, le competenze, i poteri, la capacità di collaborazione. L'analisi è stata accompagnata da proposte di regole, policy e soluzioni operative.

1.2.4. *Le European Supervisory Authorities*

Le European Supervisory Authorities (ESAs)⁵⁵ sono state istituite nel 2010 quale parte dello European System of Financial Supervision (ESFS). Esse rappresentano l'evoluzione dei Gruppi di Lavoro di secondo livello che, nel previgente sistema, fornivano supporto alla Commissione per la predisposizione della disciplina attuativa. All'EBA, in particolare, sono attribuiti compiti di regolamentazione e di coordinamento per l'attuazione delle disposizioni antiriciclaggio nel settore bancario e per lo svolgimento dei controlli da parte delle Autorità nazionali secondo metodi convergenti. Tali compiti confluiranno nel mandato dell'AMLA, successore dell'EBA quale Autorità europea di supervisione antiriciclaggio.

La quarta direttiva, come integrata dalla quinta, introduce regole più dettagliate in tema di supervisione antiriciclaggio, a livello nazionale e nella collaborazione internazionale. Essa, inoltre, configura un sistema di attuazione delle regole primarie attraverso disposizioni di rango secondario attribuendo all'EBA estesi compiti di elaborazione di *implementing* e *regulatory technical standards* per il settore bancario e finanziario, proposti alla Commissione per l'adozione.

Al pari degli Stati membri e delle FIU le ESAs contribuiscono alla valutazione europea dei rischi di riciclaggio e di finanziamento del terrorismo. Specificano poi il contenuto delle misure di adeguata verifica *risk-based*⁵⁶. La competenza delle ESAs nella formulazione di orientamenti su presupposti e misure dell'adeguata verifica è circoscritta al settore bancario e finanziario⁵⁷.

La direttiva affida alle ESAs il compito di elaborare "norme tecniche" in materie caratterizzate da complessità e dall'esigenza di evitare o contenere dannose difformità nazionali. L'intervento riguarda l'organizzazione interna e i presidi di cui banche e intermediari devono dotarsi nell'ambito di gruppi e nell'attività transfrontaliera⁵⁸. Le ESAs specificano inoltre le circostanze nelle quali è necessaria, per istituti di moneta elettronica e istituti di pagamento che operano in diversi Stati membri in libera prestazione, l'istituzione di un "punto di contatto centrale" responsabile, per conto "dell'intermediario di riferimento", dell'applicazione delle norme antiriciclaggio nel Paese "host" e di "facilitare la vigilanza da parte delle Autorità competenti" del medesimo Paese, anche fornendo documenti e informazioni. Ancora, le ESAs definiscono "orientamenti" per le Autorità nazionali sulle "caratteristiche di un approccio alla vigilanza basato sul rischio".

Con le modifiche apportate nel 2019 al regolamento (UE) 1093/2010, che istituisce e regola l'EBA, le competenze assegnate alle ESAs in materia di antiriciclaggio sono state consolidate in capo a tale Autorità. Le attività di coordinamento e attuazione regolamentare del sistema di vigilanza antiriciclaggio

⁵⁵ *European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA)*.

⁵⁶ Esse formulano "orientamenti indirizzati alle autorità competenti nonché agli enti creditizi e finanziari" su "fattori di rischio" e "misure da adottare" per la verifica in forma semplificata (art. 17) e rafforzata (art. 18, comma 4). Cfr. EBA, *Orientamenti ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849*, 1° marzo 2021.

⁵⁷ I relativi provvedimenti vengono adottati ai sensi dell'art. 16 dei Regolamenti (UE) 1093/2010, (UE) 1094/2010 e (UE) 1095/2010 (Regolamenti istitutivi delle ESA), cui la direttiva antiriciclaggio rinvia e che confermano che essi sono "indirizzati alle autorità competenti o agli istituti finanziari" con l'obiettivo di "istituire prassi di vigilanza uniformi, efficienti ed efficaci" e "assicurare l'applicazione comune, uniforme e coerente del diritto dell'Unione".

⁵⁸ Il comma 5 dell'art. 45 prevede in generale l'obbligo per banche e intermediari di applicare "misure supplementari" rispetto alle "politiche e procedure a livello di gruppo" previste dal comma 1, per "far fronte al rischio di riciclaggio e finanziamento del terrorismo" in filiali e succursali in Paesi terzi i cui ordinamenti non consentono l'applicazione delle relative politiche e procedure di gruppo.

sono state al contempo estese e rafforzate⁵⁹. Per l'esercizio delle articolate competenze antiriciclaggio attribuite all'EBA è istituito al suo interno un "Comitato Permanente" (*Anti-Money Laundering Standing Committee*), composto da rappresentanti delle Autorità nazionali competenti⁶⁰.

2. L'evoluzione della disciplina internazionale (P. Costanzo e M. Siani)

Il riciclaggio, nelle sue manifestazioni più significative, è svolto nei mercati finanziari, attraverso gli intermediari che vi operano e si articola sul piano internazionale. Le condotte criminose vengono ripartite in diverse fasi e tra più giurisdizioni, sfruttando diversità nelle regole e nei controlli per profittare di opportunità di anonimato, interposizione o occultamento. Un efficace sistema di prevenzione e di contrasto presuppone regole uniformi per contenere possibilità di arbitraggio e di elusione, e forme di coordinamento tra i presidi e i controlli nazionali.

L'impiego di strumenti digitali amplifica le opportunità per i criminali di separare il formale esecutore dall'effettivo titolare di beni e interessi e il luogo delle operazioni dal luogo della presenza fisica, spiazzando il paradigma della "tracciabilità", basato sulla ricostruzione "a ritroso" di tracce che portano dal denaro impiegato o trasferito alla sua origine. Il "paper trail" è ostacolato dalle discontinuità di regole e controlli e dall'applicazione di presidi concepiti per forme di operatività "tradizionale"; anche l'individuazione del titolare effettivo di beni e interessi è spesso impossibile a causa della indisponibilità di informazioni nei diversi paesi.

Azioni nazionali isolate possono essere inefficaci e talora controproducenti. È da tempo evidente la necessità di superare la portata nazionale dei presidi, sia sul versante della repressione, sia su quello della prevenzione. La consapevolezza della dimensione internazionale del riciclaggio (e del finanziamento del terrorismo) è alla base del ruolo svolto da organismi internazionali ed europei nella configurazione di un sistema di prevenzione e contrasto uniforme ed efficace.

La produzione di regole da parte di tali organismi ha condotto a un sistema "stratificato", in cui coesistono atti con portata vincolante, talora prevalenti rispetto alla normativa nazionale, strumenti pattizi di diritto internazionale di portata globale o regionale (convenzioni e dichiarazioni di principi, muniti di potere prescrittivo differenziato), "standard" e raccomandazioni che, seppur privi di portata vincolante, si caratterizzano per una capacità cogente elevata, sostenuta da meccanismi di *peer pressure*.

Al centro della regolamentazione internazionale antiriciclaggio si colloca proprio uno strumento di *soft law*: le "Raccomandazioni" del GAFI.

Il sistema antiriciclaggio internazionale è articolato ma coerente. La "primazia" riconosciuta al GAFI assicura unitarietà degli indirizzi; i reciproci richiami e rinvii consentono di ricostruire con sufficiente certezza il "sistema" in cui si inscrivono i diversi interventi; il diretto coinvolgimento di Stati e Autorità nazionali nell'elaborazione di standard e regole, in una complessa combinazione di multilateralismo e sovranazionalità, facilita la condivisione e l'adesione. Per descrivere il composito sistema di regole si illustrano separatamente le materie del contrasto penale e della prevenzione.

2.1. La "criminalizzazione" del riciclaggio e i reati presupposto.

Le prime indicazioni organiche su una fattispecie penale di "riciclaggio" in una fonte internazionale sono quelle contenute nella Convenzione delle Nazioni Unite contro il traffico di sostanze stupefacenti e psicotrope, adottata a Vienna il 19 dicembre 1988. Pur senza riferirsi al "riciclaggio", l'art. 3, comma 1,

⁵⁹ Nel nuovo assetto "l'Autorità assume un ruolo guida di coordinamento e monitoraggio nel promuovere l'integrità, la trasparenza e la sicurezza nel sistema finanziario mediante l'adozione di misure volte a prevenire e contrastare il riciclaggio e il finanziamento del terrorismo in tale sistema". L'EBA è in particolare competente per "*l'elaborazione di orientamenti e norme comuni (...) e promuoverne l'applicazione uniforme*"; le misure comprendono, tra l'altro, "progetti di norme tecniche di regolamentazione e di attuazione (...), orientamenti, raccomandazioni, (...) pareri" (art. 9-bis, comma 1, lett. c), introdotto dal citato regolamento (UE) 2019/2175).

⁶⁰ Cfr. art. 9, comma 7, del regolamento EBA.

lett. b), stabilisce l'obbligo per gli Stati firmatari di prevedere come reato, se compiute intenzionalmente, condotte di conversione, trasferimento o occultamento dei proventi di reati di produzione o spaccio di sostanze stupefacenti.

La percezione dell'eminente gravità dei reati di droga, delle motivazioni di arricchimento alla base del loro compimento da parte di organizzazioni criminali e, dunque, della necessità di rivolgere lo strumento penale specificamente su tali profili, ha indotto a estendere l'area della punibilità isolando il "postfatto" delle condotte principali (il primo individuato come fulcro motivazionale delle seconde) per rendere il "riciclaggio" un'area nuova e autonoma di incriminazione.

Sebbene, dunque, la fattispecie di "riciclaggio" assolve, nella Convenzione di Vienna, alla funzione strumentale di completare, a valle, il dispositivo di contrasto dei delitti presupposto, la Convenzione segna un punto di non ritorno: la fattispecie è destinata a consolidarsi rapidamente, al contempo estendendo l'ambito degli antefatti e acquisendo autonomia rispetto ad essi, in termini di finalità della tutela e di beni giuridici sottesi. La fattispecie coniata nella Convenzione di Vienna, specie in relazione alle condotte (conversione, trasferimento, occultamento), costituirà il modello per gli sviluppi successivi⁶¹.

Adottando analogo impianto normativo, la Convenzione del Consiglio d'Europa sul "Riciclaggio, la ricerca, il sequestro e la confisca dei proventi da reato", adottata a Strasburgo l'8 novembre 1990, menziona espressamente all'art. 6 le fattispecie di "*Laundering Offences*" (per la prima volta così definite in uno strumento internazionale) e stabilisce la necessità che esse siano previste come reato nelle legislazioni nazionali⁶².

L'ambito degli illeciti presupposto viene affrancato dal ristretto riferimento ai reati connessi alla produzione e al traffico di sostanze stupefacenti; viene introdotto un approccio "*all crimes*" mediante un rinvio generale a tutti i reati suscettibili di generare proventi (temperato però dalla previsione della possibilità per gli Stati di formulare riserve in sede di ratifica).

Le Nazioni Unite sono nuovamente intervenute sulla fattispecie penale di riciclaggio con la Convenzione contro la criminalità organizzata transnazionale, sottoscritta a Palermo nel novembre 2000⁶³. Così come nella Convenzione di Vienna il riciclaggio costituisce lo strumento per estendere la tutela penale contro il traffico di stupefacenti, nell'intervento del 2000 la fattispecie viene impiegata, in termini più vasti, per colpire gli interessi economici della criminalità organizzata. Essa svolge, dunque, ancora un ruolo di completamento di finalità specifiche di politica criminale; viene tuttavia disciplinata con tratti più autonomi, estesa a un ambito più ampio e ascrivita alla tutela di beni giuridici propri.

La Convenzione di Palermo riprende e amplia il contenuto della Convenzione di Vienna. Il reato di riciclaggio deve comprendere, quali "*predicate-crimes*", almeno tutti i "reati gravi" (art. 2) in base alla pena edittale (non inferiore a quattro anni), sulla scorta della Convenzione di Strasburgo del Consiglio d'Europa, intervenuta nel 1990. L'ambito dei reati presupposto viene quindi esteso ben al di là dei delitti di droga cui si rivolgeva la Convenzione di Vienna⁶⁴.

La Convenzione di Varsavia del 2005⁶⁵ aggiorna ed estende la disciplina penale contenuta nella Convenzione di Strasburgo. La configurazione delle condotte resta allineata alla fattispecie delle Nazioni Unite. Innovazioni vengono apportate all'ambito dei reati presupposto⁶⁶, alla fisionomia dell'elemento soggettivo⁶⁷, al regime probatorio, ai rapporti tra il riciclaggio e il suo antefatto (stabilendo la non necessità di una previa condanna per il secondo), alla previsione della responsabilità per riciclaggio

⁶¹ La Convenzione di Vienna – ratificata con la legge 5 novembre 1990, n. 328 – ha costituito "l'impalcatura fondamentale sulla quale è stato edificato il successivo quadro normativo": così F. Di Vizio, *Il riciclaggio nella prospettiva penale ed in quella amministrativa - Definizioni di riciclaggio*, Quaderni dell'Antiriciclaggio, Roma, 2017, n. 8, p. 12.

⁶² La Convenzione di Strasburgo è stata ratificata in Italia con la legge 9 agosto 1993, n. 328.

⁶³ La Convenzione è stata ratificata in Italia con la legge 16 marzo 2006, n. 146.

⁶⁴ La struttura della condotta non si discosta dal modello fornito dalla precedente Convenzione. Vengono previsti presidi antiriciclaggio non penali (identificazione della clientela da parte di banche e intermediari, conservazione delle informazioni, segnalazione delle operazioni sospette, monitoraggio del trasporto di valori da e per l'estero, collaborazione internazionale) (art. 7), in opportuno raccordo con le Raccomandazioni del GAFI.

⁶⁵ L'Italia ha ratificato la Convenzione con la Legge 28 luglio 2016, n. 153.

⁶⁶ Questo viene esteso a tutti i reati puniti, negli ordinamenti nazionali, con pena detentiva massima superiore ad un anno ovvero con una pena detentiva minima superiore a sei mesi, in linea con il criterio nel frattempo introdotto dalle Raccomandazioni del GAFI del 2003.

⁶⁷ Elemento innovativo della Convenzione è la facoltà per i Paesi aderenti di prevedere come reato ipotesi non dolose ovvero nelle quali il soggetto agente "sospettava che i beni costituivano provento di reato" ovvero "avrebbe dovuto presumere che i beni costituivano provento di reato" (art. 9, comma 3).

delle persone giuridiche. Diversamente dalle Convenzioni richiamate sopra, incentrate sulla disciplina della materia penale⁶⁸, la Convenzione di Varsavia introduce anche disposizioni che trasfondono in “hard law” i presidi preventivi previsti dagli standard del GAFI.

Le Quaranta Raccomandazioni del GAFI, adottate nel 1990 e complessivamente riformate nel 2003 e nel 2012⁶⁹, dedicano alla configurazione della fattispecie penale di riciclaggio la Raccomandazione 3. Essa conferma, anzitutto, che il riciclaggio deve essere “criminalizzato” secondo quanto stabilito dalle Convenzioni delle Nazioni Unite di Vienna e di Palermo del 1988 e del 2000, assunte dunque come “modello” internazionale di incriminazione. In più, specificando i riferimenti contenuti nelle Convenzioni citate, viene posta la necessità di estendere il reato di riciclaggio a tutti i “reati gravi”, quali illeciti presupposto da individuarsi quanto più estensivamente possibile⁷⁰.

Dal 2001 gli standard internazionali antiriciclaggio del GAFI sono stati estesi, in parte, alla prevenzione e al contrasto del finanziamento del terrorismo. In termini del tutto simili alle disposizioni sul reato di riciclaggio, la Raccomandazione n. 5 prevede la necessità di introdurre negli ordinamenti nazionali una fattispecie penale di finanziamento del terrorismo, configurata secondo il modello della Convenzione delle Nazioni Unite del 1999⁷¹.

La regolamentazione europea ha elaborato una fattispecie di riciclaggio nelle Direttive che, sebbene priva di una diretta rilevanza penale e sviluppata quale presupposto per l'applicazione delle misure preventive, ha favorito l'allineamento delle fattispecie incriminatrici al modello internazionale richiamato nel paragrafo precedente.

Nell'assenza, sino a tempi recenti, di una competenza legislativa in materia penale, le regole europee sono comunque intervenute in materia di repressione del reato di riciclaggio facendo leva sulle prerogative riconosciute nell'ambito del “terzo pilastro” della Comunità europea: vanno ricordate l'Azione Comune 98/699/GAI del 3 dicembre 1998 e, soprattutto, la Decisione-Quadro 2001/500/GAI del 26 giugno 2001, che obbligò gli Stati membri a ratificare la Convenzione di Strasburgo del Consiglio d'Europa, al contempo limitando le riserve sull'ambito dell'incriminazione del riciclaggio.

La prima direttiva antiriciclaggio (91/308/CEE del 10 giugno 1991) è di poco successiva alla Convenzione di Strasburgo del Consiglio d'Europa e, come questa, mutua dalla Convenzione di Vienna delle Nazioni Unite la disciplina della fattispecie di riciclaggio. La regolamentazione comunitaria dell'illecito ruota attorno a due nozioni: quella di “riciclaggio”, relativa alle condotte, e quella di “attività criminosa”, relativa all'ambito dei reati presupposto.

Le condotte che integrano il riciclaggio sono descritte nella prima direttiva in termini pressoché identici a quelli dell'art. 3 della Convenzione di Vienna⁷². La seconda e la terza direttiva non hanno apportato modifiche sul punto. Anche per l'individuazione dei reati presupposto la definizione di “attività criminosa” contenuta nell'art.1 della prima direttiva si attiene alle indicazioni delle coeve fonti internazionali. Essa è fondata, da un lato, sull'indicazione di un ambito minimo armonizzato di reati che devono senz'altro costituire illeciti presupposto (si tratta dei reati “specificati nell'art. 3, par. 1, lett. a) della

⁶⁸ Ma si veda il citato art. 7 della Convenzione ONU di Palermo e il rinvio in esso agli standard in materia preventiva.

⁶⁹ L'ambito delle Raccomandazioni è stato esteso nel 2001 al contrasto del finanziamento del terrorismo, con l'introduzione di nove “Raccomandazioni speciali”, e nel 2008 al finanziamento della proliferazione di armi di distruzione di massa, in conformità alle relative Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite. Con la revisione organica completata a febbraio 2012 gli standard antiterrorismo sono stati integrati nel corpo delle Quaranta Raccomandazioni. Queste sono state poi ripetutamente modificate e aggiornate negli anni successivi, attraverso interventi in materie specifiche.

⁷⁰ Sono possibili diversi approcci: 1) inclusione di tutti i reati (*all offences approach*); 2) applicazione di una “soglia” (categorie di reati gravi o pena edittale massima o minima; *threshold approach*); 3) definizione di una lista di reati rilevanti (*list approach*); 4) combinazione dei criteri precedenti. La punibilità si estende ai casi di reati presupposto commessi all'estero; è prevista la condizione della “*double criminality*”, ma con facoltà per i Paesi di discostarsene. Oltre alla configurazione sostanziale del reato e dei suoi presupposti, le Raccomandazioni contengono previsioni in materia di confisca (Raccomandazione 4) e di cooperazione e assistenza giudiziaria internazionale (Raccomandazioni 36-39).

⁷¹ I presidi penali sono accompagnati dal richiamo al rispetto delle Risoluzioni del Consiglio di Sicurezza delle Nazioni Unite che introducono e disciplinano sanzioni finanziarie di “congelamento” volte a impedire flussi di fondi a supporto di attività o organizzazioni terroristiche (Raccomandazione 6). Tali misure sono estese anche alla materia del contrasto del finanziamento della proliferazione di armi di distruzione di massa (Raccomandazione 7).

⁷² Rilevano, dunque, la “conversione o il trasferimento” effettuati conoscendo la provenienza illecita dei beni coinvolti, al duplice, alternativo scopo di occultare o dissimulare la provenienza illecita ovvero di aiutare altri a sottrarsi alle conseguenze giuridiche delle proprie azioni; “l'occultamento o la dissimulazione della natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o diritti sugli stessi”; “l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza” della loro provenienza illecita.

Convenzione di Vienna, connessi al traffico di stupefacenti) e, d'altro lato, sul rinvio a ulteriori illeciti individuati dagli Stati membri, cui è dunque rimesso l'ampliamento dell'ambito minimo.

La seconda direttiva (2001/97/CE del 4 dicembre 2001) amplia considerevolmente il “catalogo” delle fattispecie presupposto integrando, nell'art.1, la definizione di “attività criminosa”. La tecnica normativa impiegata per estendere l'intervento di armonizzazione si basa sia sul riferimento a fattispecie specifiche, sia sul rinvio a categorie generali di illeciti non “nominati”.

A fianco dei reati previsti nell'art. 3, par. 1, lett. a), della Convenzione di Vienna, vengono richiamate “le attività delle organizzazioni criminali”, quali definite nell'Azione Comune del Consiglio 98/733/GAI, la frode, perlomeno grave, come definita nella Convenzione sulla tutela degli interessi finanziari delle Comunità Europee, la corruzione. Viene inoltre fatto riferimento a “un reato che possa fruttare consistenti proventi e sia punibile con una severa pena detentiva in base al diritto penale dello Stato membro”. Viene confermata la clausola contenuta nella prima direttiva, secondo cui gli Stati membri possano estendere il novero dei reati presupposto a livello nazionale.

Con la terza direttiva (CE 2005/60 del 26 ottobre 2005) l'area dei reati presupposto viene allineata a quella dei “reati gravi” di cui alla richiamata Azione Comune 98/699/GAI. Viene eliminato il riferimento generico a reati suscettibili di generare proventi significativi e, adottando un approccio per “soglia”, sono richiamati i reati puniti con una pena edittale superiore a un anno ovvero, per gli Stati ove sono previste soglie minime, di durata minima superiore a sei mesi; vengono inoltre aggiunte le condotte di finanziamento del terrorismo, con rinvio alla Decisione-Quadro 2002/475/GAI.

Per la definizione dell'elemento soggettivo del riciclaggio, le tre Direttive riproducono le disposizioni delle Convenzioni di Vienna e di Strasburgo. Le condotte devono essere commesse “intenzionalmente”, richiedendosi dunque il dolo; l'onere probatorio è però alleviato: “la conoscenza, l'intenzione o la finalità (...) possono essere accertate in base a circostanze di fatto obiettive”.

La quarta direttiva antiriciclaggio (UE 2015/849 del 20 maggio 2015) non introduce innovazioni rispetto alla tipizzazione delle condotte di riciclaggio, ancorate alla consolidata tripartizione, e al loro elemento psicologico. Quanto alla definizione di “attività criminosa”, l'art. 3, punto 4, aggiunge alle categorie di reati presupposto già tipizzate i “reati fiscali”, connessi alle imposte dirette e indirette⁷³.

La quinta direttiva (UE 2018/843 del 30 maggio 2018) non modifica aspetti sostanziali della fattispecie di riciclaggio⁷⁴.

In coerenza con la natura degli strumenti e con i limiti della competenza legislativa europea, sebbene il riciclaggio sia indicato quale illecito dalle Direttive, esso non è qualificato come reato. L'art. 2 della direttiva 91/308/CEE (con una previsione immutata nelle Direttive seguenti), infatti, si limita a disporre che i “Paesi membri devono provvedere a che il riciclaggio sia vietato”⁷⁵.

Competenze legislative dell'Unione europea in materia penale sono state introdotte con le modifiche al Trattato sull'Unione apportate dal Trattato di Lisbona⁷⁶ (artt. 82 e 83). L'art 83, in particolare, attribuisce all'Unione il potere di stabilire norme minime (attraverso Direttive) per la definizione di reati e sanzioni in materie “che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni”. La fattispecie di riciclaggio viene esplicitamente inclusa in questo ambito.

La disciplina penale europea del riciclaggio è contenuta nella direttiva (UE) 2018/1673 del 23 ottobre 2018 sulla “lotta al riciclaggio mediante il diritto penale”. Essa introduce misure armonizzate sulle condotte, i reati presupposto, le sanzioni.

⁷³ Pur senza pervenire a una univoca individuazione armonizzata delle fattispecie rilevanti, la quarta direttiva segna dunque l'estensione del perimetro del riciclaggio alla materia fiscale (cfr. il considerando 11).

⁷⁴ Il riferimento ai reati di terrorismo viene aggiornato, sostituendo il rinvio alla Decisione Quadro 2002/475/GAI con quello alla sopravvenuta direttiva (UE) 2017/541. Analogamente, il riferimento ai reati associativi previsti dall'Azione Comune 98/733/GAI viene aggiornato mediante il richiamo alla attività delle organizzazioni criminali quali definite all'art. 1, punto 1, della successiva Decisione-Quadro 2008/841/GAI.

⁷⁵ Tale divieto poteva pertanto essere accompagnato da sanzioni di natura non penale. Ad ogni modo, come si è accennato, la qualificazione del riciclaggio di proventi di “reati gravi” come illecito penalmente rilevante in ciascun Paese membro era già all'epoca richiesta dalla Convenzione di Strasburgo del Consiglio d'Europa e dalle limitazioni alla possibilità di apporre riserve in sede di ratifica in relazione a tali reati, introdotte con l'Azione Comune n.98/699/GAI, poi sostituita dalla Decisione Quadro 2001/500/GAI.

⁷⁶ Sottoscritto il 13 dicembre 2007, ratificato dall'Italia con Legge n. 130 del 2008.

Le condotte restano coerenti con il consolidato modello internazionale (art. 3, comma 1). In linea con le richiamate Convenzioni e con le Raccomandazioni del GAFI, l'elemento soggettivo viene esteso a profili di "negligenza" (art. 3, comma 2). Viene stabilita la rilevanza di reati presupposto commessi all'estero e l'autonomia del riciclaggio rispetto alle sorti processuali dei reati presupposto (art. 3, comma 3). Questi ultimi vengono individuati dall'art. 2 in termini ampi, da un lato richiamando qualsiasi reato punibile entro determinati limiti edittali massimi o minimi e, d'altro lato, elencando ventidue fattispecie specifiche considerate "gravi" da includere in ogni caso nel perimetro.

L'intervento di armonizzazione è stato esteso anche ai reati di terrorismo.

La richiamata direttiva (UE) 2017/541 delinea un quadro organico di fattispecie di "terrorismo" riprendendo le ipotesi previste dalla Decisione Quadro 2002/475/GAI e introducendo quattro nuove *figurae criminis* (art. 11); una di queste riguarda il finanziamento del terrorismo. Le condotte da criminalizzare consistono nella fornitura o raccolta di capitali eseguite in qualsiasi modo, direttamente o indirettamente, "con l'intenzione che tali capitali siano utilizzati, o nella consapevolezza che saranno utilizzati", per commettere o per contribuire alla commissione di reati di terrorismo. La direttiva prevede inoltre che, in ipotesi determinate, non è necessario che i capitali siano effettivamente utilizzati per la commissione del reato, né occorre che l'autore sia a conoscenza dello specifico reato-obiettivo. Si tratta, dunque, di disposizioni che anticipano la soglia di punibilità: la possibilità di punire le condotte di finanziamento prescinde infatti sia dall'effettiva commissione di un reato di terrorismo sia dal collegamento con uno specifico atto di terrorismo.

2.2. La prevenzione e il contrasto sul piano finanziario.

Un secondo gruppo di regole internazionali ed europee affronta il riciclaggio quale fenomeno economico, introducendo misure per la prevenzione e il contrasto sul piano finanziario. Tali regole sottendono due motivi di fondo: da un lato, la tutela del sistema finanziario legale e degli intermediari che vi operano rispetto alle distorsioni e ai rischi derivanti dall'impiego di disponibilità illecite; d'altro lato, la prevenzione e il contrasto del riciclaggio attraverso misure fondate sulla identificazione e sulla conoscenza della clientela, sulla conservazione della "traccia" delle operazioni compiute, sulla "collaborazione attiva" espressa nella rilevazione e segnalazione di operazioni di natura sospetta.

Tale distinzione, tuttavia, ha valore per lo più convenzionale e, dunque, non deve essere sopravvalutata: le stesse misure e istituti sono assai spesso efficaci sia per la protezione degli intermediari e dei mercati dai rischi di inquinamento criminale sia per l'individuazione di fenomeni di riciclaggio e di criminalità economica sul piano finanziario.

L'ambito di intervento delle Nazioni Unite, come si è visto, si concentra soprattutto sulla materia penale con l'elaborazione di fattispecie di "riciclaggio" e "finanziamento del terrorismo" universalmente accettate quali modelli di incriminazione. Nondimeno, la Convenzione di Palermo del 2000 richiama i presidi per la prevenzione del riciclaggio quali si andavano delineando negli standard internazionali in fase di sviluppo in quegli anni, formulando alcune importanti precisazioni.

L'art. 7 della Convenzione ribadisce alcuni dei principali istituti regolati nelle Raccomandazioni del GAFI, prevedendo che gli Stati debbano: a) introdurre obblighi e misure per la prevenzione e la rilevazione del riciclaggio nel sistema bancario e finanziario nonché in settori non finanziari particolarmente esposti; b) assicurare che le Autorità competenti nella lotta al riciclaggio siano in grado di cooperare e scambiare informazioni, a livello nazionale e internazionale. Inoltre, vengono previste misure volte al monitoraggio del trasferimento transfrontaliero al seguito di "denaro contante", senza ostacolare la circolazione di capitali.

Nella Raccomandazione del Comitato dei Ministri del Consiglio d'Europa R 80/10 del 27 giugno 1980 si è soliti individuare il primo strumento internazionale dedicato alla prevenzione del riciclaggio sul piano finanziario. Pur senza produrre effetti vincolanti per gli Stati, la Raccomandazione enuncia alcuni dei principi che costituiranno la base del sistema antiriciclaggio preventivo.

Al centro viene posto il ruolo del sistema finanziario, bancario in particolare. La Raccomandazione indica la necessità che le banche verifichino l'identità della clientela; che siano introdotte forme di collaborazione tra le banche e le Autorità competenti agli accertamenti sulle operazioni attinenti a disponibilità di provenienza criminosa; che siano previste, per le banche, misure complementari consistenti, ad esempio, nella formazione del personale per riconoscere ed evitare le operazioni illecite e nella definizione di forme di controllo interno.

La Convenzione di Varsavia del 2005 si rivolge anche alle materie preventive. L'art. 13 ("*Measures to prevent money laundering*") enuncia anzitutto la necessità, per gli Stati, di introdurre una disciplina organica di obblighi e di controlli in conformità con le Raccomandazioni del GAFI, alle quali viene fatto integrale rinvio (comma 1).

Vengono poi richiamati alcuni istituti o gruppi di disposizioni che è senz'altro necessario attuare negli ordinamenti nazionali: l'identificazione, la verifica dell'identità e gli obblighi di adeguata verifica della clientela; la segnalazione di operazioni sospette; la conservazione delle informazioni; l'organizzazione e il controllo interno; sistemi di controllo e supervisione da parte di Autorità competenti sulla *compliance*, calibrati in funzione dei rischi; monitoraggio del trasporto transfrontaliero al seguito di denaro contante e strumenti al portatore. Particolare enfasi è posta sull'istituzione della FIU, definita in linea con le indicazioni del GAFI e del Gruppo Egmont, sulle funzioni e i poteri di cui essa deve essere dotata nello svolgimento dei compiti domestici (art. 12) e nella collaborazione internazionale (art. 46). La Convenzione prevede che la FIU deve essere in grado di sospendere operazioni sospette, per consentire l'applicazione di misure di sequestro da parte dell'Autorità Giudiziaria ovvero su richiesta (per analoghe esigenze) di controparti estere⁷⁷.

Le Quaranta Raccomandazioni del GAFI definiscono un compendio particolarmente completo di standard⁷⁸ cui devono conformarsi i presidi nazionali. Gli standard preventivi sono fondati su un "approccio basato sul rischio" (*risk-based approach*)⁷⁹ che richiede agli Stati, alle Autorità competenti e ai soggetti obbligati di commisurare le regole, i controlli, la *compliance* all'intensità dei rischi da fronteggiare e di allocare le risorse in maniera ugualmente commisurata⁸⁰. Il profilo di rischio, complessivo e articolato per settori, fornisce il parametro per la configurazione delle regole e degli obblighi, nel contenuto e nell'intensità. Ovvie implicazioni sono la natura non "deterministica" delle regole *risk-based* e la discrezionalità, più o meno ampia, lasciata ai soggetti obbligati nell'individuazione delle misure e dei comportamenti da adottare in concreto.

La Raccomandazione 2 completa la cornice istituzionale per la valutazione nazionale dei rischi e la pianificazione degli interventi conseguenti, prevedendo la necessità di istituire meccanismi di coordinamento delle politiche antiriciclaggio e di cooperazione tra le Autorità domestiche competenti. La valutazione nazionale dei rischi, oltre a informare le regole e le politiche pubbliche, deve essere tenuta presente dagli intermediari e dagli altri soggetti obbligati per la predisposizione di "*risk-assessment*" aziendali, sulla base dei quali devono essere configurate le caratteristiche dell'organizzazione interna a presidio dei rischi individuati e devono essere calibrate le misure, entro i limiti stabiliti dalla normativa⁸¹.

La natura e l'intensità dell'esposizione a rischi di riciclaggio e finanziamento del terrorismo costituiscono anche i parametri di riferimento per le Autorità di supervisione nello svolgimento dei controlli sulla *compliance* da parte dei soggetti obbligati in un contesto di risorse date (cfr. Raccomandazioni 26 e 28).

Le Raccomandazioni dalla 9 alla 23 sono dedicate alle "misure rivolte ad intermediari finanziari e imprese non finanziarie per prevenire il riciclaggio e il finanziamento del terrorismo". L'ambito soggettivo di applicazione comprende "financial institutions" e "designated non financial businesses and professions"⁸².

Sullo sfondo vengono posti generali divieti di derogare agli obblighi antiriciclaggio in virtù di prerogative di "segreto bancario"⁸³ ovvero di consentire forme di anonimato in qualsiasi operazione o

⁷⁷ Art. 47. Queste disposizioni vanno oltre gli standard del GAFI e trovano riscontro nelle Direttive europee.

⁷⁸ Ne fanno parte integrante, con le Raccomandazioni, le relative "Note Interpretative" e l'annesso "Glossario".

⁷⁹ L'approccio basato sul rischio è stato introdotto in occasione della sostanziale riforma delle Raccomandazioni completata nel 2003; esso sostituisce il precedente approccio basato sulle regole, con estese conseguenze sulla configurazione dei presidi, sulla compliance, sui controlli. Cfr. P. Costanzo, *The risk-based approach to Anti-Money Laundering and Counter-Terrorist Financing in International and EU standards. What it is, what it entails*, in Edward Elgar, *Research Handbook on Money Laundering*, 2013, pp. 349 ss.

⁸⁰ A fondamento di tale approccio è posto il *risk assessment* nazionale, esercizio di valutazione da svolgersi su base periodica. Esso impiega metodologie e informazioni dettagliate per determinare le "minacce" di riciclaggio e finanziamento del terrorismo che interessano i vari settori esposti; le minacce vengono confrontate con le "vulnerabilità" del sistema di prevenzione e contrasto per giungere a una misurazione del "rischio" residuo, relativo quindi a minacce non (del tutto) presidiate.

⁸¹ Cfr., in particolare, le Raccomandazioni 1, 10 e 18.

⁸² Con le modifiche apportate nel 2018 sono stati inclusi tra i soggetti obbligati i prestatori di servizi in *virtual asset* (*Virtual Asset Service Providers – VASP*). La nuova Raccomandazione 15 estende ad essi l'insieme dei presidi preventivi, relativi in particolare alla valutazione dei rischi, all'adeguata verifica, alla conservazione dei dati, alla segnalazione di operazioni sospette⁸². La Raccomandazione prevede anche la necessità di sottoporre i VASP a regimi autorizzativi ("*licensing*" o "*registration*") per l'esercizio dell'attività e lo svolgimento dei relativi controlli. Le modifiche apportate alla Raccomandazione 16 estendono al trasferimento di *virtual asset* gli obblighi di trasparenza e tracciabilità consistenti nell'inclusione di informazioni sull'ordinante e sul beneficiario nei dati che devono accompagnare il trasferimento nei suoi molteplici passaggi (c.d. "*travel rule*").

⁸³ Tale previsione, che oggi costituisce una premessa scontata su cui poggia il sistema antiriciclaggio nei molteplici flussi informativi in cui si articola, costituisce una conquista faticosa, frutto di laboriosi negoziati sino ad anni recenti. Ancora oggi, le valutazioni di ordinamenti nazionali mostrano la persistenza di istituti o prassi volti a limitare l'accesso a informazioni relative a clienti di istituzioni finanziarie,

rapporto⁸⁴. Agli intermediari devono essere anzitutto riferiti obblighi di identificazione della clientela, in relazione all'apertura di "relazioni di affari" e all'effettuazione di transazioni significative, specie se queste sono riconducibili a fatti di riciclaggio ovvero se sussistono dubbi sui dati identificativi già forniti. È inoltre prevista la necessità di individuare l'identità dei soggetti in favore dei quali vengono effettivamente aperti i rapporti o compiute le operazioni ("titolari effettivi"), specie con riguardo alla interposizione di strutture societarie. Più in generale, l'identificazione è parte degli adempimenti di "due diligence" che, come previsto nella Raccomandazione 10, possono essere graduati in funzione del rischio⁸⁵. È inoltre previsto l'obbligo di conservare per almeno cinque anni la documentazione acquisita sull'identità e sull'attività dei clienti (Raccomandazione 11).

In tema di "trasparenza" e accessibilità a informazioni sulla titolarità effettiva, la Raccomandazione 24 prevede l'istituzione in ciascun Paese di meccanismi per la raccolta e la conservazione di informazioni sull'assetto societario e sulla titolarità effettiva degli enti e delle società.

Altre misure sono rivolte all'individuazione e alla segnalazione di operazioni riconducibili ad attività illecite. In un'ottica di "collaborazione attiva", i soggetti obbligati, "se sospettano o hanno ragionevoli motivi di sospettare che i fondi provengano da attività illecite o siano connessi al finanziamento del terrorismo", devono immediatamente effettuare una segnalazione alla FIU⁸⁶. La Raccomandazione 29 stabilisce la necessità che gli Stati costituiscano una FIU quale centro nazionale per la ricezione, l'analisi e la trasmissione delle segnalazioni di operazioni sospette e di altre informazioni concernenti possibili fatti di riciclaggio o di finanziamento del terrorismo.

L'obbligo di rilevare e segnalare le operazioni sospette è accompagnato da disposizioni volte a consentire e incoraggiare la collaborazione attiva eliminando ostacoli giuridici e materiali. Da un lato, i soggetti segnalanti (sia gli enti obbligati sia i dipendenti di questi), quando procedono in "buona fede" alle segnalazioni, devono essere esentati da qualsiasi forma di responsabilità sul piano civile (ad esempio, per la violazione di obblighi contrattuali nei confronti dei clienti segnalati), penale e amministrativo (Raccomandazione 21). D'altro lato, le Autorità nazionali competenti devono fornire indicazioni per l'individuazione di comportamenti sospetti e trasmettere informazioni di ritorno (*feedback*) sullo sviluppo delle segnalazioni (Raccomandazione 34).

Ulteriori disposizioni sono rivolte a evitare l'inconsapevole coinvolgimento in attività illecite e ad assicurare l'efficace *compliance* attraverso adeguati presidi organizzativi⁸⁷. Agli obblighi per gli intermediari corrisponde la previsione di forme di regolamentazione e di supervisione per la verifica della conformità (Raccomandazione 26).

In particolare, è previsto che la supervisione sugli intermediari cui si riferiscono i "Core Principles"⁸⁸ debba svolgersi anche per le finalità di *compliance* antiriciclaggio e che gli altri intermediari debbano essere autorizzati e vigilati con riguardo ai rischi di riciclaggio nei rispettivi settori (viene fatto riferimento alle imprese attive nel *money transfer* e nel cambio-valuta). Adeguate forme di regolamentazione e controllo vengono prescritte anche per gli operatori non finanziari (Raccomandazione 28).

Le Autorità di supervisione devono essere dotate di poteri adeguati; le sanzioni per la violazione dei presidi devono essere effettive, proporzionate e dissuasive (Raccomandazioni 27 e 35).

imprese o professionisti, motivati da "garanzie" di riservatezza professionale ovvero di "*data protection*" e spesso ammantati di obiettivi di tutela di diritti "fondamentali" degli interessati.

⁸⁴ Cfr. la Raccomandazione 10, recante un divieto assoluto di intrattenere conti anonimi o intestati a nominativi fittizi.

⁸⁵ In considerazione del più elevato livello di rischio, adempimenti "rafforzati" di adeguata verifica devono essere svolti in relazione a Persone Politicamente Esposte ("PEP") e loro familiari, all'intrattenimento di rapporti di corrispondenza internazionali con altri intermediari e ad attività che comportano l'impiego di tecnologie operative di carattere innovativo o la commercializzazione di nuovi prodotti finanziari (Raccomandazioni 12, 13, 15). Specifiche disposizioni vengono dettate con riferimento alle giurisdizioni individuate periodicamente dal GAFI come ad alto rischio di riciclaggio (Raccomandazione 19). Presidi mirati sono previsti per contenere i rischi dell'operatività "a distanza" (*non face to face*) e per l'identificazione di soggetti introdotti da intermediari o altri terzi (assicurando pur sempre determinate cautele; Raccomandazione 17).

⁸⁶ Raccomandazione 20. L'inoltro della segnalazione è presidiato da vincoli di riservatezza e dal divieto di "tipping-off" (Raccomandazione 21).

⁸⁷ Ad esempio, la Raccomandazione 18 prevede la necessità di sviluppare "programmi contro il riciclaggio" che comprendano, in particolare, la definizione di misure di controllo interno e di formazione.

⁸⁸ Nel Glossario si chiarisce che il riferimento è ai *Core Principles for Effective Banking Supervision*, adottati dal Comitato di Basilea nel 1997, agli *Objectives and Principles for Securities Regulation*, adottati dalla IOSCO nel 1998, e agli *Insurance Supervisory Principles*, adottati dalla IAIS nel 1997.

2.3. Il sistema europeo

Le disposizioni antiriciclaggio dell'Unione europea, in dipendenza delle caratteristiche della fonte, esercitano effetti vincolanti per gli Stati membri o per i soggetti al loro interno. La composita e stratificata legislazione antiriciclaggio europea si articola infatti in molteplici strumenti: regolamenti, direttive e, in passato, decisioni quadro. Il corpo normativo principale è stato sviluppato attraverso direttive.

Le cinque Direttive “antiriciclaggio” adottate tra il 1991 e il 2018 sono improntate a un approccio di contenuta armonizzazione, sebbene gli interventi più recenti (con la terza e soprattutto con la quarta direttiva del 2015) siano caratterizzati da disposizioni dettagliate che lasciano meno spazio alla discrezionalità nazionale. Per conseguenza, sussistono ancora significative differenze tra le soluzioni nazionali, con discrepanze e carenze, che generano bassi livelli di efficacia e opportunità di elusione (per i criminali) e di arbitraggio (per i soggetti obbligati).

La disciplina europea della prevenzione antiriciclaggio si è sviluppata lungo alcune direttrici principali: il progressivo ampliamento del novero dei soggetti destinatari degli obblighi; l'arricchimento e l'estensione di tali obblighi (ad esempio, dalla semplice identificazione della clientela ad articolate misure di “due diligence”); la configurazione di Autorità competenti, in particolare la FIU, e la definizione di “statuti” sempre più dettagliati sull'organizzazione, i compiti, la collaborazione domestica e internazionale. Parametro essenziale nell'evoluzione delle regole europee sono state le Raccomandazioni del GAFI, a loro volta, come si è visto, ripetutamente riviste e aggiornate.

L'ambito soggettivo di applicazione includeva originariamente gli “enti creditizi”, ovvero banche⁸⁹, “enti finanziari”⁹⁰, imprese di assicurazione, imprese di investimento, organismi di investimento collettivo che commercializzano le proprie azioni o quote. L'art. 2-*bis*, inserito dalla direttiva 2001/97/CE, aggiunse categorie di soggetti esercenti attività non finanziarie (in particolare liberi professionisti e case da gioco) ai quali estendere i presidi in virtù dell'esposizione a rischi nei rispettivi settori. Per gli avvocati e gli altri professionisti “legali” l'applicazione degli obblighi è scriminata in base al tipo dell'attività svolta⁹¹. L'ambito di applicazione era completato dal riferimento alla necessità per gli Stati membri di estendere la disciplina nazionale, in tutto o in parte, a ulteriori imprese e professionisti esercenti “attività suscettibili di utilizzazione a fini di riciclaggio” (secondo la valutazione di ciascun Paese).

I soggetti sopra richiamati erano destinatari di obblighi di identificazione della clientela e di conservazione documentale, in relazione all'apertura di “rapporti di affari” e al compimento di operazioni di importo pari o superiore a una determinata soglia. Agli stessi soggetti doveva essere riferito l'obbligo di rilevare e segnalare ad apposite “Autorità responsabili per la lotta contro il riciclaggio” (poi definite “Financial Intelligence Unit” e progressivamente disciplinate) le operazioni sospette di riciclaggio. Altre disposizioni, alcune delle quali confermate e aggiornate dalle successive Direttive, erano dedicate alla sospensione delle operazioni segnalate, all'esonero da responsabilità nell'effettuazione “in buona fede” delle segnalazioni, al dovere per le Autorità competenti per i controlli di settore di informare la FIU circa operazioni sospette eventualmente rilevate, all'adozione da parte dei soggetti obbligati di adeguate misure di controllo interno e di formazione, alla costituzione di un “Comitato di Contatto” europeo, presieduto dalla Commissione e composto da rappresentanti degli Stati membri, con compiti volti a favorire l'applicazione uniforme della disciplina comune.

Con la terza direttiva del 2005 l'ambito soggettivo è stato esteso ai prestatori di servizi relativi a società o *trust* e ai soggetti che commerciano beni con pagamenti in contanti di importo superiore a 15.000 euro. La direttiva, soprattutto, ha introdotto in Europa l'approccio basato sul rischio nel frattempo regolato nelle Raccomandazioni del GAFI, con implicazioni soprattutto per la *compliance* e per i controlli. Il contenuto delle misure preventive viene, in conseguenza, profondamente innovato ed esteso. In particolare, il requisito dell'identificazione (consistente nell'acquisizione di informazioni sull'identità, secondo il principio “*Know Your Customer*”, con finalità semplicemente conoscitive) viene sostituito da un più ampio dovere di adeguata verifica (“*Customer Due Diligence*”, caratterizzato da elementi di valutazione e di giudizio), da esplicarsi in funzione del grado di rischio, in forma “semplificata”, “ordinaria” o “rafforzata”. La verifica si articola in molteplici misure (identificazione, verifica dell'identità, monitoraggio) da calibrare nel contenuto e nelle modalità sul caso concreto.

⁸⁹ Secondo la definizione della direttiva 2000/12/CE, comprendente anche gli istituti emittenti moneta elettronica.

⁹⁰ Intermediari che svolgono una o più delle attività indicate nei punti da 2 a 12 e 14 della direttiva 2000/12/CE.

⁹¹ Vengono escluse le attività connesse all'assistenza prestata ai clienti per l'esercizio del diritto alla difesa in giudizio; sono incluse attività di consulenza e assistenza in materia finanziaria, societaria, commerciale.

Diversamente dalla mera identificazione, “consumata” nel momento genetico del rapporto (fermo il successivo aggiornamento dei dati raccolti), l’adeguata verifica si configura come un adempimento “di durata”: le fasi iniziali di identificazione e verifica (rivolte al cliente e ad altri soggetti collegati, specie attraverso forme più meno dirette di “titolarità”, “legale” o “effettiva”) sono seguite, nello svolgimento del rapporto, da fasi permanenti di riscontro e valutazione sulle modifiche nell’assetto degli interessi⁹², sull’origine dei fondi e sugli scopi perseguiti nonché dal monitoraggio delle attività svolte, a fini di controllo, su coerenza, rischi e sconfinamento in comportamenti anomali. Senza soluzioni di continuità, attraverso il monitoraggio, l’adeguata verifica si congiunge alla rilevazione di anomalie e operazioni sospette da segnalare alla FIU.

La terza direttiva interviene anche su caratteristiche e compiti delle FIU, estendendone poteri e capacità di collaborazione. In sintonia con i coevi standard del GAFI e con la Convenzione di Varsavia del Consiglio d’Europa, la direttiva prevede l’istituzione di “Financial Intelligence Unit” compendiandone, nella dettagliata definizione⁹³, funzioni e poteri. In particolare, la FIU è l’Autorità centrale nazionale che riceve le segnalazioni di operazioni sospette, svolge analisi finanziaria, accede alle necessarie informazioni “finanziarie”, “amministrative” e “investigative”, collabora con controparti estere, “dissemina” i risultati alle competenti Autorità investigative o giudiziarie (artt. 21 e 22).

La quarta direttiva ha integralmente sostituito la precedente, consolidando e aggiornando l’intero corpo della regolamentazione antiriciclaggio preventiva europea. La quinta direttiva ha introdotto integrazioni al testo del 2015, aumentandone il grado di dettaglio e la portata armonizzante, ma senza stravolgerlo o sostituirlo.

La quarta direttiva allinea la disciplina europea alle Raccomandazioni del GAFI, nuovamente modificate nel 2012. L’approccio basato sul rischio viene confermato e ulteriormente articolato per meglio conciliare flessibilità e uniformità. La Commissione e gli Stati membri sono tenuti alla periodica valutazione dei rischi a cui sono esposti, rispettivamente, il Mercato Interno nel suo complesso e le singole giurisdizioni (art. 6 e 7). I soggetti obbligati, in coerenza con il Supranational e il National Risk Assessment, sono tenuti a valutare la propria esposizione ai rischi, tenendo conto tra l’altro delle attività svolte, dei servizi e dei prodotti offerti, delle classi di clientela, di fattori geografici. Per rendere possibile la *compliance* sistematica e puntuale rispetto alle specifiche misure, è prevista la necessità di politiche, controlli interni e procedure per mitigare e gestire efficacemente l’esposizione (art. 8). Nel caso di soggetti appartenenti a gruppi, la valutazione dei rischi e la configurazione delle politiche e procedure di presidio e mitigazione devono trovare attuazione a livello consolidato (artt. 45 e ss.). La direttiva conferma e precisa il novero dei soggetti destinatari degli obblighi antiriciclaggio, nel settore bancario-finanziario e nei comparti non finanziari, chiarendo e aggiornando i collegamenti con le rispettive discipline di settore (art. 2, par. 1)⁹⁴.

L’ambito soggettivo di applicazione è ulteriormente aggiornato e precisato dalla quinta direttiva. Questa fa riferimento a commercianti o intermediari nel commercio di opere d’arte nonché a gallerie d’arte e case d’asta, per operazioni di valore almeno pari a 10.000 euro, e a “porti franchi”, tenuti a obblighi di prevenzione e monitoraggio per operazioni di sdoganamento e custodia. La direttiva ha inoltre esteso la portata degli obblighi ai *VASP*, in relazione alla prestazione di servizi di cambio tra “valute virtuali” e valute aventi corso legale nonché a prestatori di servizi di “portafoglio digitale”.

Si tratta di un’importante novità che, come per l’analogo coevo aggiornamento degli standard del GAFI, scaturisce dalla consapevolezza che l’impiego di nuove tecnologie trasforma le attività finanziarie e talora, come nel caso dei “*crypto-asset*”, genera forme e specie inedite che, a loro volta, portano con sé nuovi rischi di utilizzo illecito. La prima risposta apprestata dal GAFI e dal legislatore europeo va nel senso di estendere alle nuove attività e figure di “intermediari” gli istituti e gli obblighi antiriciclaggio “tradizionali”, sia pure accompagnati da istruzioni e linee-guida per adattare i presidi ai nuovi operatori, alle loro attività e agli strumenti impiegati.

Le innovazioni tecnologiche determinano discontinuità nelle caratteristiche di attività finanziarie, di soggetti che le svolgono, di modalità di prestazione. La capacità dei presidi antiriciclaggio consolidati, configurati per soggetti e attività “tradizionali”, di esercitare un’efficace mitigazione e prevenzione nei nuovi comparti resta da verificare.

Due esempi possono essere richiamati per illustrare la questione. L’applicazione degli obblighi e il radicamento delle competenze delle Autorità sono determinati dal presupposto “territoriale” del luogo dello stabilimento fisico dei soggetti

⁹² Ad esempio, in relazione a cambiamenti in compagini societarie, rapporti partecipativi, titolarità legale o effettiva.

⁹³ Allineata alle indicazioni del GAFI e, come queste, aderente alla definizione di “FIU” coniata dal Gruppo Egmont.

⁹⁴ Accanto alle case da gioco, vengono inclusi i prestatori di servizi di gioco d’azzardo, prevedendo esenzioni in casi di basso rischio. Vengono resi più stringenti e dettagliati i requisiti per l’esonero dei soggetti che esercitano un’attività finanziaria in maniera occasionale o su scala molto limitata. Viene confermata la necessità di integrare il novero minimo di soggetti obbligati aggiungendo categorie esposte a rischi rilevanti a livello nazionale.

obbligati. Nel caso, in particolare, degli operatori in “crypto-asset” le caratteristiche immateriali dell’organizzazione, degli strumenti per offrire i servizi, dei canali di distribuzione comportano una naturale “delocalizzazione”: a fronte di infrastrutture fisiche snelle e organizzazioni aziendali semplificate, le attività vengono svolte, per loro stessa natura, in mercati virtualmente globali, senza alcuna limitazione derivante da confini territoriali.

Le caratteristiche elettroniche e il “luogo” nel quale le nuove attività vengono svolte (la rete Internet e il cyberspazio) pongono anche in evidenza limiti degli strumenti informativi e di analisi a disposizione delle Autorità. Queste dovrebbero essere in grado di seguire e tracciare attività svolte con mezzi tecnologici innovativi, senza limitarsi ad attendere, al termine delle fasi di produzione e trasformazione, che i proventi illeciti, ormai difficili da ricondurre alla loro origine, siano immessi nel circuito finanziario tradizionale (ad esempio, con la conversione di “crypto-asset” in valuta “fiat”).

La quarta e la quinta direttiva confermano l’impianto dei presidi preventivi, apportando limitati aggiornamenti. Viene ribadito il divieto di conti, libretti di risparmio o cassette di sicurezza anonimi. Le misure di adeguata verifica basate sul rischio vengono confermate e precisate; occorre identificare e verificare l’identità del cliente e del “titolare effettivo” e svolgere un controllo costante sul rapporto e sulle operazioni effettuate, valutandone la coerenza con le caratteristiche del cliente, delle sue attività e del suo profilo di rischio, tenendo conto dell’origine dei fondi⁹⁵.

La quarta direttiva introduce disposizioni sulla trasparenza della titolarità effettiva di società e trust. È prevista l’istituzione, in ciascun Paese membro, di registri pubblici centrali con informazioni sui titolari effettivi da rendere accessibili alle Autorità competenti, tra cui le FIU, nonché ai soggetti obbligati per l’adempimento dei doveri di adeguata verifica (artt. 30 e 31).

Ampio spazio è dedicato ai presidi in materia di operazioni sospette, con riguardo ai doveri di rilevazione e segnalazione e al ruolo delle FIU nelle analisi e nella collaborazione. Viene estesa la capacità delle FIU di acquisire informazioni da archivi esterni, da altre Autorità, dai soggetti obbligati. Sul versante della collaborazione internazionale viene previsto che le FIU debbano acquisire e fornire le informazioni richieste da controparti estere, esercitando i medesimi poteri disponibili per l’analisi domestica. I casi di rifiuto della collaborazione e di diniego del consenso per l’utilizzo e l’ulteriore comunicazione delle informazioni scambiate vengono confinati in ipotesi del tutto residuali. Per mitigare le rigidità del criterio “territoriale”, per le segnalazioni di operazioni sospette, inviate alla FIU del Paese dove è stabilito il segnalante ancorché l’operazione sia posta in essere in un Paese diverso (in libera prestazione di servizi), la quarta direttiva ha introdotto forme di scambio “automatico” di segnalazioni “cross-border” a beneficio delle Unità degli Stati in cui ha luogo l’operatività sospetta (art. 53).

La quarta direttiva, inoltre, “istituzionalizza” la Piattaforma delle FIU dell’Unione, attiva sin dal 2006, definendone un articolato mandato per l’impulso e il coordinamento delle attività e della collaborazione delle FIU (art. 51). La quinta direttiva, tenendo conto delle riflessioni sulla revisione del sistema antiriciclaggio europeo indotte dai risultati del “Mapping Exercise and Gap Analysis on FIUs’ Powers and Obstacles for Obtaining and Exchanging Information” della Piattaforma (2016) e dai gravi episodi di riciclaggio nel settore bancario europeo, incarica la Commissione di svolgere una valutazione sull’efficacia della cooperazione tra le FIU dell’Unione e sulla necessità di istituire un “meccanismo di coordinamento e supporto” sovranazionale (art. 65). Tali spunti, come si vedrà tra breve, trovano sviluppo nelle proposte legislative presentate dalla Commissione con l’AML Package.

Il corpo principale del sistema delle regole europee antiriciclaggio, formato dalle richiamate Direttive, è completato da provvedimenti dedicati a materie specifiche. Va menzionato il regolamento (UE) 2015/847, “riguardante i dati informativi che accompagnano i trasferimenti di fondi”, inviati o ricevuti da banche o altri intermediari che prestano servizi di pagamento.

Esso sostituisce il precedente regolamento del 2005⁹⁶ e aggiorna le disposizioni sulla necessità di includere nei messaggi che accompagnano i trasferimenti (bonifici o rimesse non bancarie) informazioni complete sull’ordinante e sul beneficiario, in modo da consentire una piena tracciabilità del denaro nei suoi movimenti. I dati identificativi devono accompagnare i fondi lungo l’intera catena dei trasferimenti, anche nei casi di intervento di intermediari con compiti di “corrispondenza” tra quello

⁹⁵ Vengono confermati anche gli obblighi di aggiornamento documentale (art. 14) e di conservazione dei dati acquisiti attraverso l’adeguata verifica (art. 40).

⁹⁶ Regolamento (CE) n. 1781/2005.

di partenza e quello di destinazione. Deve essere assicurata l'eventuale applicazione di misure di "congelamento", connesse a sanzioni finanziarie internazionali, e di rilevazione e segnalazione di operazioni sospette.

Il regolamento (UE) 2018/1672⁹⁷ prevede misure volte al monitoraggio del trasporto fisico transfrontaliero di "denaro contante", in entrata e in uscita dal territorio dell'Unione, nonché alla condivisione e all'utilizzo delle relative informazioni.

L'obbligo di dichiarazione riguarda un ampio novero di mezzi di pagamento e di "valori"⁹⁸; essa va resa da chiunque effettui trasferimenti fisici di valore pari o superiore a 10.000 euro, nei confronti di Autorità nazionali competenti (di norma, gli organi doganali). Queste sono tenute a rendere disponibili alla FIU del rispettivo paese i dati delle dichiarazioni⁹⁹ nonché informazioni su casi di sospetto di riciclaggio o finanziamento del terrorismo ovvero ipotesi di violazione dell'obbligo di dichiarazione riscontrate nei controlli.

2.4. Le proposte legislative dell'AML Package

L'AML Package, pubblicato dalla Commissione il 20 luglio 2021, si compone di quattro proposte legislative per tre regolamenti e una sesta direttiva antiriciclaggio; esso costituisce l'esito di un lungo percorso di approfondimenti e analisi, svolti attraverso ampi confronti e consultazioni.

Gli spunti iniziali per una revisione del sistema antiriciclaggio europeo e l'istituzione di forme di raccordo e accentramento sovranazionale sono maturati nel comparto delle FIU, per rafforzarne l'azione e la collaborazione. Un forte impulso è stato poi impresso dalle crisi di banche europee succedutesi in serie numerosa nel periodo 2012-2018, determinate dal coinvolgimento in fenomeni di riciclaggio di vasta portata e dalle gravi carenze emerse nella *compliance* e nei sistemi di controllo¹⁰⁰. La consapevolezza della fragilità del sistema complessivo porta a estendere il fronte di attenzione per una organica riforma. La Commissione pubblica a luglio 2019 quattro Rapporti (sulla supervisione antiriciclaggio, sull'attività delle FIU, sulla interconnessione di registri bancari, sui rischi sovranazionali) e nel maggio 2020 un Piano d'Azione "*For a comprehensive Union policy on preventing money laundering and terrorist financing*", delineando le ampie linee di intervento concretizzatesi nelle proposte legislative dell'AML Package.

Il quadro regolamentare e istituzionale delineato, per molti aspetti in continuità con l'attuale, introduce cambiamenti significativi in materie già regolate e aspetti di sostanziale novità. È mantenuta l'impostazione "risk-based" della *compliance* e dei controlli, ma viene accentuata la convergenza attraverso regolamenti con disposizioni più dettagliate e di diretta applicazione per un *rulebook* europeo antiriciclaggio, da completare con regole secondarie di dettaglio. Viene inoltre introdotto un livello sovranazionale di funzioni, ulteriore rispetto alle attività domestiche e di collaborazione internazionale; è istituita una *Anti-Money Laundering Authority* europea con compiti di convergenza di regole e metodi, di coordinamento e supporto delle Autorità nazionali, di intervento diretto.

L'Autorità, con caratteristiche peculiari nel panorama delle agenzie dell'Unione, eserciterà due ruoli distinti: quello di supervisore antiriciclaggio, accentrando le competenze di coordinamento sinora attribuite alle ESAs e all'EBA in particolare nonché responsabilità di supervisione diretta sinora prerogativa delle Autorità nazionali; quello di "Meccanismo di supporto e coordinamento" per le FIU. Le funzioni di queste ultime resteranno radicate a livello nazionale, ma verranno svolte con modalità uniformi, coordinate e in alcuni casi congiunte per lo svolgimento di analisi.

Una proposta di regolamento raccoglie le disposizioni relative agli obblighi preventivi. Tali disposizioni riceveranno diretta applicazione ed eserciteranno un più intenso effetto armonizzante, formando il nucleo del *rulebook* antiriciclaggio.

⁹⁷ Tale regolamento ha abrogato il precedente regolamento (CE) 1889/2005.

⁹⁸ Sussunti nella dettagliata definizione di "contante" di cui all'art. 1 del regolamento 2018/1672.

⁹⁹ Le autorità nazionali conferiscono i dati raccolti al *Customs Information System*, tenuto dall'Ufficio europeo antifrode (OLAF). Le FIU hanno accesso a tale sistema centralizzato per consultare e utilizzare le relative informazioni.

¹⁰⁰ Il sistema bancario e finanziario europeo, in particolare nelle regioni baltiche e scandinave, ma anche nel Regno Unito (all'epoca membro dell'Unione) e a Malta, è stato investito da fondi illeciti di provenienza russa. I presidi antiriciclaggio si sono dimostrati inadeguati anche a causa della scarsità di risorse disponibili, dell'assenza di metodi adeguati di presidio e della mancanza di meccanismi efficienti di collaborazione, domestica e internazionale. Cfr. Rapporto della Commissione europea *On the assessment of recent alleged money laundering cases involving EU credit institutions*, 24 luglio 2019.

L'ambito di applicazione viene chiarito ed esteso a ulteriori categorie di soggetti, anche tenendo conto dell'evoluzione tecnologica e delle forme operative. Nel comparto finanziario, il *rulebook* antiriciclaggio viene applicato alle diverse figure di *crypto-asset service provider* (in raccordo con la Proposta di regolamento "MiCA") e alle imprese che svolgono attività di *crowdfunding* (a loro volta oggetto di regolamentazione in sede europea). L'ambito dei soggetti obbligati viene aggiornato anche nel comparto non finanziario, estendendolo in particolare a mediatori nell'erogazione di crediti, commercianti di beni di elevato valore e professionisti nelle procedure di *Visa for investment*.

L'obiettivo prioritario dell'armonizzazione perseguito con l'AML Package non incoraggia pratiche di "gold plating" nazionale, basate su liste locali più ampie di soggetti obbligati. Tali variazioni non sono precluse; tuttavia, gli Stati membri che intendono inserire o mantenere ulteriori figure soggettive devono inviare un'apposita "notifica" alla Commissione europea, la quale attiva una complessa procedura di valutazione sulla possibile rilevanza sovranazionale dell'iniziativa.

Il sistema che ne risulta, basato su una lista minima armonizzata di soggetti obbligati e su possibili integrazioni nazionali attraverso una procedura di notifica e valutazione da parte della Commissione, potrebbe indurre effetti di livellamento al ribasso in paesi che, come l'Italia, sono caratterizzati da un novero ampio di soggetti obbligati. Potrebbe rivelarsi meno agevole rispondere con la necessaria flessibilità a rischi di riciclaggio o finanziamento del terrorismo che si manifestino in comparti specifici a livello nazionale, come richiesto dagli standard "risk-based" del GAFI. Pur con i benefici della maggiore armonizzazione, la lista minima europea di soggetti obbligati non appare sufficientemente estesa. In essa non figurano categorie di soggetti che manifestano rischi significativi o possono contribuire al sistema della prevenzione. Va fatto riferimento, ad esempio, a imprese che gestiscono circuiti elettronici di pagamento, a soggetti che operano in assenza di stabilimento (online), a categorie di pubbliche amministrazioni.

La disciplina sugli obblighi di adeguata verifica riguarda i presupposti, il contenuto, l'intensità dei presidi. Per evitare, o ridurre al minimo, le discrepanze, regole di dettaglio vengono rivolte a ciascun adempimento (dalla identificazione iniziale al monitoraggio dei rapporti) e alla declinazione di questi, in base al rischio, nelle modalità ordinaria, semplificata e rafforzata.

Il *rulebook* comprende anche disposizioni sulla raccolta e sulla conservazione di dati relativi a clienti, operazioni e rapporti nonché regole sulla rilevazione e segnalazione alla FIU di operazioni sospette. Queste ultime poggiano su una migliore precisazione dei presupposti e dei fattori di valutazione del "sospetto". Il *rulebook* al riguardo verrà integrato da previsioni applicative dell'AMLA, con ampio margine per istruzioni mirate da parte delle Autorità nazionali.

I soggetti obbligati devono dotarsi di assetti organizzativi, politiche e procedure interne per assicurare l'efficace *compliance*, in maniera commisurata ai rischi. Le nuove regole definiscono in dettaglio i presidi sulle strutture e sullo staff, le funzioni di *compliance*, le modalità per la valutazione dei rischi ai quali i presidi devono essere commisurati. La disciplina si rivolge partitamente a singole imprese e a gruppi e, tra questi, ai conglomerati con articolazioni estere, nell'Unione o in Stati terzi.

Il regolamento compendia, ed espande, la delicata materia dell'individuazione di Paesi terzi "ad alto rischio", precisando modalità di valutazione delle "deficienze strategiche" e della compilazione della relativa "lista nera" da parte della Commissione europea. Vengono prospettati limiti all'utilizzo di denaro contante e di strumenti al portatore, già presenti in numerosi Paesi membri, ma tuttora privi di una base legale europea che li renda obbligatori e sufficientemente uniformi.

La proposta di sesta direttiva antiriciclaggio si rivolge a materie per le quali non è possibile o desiderabile un intervento di massima armonizzazione, che comprimerebbe margini necessari di flessibilità nazionale. Nella direttiva sono anzitutto compendiate le disposizioni che informano l'approccio basato sul rischio, architrave del complessivo sistema. La disciplina si pone in continuità con quella vigente, aggiungendo dettagli e precisazioni.

La Commissione ha il compito di elaborare un *Supra-National Risk Assessment* per la stima di rischi, di origine interna o esterna, che posseggono natura transnazionale, non sono facilmente rilevabili da singoli Stati membri e investono parti significative del Mercato Interno. Il rapporto va predisposto con l'apporto dell'AMLA (che adotta un apposito "parere sui rischi osservati"), di esperti degli Stati membri, delle Autorità di vigilanza e delle FIU e va aggiornato con cadenza biennale. La Commissione formula "raccomandazioni" agli Stati membri sulle misure da adottare a fronte dei rischi di matrice sovranazionale. Gli Stati possono discostarsi, ma devono indicare le ragioni secondo un meccanismo "*comply or explain*". Gli

Stati membri devono a loro volta svolgere valutazioni accurate dei rischi di rilievo nazionale, istituendo appositi meccanismi di coordinamento in grado di raccogliere informazioni e analisi da un ampio spettro di Autorità, su una vasta gamma di fattori di minaccia e di vulnerabilità. I risultati devono essere condivisi e mutualizzati con la Commissione, con l'AMLA e con gli altri Stati membri. Il *Supra-national risk assessment* e la valutazione nazionale devono essere resi disponibili ai soggetti obbligati, che ne tengono conto ciascuno per la valutazione dei rischi cui è esposto in relazione al comparto, alle caratteristiche di attività e prodotti, alla fisionomia della clientela. I doveri di ricognizione si estendono, per i Paesi membri, alla raccolta di statistiche per monitorare l'efficacia dei molteplici comparti del sistema. La direttiva contiene un dettagliato elenco di categorie di dati e informazioni da raccogliere e valutare; esse vanno trasmesse alla Commissione e, in parte, all'AMLA che, tra l'altro, ne curano la pubblicazione.

La disciplina dei registri dei titolari effettivi di società, enti, trust e istituti affini viene ampliata e specificata nella direttiva, tenendo conto dell'esperienza maturata dopo la quarta direttiva del 2015.

Gli interventi riguardano la definizione di "titolare effettivo" (rilevante anche ai fini dell'adeguata verifica), l'individuazione delle informazioni da acquisire e conservare, il regime per l'accesso ai dati, la previsione di meccanismi di riscontro e correzione delle informazioni, in presenza di discrepanze, ad esempio, rispetto a quelle disponibili alle Autorità o acquisite dai soggetti obbligati sulla propria clientela. Vengono attribuiti a una figura nazionale di "organismo responsabile dei registri centrali" compiti di gestione dei registri e delle procedure di accesso e di controllo dei dati, con poteri di acquisire riscontri dalle stesse società, enti o trust, anche mediante ispezioni, sulla rispettiva titolarità effettiva. L'Organismo è tenuto a segnalare alla FIU ipotesi di sospetto di riciclaggio o finanziamento del terrorismo emerse nei controlli. La proposta di direttiva, inoltre, raccoglie e aggiorna le disposizioni sull'istituzione e sulla tenuta di altri "registri" centrali nazionali con informazioni utili per le attività della FIU e delle altre Autorità competenti: essi riguardano conti bancari e proprietà immobiliari. I registri nazionali dei titolari effettivi e dei conti bancari dovranno, rispettivamente, essere interconnessi, consentendo in qualsiasi Paese membro di ottenere informazioni ovunque presenti nell'intera Unione.

La proposta di direttiva compendia anche le regole sulle FIU e sulle Autorità nazionali di supervisione antiriciclaggio, con riguardo alla dimensione domestica e alla collaborazione, nazionale e internazionale. La sesta direttiva costituirà la fonte normativa "fondante" per le FIU: ne prevede l'istituzione quali Autorità specializzate e tipizzate, con propria distinta soggettività; ne indica le caratteristiche e i compiti; ne determina i poteri e le capacità di collaborazione. Le disposizioni, in coerenza con lo strumento della direttiva, non si spingono in generale a un punto di armonizzazione elevato, pur collocandosi su un livello di dettaglio maggiore delle precedenti. L'intento è quello di consentire ai Paesi membri di calare i requisiti indicati in strutture istituzionali che riflettano e si adattino alla fisionomia del sistema nazionale, individuando il "modello" localmente più efficace e in grado di assicurare connessioni fluide con i diversi interlocutori, privati e pubblici.

A fronte di indubbi vantaggi, la flessibilità nazionale nella configurazione delle FIU comporta controindicazioni ormai ben note¹⁰¹. Essa determina significative differenze che, a loro volta, si traducono in variazioni nel grado di efficacia da un Paese all'altro, disallineamenti in prassi, metodi e informazioni, con conseguenti inefficienze nella collaborazione reciproca. È proprio a tali inconvenienti, tra l'altro, che l'AMLA è chiamata a porre rimedio nel suo ruolo di Meccanismo per le FIU.

Nonostante l'approccio "a maglie larghe", le disposizioni sulle FIU vengono notevolmente arricchite. Viene confermato il principio di neutralità circa la natura istituzionale e lo status organizzativo, con la relativa flessibilità nelle caratteristiche e nella collocazione della FIU nell'apparato pubblico. La direttiva precisa tuttavia le condizioni che devono essere in ogni caso rispettate, in linea con la quinta direttiva, ma con un più elevato grado di dettaglio e un maggior effetto di convergenza.

Indipendenza. Lo "statuto" di autonomia e indipendenza della FIU è declinato sui versanti complementari dell'operatività e dell'organizzazione. Sul primo, la FIU "ha l'autorità e la capacità di svolgere liberamente le sue funzioni". Per lo svolgimento efficace e neutrale dei compiti connessi alla rilevazione di casi di riciclaggio, reati presupposto e finanziamento del terrorismo (sovente correlati alla sfera pubblica e intrecciati con il potere politico, come altrettanto di frequente a negligenza o *mala gestio* di imprese e alle dinamiche di interessi del settore privato), la FIU deve essere sottratta a qualsiasi forma di "cattura", sia da parte pubblica sia da parte privata: essa deve essere "esente da indebite influenze o ingerenze politiche, governative o del settore privato". Sul versante organizzativo, l'indipendenza deve essere assicurata a prescindere dall'assetto istituzionale definito a livello nazionale; anche "quando la FIU

¹⁰¹ La rilevanza delle caratteristiche istituzionali e organizzative delle FIU per l'efficacia dei compiti di analisi e collaborazione, e i limiti del principio di "neutralità" dello status, accolto nelle regole europee, sono illustrati nel più volte richiamato "Mapping Exercise" della Piattaforma delle FIU.

è situata all'interno della struttura esistente di un'altra Autorità, le funzioni fondamentali della FIU sono indipendenti e operativamente separate dalle altre funzioni dell'Autorità ospitante”.

Risorse. Le recenti esperienze di “fallimenti” dei controlli e dei presidi antiriciclaggio, cui il Package intende rispondere, mostra che la debolezza dell'azione è spesso causata dalla scarsità delle risorse disponibili alle Autorità, in termini di mezzi finanziari e di personale. Per le FIU, si tratta ancora una volta di una conseguenza della flessibilità e della “neutralità” delle regole europee sulle scelte organizzative, cui conseguono politiche nazionali di risparmio di corto respiro. La proposta di direttiva insiste sulla necessità di dotare le FIU di “risorse finanziarie, umane e tecniche adeguate” e renderle “in grado di ottenere e impiegare le risorse necessarie per svolgere le loro funzioni”. L'adeguatezza deve essere anche qualitativa, non solo numerica: “Il loro personale è di alta integrità e opportunamente qualificato e mantiene standard professionali elevati”.

Funzioni. Vengono ribaditi, nella definizione di “FIU”, i tratti qualificanti della ricezione di informazioni, dell'analisi e della disseminazione, con importanti elementi aggiuntivi. Le FIU ricevono segnalazioni di possibili casi di riciclaggio, oltre che dai soggetti obbligati, da altre Autorità nazionali quali i supervisor (art. 48), dalle agenzie doganali (artt. 17 e 18), dagli organismi responsabili dei registri dei titolari effettivi (art. 10, comma 10). Viene ribadita la bipartizione tra analisi “operativa” e “strategica”, entrambe essenziali. La proposta di direttiva mantiene anche la descrizione delle due attività, presente nella direttiva in vigore e allineata alle indicazioni del GAFL. Si tratta, tuttavia, di riferimenti generici a fronte dei quali sussistono ampie differenze nelle pratiche nazionali di “analisi”, con connesse incertezze sulla natura della funzione, i metodi, le informazioni, gli obiettivi. Carenze su questo aspetto nevralgico emergono nei livelli di efficacia nazionale e nella collaborazione internazionale (ad esempio per le analisi congiunte). La direttiva, anche su questo punto indirizzata dai risultati del “Mapping Exercise”, affida all'AMLA il compito di favorire chiarezza e convergenza.

Poteri. L'adeguata capacità della FIU di acquisire informazioni costituisce un presupposto essenziale per l'efficace svolgimento delle analisi. Nella direttiva vigente viene richiamato un generico requisito di “multidisciplinarietà” secondo cui, qualunque sia la natura della FIU, questa deve in ogni caso disporre di informazioni “finanziarie”, “amministrative” e “investigative”. Tali generi di dati non sono tuttavia descritti né sono individuate le “specie” di informazioni cui in concreto le FIU devono avere accesso in relazione a ciascuno di essi. Come posto in evidenza dal “Mapping Exercise”, la disponibilità di informazioni varia da Paese a Paese, è influenzata dalle caratteristiche istituzionali della FIU, rivela carenze nello spettro di dati (specie con riguardo a quelli “finanziari” e “investigativi”, anche per la persistenza di vincoli di segretezza). La direttiva introduce dettagliate previsioni sui poteri informativi delle FIU, riducendo al minimo il margine di recepimento nazionale¹⁰². Essa ribadisce inoltre la capacità della FIU di ottenere informazioni da qualsiasi soggetto obbligato, a prescindere dall'effettuazione di segnalazioni di operazioni sospette. Anche il potere di sospensione viene precisato e ampliato: esso riguarda non più solo operazioni, ma anche conti e altri rapporti; questi possono essere temporaneamente bloccati o “congelati” a prescindere dal riferimento a particolari transazioni.

Collaborazione. La proposta di direttiva conferma e amplia il sistema della collaborazione tra le FIU e tra queste e altre “Autorità competenti”. Per rendere più efficaci e uniformi i flussi informativi tenendo conto delle criticità emerse nella prassi, all'AMLA viene affidato il compito di precisare formati e contenuti nonché criteri per l'individuazione delle segnalazioni cross-border che le FIU devono scambiarsi. Viene rafforzata la base legale che riconosce FIU.net quale infrastruttura dedicata alla collaborazione tra FIU, allocata presso l'AMLA che ne assicura lo sviluppo. L'utilizzo e la disseminazione delle informazioni scambiate restano subordinate al consenso delle FIU interessate; questo non può essere rifiutato se non in casi eccezionali, sui quali sono auspicabili indicazioni di dettaglio da parte dell'AMLA per favorire linee di condotta omogenee. Viene anche delineato nella direttiva un complesso

¹⁰² Nell'art. 18 vengono partitamente individuate le tipologie di fonti cui le FIU devono, come minimo, avere accesso: quelle finanziarie sono sei; ben diciannove quelle amministrative; i dati investigativi vengono a loro volta individuati in maniera ampia, includendovi “qualsiasi tipo di informazioni o dati disponibili o acquisibili senza l'adozione di misure coercitive, relativi a indagini in corso e concluse e ai provvedimenti adottati”. Le FIU devono avere di regola accesso diretto e immediato a queste fonti; nei casi di accesso indiretto, il soggetto in possesso dei dati è tenuto a fornire riscontro tempestivo.

sistema di collaborazione e scambio reciproco di informazioni tra “Autorità competenti”, ivi incluse le FIU e gli organi di supervisione (artt. 45 ss.).

3. Il riciclaggio nella prospettiva penale ed in quella amministrativa (F. Di Vizio)

La prospettiva definitoria ha avuto un ruolo centrale nell'evoluzione dell'incriminazione del riciclaggio, segnata dall'ampliamento dell'interesse rispetto ai distinti contenuti del fenomeno finanziario e dall'irrobustimento della consapevolezza dei suoi deleteri effetti macroeconomici¹⁰³. In tal senso, l'analisi economica si incentra prevalentemente verso gli effetti sostanziali del meccanismo di “trasformazione di un potere di acquisto potenziale in effettivo”¹⁰⁴ e sui riflessi rispetto alle condizioni di concorrenza imprenditoriale, nonché al corretto funzionamento dei mercati e dei meccanismi di allocazione delle risorse. Tale sensibilità non si è ancora completamente tradotta nella dimensione giuridica, concentrata sulla dissimulazione dell'origine dei beni di provenienza criminosa con abuso degli strumenti offerti all'agire economico e finanziario. Tradizionale è l'articolata suddivisione delle attività e delle fasi in cui il riciclaggio si svolge, identificabili nel collocamento (placement), nella stratificazione-movimentazione (layering) e nell'investimento (integration)¹⁰⁵.

La direttrice di sviluppo giuridico del contrasto del riciclaggio segnala l'espansione dell'attribuzione del carattere illecito a nuove condotte connotate dall'attitudine dissimulatoria dell'origine dei proventi; ma è come se la dilatazione della rilevanza illecita della dissimulazione stesse accrescendo la coscienza dei pregiudizievoli effetti economici scaturenti dall'utilizzazione dei proventi illeciti, scaturendo una più vasta criminalizzazione di diverse forme di impiego anche non decettive. Per tale ragione, il contrasto all'accumulazione di patrimoni illeciti si è strutturato attraverso diverse tipologie di modelli. Nell'ambito penale classico, gli strumenti sono connotati da matrice repressiva e qualificabili come sanzioni o misure di sicurezza accessorie a sentenze di condanna emesse in relazione a verificate responsabilità di persone fisiche per reati¹⁰⁶. In ambito amministrativo, infine, tra i sistemi preventivi più sviluppati vi è proprio l'apparato delineato dal D.lgs. 231/2007.

La regolamentazione penale del riciclaggio è contraddistinta da un progressivo potenziamento dell'autonomo disvalore giuridico dei diversi contenuti del riciclaggio quale fenomeno economico-finanziario¹⁰⁷. Abbandonata la primigenia prospettiva retrospettiva, volta a rafforzare la tutela dei beni giuridici presidiati dai reati-principali, riferendo al riciclaggio natura accessoria del reato matrice e focalizzando le ragioni della repressione sull'ostacolo frapposto alla punibilità del reato “scaturigine”, le condotte di riciclaggio in senso lato (descritte dagli artt. 648-bis, 648-ter, 648-ter.1, 512-bis c.p.) sono assunte a disvalori autonomi con progressiva criminalizzazione dell'impiego economico delle risorse illecite. Ne è scaturito un complesso di norme che, con il reato di ricettazione, integrano il sistema di contrasto ai fenomeni di circolazione, accumulo e consolidamento dei profitti illeciti¹⁰⁸.

¹⁰³ Per l'analisi del riciclaggio quale fenomeno economico-finanziario cfr. G. Castaldi, *La definizione di riciclaggio e di finanziamento del terrorismo: le Raccomandazioni GAFI*, in G. Castaldi e C. Conforti (a cura di), *Manuale Antiriciclaggio*, Roma, 2013, p. 77 e ss.

¹⁰⁴ In tema P. Vigna, *Il fenomeno criminale*, in E. Cappa e L.D. Cerqua (a cura di), *Il riciclaggio del denaro. Il fenomeno, il reato, le norme di contrasto*, Milano, 2012, p. 3, ss.; Masciandaro, *Banche e riciclaggio*, Milano, 1994.

¹⁰⁵ Nella prima fase i proventi illeciti vengono materialmente collocati presso terzi (ad esempio presso un intermediario finanziario, eventualmente anche all'estero). Segue la fase della movimentazione dei capitali, mediante un insieme di operazioni (trasferimenti, bonifici, prestiti, pagamenti, etc.) volte a *separare* il capitale dall'origine illecita, impedendo di riconoscerla. Infine, i capitali di origine criminale vengono integrati nei circuiti dell'economia lecita, attraverso l'*investimento* in beni immobili, beni di lusso, aziende ed altri valori. Per Castaldi, *op. cit.*, 77, la tripartizione corrisponde all'evoluzione dell'originaria impostazione bifasica, sulla quale era impiantata l'originaria legislazione penale nazionale, focalizzata sul “lavaggio” (*money laundering*) del denaro o di altri beni, e “l'impiego” (*recycling*).

¹⁰⁶ In termini complementari le *misure di prevenzione* hanno riguardo alla pericolosità sociale delle persone e dei beni, rivelata all'esito di una verifica indiziaria o probabilistica svolta nel contesto di un procedimento giudiziario, senza necessario collegamento con l'accertamento della responsabilità penale del soggetto passivo dell'ablazione. Cfr. Corte cost. n. 24/2017 per la ratio e lo statuto di garanzie costituzionali e convenzionali delle misure di prevenzione; in tema, cfr. Corte Edu, sentenza 23 febbraio 2017, de Tommaso contro Italia, § 143 e Cass. Sez. Un. Spinelli n. 4880/2015.

¹⁰⁷ Per l'evoluzione storico-comparata della definizione sotto l'impulso delle fonti internazionali e sovranazionali cfr. Di Vizio, *Il riciclaggio nella prospettiva penale ed in quella amministrativa. Definizioni di riciclaggio*, in Quaderni dell'antiriciclaggio. Analisi e studi n. 8, Roma, 2017.

¹⁰⁸ Per un'analisi cfr. Cass. Pen. Sez. 2, n. 24273/2021.

3.1. Il riciclaggio

In base all'art. 648-bis, comma 1, del codice penale “*Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000*”. Il successivo comma 2, inserito dall'art. 1, comma 1, lett. d), n. 2), D.lgs. 8 novembre 2021, n. 195, prevede che “*la pena è della reclusione da due a sei anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi*”. I commi 3 e 4 dell'art. 648-bis c.p., inoltre, descrivono forme circostanziate: “*La pena è aumentata quando il fatto è commesso nell'esercizio di un'attività professionale*” (art. 648-bis, comma 3, c.p.)¹⁰⁹; “*la pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni*” (art. 648-bis, comma 4, c.p.). Si applica l'ultimo comma dell'art. 648 c.p.¹¹⁰.

L'attuale configurazione normativa del reato si caratterizza per una significativa estensione della portata della fattispecie, essendo stati progressivamente ampliati i reati presupposti, la condotta, l'oggetto iniziale (“altre operazioni” “in relazione” – e non su – a denari, beni ed utilità di provenienza criminosa in modo da ostacolarne l'identificazione) e quello finale (potendo trattarsi, in tutte le condotte di denaro, beni, utilità ma anche di “cose” di diversa natura, pure sprovviste di valore economico, restando punibile anche la sostituzione “eterologa”)¹¹¹. Con l'art. 23 della legge 19 marzo 1990 n. 55, la fattispecie ha acquisito la denominazione “Riciclaggio” e visto ridimensionata l'esclusiva valutazione retrospettiva. L'evoluzione normativa ha registrato un punto di svolta con la L. 9 agosto 1993 n. 328, che ha esteso a tutti i delitti non colposi (dolosi e preterintenzionali) lo statuto di attività criminale matrice del riciclaggio in esame, in linea con le indicazioni della Convenzione di Strasburgo del 1990 e della prima direttiva europea antiriciclaggio del 1991; successivamente la necessità di adeguare la normativa italiana alla direttiva (UE) 2018/1673, per le porzioni già non conformi, ha condotto al varo del D.lgs. 8 novembre 2021, n. 195¹¹² che ha dilatato i reati presupposto dei reati del riciclaggio alle contravvenzioni (purché punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi), con nuove e autonome cornici edittali (cfr. art. 648-bis, comma 2), e ai beni provenienti da *qualsiasi delitto*, anche colposo (come già previsto per ricettazione e reimpiego). Segno che l'attenzione penale è rivolta sui *proventi*, più che sugli specifici reati matrice, sollevando parzialmente dalla necessità di definire contorni, punibilità e responsabilità soggettive rispetto a questi ultimi¹¹³. La condizione di provenienza del denaro, dei beni e

¹⁰⁹ Aggravante oggettiva, estendibile a tutti i concorrenti (Cass. Pen. Sez. 6, n.43534/2012, Rv. 253796 – 01).

¹¹⁰ Il delitto di configura anche quando l'autore del reato da cui il denaro o le cose provengono non è imputabile non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato.

¹¹¹ Tali dilatazioni hanno esercitato influenza sull'arricchimento del *bene giuridico* (interessi patrimoniali, amministrazione della giustizia, ordinato funzionamento e integrità del sistema economico complessivo).

¹¹² Per primi commenti cfr. Giunta, *L'Europa chiede un ulteriore giro di vite nel contrasto del riciclaggio*, in *disCrimen*, 30.9.2021; Bellagamba, *La riforma del riciclaggio è legge: un'occasione mancata per andare oltre il mero recepimento della direttiva europea*, in *Diritto penale e processo*, 4/2022, p. 445 e ss.

¹¹³ In linea con la mutata impostazione, la giurisprudenza consolidasi in relazione all'accertamento o alle vicende del reato presupposto. A titolo esemplificativo: l'accertamento del reato presupposto non deve essere contenuto in una sentenza irrevocabile, pronunciata in esito ad autonomo processo, bastando che la sussistenza risulti processualmente al giudice chiamato a decidere della ricettazione o del riciclaggio, emergendo una provenienza illecita delle utilità oggetto delle operazioni compiute, in base a prove logiche; è necessario che il reato presupposto risulti, alla stregua degli elementi di fatto acquisiti ed interpretati secondo logica, almeno astrattamente configurabile (v. Cass. Pen. Sez. 6, n. 28715/2013 Rv. 257206) e che il fatto costitutivo di tale reato non sia stato giudizialmente escluso, nella sua materialità, in modo definitivo e che il giudice procedente per il riciclaggio ne abbia incidentalmente ritenuto la sussistenza (Cass. Pen. Sez. 2, n. 7795/2014, Rv. 259007); l'esistenza del reato presupposto è evincibile non solo dalla mancata giustificazione del possesso di somme di denaro ma dalla mancata giustificazione di una serie di operazioni bancarie prive di ragionevole fine e senza effettivo incremento o utilizzazione del capitale economicamente apprezzabile, con operazioni prive di senso dal punto di vista della gestione patrimoniale, rafforzando l'elemento dell'assenza di lecite fonti di reddito (Cass. Pen. Sez. 2, n. 35763/2010); ovvero da operazioni particolarmente opache contrastanti con riferite giustificazioni economiche di movimentazioni finanziarie afferenti conti cifrati e società domiciliate in Paesi offshore (Cass. Pen. Sez. 2, n. 32936/2012). Per la punibilità del riciclaggio non devono essere individuati gli autori del reato presupposto, potendo anche essere rimasto a carico di ignoti (Cass., 9410/1990) né è necessario che sia identificato con precisione il soggetto passivo (Cass. Pen. Sez. 2, n. 546/2011, cit.); non rileva neppure che gli autori del reato presupposto siano non imputabili o non punibili (art. 648, u.c. c.p.); se prima della riforma del 2021 era ritenuta imprescindibile la natura delittuosa e non colposa del reato presupposto, non è stata mai richiesta l'esatta qualificazione di esso o l'individuazione della sua precisa tipologia (Cass. Pen. Sez. 2, n. 546/2011, cit.), potendo essere costituito anche da un reato commesso all'estero, per cui manchi la condizione di

delle utilità da attività criminose vale a limitarle a quelle dalle quali può scaturire, per nesso di derivazione, un lucro (prodotto, profitto e prezzo ovvero qualsiasi altro arricchimento consistente in un incremento e ovvero nel mancato decremento), tradottosi in denaro, beni ed altre utilità riciclabili. La giurisprudenza di legittimità ha segnalato i limiti alla configurabilità del riciclaggio rispetto a peculiari *predicate crimes*¹¹⁴. Sono noti, in particolare, i contrasti ermeneutici in merito alla riciclabilità dei risparmi di imposta dei reati tributari dichiarativi, con riferimento a quelli inerenti le imposte dirette¹¹⁵.

La struttura del reato ne ha tratto una maggiore flessibilità ed attitudine al contrasto di fenomeni in evoluzione, come l'autonomia della condotta e il disvalore giuridico della fattispecie, rilevata anche dalla costruzione del dolo in chiave generica, rifuggendo tipizzazioni normative di finalità estranee alla configurazione oggettiva. Autonomia già timidamente rivelata dal rinvio da parte dell'ultimo comma dell'art. 648-*bis* c.p. all'ultimo comma dell'art. 648 c.p., presente sin dalla versione del 1978¹¹⁶.

Sotto il profilo dell'elemento oggettivo la condotta incriminata consiste nel sostituire o trasferire denaro, beni o altre utilità provenienti dai ricordati reati ovvero nel compimento di altre operazioni in modo da ostacolare l'identificazione della provenienza criminosa. Nel concetto di sostituzione rientrano tutte le attività dirette alla c.d. "ripulitura" del denaro sporco, al fine di separarlo da ogni possibile collegamento con il reato presupposto che lo ha originato, rimpiazzandolo con valori puliti¹¹⁷. La condotta di trasferimento, invece, è una specificazione della sostituzione che colpisce le condotte di movimentazione (da un soggetto ad altro soggetto o da un luogo ad un altro) ai fini di ripulitura che si avvalgono di strumenti negoziali o giuridici; secondo la giurisprudenza rileva penalmente anche il trasferimento materiale da un luogo ad un altro dei proventi illeciti ove ciò renda di fatto più difficoltosa l'identificazione dell'origine illecita. Rileva, dunque, sia il "trasferimento" giuridico (cessione della proprietà o dell'uso ad altri), sia quello fisico¹¹⁸, ove l'allontanamento dei beni o delle altre utilità dai luoghi della loro produzione ed acquisizione valga ad ostacolarne la possibilità di identificazione¹¹⁹. Il riferimento, poi, al compimento di altre operazioni in modo da ostacolare l'identificazione della provenienza criminosa consente di colpire efficacemente le tecniche di ripulitura più fantasiose e articolate¹²⁰.

La descrizione normativa delle condotte tipiche induce ad escludere la configurabilità del riciclaggio mono-soggettivo mediante omissione¹²¹. Infatti, la terminologia usata è esplicita nel richiamare condotte di natura attiva¹²². Una responsabilità concorsuale omissiva impropria appare configurabile, pur tra

procedibilità, in carenza di richiesta ministeriale; infine, il riciclaggio non richiede interessenze fra l'autore del reato presupposto ed il riciclatore, né la conoscenza tra i due soggetti né la conoscenza da parte del riciclatore dell'identità dell'autore del reato presupposto (Cass. Pen. Sez. 2, 35763/2010, cit.).

¹¹⁴ Per un quadro delle questioni in tema di reati presupposti, specie tributari, cfr. Di Vizio, *Profili penali dell'attività bancaria*, Milano, 2020, pp. 141-152; per la bancarotta fraudolenta *contra*: Cass. Pen. Sez. 2, n. 23052/2015, Rv 264040; a favore Cass. Pen. sez. V, n. 572/2017, Rv. 268600; Cass. Pen. Sez. 2, n. 51535/2019.

¹¹⁵ A favore Cass. Pen. Sez. 2 n. 6061/2012, Gallo, Rv 252701, con l'ulteriore limite ontologico della precedente consumazione del reato di natura fiscale necessario per ipotizzare la derivazione da esso del profitto illecito (Cass. Pen. Sez. 2, 3889/2020).

¹¹⁶ Dalla disposizione è inferita l'insensibilità della punibilità del riciclaggio rispetto all'estinzione dell'illecito base (art. 170, comma 1, c.p.) allorché quest'ultima intervenga dopo il compimento del riciclaggio, diversamente dall'evenienza in cui intervenga prima. La stessa soluzione viene preferita in caso di sopravvenuta abolitio criminis, depenalizzazione o derubricazione dell'antefatto in illecito civile dopo la consumazione del riciclaggio. Sul punto, quanto alla ricettazione, per l'estinzione e l'abrogazione del reato presupposto, cfr. Cass. Pen. Sez. 2, n. 36281/2003; per l'incompatibilità del reato presupposto con la normativa comunitaria cfr. Cass. Pen. Sez. 3, n. 30591/2014, Rv. 259957; per la mancanza di una condizione di procedibilità prevista dall'art. 10 cod. pen. in relazione alla commissione all'estero, da parte di uno straniero, del delitto ai danni di un cittadino italiano cfr. Cass. Pen. Sez. 2, n. 22343/2010, Rv. 247527; per difetto di querela cfr. Cass. Pen. Sez. 2, n. 33478/2010, Rv. 248248; in materia di riciclaggio, per causa di non punibilità sopravvenuta del reato presupposto, come nel caso del condono tributario, non modificando la genetica provenienza criminosa del bene cfr. Cass. Pen. Sez. 2, n. 23396/2005.

¹¹⁷ Cass. Pen. Sez. 2 n. 7503/2022.

¹¹⁸ Cass. Pen. Sez. 2, n. 18607/2010, Rv. 247540; Id., n. 36779/2006 Rv. 235060.

¹¹⁹ Come nel caso di movimentazioni di denaro attraverso i sistemi elettronici di pagamento.

¹²⁰ Cfr. Cass. Pen. Sez. 2 n. 7503/2022.

¹²¹ In tal senso, U. Liguori, *Le modifiche legislative: l'ampliamento dei reati presupposto e delle condotte principali (panorama giurisprudenziale)*, in A. Manna (a cura di), *Riciclaggio e reati connessi all'intermediazione mobiliare*, Torino, 2000, p. 90.

¹²² G.M. Flick, *Accessi al settore finanziario e segnalazioni degli intermediari: controlli, obblighi e responsabilità*, in RIDPP, 1994, p. 1217.

contrasti, a carico dei soggetti tenuti ad impedire le condotte di riciclaggio, allorché siano tenuti a segnalare le operazioni sospette, nei limiti in cui possono essere ritenuti giuridicamente obbligati ad impedire un'operazione di riciclaggio in itinere e sempre che la loro condotta omissiva sia sorretta dal necessario dolo¹²³. In tutti i casi si tratta di reato istantaneo di mera condotta e di pericolo concreto per cui l'azione del soggetto attivo, che può essere chiunque, dovrà risultare concretamente idonea a dissimulare l'origine illecita dei proventi, non essendo necessario che si verifichi l'evento, ossia che si porti a termine la dissimulazione; occorre, quindi, che la condotta dia luogo ad una difficoltà nell'individuazione della provenienza criminosa dei beni senza determinare un'oggettiva impossibilità di accertare l'origine criminosa dei valori. Integra il delitto il compimento di operazioni volte non solo ad impedire in modo definitivo, ma anche a rendere difficile l'accertamento della provenienza del denaro, dei beni o delle altre utilità, attraverso un qualsiasi espediente che consista nell'aggirare la libera e normale esecuzione dell'attività posta in essere¹²⁴. Va precisato che il delitto si consuma con la realizzazione dell'effetto dissimulatorio conseguente alle condotte tipiche previste dall'art. 648-bis, primo comma, c.p., non essendo invece necessario che il compendio "ripulito" sia restituito a chi l'aveva movimentato¹²⁵. L'attitudine decettiva delle condotte accomuna tutte le ipotesi alternativamente previste dalla norma, segnalandosi come loro autentico disvalore¹²⁶, oltre che elemento distintivo rispetto alla ricettazione. Nessuna condotta è punibile ai sensi dell'art. 648-bis c.p. se non è riscontrabile in essa l'attitudine dissimulatoria, salvo l'integrazione, ove ne sussistano i requisiti, di altri reati (quali la ricettazione, il favoreggiamento personale o reale, l'acquisto di cose di sospetta provenienza). La riformulazione delle condotte ha dissolto i dubbi sulla configurabilità del reato nella forma tentata¹²⁷.

L'elemento soggettivo del delitto è integrato dal dolo generico, che ricomprende la volontà di compiere le attività volte ad ostacolare l'identificazione della provenienza criminosa di beni o altre utilità, nella consapevolezza di tale origine, senza riferimento a scopi di profitto e/o di lucro¹²⁸. La prova può essere raggiunta anche sulla base dell'omessa o non attendibile indicazione della provenienza della cosa ricevuta, rivelatrice di una volontà di occultamento logicamente spiegabile con un acquisto in mala fede¹²⁹ e comunque sulla base degli elementi che confortano la dimostrazione in via logico-indiziaria della provenienza criminosa, ossia le caratteristiche oggettive dell'operazione posta in essere, le connotazioni soggettive delle parti contraenti (fiduciario operante in Paese off-shore, qualità di parte contraente di società di diritto estero prive di concreta operatività e di reali finalità imprenditoriali) e delle eventuali anomalie dell'operazione stessa (operazione priva di plausibile giustificazione sul piano economico o giuridico, col ricorso a società di comodo o domiciliate in paesi a fiscalità privilegiata o alla interposizione fittizia soggettiva, estero vestizione dell'operazione stessa). Semplificazione deriva dalla compatibilità del dolo eventuale con il delitto di riciclaggio¹³⁰.

3.2. Impiego di denaro, beni o utilità di provenienza illecita

In base all'art. 648-ter, comma 1, c.p. "*Chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648-bis, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto, è punito con la reclusione da quattro a dodici anni e con la multa da 5.000 euro a 25.000 euro*". In virtù del successivo comma 2 "*La pena è della reclusione da due a sei anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a*

¹²³ Contra M. Giglioli, *Profili problematici inerenti al reato di riciclaggio*, in V. Maiello e L. Della Ragione (a cura di), *Riciclaggio e reati nella gestione dei flussi di denaro sporco*, Milano, 2018, p. 240 e ss.; a favore dell'ipotizzabilità del concorso omissivo improprio dei soggetti tenuti all'inoltro delle s.o.s. cfr. Cass. Pen. Sez. 6, n. 37098/2012 e Cass. Pen. Sez. 2, 29452/2013.

¹²⁴ Cass. Pen., Sez. 6, 18 dicembre 2007, n. 16980; v. anche Cass. Pen. Sez. 2, 12 gennaio 2006, n. 2818.

¹²⁵ Cass. Pen. Sez. 2, n. 1857/2017 Rv. 269316 – 01.

¹²⁶ Cass. Pen. Sez. 2, n. 25940/2013, Rv. 256454.

¹²⁷ Così Cass. Pen. Sez. 2, n. 1960/2015, Rv. 262506.

¹²⁸ In tal senso, Cass. Pen. Sez. 2, n. 546/2011, Rv. 249444.

¹²⁹ Così Cass. Pen. Sez. 2, 546/2011.

¹³⁰ A favore Cass. Pen. Sez. 2, n. 8330/2014, Rv. 259010; Id. 7503/2022.

sei mesi”. I successivi commi dell’art. 648-ter c.p. descrivono figure circostanziali: la pena è aumentata quando il fatto è commesso nell’esercizio di un’attività professionale¹³¹ (art. 648-ter, comma 3 c.p.) ed è diminuita nell’ipotesi di cui al quarto comma dell’art. 648¹³² c.p. (art. 648-ter, comma 4 c.p.). Ai sensi dell’art. 648-ter, comma 5, c.p. si applica l’ultimo comma dell’art. 648 c.p., che assicura l’applicazione del delitto anche quando l’autore del reato, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato.

Il delitto costituisce fattispecie residuale, che mira a tutelare la genuinità del libero mercato da qualunque forma di inquinamento proveniente dall’immissione di somme di provenienza illecita nei normali circuiti economici e finanziari¹³³. Rispetto a quello di riciclaggio, il reimpiego presenta una più sviluppata lesività economica (sotto il profilo della regolarità degli scambi e della leale concorrenza tra operatori) compensata da un minor pregiudizio dell’amministrazione della giustizia. Si tratta di reato commissivo a forma libera.

La condotta consiste nell’impiego dei proventi criminosi in attività economiche o finanziarie. La norma incriminatrice si esprime in termini generici, laddove punisce l’“impiego” del denaro, dei beni o delle altre utilità provenienti da reato in “attività economiche o finanziarie”. Il primo impiego consuma il reato, suscettibile di essere realizzato anche in forma tentata. Il termine “impiego” rimanda a nozioni volutamente non tecniche, dovendosi intendere per tale qualsiasi tipo e qualsiasi forma di “utilizzo” e/o di “investimento” dei capitali illeciti, con l’unica specificazione e limitazione che si tratti di un impiego in attività economiche o finanziarie¹³⁴. Tale ampiezza è criticata quale carenza di tassatività. Non ancora risolta in giurisprudenza la questione se l’impiego prescindendo da un uso dei proventi illeciti sostenuto da fine speculativo o se richieda un investimento finalizzato da fine di profitto¹³⁵.

Controversa¹³⁶ è la necessaria connotazione dissimulativa della condotta di impiego di denaro, beni o altre utilità provenienti da reato in attività economiche o finanziarie *ex* art. 648-ter c.p. Il dissidio ha riverberi sulla struttura dell’elemento soggettivo. Per una prima opinione ricettazione, riciclaggio e impiego di beni di provenienza illecita, fattispecie in rapporto di specialità, si distinguono per l’elemento soggettivo: la ricettazione richiede una generica finalità di profitto, il riciclaggio esige lo scopo ulteriore di far perdere le tracce dell’origine illecita, l’impiego, infine, che tale scopo sia perseguito facendo ricorso ad attività economiche o finanziarie¹³⁷. Per contro l’attitudine decettiva svanisce ove si valorizzi il fatto che, almeno a livello normativo, il delitto di impiego non richiede una condotta idonea a dissimulare la provenienza criminosa del suo oggetto né esige, ai fini del dolo, la volontà di dissimularla¹³⁸.

La nozione di attività economica o finanziaria è desumibile dagli artt. 2082, 2135, 2195 c.c. e fa riferimento non solo all’attività produttiva in senso stretto, ossia a quella diretta a creare nuovi beni o servizi, ma anche all’attività di scambio e di distribuzione dei beni nel mercato del consumo, nonché ad ogni altra attività che possa rientrare in una di quelle elencate nelle sopra menzionate norme del codice civile¹³⁹. In essa è compresa anche l’attività di finanziamento a titolo oneroso, come la concessione di mutui¹⁴⁰. In difetto di indicazioni testuali contrarie, l’impiego penalmente perseguibile in attività

¹³¹ In tema non rilevano esclusivamente le attività per il cui esercizio è richiesta l’iscrizione ad un particolare albo o una speciale abilitazione, ma qualunque attività economica o finanziaria diretta a creare nuovi beni e servizi o allo scambio e distribuzione di beni nel mercato del consumo (Cass. Pen. Sez. 2, n.3026/2017, Rv. 269166 – 01).

¹³² Se il fatto è di particolare tenuità, si applica la pena della reclusione sino a sei anni e della multa sino a euro 1.000 nel caso di denaro o cose provenienti da delitto e la pena della reclusione sino a tre anni e della multa sino a euro 800 nel caso di denaro o cose provenienti da contravvenzione.

¹³³ Cass. Pen. Sez. 2, 5 novembre 2013-25 febbraio 2014, n. 9026.

¹³⁴ Cass. Pen. Sez. 2, n. 5546 del 11/12/2013, dep. 2014, Cuppari, Rv. 258204.

¹³⁵ V. Manes, *Delitti contro il patrimonio mediante frode*, in Diritto penale, Lineamenti di parte speciale, VII ed., Bologna, 2016, p. 869.

¹³⁶ *A favore*, Cass. Pen. Sez.2, n. 26796/2021, Rv. 281552 - 03; *contra*, Cass. Pen. Sez. 2, n. 24273/2021, Rv. 281626 - 01.

¹³⁷ Cass. Pen. Sez. 2, n. 33076/2016 cit.

¹³⁸ Cass. Pen. Sez. 2, n. 43387/2019, Rv. 277997 – 03 per cui occorre la mera coscienza e volontà di destinare ad un impiego economicamente utile i capitali illeciti, con la consapevolezza, anche solo generica, della loro provenienza criminosa.

¹³⁹ Cass. Pen. Sez. 2, n. 38422/2018; Id., n. 33076/2016; Id., n. 5546/2014.

¹⁴⁰ Cass. Pen. Sez. 2, n. 5546/2014, Rv. 258204.

economiche e/o finanziarie non esige un limite quantitativo minimo al valore dell'investimento: può bastare anche il reimpiego di una modesta somma di denaro provento di una qualsiasi attività criminosa. Per la configurabilità del reato non occorre che il reimpiego del danaro o degli altri beni provenienti da reato avvenga in attività lecite. Tenuto conto delle finalità perseguite dall'art. 648-ter c.p., infatti, al fine di escludere la configurabilità del reato, nessuna rilevanza riveste l'eventuale illiceità dell'attività economica o finanziaria nella quale sono impiegate somme di denaro di provenienza illecita; anzi, "in tal caso l'offesa arrecata dalla condotta al bene tutelato è anche maggiore"¹⁴¹. Non è necessario neppure che le attività di reimpiego siano svolte professionalmente¹⁴², potendo essere realizzate anche in modo sporadico od occasionale. La descrizione normativa impedisce di ricondurre al fatto tipico ogni diverso impiego (dunque non economico né finanziario) dei proventi criminosi.

Sono evidenti, in ogni caso, spazi di larga sovrapposizione della condotta di impiego rispetto al reato *ex* art. 648-bis c.p., la cui integrazione, al pari del caso del concorso nel reato base e nel reato di ricettazione, preclude la configurazione del primo, riducendone l'applicazione¹⁴³.

3.3. Trasferimento fraudolento di valori.

Ai sensi dell'art. 512-bis c.p. salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli artt. 648, 648-bis e 648-ter, è punito con la reclusione da due a sei anni. La norma ha trasposto in seno al codice penale la previsione dell'art. 12-*quinqüies*, comma 1, DL 8 giugno 1992, n. 306, convertito con mod. dalla L. 7 agosto 1992, n. 356, con la quale l'apparato penale è stato dotato di un ulteriore strumento di contrasto di condotte riciclatorie¹⁴⁴. Ad essere colpita è la costituzione di una situazione di difformità tra apparenza giuridico-formale e reale titolarità o disponibilità di fatto dell'oggetto della condotta.

L'espressione "attribuzione fittizia" è intesa secondo un'accezione ampia, che ricomprende non solo le forme negoziali tradizionali, ma qualsiasi tipologia di atto idonea a creare un apparente rapporto di signoria tra un determinato soggetto e il bene, rispetto al quale permanga intatto il potere di colui che effettua l'attribuzione patrimoniale, per conto o nell'interesse del quale la stessa è operata¹⁴⁵. In sostanza, qualunque forma di dissociazione tra titolarità formale ed effettivo potere direzionale su beni patrimoniali e strutture aziendali oggetto del trasferimento¹⁴⁶. Il termine "disponibilità" richiama poteri di fatto, mentre l'espressione "titolarità" una relazione giuridicamente significativa tra i valori ed il destinatario del trasferimento, anche fuori da rigidi schemi civilistici¹⁴⁷. A sua volta la fittizietà evoca le usuali ipotesi di simulazione, assoluta o relativa, ma anche ogni situazione in cui resti inalterata l'effettiva signoria sulla cosa da parte del trasferente¹⁴⁸. Se l'attribuzione della titolarità o della disponibilità della cosa non richiede l'inquadramento in rigorosi schemi civilistici, la stessa deve comportare, quantomeno, il fittizio conferimento di una apprezzabile signoria sulla "res"¹⁴⁹.

¹⁴¹ Cass. Pen. Sez. 2 n. 9026/2014.

¹⁴² Cass. Pen., Sez. 2, n. 9026/2014.

¹⁴³ Cass. Pen. Sez. 2, n. 4800/2010; Id., n. 5547/2014 per gli elementi specializzanti dell'impiego.

¹⁴⁴ In tema cfr. Pellegrino, *Il trasferimento fraudolento di valori*, in Maiello (a cura di) *La Legislazione penale in materia di criminalità organizzata, misure di prevenzione ed armi*, Torino, 2015, p. 5.

¹⁴⁵ Cass. Pen. Sez. I, n. 17546/2017.

¹⁴⁶ A. Balsamo e G. De Amicis, *L'art. 12-*quinqüies* della l. n. 356/1992 e la tutela del sistema economico contro le nuove strategie delle organizzazioni criminali: repressione penale "anticipata" e prospettive di collaborazione internazionale*, in Cass. pen., 2003, p. 2081.

¹⁴⁷ A. Balsamo e G. De Amicis, *op. cit.*, 2082.

¹⁴⁸ R. Belfiore, *Art. 12-*quinqüies* DL 8 giugno 1992, n. 306*, sub voce Criminalità organizzata-riciclaggio, in F. Palazzo e C. Paliero (a cura di), *Commentario breve alle leggi penali complementari*, 2° edizione, Padova, 2007, p. 925.

¹⁴⁹ Non basta ad integrare il reato né la mera nomina ad amministratore, ancorché fittizio, di una società di capitali (Cass. Pen. Sez. 5, n. 48415/2014 Rv. 261027) né la prova che l'indagato rivesta la funzione di amministratore di fatto della società delle cui quote s'ipotizza la fittizia intestazione, essendo invece necessario l'accertamento della titolarità sostanziale delle quote, attraverso l'attribuzione della qualifica di socio di fatto (Cass. Pen. Sez. 6, n. 37375/2014, Rv. 261655).

Tipiche attribuzioni patrimoniali fittizie sono state riconosciute nelle seguenti evenienze: (i) intestazione a terzi di quote sociali da parte del titolare, al fine di eludere le disposizioni di legge in materia di prevenzione patrimoniale; (ii) condotta dell'amministratore di fatto o di diritto che, non essendo titolare delle quote, si adoperi in qualsiasi modo per favorire la realizzazione della condotta elusiva¹⁵⁰; (iii) attribuzione fittizia da parte dell'affittante di un ramo di azienda, diretta a creare una realtà giuridica apparente nell'interesse del reale "dominus", come nell'affitto di azienda gestita da un prestanome per occultare i proventi di reati associativi¹⁵¹; (iv) acquisizione della qualità di socio occulto in una società già esistente, con partecipazione alla gestione di impresa e agli utili derivanti dall'attività imprenditoriale¹⁵², in modo da acquisire la contitolarità (anche in quota) della proprietà aziendale e degli utili; (v) fittizia costituzione di una società commerciale attraverso l'intestazione di quote a prestanome da parte dei reali proprietari, in realtà amministratori e soci occulti di altra società dichiarata fallita¹⁵³.

Nel caso di intestazione nella forma dell'acquisto, ai fini dell'integrazione del reato, non è sufficiente accertare la mera disponibilità del bene da parte di chi non ne risulta formalmente titolare, occorrendo la prova, anche indiziaria, della provenienza delle risorse economiche impiegate per l'acquisto da parte del soggetto che intenda eludere l'applicazione di misure di prevenzione¹⁵⁴.

Non è richiesta la concreta capacità elusiva dell'operazione¹⁵⁵. Si tratta di reato di pericolo, per la cui commissione è sufficiente che l'agente, sottoposto o suscettibile di essere sottoposto ad una misura di prevenzione patrimoniale, e il concorrente necessario, compiano un qualsiasi negozio giuridico con la finalità elusiva prevista dalla norma. La valutazione del pericolo di elusione deve essere compiuta *ex ante* e su base parziale, alla stregua delle circostanze conosciute o conoscibili al momento della condotta¹⁵⁶. Da ciò derivano plurime conseguenze sulla configurabilità del reato, integrato: - anche in presenza di condotte aventi ad oggetto beni che non provengono necessariamente da reato¹⁵⁷; - anche laddove i beni del soggetto sottoposto o sottoponibile a misura di prevenzione patrimoniale siano intestati fraudolentemente a soggetti (come il coniuge, i figli, le persone stabilmente conviventi, i parenti e gli affini entro il grado indicato dalla legge) per i quali opera la presunzione d'interposizione fittizia prevista dall'art. 26, comma 2, del D.lgs. 159 del 2011, e prima dall'art. 2-*ter* della legge n. 575 del 1965¹⁵⁸.

Tra i valori trasferibili ("denaro, beni o altre utilità") sono ricompresi tutti i cespiti di apprezzabile valore economico¹⁵⁹. L'attribuzione patrimoniale può legittimamente includere, perciò, anche un'azienda, un'attività imprenditoriale o una società¹⁶⁰; ciò con riferimento tanto al momento iniziale dell'impresa quanto a una fase successiva, allorquando in una società, sorta in modo lecito, si inserisca un socio occulto, che avvalendosi dell'interposizione fittizia, persegua le finalità illecite previste dalla norma incriminatrice¹⁶¹. L'oggetto del reato non deve costituire, necessariamente, provento criminoso anche se in proposito occorre svolgere alcune precisazioni. Ciò è indiscusso ove la condotta sia connotata dal dolo di elusione delle disposizioni di legge in materia di misure di prevenzione patrimoniale o di contrabbando. L'origine penalmente illecita dell'oggetto, invece, risulterà stabilmente ricorrente in caso di connessione con la finalità di agevolare la commissione dei delitti di ricettazione, riciclaggio o reimpiego. Qui, infatti, la connessione rispetto a tale futuro impiego criminale del bene si gioverà proprio della prova della sua

¹⁵⁰ Integrano comportamenti elusivi la scelta delle persone alle quali fittiziamente intestare quote sociali, ovvero trasferire le quote sociali, la tenuta dei contatti con i professionisti che devono realizzare tali operazioni o la scelta degli amministratori fittizi che coprono il reale titolare delle quote (Cass. Pen. Sez. 2, n. 41433/2016).

¹⁵¹ Cass. Pen. Sez. 2, n. 52616/2014; Id., n. 19123/2013.

¹⁵² Cass. Pen. Sez. 1, n. 43049/2003 in Riv. Pen., 2004, 1027, per l'impresa a partecipazione mafiosa, con riferimento all'instaurazione di rapporti di cointeressenza tra imprese sorte nel rispetto della legalità ed esponenti mafiosi, che in esse investano capitali ed esprimano capacità di condizionamento del mercato.

¹⁵³ Cass. Pen. Sez. 1, n. 6939/2011.

¹⁵⁴ Cass. Pen. n. 26931/2018, Rv. 273419; Id., 35826/2019.

¹⁵⁵ Componente estranea agli elementi costitutivi del fatto incriminato (Cass. Pen. Sez. 5 n. 40278/2016, Rv. 268200).

¹⁵⁶ Cass. Pen. Sez. 2, n. 12871 del 9 marzo 2016, Rv. 266661.

¹⁵⁷ Cass. Pen. Sez. 2 n. 13448/2015, Rv. 266438; Id., n. 28300/2019, Rv. 276216 – 01.

¹⁵⁸ Cass. Pen. Sez. 2, n. 7999/2017; Id., n. 13843/2019, Rv. 275372.

¹⁵⁹ F. Mucciarelli, *Modifiche urgenti al nuovo codice di procedura penale e provvedimenti di contrasto alla criminalità mafiosa*, DL n. 396/1992, in *Legisl. Pen.*, 1993, p. 158.

¹⁶⁰ Cass. Pen. Sez. 2, n. 52616/2014, Rv. 261613.

¹⁶¹ Cass. Pen. Sez. 2, n. 5647/2014, Rv. 258343.

origine criminosa ed immaginare che la provenienza criminosa rispetto al riciclaggio non preesista ma sia conferita dal delitto di trasferimento fraudolento renderebbe non distinguibili le condotte¹⁶². Può ipotizzarsi però il caso in cui l'attribuzione fittizia del bene di origine lecita sia operata in funzione di un futuro scambio del bene con altro di provenienza criminosa al fine di mantenere schermata l'identità dell'autentico dominus e agevolare il successo di operazioni di riciclaggio, reimpiego e ricettazione. Anche le operazioni riciclatorie, del resto, non devono svolgersi direttamente sul provento criminoso ma "in relazione" ad esso. Se è pacifico che il reato presupposto di quello di riciclaggio non deve essere giudizialmente accertato e la sua prova può scaturire anche da elementi logici¹⁶³, lo stesso insegnamento è richiamabile per il reato presupposto di quello di intestazione fittizia, volta ad agevolare il riciclaggio¹⁶⁴. La sussidiarietà rispetto al più grave delitto *ex art. 648-bis c.p.* ha spinto ad interrogarsi sui reali spazi di autonomia della fattispecie in analisi; recenti pronunce¹⁶⁵ hanno ammesso che essa concorre con quella di riciclaggio e ne può rappresentare il reato-presupposto¹⁶⁶. L'ambito di più sicura praticabilità dell'intestazione fittizia è stato individuato nella possibilità di punire anche l'autore del reato presupposto, delineandosi come prima forma di autoriciclaggio punito dall'ordinamento nazionale¹⁶⁷.

3.4. L'autoriciclaggio

Ai sensi dell'art. 648-ter.1 c.p. "*Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*". In virtù dell'art. 648-ter.1, c.p., poi, "*La pena è della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 quando il fatto riguarda denaro o cose provenienti da contravvenzione punita con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi*".

Variegato il quadro delle circostanze¹⁶⁸. L'art. 648-ter 1 assicura specifiche previsioni in punto di punibilità: fuori dei casi di cui ai commi da 1 a 4, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale (art. 648-ter, comma 5, c.p.). Si applica l'ultimo comma dell'art. 648 che assicura l'applicazione del delitto anche quando il co-autore del reato, da cui il denaro o le cose provengono, non è imputabile o non è punibile ovvero quando manchi una condizione di procedibilità riferita a tale reato (art. 648-ter.1 ultimo comma). Ai sensi dell'art. 9, comma 4, c.p., dopo l'intervento del D.lgs. 195/2021, nel caso di autoriciclaggio commesso dal cittadino all'estero la richiesta del Ministro della Giustizia o l'istanza o la querela della persona offesa non sono necessarie.

La legge n. 186 del 15.12.2014 ha introdotto il reato di autoriciclaggio, riservato all'autore (e al concorrente) del reato presupposto che impieghi, sostituisca, trasferisca, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità di provenienza criminosa. La rilevanza penale delle condotte tipiche è condizionata dalla loro *idoneità ad ostacolare concretamente* l'identificazione della

¹⁶² Palazzi, *I rapporti tra il delitto di autoriciclaggio e quello di trasferimento fraudolento di valori*, in E. Mezzetti e D. Piva (a cura di), *Punire l'autoriciclaggio, Come, Quando e Perché*, 2016, p. 55 e ss.

¹⁶³ Cass. Pen. Sez. 6, n. 28715/2013, Alvaro, Rv, 257205; Cass. Pen. sez2, n. 546 del 7 gennaio 2011, Rv. 249444.

¹⁶⁴ Cass. Pen. Sez. 2, n. 3935/2017.

¹⁶⁵ Cass. Pen. Sez. 6, n. 18496/2012, Rv 252658.

¹⁶⁶ Cass. Pen. Sez. 2, n. 39756 /2011, Rv 251190.

¹⁶⁷ Cass. Sez. Un., n. 25191/2014, Rv. 259590.

¹⁶⁸ In primis, la pena è diminuita se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni (art. 648-ter, comma 3, c.p.), salvo che il denaro, i beni o le altre utilità provengano da un delitto commesso con le condizioni o le finalità di cui all'art. 416-bis.1 (art. 648-ter comma 4, c.p.). La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto (art. 648-ter.1, comma 6, c.p.). Inoltre, la pena è aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale (art. 648-ter, comma 6, c.p.).

provenienza criminosa del loro oggetto. Ad essere criminalizzata è la *re-immissione occulta* in ambiente economico dei frutti dell'illegalità da parte del responsabile di essa, ponendo uno stimolo a non utilizzare in forma nascosta il provento criminoso e rafforzando l'azione deterrente dei reati presupposti. Lo scopo dell'incriminazione diventa, dunque, componente inscindibile del bene giuridico complesso¹⁶⁹. La limitazione della rilevanza penale delle condotte tipiche a quelle realizzate in ambiente economico-sociale¹⁷⁰, emergente dalla destinazione dei proventi illeciti in attività economiche, finanziarie, imprenditoriali o speculative è rimarcata dall'art. 648-ter.1, comma 5, c.p., alla cui stregua "*non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale*". La Cassazione ha però definito la portata di quest'ultima clausola di non punibilità escludendone l'applicabilità alle condotte descritte nei commi precedenti (in cui è previsto l'impiego economico-sociale dissimulato) e ritenendo che l'agente possa andare esente da responsabilità penale soltanto se utilizzi o goda dei beni proventi del reato presupposto in modo diretto e senza che compia su di essi alcuna operazione atta ad ostacolare concretamente l'identificazione della loro provenienza criminosa¹⁷¹.

Ciò comporta anche che ove la fattispecie prevista del primo comma dall'art. 648-ter.1 c.p. sia integrata in tutti i suoi requisiti (con l'impiego, la sostituzione o il trasferimento dei proventi illeciti nelle quattro ampie categorie di attività delineate dalla fattispecie, laddove connotati da concreta idoneità di camuffamento), l'agente è sanzionabile penalmente, restando indifferente che, alla fine delle operazioni di autoriciclaggio, egli abbia "meramente" utilizzato o goduto personalmente dei suddetti beni a titolo personale. La non punibilità ex art. 648-ter.1, comma 5, c.p., trova una sua logica e coerente spiegazione nel divieto del *ne bis in idem* sostanziale ma solo a condizione che l'agente si limiti al mero utilizzo o godimento dei beni provento del reato presupposto senza che ponga in essere alcuna attività decettiva al fine di ostacolarne l'identificazione quand'anche per utilizzare o meglio godere dei suddetti beni¹⁷². Tale interpretazione comporta una problematica rimodulazione dei contenuti dell'autoriciclaggio, delineando un'ulteriore fattispecie "a consumazione anticipata", nascosta dietro le pieghe della clausola di non punibilità ex art. 648-ter.1., comma 4, c.p. e per taluni aspetti distinta da quella del primo comma dello stesso articolo¹⁷³.

In linea con l'art. 648-bis c.p., la novella del 2014 ha previsto per l'autoriciclaggio lo stesso oggetto materiale ("*denaro, beni o altre utilità*"), pene diversificate in ragione della gravità del reato presupposto¹⁷⁴ e il rinvio all'ultimo comma dell'art. 648 c.p.¹⁷⁵. Ancora, il nuovo reato costituisce reato-presupposto della responsabilità degli enti di cui al D.lgs. 8.6.2001, n. 231 (art. 25-*octies*) e ad esso si applica la disciplina della confisca di cui all'art. 648-*quater* c.p. Viene prevista la circostanza aggravante ad effetto comune costituita "*dall'aver commesso il fatto nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale*", ampliando quella tipica del riciclaggio e del reimpiego (limitata all'attività professionale). Innovativa la circostanza attenuante ad effetto speciale prevista per essersi l'autore efficacemente adoperato per evitare che le condotte fossero portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal reato.

¹⁶⁹ F. Mucciarelli, *Qualche nota sul delitto di autoriciclaggio*, in *Diritto penale contemporaneo*, Rivista trimestrale 1/2015, p. 112.

¹⁷⁰ L'indicazione normativa delle attività in cui il denaro, profitto del reato presupposto, può essere impiegato o trasferito, individua macroaree accomunate dalla caratteristica dell'impiego finalizzato al conseguimento di un utile, con conseguente inquinamento del circuito economico, nel quale vengono immessi denaro o altre utilità di provenienza criminosa che il reo vuole occultare (in termini Cass. Pen. Sez. 2, 13795/2019); nel concetto di "attività speculativa" (della quale il legislatore, non a caso, non offre rigida definizione) rientrano tutte le attività in cui il soggetto ricerca il raggiungimento di un utile, anche assumendosi il rischio di considerevoli perdite (Cass. Pen. Sez. 2, n. 27023/2022).

¹⁷¹ Cass. Pen., Sez. 2, 7 giugno 2018-5 luglio 2018, n. 30399.

¹⁷² Così Cass. Pen., Sez., 2, n. 13795 del 7 marzo 2019; Cass, n. 30399/2018, cit.; Cass. 36522/2019.

¹⁷³ Il concreto carattere dissimulatorio dell'origine criminosa del provento è in effetti dato identitario dell'autoriciclaggio; lo stesso costituisce elemento espresso e non autosufficiente della fattispecie del primo comma mentre nella fattispecie penale "nascosta" del quarto comma, oltre lo spazio della causa di non punibilità, diventa elemento tipico, per quanto inespresso, e autonomo, che finisce per recuperare la categoria residuale delle operazioni dissimulatorie, anche fuori della configurazione solo tentata del reato. Il verificarsi di questo camuffamento - quale operazione atta ad ostacolare concretamente l'identificazione della loro provenienza criminosa - sembrerebbe rilevare penalmente in quanto lesivo dell'esigenza di sterilizzazione del provento criminoso, ancor prima che lo stesso venga impiegato, trasferito o sostituito in ambiente economico, allentando una delle condizioni costitutive del delitto previsto dal primo comma dell'art. 648-ter.1. (in tema Di Vizio, *Profili penali*, pp. 241 e ss.).

¹⁷⁴ Sulla maggiore pregnanza della verifica incidentale del reato presupposto nel caso dell'autoriciclaggio, cfr. A.M. Maugeri, *L'autoriciclaggio dei proventi dei delitti tributari*, in E. Mezzetti e D. Piva (a cura di), *Punire l'autoriciclaggio. Come, quando e perché*, Torino, 2016, p. 150.

¹⁷⁵ Il concorrente nel reato è punibile anche nel caso in cui l'autore del reato presupposto non sia imputabile, punibile, ovvero quando faccia difetto una condizione di procedibilità.

Per la formulazione finale, la nuova fattispecie penale ha ricevuto critiche in dottrina, volte a segnalare l'effetto paradossale di un trattamento peggiore della re-immissione economico-sociale del provento illecito rispetto all'utilizzo personale ed edonistico di esso¹⁷⁶. È stata, inoltre, ipotizzata la non punibilità del concorrente rispetto a condotte di riciclaggio implicanti la destinazione del provento criminoso "*alla mera utilizzazione o al godimento personale*", ove intesa quale causa oggettiva di esclusione del tipo¹⁷⁷ e la persistente non punibilità dell'autoriciclaggio da "reati pregressi" commessi prima dell'entrata in vigore dell'art. 648-ter.1 c.p.¹⁷⁸. Non è mancata la prospettazione dell'ampliamento del concorso in autoriciclaggio, a discapito delle altre fattispecie di riciclaggio e la necessità di offrire un contenuto pregnante all'avverbio "*concretamente*" riferito all'idoneità decettiva¹⁷⁹ della condotta rispetto all'accertamento dell'identificazione della provenienza criminosa del bene materiale originario.

Negli anni successivi all'entrata in vigore delle fattispecie la giurisprudenza ha contribuito a dipanare molti degli aspetti segnalati.

In punto di soggetti attivi, ad esempio, è stato chiarito che integra il reato di *riciclaggio* la condotta di colui che, non avendo concorso nel reato presupposto, contribuisca alla realizzazione dell'autoriciclaggio da parte dell'autore del reato-presupposto, in quanto il reato di cui all'art. 648-ter.1 c.p. è configurabile solo nei confronti dell'*intranseus*¹⁸⁰. La natura dei reati presupposti è stata riconosciuta per i *reati di falso* solo se da essi derivi, come effetto diretto, un provento di natura patrimoniale per l'agente, idoneo ad essere riciclato, come nel caso del delitto *ex art. 316-ter c.p.*¹⁸¹ o nel caso di decreti di pagamento falsificati in favore del percipiente¹⁸². Parimenti è a dirsi per la *bancarotta fraudolenta*, anche nel caso di condotte distrattive compiute prima della dichiarazione di fallimento, in tutti i casi in cui tali condotte siano "*ab origine*" qualificabili come appropriazione indebita¹⁸³, ma a condizione che l'impiego dei beni dell'impresa fallita o del loro ricavato in attività a queste estranee avvenga con modalità idonee a renderne obiettivamente difficoltosa l'individuazione dell'origine criminosa e che non si realizzi attraverso la destinazione al mero utilizzo o godimento personale dell'agente¹⁸⁴: non è sufficiente il mero trasferimento di somme, oggetto di distrazione fallimentare, a favore di imprese operative, occorrendo un *quid pluri* che denoti l'attitudine dissimulatoria della condotta rispetto alla provenienza criminosa del bene¹⁸⁵. Per altre figure criminose è stata esclusa la natura di reati matrice¹⁸⁶. Anche in tema di autoriciclaggio, è stata esclusa la necessità che la sussistenza del reato presupposto sia stata accertata da una sentenza di condanna passata in giudicato, essendo sufficiente che il fatto costitutivo non sia stato giudizialmente escluso, nella sua materialità, in modo definitivo e che il giudice procedente per il riciclaggio o autoriciclaggio ne abbia incidentalmente ritenuto la sussistenza¹⁸⁷.

¹⁷⁶ Cfr. S. Cavallini e L. Troyer, *Apocalittici o integrati? Il nuovo reato di autoriciclaggio: ragionevoli sentieri ermeneutici all'ombra del "vicino ingombrante"* in Diritto penale Contemporaneo, 1/2015, p. 95 e ss.; F. Sgubbi, *Il nuovo delitto di "Autoriciclaggio": una fonte inesauribile di "effetti perversi" dell'azione legislativa*, Diritto penale Contemporaneo, 1/2015, 137 e ss.

¹⁷⁷ F. Mucciarelli, *Qualche nota sul delitto di autoriciclaggio*, in Diritto penale Contemporaneo, 1/2015.

¹⁷⁸ Contra Cass. Pen., n. 3691/2016 affermato che il reato di autoriciclaggio si configura anche quando il reato presupposto è stato commesso in data anteriore a quella di entrata in vigore del nuovo articolo 648-ter.1, c.p.

¹⁷⁹ In tema di autoriciclaggio il criterio da seguire ai fini dell'individuazione della condotta dissimulatoria è quello della idoneità *ex ante*, sulla base degli elementi di fatto sussistenti nel momento della sua realizzazione, ad ostacolare l'identificazione della provenienza criminosa del bene, senza che il successivo disvelamento dell'illecito per effetto degli accertamenti compiuti (grazie alla tracciabilità delle operazioni poste in essere fra diverse società), determini automaticamente una condizione di inidoneità dell'azione per difetto di concreta capacità decettiva (Cass. Pen. Sez. 2, n. 16059/2020, Rv. 279407 – 01). Non occorre che l'agente ponga in essere una condotta di impiego, sostituzione o trasferimento del denaro, beni o altre utilità che comporti un assoluto impedimento alla identificazione della provenienza criminosa degli stessi, essendo, al contrario, sufficiente una qualunque attività, concretamente idonea anche solo ad ostacolare gli accertamenti sulla loro provenienza (Cass. Pen. Sez. 2, n. 36121/2019, Rv. 276974 – 01). In tema di criptovalute cfr. Cass. Pen. Sez. 2, n. 27023/2022.

¹⁸⁰ Cass. Pen. Sez. 2, n. 16519/2021, Rv. 281596; per una diversa ricostruzione cfr. C. Brunelli, *Autoriciclaggio: profili del concorso di persone*, in E. Mezzetti e D. Piva (a cura di), *Punire l'autoriciclaggio, Come, Quando e Perché*, cit., p. 22.

¹⁸¹ Cass. Pen. Sez. 2, n. 14101/2019 ha escluso tale carattere per il falso di cui all'art. 5-septies DL n. 167/1990.

¹⁸² Cass. Pen. Sez. 2, n. 7176/2021, Rv. 280620 – 01.

¹⁸³ Cass. Pen. Sez. 5, n. 1203/2020, Rv. 277854 – 02.

¹⁸⁴ Cass. Pen. Sez. 5, n. 1203/2020, Rv. 277854 – 01.

¹⁸⁵ Cass. Pen. Sez. 5, n. 38919/2019, Rv. 276853 – 01.

¹⁸⁶ Non possono essere reati presupposto dell'autoriciclaggio: il delitto di intestazione fraudolenta di valori, poiché l'autoriciclaggio richiede l'autonomia provenienza illecita dei beni che ne sono oggetto (Cass. Pen. Sez. 6, n. 22417/2022 Rv. 283319 – 03 per la quale i rapporti tra i due reati sono regolati dal criterio di consunzione, in applicazione della clausola di sussidiarietà contenuta nell'art. 512-bis c.p., salvo il caso in cui l'intestazione fraudolenta abbia finalità elusiva delle disposizioni in materia di prevenzione); il reimpiego di somme derivanti da evasione fiscale "*sotto soglia*", difettando il necessario reato presupposto, in quanto le soglie di punibilità previste dal D.lgs. 10 marzo 2000, n. 74, rientrano tra gli elementi costitutivi del reato (Cass. Pen. Sez. 2, n. 11986/2021, Rv. 280995 – 01); le condotte dissimulatorie coincidenti con l'elemento materiale dell'autoriciclaggio (Cass. Pen. Sez. 2, n. 7074/2021, Rv. 280619 – 01).

¹⁸⁷ Cass. Pen. Sez. 2, n. 42052/2019, Rv. 277609 – 02.

Ulteriori chiarimenti giurisprudenziali sono stati offerti in merito agli impieghi tipici¹⁸⁸, alla loro idoneità decettiva¹⁸⁹, alla consumazione¹⁹⁰ e ai rapporti con altri reati¹⁹¹. Il D.lgs. 195/2021, oltre ad estendere reati presupposto alle contravvenzioni (punte con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi) e a qualsiasi delitto, anche colposo, ha previsto la giurisdizione italiana per i fatti di autoriciclaggio (oltre che di ricettazione) commessi dal cittadino all'estero, escludendo la necessità della richiesta del Ministro della Giustizia.

3.5. La nozione di riciclaggio amministrativo prevista dall'art. 2 del D.lgs. 231/2007

L'art. 2 del D.lgs. 21 novembre 2007, n. 231 fissa le definizioni di riciclaggio e di finanziamento del terrorismo rilevanti ai fini del sistema preventivo amministrativo. Si tratta di nozioni di grande significato, essendo presupposte dalle misure apprestate per la tutela preventiva dell'integrità del sistema economico e finanziario e della correttezza dei comportamenti degli operatori tenuti alla loro osservanza, allestita in coordinamento con l'attività di repressione dei reati di riciclaggio, di quelli presupposti e del finanziamento del terrorismo. Anche la collocazione sistematica dell'art. 2 cit., inserito nel Titolo I del D.lgs. 231/2007, subito dopo le definizioni dell'art. 1, testimonia l'importanza dell'enunciazione normativa del significato di tali espressioni per la complessiva funzionalità dell'impianto preventivo e per il corretto adempimento degli obblighi di collaborazione attiva e passiva sui quali il medesimo è edificato.

Nel caso del riciclaggio, si tratta di nozione marcatamente settoriale, con contenuto in parte eccentrico rispetto a quella penale. È il sospetto di riciclaggio, inteso secondo la peculiare accezione che si verrà ad esporre, ad attivare obblighi di adeguata verifica del cliente e del titolare effettivo indipendentemente da qualsiasi deroga, esenzione o soglia applicabile (art. 17, comma 2, lett. c) e a porsi quale parametro oggettivo del sospetto che origina l'inoltro di una segnalazione (art. 35 del D.lgs. 231/2007). D'altro canto, è il pericolo di riciclaggio, nel significato delineato dall'art. 2 del D.lgs. 231 cit., a costituire il riferimento dell'approccio basato sul rischio, attraverso misure proporzionate anche alle peculiarità organizzative, economiche e dimensionali dei soggetti obbligati. Il sintagma "ai fini" (anche se non più sostenuto dal rafforzativo "soli") indica come essa sia peculiare dell'ordinamento amministrativo, qualificandosi in rapporto alla prevenzione e al contrasto dell'uso del sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo. La circostanza orienta a ritenere che anche le espressioni impiegate nell'enunciazione della nozione possano prescindere dalle regole elaborate nel contesto della riflessione penalistica¹⁹². Può ritenersi, dunque, che le espressioni rilevino, anzitutto, per il

¹⁸⁸ Integrano condotte di impiego tipico, allorché atte a ostacolare concretamente l'identificazione della provenienza criminosa: l'immissione nel mercato dei beni provento di furto mediante vendita a terzi (Cass. Pen. Sez. 2, n. 36180/2021 Rv. 81967 – 01); il versamento di denaro, provento del delitto di appropriazione indebita, presso un istituto bancario per estinguere debiti ed ipoteche immobiliari (Cass. Pen. Sez. 2, n. 35260/2021 Rv. 281942); il reinvestimento del profitto illecito in attività economiche, finanziarie o speculative attuato attraverso la sua intestazione ad un terzo, persona fisica ovvero società di persone o capitali (Cass. Pen. Sez. 2, n. 16059/2020, Rv. 279407 – 02); il pagamento di fatture emesse per operazioni inesistenti, con successiva retrocessione dei relativi importi in contanti, configurandosi un impiego in attività economiche e finanziarie dell'utilità di provenienza illecita (Cass. Pen. Sez. 2, n. 9755/2020, Rv. 278513); l'esercizio di un'attività imprenditoriale attraverso un'azienda compendio del reato di bancarotta fraudolenta (Cass. Pen. Sez. 2, n. 37503/2019, Rv. 277514 – 01); il gioco d'azzardo e le scommesse (Cass. Pen. Sez. 2, n. 13795/2019, Rv. 275528; *Diff. Cass. Pen. Sez. 2, n. 9751/2019, Rv. 276499 – 01*); l'investimento dei proventi criminali in valute virtuali (Cass. Pen. Sez. 2, n. 27023/2022, cit.).

¹⁸⁹ Cfr. Cass. Pen. Sez. 2, n. 36121/2019, Rv. 276974, in *Studium juris*, 2020, 4, 501.

¹⁹⁰ Il reato di autoriciclaggio ha natura istantanea e si consuma nel momento in cui tenute le condotte di impiego, sostituzione o trasformazione di beni costituenti l'oggetto materiale del reato presupposto, nessun rilievo dovendo quindi riconoscersi, ai fini della consumazione, alla circostanza che gli effetti delle condotte indicate si protraggono nel tempo. (Cass. Pen. Sez. 2, n. 38838/2019, Rv. 277098 – 01). Il delitto di autoriciclaggio non può consumarsi, neanche nella forma tentata, prima che si perfezioni il reato presupposto (Cass. Pen. Sez. 5, n. 138/2022, Rv. 282730 – 01).

¹⁹¹ Il reato di autoriciclaggio di cui all'art. 648-ter.1 c.p., ove commesso dall'appartenente ad un'associazione per delinquere di tipo mafioso, concorre con quello di partecipazione a tale associazione aggravato dal finanziamento di attività illecite, di cui all'art. 416-bis, comma sesto, cod. pen., stante l'obiettivo diversità dei rispettivi elementi costitutivi, in quanto solo l'art. 648-ter.1 c.p., e non anche l'aggravante di cui all'art. 416-bis, comma sesto, c.p., richiede che l'autore agisca in modo da ostacolare concretamente l'identificazione della provenienza criminosa dei beni oggetto di reimpiego (Cass. Pen. Sez. 2, n. 5656/2022 Rv. 282626 – 01).

¹⁹² Si considerino i requisiti organizzativi minimi per la costituzione di un'associazione per delinquere o l'idoneità ed univocità degli atti ai fini dell'integrazione del tentativo.

comune significato descrittivo usualmente loro abbinato e percepibile dai destinatari della normativa. Del resto, l'art. 2, comma 3, del D.lgs. 231/2007 è testuale nell'affermare che l'azione di prevenzione è *“svolta in coordinamento con le attività di repressione dei reati di riciclaggio, di quelli ad esso presupposti e dei reati di finanziamento del terrorismo”*, legittimando una differenziazione di strumenti e categorie sistematiche.

Distinte sono le operazioni che concretano il riciclaggio amministrativo, di cui viene offerta una descrizione invariata rispetto alla formulazione introdotta nel 2007. Esse sono rappresentate, anzitutto, dalla conversione o dal trasferimento di beni, in quanto corredate dallo scopo di occultamento o dissimulazione della provenienza criminosa (art. 2, comma 4, lett. a). L'attitudine ad ostacolare l'identificazione della provenienza illecita si trasforma da necessaria caratteristica oggettiva dell'azione di riciclaggio penale, in scopo specifico di una delle forme dell'azione di riciclaggio nella materia amministrativa, anch'esso deducibile *“da circostanze di fatto obiettive”* (art. 2, comma 5). In alternativa alla finalità decettiva, l'azione può essere accompagnata dallo scopo di aiutare chi sia coinvolto in tale attività criminosa a sottrarsi alle conseguenze giuridiche delle proprie azioni, finalità assimilabile a quella dei reati di favoreggiamento. Costituiscono riciclaggio anche le operazioni di occultamento e dissimulazione circa la reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni (art. 2, comma 4, lett. b), condotte sovrapponibili a quelle del delitto di riciclaggio. Possono integrare, infine, riciclaggio amministrativo l'acquisto, la detenzione e l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che essi provengono da un'attività criminosa (art. 2, comma 4, lett. c). Per l'acquisto e la detenzione si tratta di condotte assimilabili a quelle della ricettazione *ex art. 648 c.p.*, della quale diverge per il difetto della caratterizzazione soggettiva (dolo specifico di profitto) e per il riferimento esclusivo a reati matrice di origine delittuosa. Quanto all'utilizzazione si tratta di condotta sovrapponibile a quella di impiego *ex art. 648-ter c.p.* e di autoriciclaggio *ex art. 648-ter.1 c.p.*, sprovvista sia della limitazione della rilevanza esclusiva in contesti economico-sociali sia di vincoli modali della condotta (per parte della giurisprudenza, non necessari neppure nell'impiego *ex art. 648-ter c.p.*). Non è scomparsa la caratteristica comune delle operazioni di riciclaggio amministrativo di costituire *“azioni”*. In precedenza, tale ultima espressione, univoca in termini letterali, apriva la descrizione delle operazioni ed era associata al predicato *“commesse”* e consentiva di escludere la rilevanza di condotte meramente omissive, almeno rispetto a comportamenti mono-soggettivi. La situazione non appare variata se si considera che tutte le operazioni del comma 4 sono descritte come *“azioni”* dal successivo comma 5.

Nella versione originaria del 2007 ulteriore connotato comune delle azioni di riciclaggio era l'*“intenzionalità”*, rilevanti *“se commesse intenzionalmente”* come rivelabile *“da circostanze di fatto obiettive”*. Ora residua solo l'indicazione che *“la conoscenza, l'intenzione o la finalità, che debbono costituire un elemento delle azioni di cui al comma 4 possono essere dedotte da circostanze di fatto obiettive”*.

In passato si era notato come ciò fosse coerente con l'autonomia della definizione di riciclaggio amministrativo. In quest'ultima, infatti, l'intenzionalità (condizione psichica dell'agente) era riferita alle azioni (ovvero alla condotta) e non ad elementi esteriori rispetto ad essa, quali i presupposti ed i risultati, né ai suoi *scopi ulteriori*, come avviene nella sistematica penalistica. Perciò si riteneva che l'intenzionalità contenesse il perimetro delle condotte d'interesse del sistema amministrativo escludendo, anzitutto, quelle non attribuibili psichicamente al soggetto (si pensi all'incoscienza indipendente dalla volontà o di forza maggiore) ovvero ammettendo solo quelle *“umane”*, originate da un impulso cosciente del volere. Inoltre, l'espressione confermava il disinteresse del sistema amministrativo per le azioni di riciclaggio colposo e preterintenzionale. Sotto questo profilo, quindi, la novella del 2017 apre ad una lettura per la quale l'intenzionalità diviene connotato riservato delle azioni che prevedono scopi decettivi o di favoreggiamento (sostanzialmente quelle *ex art. 2, comma 4, lett. a)*; invece, ferma la necessaria conoscenza dell'origine criminosa dei beni (ovvero del presupposto dell'azione) per le diverse operazioni di riciclaggio amministrativo *ex art. 2, comma 4, lett. b) e c)* (di occultamento, dissimulazione, acquisto, detenzione o utilizzazione) l'interesse preventivo si estende anche alle condotte negligenze e prive di scopi specifici.

Le azioni di riciclaggio possono essere realizzate individualmente ovvero assieme (in *“partecipazione”*) ad altre persone. In quest'ultimo caso, l'alternativa è tra un'azione in associazione con altri ovvero in concorso, nelle diversificate forme del contributo morale o materiale, situazioni evidentemente distinte, seppure non richiamate nel rigoroso significato penalistico¹⁹³. Il concorso è esemplificato dalle espressioni *“aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di*

¹⁹³ Cfr. Cass. Pen. Sez. 2, n. 16339/2013 in tema di elementi dell'associazione per delinquere.

agevolarne l'esecuzione". Il verbo "istigare" risulta provvisto di plurima valenza. Anzitutto, richiama la particolare forma di integrazione del concorso morale, quale partecipazione psichica realizzata dal soggetto che rafforza l'altrui proposito criminoso già esistente. Non ne risulta estranea quella del c.d. "determinatore", ovvero di colui che fa sorgere in altri un proposito criminoso prima inesistente, evocata altresì dall'espressione "consigliare", che richiama contributi tecnici volti a fornire all'organizzatore o all'esecutore notizie necessarie oltre che agevolatrici. Non essendo del tutto inquadrabili nelle categorie penalistiche, le forme di contributo richiamate dai termini "istigare" e "consigliare" rivelano, piuttosto, l'interesse per le più svariate configurazioni della partecipazione morale, sia essa un contributo necessario (di determinazione) o agevolatore (di rafforzamento) dell'altrui azione.

La conclusione è confortata dalla compresenza nella norma definitoria, assieme a quella di "agevolazione" dell'esecuzione, dell'espressione "aiutare", di portata descrittiva più estesa, riferibile sia alle forme di contributo morale che a quelle di contributo materiale (nelle forme del contributo fisico essenziale o agevolatore). Diversamente dall'evenienza di azione mono-soggettiva, nel caso di azione di riciclaggio amministrativo "partecipata" non può escludersi che l'agevolazione o l'aiuto possa esprimersi in forma omissiva, limitatamente ai soggetti, titolari di posizioni di garanzia e gravati di doveri di vigilanza, che omettano di impedirla. Non è estranea al significato dell'espressione "istigare" né all'impostazione preventiva del sistema, la condotta mono-soggettiva pur connotata dall'inedoneità ad integrare forme di tentativo punibile, consistendo in una sollecitazione rivolta ad altri, anche non accolta, alla commissione delle azioni tipizzate. La rilevanza di un tal contegno segnala la peculiare dilatazione dell'interesse del sistema amministrativo, maggiore di quello riconoscibile nel contesto penale, ove l'irrelevanza dell'istigazione a commettere un reato, anche accolta ma non seguita dalla commissione di esso è la regola (art. 115, commi 3 e 4, c.p.), essendo affidata alla legge la definizione delle deroghe (art. 115, comma 1, c.p.) e delle possibili conseguenze per le evenienze più gravi di istigazione a compiere delitti (art. 115, comma 4, c.p.). Inoltre, rilevante è anche solo il "tentativo" di perpetrare una delle azioni di riciclaggio amministrativo. Anche sul punto deve ribadirsi la portata settoriale della definizione, senza l'ancoraggio alle rigide condizioni di punibilità del tentativo di rilevanza penalistica, considerata la rilevanza della semplice istigazione non accolta. La circostanza consiglia di prescindere dalle caratteristiche di idoneità ed univocità delle azioni, assumendo l'interesse amministrativo per gli atti preparatori.

Altro elemento che le azioni di riciclaggio devono avere in comune è l'oggetto. Quest'ultimo è rappresentato da "beni" provenienti da "un'attività criminosa". Procedendo da quest'ultima, "l'attività criminosa" capace di originare i beni interessati dalle operazioni di riciclaggio amministrativo, sino alla novella del D.lgs. 90/2017, identificava una categoria di reati più vasta di quella prevista dagli artt. 648-*bis*, 648-*ter*.1 e 648-*ter*.c.p. e 12-*quinq*ues DL 306/1992. Tali fattispecie penali, infatti, richiedevano, quantomeno, la natura delittuosa del reato-matrice, nei primi due casi esigendo anche che le condotte di quest'ultimo fossero sostenute da elemento soggettivo non colposo. Diversamente, l'art. 2 del D.lgs. 231/2007 richiedeva solo la provenienza da un'attività criminosa che ammetteva la natura anche contravvenzionale del reato scaturigine dei beni e la consumazione di esso con contegno colposo o preterintenzionale.

Tale interpretazione era avvalorata dal dato letterale, atteso che il termine "crimine" delinea una nozione di genere, comprensiva anche dei reati contravvenzionali, oltre che coerente con la logica anticipatoria del sistema. Ulteriore conferma poteva trarsi dalla definizione di "attività criminosa" offerta dalla terza direttiva antiriciclaggio, all'art. 3, paragrafi 4 e 5, alla quale erano riconducibili molte fattispecie contravvenzionali delineate alla legislazione penale italiana. In questo quadro di approdi solidi, volti a sottrarre alibi rispetto ad inerzie o condotte attendiste giustificate dalla difficoltà di pervenire all'esatta identificazione della tipologia di reato all'origine dei beni oggetto delle condotte riciclatorie, è intervenuta la specificazione definitoria della nozione di "attività criminosa" operata dal D.lgs. 90/2017. In assenza di anticipazione nella quarta direttiva antiriciclaggio e nella L. delega 12 agosto 2016, n. 170, in seno all'art. 1, comma 2, del D.lgs. 231/2017 è stato precisato, tra le disposizioni definitorie, che "nel presente decreto si intendono per [...] b) attività criminosa: la realizzazione o il coinvolgimento nella realizzazione di un delitto non colposo". Deve trattarsi di condotta che già presenta rilevanza penale, nel caso di delitto non essendo immaginabile che non abbia attinto, almeno, il livello minimo del tentativo punibile, non configurabile per le ipotesi contravvenzionali. La portata dell'intervento è rilevante, anzitutto, proprio sotto il profilo della delimitazione dei reati all'origine dei beni, o dei diritti sui beni, suscettibili di essere interessati dalle condotte di riciclaggio amministrativo. L'art. 2, comma 4, alle lett. a), b) e c), del D.lgs. 231/2007 richiama, infatti, espressamente tale nozione di attività criminosa, connotata da una portata selettiva più intensa di quella precedente, replicando l'esclusione della rilevanza delle contravvenzioni (anche quelle a base psicologica dolosa) e dei delitti colposi, prevista, in ambito penale, per i reati di riciclaggio ed autoriciclaggio sino al 2021¹⁹⁴.

¹⁹⁴ Dopo il D.lgs. 195/2021, con l'estensione a tutti i delitti (preterintenzionali e colposi) e alle contravvenzioni (entro i limiti edittali visti) dello statuto di reati presupposto dei reati di riciclaggio in senso lato (artt. 648, 648-*bis*, 648-*ter*, 648-*ter*.1 c.p.), la limitazione introdotta dal D.lgs. 90/2017 stride con la prospettiva preventiva del sistema in cui si innesta, proteso ad allargare l'interesse verso forme anticipatorie di quelle di interesse del sistema repressivo. Lo dimostra anche l'art. 2, comma 5, del D.lgs. 231/2007 statuendo che il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali.

La latitudine dell'origine criminosa del provento si riverbera anche sulla natura di esso, ovvero sull'oggetto delle operazioni riciclatorie, commesse o tentate. L'art. 2 richiama espressamente i "beni" suscettibili di essere interessati da tutte le operazioni di riciclaggio ed i "diritti sui beni" per le operazioni di occultamento e di dissimulazione. I termini sono provvisti di ampia portata contenutistica. Ne offre significativa conferma, ancora una volta, la terza direttiva europea, alla cui stregua sono "beni" (art. 3, par. 3) "i beni di qualsiasi tipo, materiali o immateriali, mobili o immobili, tangibili o intangibili, e i documenti o gli strumenti legali, in qualsiasi forma compresa quella elettronica o digitale, che attestano il diritto di proprietà o altri diritti sui beni medesimi". Con l'inclusione dei "diritti" su tali beni (espressa per le condotte di occultamento e dissimulazione) l'oggetto delle azioni di riciclaggio amministrativo si identifica in ogni situazione giuridica di vantaggio corrispondente all'interesse del titolare, per la porzione ritenuta non compresa nella nozione di bene. L'ampio contenuto dell'oggetto interessato al riciclaggio amministrativo, in definitiva, ricalca quello più articolato proposto dalle fattispecie del riciclaggio penale ("denaro, beni o altre utilità"). L'ampiezza della nozione (estesa ad ogni genere di diritto su di essi ed a valori immateriali ed intangibili) rende solo apparente, dunque, la maggiore estensione della condotta di riciclaggio penale realizzata attraverso "altre operazioni" di ostacolo all'identificazione della provenienza criminosa di denari, beni ed utilità, le quali possono intervenire "in relazione" e non immediatamente "sul" provento illecito originario.

Ciascuna delle azioni di riciclaggio amministrativo presuppone in colui che la compie la conoscenza della provenienza criminosa del bene, che può essere dedotta "da circostanze di fatto obiettive" (art. 2, comma 4, del D.lgs. 231/2007). Tale ultima previsione richiama essenzialmente una metodologia di accertamento della consapevolezza dell'origine criminosa del bene da parte di chi realizza l'azione di riciclaggio amministrativo, ove non partecipe dell'attività criminosa generativa. Si tratta di metodo consueto per la prova degli stati psichici, organizzata sull'analisi di circostanze esteriori rivelatrici dei primi, sulle comuni regole di esperienza e sul meccanismo inferenziale. Il riferimento espresso alla metodologia di analisi dell'elemento soggettivo, quindi, finisce per operare un richiamo alle regole di comune esperienza associate alla considerazione delle circostanze di fatto rivelatrici della conoscenza. Per contro, la prova della conoscenza della provenienza criminosa nell'autore delle operazioni di riciclaggio è in re ipsa ove lo stesso sia stato "partecipe" all'attività criminosa generatrice. Nella normativa extra-penale, quella di autoriciclaggio resta una nozione parzialmente più ampia di quella penale, se si consideri l'assenza di una causa di non punibilità (ovvero di un elemento negativo del tipo legale) quale quella della destinazione alla mera utilizzazione o al mero godimento personale *ex* art. 648-ter.1, comma 4, c.p. e l'inesistenza di vincoli modali nella condotta. Per converso, la nozione amministrativa è più ridotta quanto alle attività criminose presupposte, essendo ancora presente l'ancoraggio ai delitti non colposi, superato per l'autoriciclaggio penale.

4. Il finanziamento del terrorismo (*F. Di Vizio*)

La spinta verso la condivisione a livello sovranazionale della criminalizzazione delle diverse forme di terrorismo e del loro finanziamento ha segnato l'intera evoluzione convenzionale, nella quale robusta centralità ha rivestito il momento definitorio, sotto la spinta di molteplici organismi e fonti internazionali¹⁹⁵. Le ulteriori linee di sviluppo della disciplina internazionale antiterrorismo sono rappresentate, in primis, dalla focalizzazione dell'attenzione sulle transazioni economiche e finanziarie, al fine di individuare le risorse impiegate per sovvenzionare le azioni terroristiche e i canali attraverso i quali esse pervengono alle organizzazioni; inoltre, vi è stato il potenziamento della collaborazione tra le Nazioni per prevenire lo sfruttamento dei sistemi finanziari nazionali e internazionali a fini illeciti come il finanziamento delle attività terroristiche (c.d. fenomeno money dirtying), sviluppando le forme di cooperazione giudiziaria e omogeneizzando le misure tecniche e legislative di contrasto.

¹⁹⁵ Oltre alle risoluzioni dell'Assemblea generale e del Consiglio di sicurezza dell'ONU e alle raccomandazioni del GAFI, la disciplina internazionale ha trovato uno snodo fondamentale nella Convenzione per la repressione del finanziamento internazionale al terrorismo adottata dall'Assemblea generale delle Nazioni Unite a New York il 9 dicembre 1999. In materia cfr. i trattati conclusi in seno al Consiglio d'Europa e le direttive del Parlamento europeo e del Consiglio.

Nelle tecniche di finanziamento del terrorismo sono individuate tre fasi, simmetriche rispetto a quelle del riciclaggio¹⁹⁶: la raccolta (collection), nella quale i fondi, di natura e origine sia lecita che illecita, raggiungono un collettore principale; la trasmissione o l'occultamento (transmission or dissimulation), per celare le finalità ultime dei movimenti di capitale, utilizzando sistemi di pagamento "sotterranei", "paralleli" e alternativi al circuito bancario convenzionale (underground o parallel banking systems); l'impiego (use) del denaro o degli altri beni per il compimento di atti terroristici. Il momento decettivo caratterizza le operazioni del soggetto che investe denaro per finanziare il terrorismo non tanto rispetto all'origine delle risorse, quanto sul piano della loro destinazione, cosicché la riprovazione involge prima che il meccanismo genetico delle risorse quello del loro consumo. Diversamente dal riciclaggio, infatti, le attività di finanziamento del terrorismo si prefiggono di occultarne la destinazione e si realizzano con somme anche esigue, spesso movimentate e trasferite mediante canali specifici (sistemi alternativi di trasferimento di fondi o attraverso l'interposizione di enti senza scopo di lucro), diversi da quelli finanziari ordinari. Non manca, però, una significativa affinità di funzionamento tra i movimenti di capitali diretti ad occultarne l'illecita provenienza e i flussi finanziari volti a favorire atti di terrorismo: in entrambi i casi, infatti, è consueto il coinvolgimento di canali occulti, presenti anche in settori e centri finanziari caratterizzati da forte opacità o, comunque, la realizzazione di movimentazioni finanziarie dissimulate sotto operatività e ragioni economiche fittizie. Il settore finanziario, potendo garantire un livello di opacità superiore al normale, si rivela fortemente appetibile per le organizzazioni terroristiche capaci di sfruttare le potenzialità offerte dall'integrazione globale dei mercati finanziari per trasferire capitali da un Paese all'altro senza essere identificati e senza lasciare tracce; ciò rende decisiva l'attenzione sui canali di trasferimento del denaro anche nell'azione di contrasto del finanziamento del terrorismo. Per queste ragioni gli strumenti dell'analisi finanziaria utilizzati nella lotta al riciclaggio, sono stati estesi all'azione di contrasto del finanziamento del terrorismo internazionale, per individuare e bloccare il finanziamento dell'attività terroristica.

4.1. L'evoluzione normativa nazionale del contrasto del finanziamento del terrorismo: cenni

L'adozione da parte del legislatore italiano di adeguate misure di contrasto al *terrorismo internazionale* non è avvenuta attraverso un *corpus* normativo organico e autonomo, ma mediante una disciplina frammentaria, in esito ad interventi, stratificati nel tempo, assunti con logiche emergenziali¹⁹⁷, con i quali si sono criminalizzate diverse manifestazioni, in conformità alle indicazioni sovranazionali. Nel diritto repressivo e procedurale, sono state introdotte nuove norme penali, modificate le disposizioni di ordinamento penitenziario e processuali; sul piano amministrativo, poi, sono state rafforzate le misure di prevenzione ai sensi del D.lgs. 159/2011 e introdotti nuovi sistemi di controllo finanziario e di congelamento delle risorse economiche ai sensi dei D.lgs. 231/2007 e 109/2007. *Inizialmente* il legislatore nazionale ha preferito riproporre *strumenti repressivi e istituti già sperimentati* per fronteggiare altre manifestazioni criminali di carattere associativo come la mafia o il terrorismo di matrice politica interna¹⁹⁸, adattati alle nuove contingenze¹⁹⁹. L'impianto del codice Rocco offriva un modello di progressione di tutela dalle condotte preparatorie sino all'attuazione del programma politico eversivo e garantiva l'anticipazione della tutela penale che, da strumento di lotta al "nemico politico" degli anni Trenta, si venne trasformando in strumento utile contro il nuovo nemico del "terrorista interno" degli anni Settanta del secolo scorso²⁰⁰.

Lo sviluppo del terrorismo internazionale ha importato il passaggio dalla tutela progressiva del codice Rocco alla tutela penale a "costellazione"²⁰¹, attenta alla repressione delle attività collaterali al fenomeno associativo. Nella fenomenologia del

¹⁹⁶ R. Razzante e P. Ramunno, *Riciclaggio e finanziamento al terrorismo di matrice islamica*, Filodiritto, 3.5.2007.

¹⁹⁷ M.L. Di Bitonto, *Terrorismo internazionale, procedura penale e diritti fondamentali in Italia*, in Cass. Pen., fasc. 3, 2012, p. 1181 e ss.

¹⁹⁸ F. Viganò, *Il contrasto al terrorismo di matrice islamico-fondamentalista: il diritto penale sostanziale*, in S. De Maglie e S. Seminara (a cura di), *Terrorismo internazionale e diritto penale*, Padova, 2007, p. 159.

¹⁹⁹ C. Di Stasio, *La lotta multilivello al terrorismo internazionale. Garanzie di sicurezza versus tutela dei diritti fondamentali*, Milano, 2010, 564.

²⁰⁰ M. Pelissero, *La legislazione antiterrorismo. il prototipo del diritto penale del nemico tra garanzie e rischi di espansione* in RIDPP, fasc. 2, 2020, p. 750.

²⁰¹ L'osservazione è di M. Pelissero, *op. ult. cit.*, 751.

terrorismo internazionale, infatti, la tradizionale organizzazione, asse dei reati associativi, è frequentemente disarticolata in una struttura a rete che rende più fluidi i contatti e le modalità di azione che si avvalgono dei c.d. lupi solitari²⁰², il cui collante è l'ideologia che fomenta la violenza. L'espansione e l'anticipazione della tutela penale rispetto a condotte collaterali al fenomeno associativo riflettono criminologicamente le modalità di azione delle associazioni terroristiche e di coloro che, per condivisione ideologica, programmano autonome condotte di supporto al programma²⁰³. Questo mutamento dell'indirizzo di politica criminale si è allineato con la disciplina sovranazionale che ha imposto l'anticipazione dell'intervento penale, presente anche nell'ultima direttiva dell'Unione europea (2017/541) che ha sollecitato gli Stati membri a dare rilevanza penale ad ulteriori condotte (art. 8).

Un primo gruppo di interventi ad hoc è stato realizzato solo dopo gli attentati dell'11 settembre 2001. Con il DL 18 ottobre 2001, n. 374, conv. in l. 15 dicembre 2001, n. 231, sono state operate modifiche al codice penale e al codice di procedura penale, rimodulando le norme esistenti per fronteggiare il terrorismo interno, in modo da renderle funzionali al contrasto del terrorismo internazionale. In particolare, è stato introdotto il reato di associazione con finalità di terrorismo internazionale (art. 270-*bis* c.p.), legittimando allo svolgimento delle indagini gli uffici della Procura della Repubblica presso il Tribunale del capoluogo del distretto di Corte d'appello (art. 51, comma 3-*quater*, c.p.p.) ed estendendo anche alle indagini relative al terrorismo internazionale alcune misure già previste in materia di contrasto alle organizzazioni criminali di stampo mafioso.

L'espressa riconducibilità al terrorismo internazionale della fattispecie penale dell'art. 270-*bis* c.p., con i connessi adattamenti procedurali, è risultata decisiva per agevolare il contrasto di cellule a specifica connotazione etnico-religiosa le quali, utilizzando il territorio italiano come base logistica, sostenevano l'azione di organizzazioni terroristiche operanti in altri paesi²⁰⁴. Per la Cassazione, infatti, l'originaria formulazione dell'art. 270-*bis* c.p., punendo associazioni clandestine terroristiche aventi come obiettivo la programmazione e l'esecuzione di aggressioni eversive contro lo Stato italiano (e non contro lo Stato estero) ne precludeva l'applicazione al terrorismo internazionale²⁰⁵. Inoltre, se ai fini del riconoscimento della sussistenza del reato di criminalità organizzata (di matrice eversiva o di stampo mafioso) la giurisprudenza consolidata esigeva il radicamento territoriale del gruppo, la stabilità logistica e la condivisione quasi totale tra i vari associati della conoscenza del programma e degli obiettivi a breve e medio termine dell'organizzazione di cui essi fanno parte²⁰⁶, tali caratteristiche non erano riscontrabili nell'associazione terroristica internazionale²⁰⁷. Inoltre, nella realtà fenomenica del terrorismo internazionale, soprattutto di matrice islamica, di solito l'associazione ha una struttura cellulare che si forma e rimodula diversamente in differenti contesti spazio-territoriali, nei quali gli incontri fisici tra i partecipanti del gruppo possono essere sporadici e realizzati sulla rete *internet*²⁰⁸.

A seguito della novella in commento il delitto *ex art 270-bis c.p.* è stato reso configurabile in presenza di una struttura criminale che si prefigga la realizzazione di atti violenti qualificati dalla finalità di terrorismo anche internazionale provvista della capacità di dare agli stessi effettiva realizzazione, non essendo sufficiente una mera attività di proselitismo ed indottrinamento, finalizzata ad inculcare una visione positiva del martirio per la causa islamica e ad acquisire generica disponibilità ad unirsi ai combattenti in suo nome²⁰⁹.

In presenza di una struttura organizzata sia pure in modo rudimentale il delitto di partecipazione ad un'associazione con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico, di cui all'art. 270-*bis* c.p., è ritenuto

²⁰² Cass. Pen. Sez. 1, 9 ottobre 2018, n. 51654.

²⁰³ F. Viganò, *Minaccia dei "lupi solitari" e risposte dell'ordinamento: alla ricerca di un delicato equilibrio tra diritto penale, misure di prevenzione e diritti fondamentali della persona*, in R. Kistoris e F. Viganò (a cura di), *Il nuovo pacchetto antiterrorismo*, Torino, 2015.

²⁰⁴ G. Salvini, *L'associazione finalizzata al terrorismo internazionale: problemi di definizione e prova della finalità terroristica*, in Cass. Pen., 2006, p. 3366.

²⁰⁵ Cass. Pen. Sez. VI, 30 gennaio 1996, Bendebka, in Giust. pen., 1997, c. 158. Prima della ricordata modifica dell'art. 270-*bis* c.p., la possibilità di perseguire in Italia gruppi organizzati criminali anche clandestini i quali, attraverso le attività svolte sul suolo italiano, avessero favorito la commissione di atti violenti contro l'ordinamento di Stati stranieri, era consentita nei ristretti limiti dell'associazione a delinquere (art. 416 c.p.) o di altri reati strumentali a quell'obiettivo, senza l'impiego degli strumenti investigativi processuali e penali (intercettazioni, custodia cautelare, trattamento penitenziario, ecc.) già collaudati in passato per la repressione del terrorismo interno.

²⁰⁶ E. Rosi, *Terrorismo internazionale: anticipazione della tutela penale e garanzie giurisdizionali*, in Dir. pen. proc., 2008, p. 458.

²⁰⁷ La stessa frequentemente è connotata da distanza spaziale tra singolo o singola cellula all'inizio della catena operativa, mentre l'obiettivo da colpire è affidato ad altri, ubicato in diverso luogo e non conoscibile in anticipo perché non ancora predefinito; in tema G. Salvini, *L'associazione finalizzata al terrorismo*, cit., p. 3383.

²⁰⁸ Nel senso che le strutture cellulari proprie delle associazioni criminose di matrice terroristica islamica sono caratterizzate da estrema flessibilità interna, così da rimodularsi secondo le pratiche esigenze che di volta in volta si presentano, oltre che in condizioni di operare anche contemporaneamente in più Stati, o in tempi diversi, con contatti fisici, telefonici o comunque a distanza anche sporadici cfr. Cass. Sez. fer., 18 agosto 2009, n. 34180, in Cass. pen., 2010, p. 3411.

²⁰⁹ Così Cass. Pen. Sez. 5, n. 48001/2016 Rv. 268164 - 01 ha ritenuto insussistente il delitto per la limitata operatività del gruppo mentre l'attività di mero proselitismo e indottrinamento è valutabile ai fini dell'applicazione di misure di prevenzione,

configurabile con una condotta di adesione ideologica che si sostanzia in seri propositi criminali diretti alla realizzazione delle finalità associative, senza che sia necessario, data la natura di reato di pericolo presunto, che si abbia l'inizio di materiale esecuzione del programma criminale²¹⁰. La seconda fase di potenziamento del diritto interno nel contrasto del terrorismo è riferibile al DL 27 luglio 2005, n. 144. Oltre a mutamenti di procedura penale di portata generale, il legislatore, per limitare il rischio di contrasti interpretativi, ha declinato in termini normativi la nozione di "condotta con finalità di terrorismo" (art. 270-*sexies* c.p.), introdotto le nuove fattispecie di arruolamento (artt. 270-*quater*²¹¹) e di addestramento con finalità di terrorismo anche internazionale (art. 270-*quinqüies* c.p.²¹²) ed esteso ai fatti di terrorismo internazionale istituti già previsti per il contrasto della criminalità organizzata di stampo mafioso²¹³.

Con il "pacchetto" antiterrorismo del 2015, poi, il legislatore italiano ha attuato obblighi di diritto internazionale e autorizzato un *generale arretramento della soglia di rilevanza penale, rendendo punibili alcuni atti meramente preparatori*. In dettaglio, con il DL n. 7 del 18 febbraio 2015 ha introdotto ed esteso norme penali modificando la normativa in materia di terrorismo per incriminare le condotte dei *foreign terrorist fighters*. Sono state coniate nuove fattispecie di delitto in materia di terrorismo, aggiungendo un secondo comma all'art. 270-*quater* c.p.²¹⁴, introducendo l'art. 270-*quater*.1 c.p.²¹⁵, modificando l'art. 270-*quinqüies* c.p.²¹⁶ e, da ultimo, aggiungendo la pena accessoria della perdita della potestà genitoriale, qualora coinvolto un minore, nel caso di condanna per i delitti *ex* artt. 270-*bis*, 270-*ter*, 270-*quater*, 270-*quater*.1 e 270-*quinqüies* c.p.

La legge 153/2016²¹⁷ ha operato ulteriori innovazioni nel Codice penale²¹⁸. In primo luogo, ha inserito l'art. 270-*quinqüies*.1 c.p., che punisce chiunque, al di fuori dei casi di cui agli artt. 270-*bis* e 270-*quater*.1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'art. 270-*sexies*, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte, con la reclusione da sette a quindici anni. Il secondo comma della disposizione, inoltre, prevede che chiunque deposita o custodisce i beni o il denaro indicati al primo comma è punito con la reclusione da cinque a dieci anni²¹⁹. In secondo luogo, ha introdotto gli artt. 270-*quinqüies*.2 e 270-*septies* c.p.,

²¹⁰ Così Cass. Pen. Sez. 2, n. 24994/2006 Rv. 234345 – 01.

²¹¹ Per una ricostruzione della fattispecie cfr. Cass. Pen. Sez. 4, n. 23828/2019; sulla nozione di arruolamento va segnalato il contrasto tra Cass., Sez. 1, n. 40699/2015, Elezi, Rv. 264719 e Cass. Pen. Sez. 2, n. 23618/2019; per quest'ultima la condotta di arruolamento passivo prevista dall'art. 270-*quater* comma 2 cod. pen. non è necessaria la prova del "serio accordo" con la associazione, ma è sufficiente la prova dell'integrale disponibilità del neo-terrorista al compimento di tutte le azioni necessarie al raggiungimento degli scopi eversivi propagandati da Al Qaeda.

²¹² Ai fini della configurabilità del reato di addestramento ad attività con finalità di terrorismo anche internazionale, commesso dalla persona che abbia acquisito autonomamente informazioni strumentali al compimento di atti con la suddetta finalità, è comunque necessario che il soggetto agente ponga in essere comportamenti significativi sul piano materiale, univocamente diretti alla commissione delle condotte di cui all'art. 270-*sexies* c.p., senza limitarsi ad una mera attività di raccolta di dati informativi o a manifestare le proprie scelte ideologiche (così Cass. Pen. Sez. 5, n. 22066/2020, Rv. 279495 – 02).

²¹³ G. Salvini, *I colloqui investigativi e i permessi di soggiorno a fini investigativi per il contrasto al terrorismo internazionale*, in *Le nuove norme di contrasto al terrorismo*, A.A. Dalia (a cura di), Milano, 2006, p. 2.

²¹⁴ Tale norma punisce con la pena della reclusione da cinque a otto anni, fuori dai casi di cui all'art. 270-*bis* c.p. e salvo il caso di addestramento (art. 270-*quinqüies* c.p.), la persona che viene arruolata dai soggetti che commettono il delitto di cui al primo comma; in tal modo sono incriminati i c.d. lupi solitari, soggetti i quali, pur non facendo tecnicamente parte delle associazioni di cui all'art. 270-*bis* c.p., arruolano e vengono arruolati al fine di commettere atti terroristici. In tema di arruolamento con finalità di terrorismo anche internazionale, Cass. Pen. Sez.1, n. 40699/2015, Rv. 264719 – 01.

²¹⁵ Si tratta della fattispecie di "organizzazione di trasferimenti per finalità di terrorismo" che punisce, fuori dai casi di cui agli artt. 270-*bis* e 270-*quater*, chiunque organizza, finanzia o propaganda viaggi in territorio estero, finalizzati al compimento delle condotte di cui all'art. 270-*sexies* c.p., con la pena della reclusione da cinque a otto anni. Sulla problematicità della figura criminosa e sul suo "risicato" ambito di applicazione cfr. A. Marino, *Il sistema antiterrorismo alla luce della l. 43/2015: un esempio di "diritto penale del nemico?"*, in RIDDP, fasc. 3, 2016, p. 1420 e ss.

²¹⁶ Ne è stato ampliato l'ambito di applicazione: accanto a colui il quale addestra o comunque fornisce istruzioni sulla preparazione o sull'uso di materiali esplosivi, di armi da fuoco o di altre armi, di sostanze chimiche o batteriologiche nocive o pericolose, nonché di ogni altra tecnica o metodo per il compimento di atti di violenza ovvero di sabotaggio di servizi pubblici essenziali, con finalità di terrorismo, ed alla persona addestrata, la norma punisce, adesso, anche la persona che avendo acquisito, anche autonomamente, le istruzioni per il compimento degli atti di cui al primo periodo, pone in essere comportamenti univocamente finalizzati alla commissione delle condotte di cui all'art. 270-*sexies* c.p.

²¹⁷ Per un'analisi delle soluzioni individuate dal legislatore italiano e sulla loro compatibilità con i principi costituzionali di legalità, offensività, materialità e colpevolezza cfr. A. Marino, *op.cit.*, p. 1388.

²¹⁸ Per una ricostruzione critica, cfr. A. Marino, *op. cit.*, pp. 1389-1426.

²¹⁹ La norma, finalizzata a punire il finanziamento di condotte con finalità di terrorismo, dovrebbe colmare una lacuna del sistema, incriminando i finanziatori di atti terroristici organizzati al di fuori di un'associazione *ex* art. 270-*bis* c.p.

disposizioni collegate dal punto di vista finalistico, che mirano a reprimere i focolai terroristici alla base, sottraendo loro le disponibilità materiali ed economiche²²⁰. Infine, la riforma ha inserito l'art. 280-ter c.p., rubricato "atti di terrorismo nucleare", disposizione che contiene in realtà due diverse incriminazioni, correlate strettamente alla finalità di cui all'art. 270-sexies.

La forte anticipazione della tutela e la soggettivizzazione delle fattispecie, accomunate dalla direzione finalistica della condotta, intensificano il pericolo di rarefazione dell'offensività del fatto tipico²²¹; in particolare, nelle nuove fattispecie di arruolamento, addestramento, istruzione, organizzazione di viaggi, il dolo specifico, che dovrebbe qualificare il disvalore del fatto, fatica ad assolvere la funzione penalmente tipizzante, perché sono incriminate condotte molto anticipate e distanti da quelle terminali provviste di effettiva dimensione lesiva²²².

4.2. La nozione di finanziamento del terrorismo prevista dall'art. 2, comma 6, del D.lgs. 231/2007

Il D.lgs. 90/2017 ha riscritto il D.lgs. 231/2007, apportandovi modifiche. Ai fini che interessano il novellato art. 2, comma 6, del D.lgs. 231/2007 ha esplicitato in termini più estesi la *definizione di finanziamento del terrorismo* rilevante ai fini dell'applicazione delle norme contenute nel decreto ai fini di prevenzione e contrasto dell'uso del sistema economico e finanziario a scopo di riciclaggio e finanziamento del terrorismo²²³. Ai sensi del rivisitato art. 2, comma 6, infatti, "*ai fini di cui al comma 1*", "*s'intende per finanziamento del terrorismo qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette*". Si tratta di una definizione assai ampia, coincidente con quella accolta nel linguaggio comune, in grado di comprendere attività lecite (*money transfer, hawala*) ed illecite (finanziamento attraverso fatti costitutivi di reato, come il traffico di stupefacenti o il favoreggiamento dell'immigrazione illegale)²²⁴.

La condotta, a forma libera, si qualifica per progressive tensioni finalistiche, che potrebbero definirsi di primo (verso possibili servizi di gestione di fondi e di risorse economiche) e secondo grado (verso la possibile destinazione successiva dei fondi per finalità di terrorismo).

La prima finalità dell'attività è rivelata dal predicato "diretta" e si identifica nel mero orientamento verso servizi omogenei rispetto alla natura dei fondi e delle risorse economiche (la fornitura, raccolta, la provvista, l'intermediazione, il deposito, la custodia o l'erogazione) solo apparentemente tipici poiché rilevano "in qualunque modo" realizzati, in linea con l'ampiezza contenutistica del concetto di fondi (cfr. art. 1, comma 2, lett. q, D.lgs. 231/2007; art. 1, lett. f, D.lgs. 109/2007) e di risorse economiche (cfr. art. 1, comma 2, lett. mm, D.lgs. 231/2007 e art. 1, lett. f, D.lgs. 109/2007) quali valori di origine anche leciti.

La finalità di "secondo grado" si sostanzia di una condizione potenziale, rappresentata dalla "utilizzabilità", diretta o indiretta, dei fondi, rilevanti per la loro destinabilità al compimento di una o più condotte, con finalità di terrorismo. Anche in tal caso il legislatore si preoccupa di mantenere ampio lo spazio di interesse sancendo l'irrilevanza dell'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte con finalità terroristiche.

²²⁰ Viene incriminato chiunque ponga in essere condotte di sottrazione di beni o denaro sottoposti a sequestro per finalità di prevenzione del finanziamento delle condotte terroristiche; inoltre è prevista l'obbligatorietà, alle condizioni dell'art. 270-septies c.p., della confisca dei beni, utilizzati o destinati al compimento di reati di terrorismo, nel caso di condanna per taluno dei delitti con la finalità di cui all'art. 270-sexies c.p.

²²¹ Di offensività debole parla V. Militello, *La prevenzione del terrorismo*, in Dir. pen. cont. - Riv. trim., 2017, p. 6; nella stessa prospettiva l'analisi di F. Palazzo, *Nemico-nemici-nemico: una sequenza inquietante per il futuro del diritto penale*, in RIDPP, 2/2020, p. 708.

²²² A. Cavaliere, *Considerazioni critiche intorno al DL antiterrorismo, n. 7 del 18 febbraio 2015*, in Dir. pen. cont., 31 marzo 2015; G. Leo, *Nuove norme in materia di terrorismo*, in Dir. pen. cont., 19 ottobre 2016, pp. 5 ss.; A. Peccioli, *Punibilità di atti preparatori alla realizzazione di condotte terroristiche*, in Studium iuris, 2015, pp. 770 ss.

²²³ La stessa definizione è prevista dall'art. 1, comma 1, lett. d, D.lgs. 22 giugno 2007, n. 109.

²²⁴ Cfr. M. Cerfeda, *Le 'nuove' misure di congelamento nazionali e il traffico di capitali volti al finanziamento del terrorismo*, in Dir. pen. cont. Riv. trim., 2018, 21 ss.; V. Aragona, *Il contrasto al finanziamento del terrorismo*, in Dir. pen. cont. - Riv. trim., 2017, pp. 96 ss.

Il maggior sforzo delimitativo rispetto alla precedente definizione del 2007 s'infrange contro l'ampiezza del rinvio alle *norme penali* che valgono qui a definire, *anche ai fini amministrativi* di prevenzione del finanziamento del terrorismo, la *finalità di terrorismo* delle attività. In questo caso, infatti, la definizione penalistica ha contenuti già così anticipati da non rendere necessaria una nozione settoriale amministrativa e da essere convenientemente utilizzabile a fini preventivi.

L'art. 270-*sexies* c.p. definisce la condotta terroristica sotto il profilo oggettivo in quanto in grado di "arrecare grave danno" ad un Paese o ad un'organizzazione internazionale, e, sul versante *soggettivo*, la qualifica attraverso tipici riferimenti finalistici alternativi, in quanto posta in essere "allo scopo di": (i) intimidire la popolazione; (ii) o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale.

La connotazione terroristica è prevista anche per tutte "le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia". In tal modo la portata delimitativa della definizione *ex* art. 2, comma 6, D.lgs. 231/2007, scaturente dal rinvio alla definizione della finalità di terrorismo secondo le previsioni delle leggi penali, risulta ridimensionata, operando il rinvio all'intero quadro convenzionale vincolante per l'Italia in materia.

Inoltre, l'inserimento nel codice penale, all'art. 270-*bis*.1, dell'aggravante *ex* art. 1 DL 15 dicembre 1979, n. 625, prevista per i reati commessi per finalità di terrorismo o di eversione dell'ordine democratico e ritenuta dalla giurisprudenza pacificamente applicabile a tutti i reati, stempera ulteriormente la portata selettiva della definizione.

Sotto questo profilo, piuttosto, è utile ricordare che per la finalità di terrorismo di cui all'art. 270-*sexies* del codice penale non basta che l'agente abbia intenzione di arrecare un grave danno al Paese, ma occorre che la sua condotta crei la possibilità concreta - per la natura ed il contesto obiettivo dell'azione, nonché degli strumenti di aggressione in concreto utilizzati - che esso si verifichi, nei termini di un reale impatto intimidatorio sulla popolazione, tale da ripercuotersi sulle condizioni di vita e sulla sicurezza dell'intera collettività, posto che solo in presenza di tali condizioni lo Stato potrebbe sentirsi effettivamente coartato nelle sue decisioni; non è sufficiente la direzione dell'atteggiamento psicologico dell'agente, occorrendo che la condotta posta in essere sia concretamente idonea a realizzare uno degli scopi indicati nel predetto articolo, determinando un evento di pericolo di portata tale da incidere sugli interessi dell'intero Paese²²⁵.

²²⁵ Cass. Pen. Sez. 1, n. 47479/2015.

CAPITOLO 2

Autorità

(a cura di C. Clemente)

1. Ministro e Ministero dell'Economia (*I. Borrello e V. Tusini Cottafavi*)

Il Capo II del D.lgs. 231/2007, intitolato “Autorità, vigilanza e Pubbliche amministrazioni”, delinea un “sistema” di autorità specializzate - alcune con funzioni di indirizzo e coordinamento sul piano politico/amministrativo, altre di natura eminentemente tecnica - preordinato a sviluppare una “rete” di relazioni istituzionali che, per funzionare efficacemente, esige lo sviluppo di significative sinergie.

Il sistema vede all’apice il Ministro dell’Economia e delle finanze, responsabile delle politiche e delle strategie in materia, e il Ministero, come autorità preposta all’attuazione delle medesime. Presso quest’ultimo è inoltre collocata una fondamentale istanza di coordinamento tra tutte le autorità impegnate nell’azione di prevenzione e contrasto, rappresentata dal Comitato di Sicurezza Finanziaria (CSF), organismo collegiale con rilevanti competenze decisionali e consultive.

1.1. Il Ministro dell'Economia e delle finanze

Il Ministro dell’Economia e delle finanze è l’organo di governo cui spetta di indirizzare le politiche nazionali di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, assicurandone la rispondenza formale e l’efficacia rispetto agli standard internazionali e alle regole europee. Ancorché l’azione di prevenzione e contrasto chiami in causa, a livello nazionale, l’intervento e le competenze specializzate di una pluralità di istituzioni e autorità pubbliche, alcune afferenti all’apparato amministrativo pubblico più tradizionale, altre riferibili al modello delle amministrazioni indipendenti, altre ancora appartenenti alle forze di polizia e al potere giudiziario, è nel Ministro dell’Economia che tale azione viene ricondotta a unità e riceve un impulso e un indirizzo connotati in senso marcatamente politico²²⁶.

Tale posizione del Ministro dell’Economia trova base giuridica sia nel D.lgs. 231/2007 sia nel complementare D.lgs. 109/2007, recante le disposizioni nazionali di attuazione della normativa internazionale in tema di congelamenti e sanzioni economiche, con i relativi obblighi degli operatori e competenze istituzionali.

L’art. 4, comma 1, del D.lgs. 231/2007, assegna al Ministro dell’Economia la responsabilità delle politiche di prevenzione dell’utilizzo del sistema finanziario e di quello economico per fini di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo. In tale ruolo il Ministro presenta al Parlamento, entro il 30 giugno di ogni anno, la relazione sullo stato dell’azione di prevenzione del riciclaggio e del finanziamento del terrorismo, elaborata dal Comitato di sicurezza finanziaria, alla quale è allegato il rapporto predisposto dalla UIF sull’attività svolta nonché la relazione predisposta dalla Banca d’Italia in merito ai mezzi finanziari e alle risorse ad essa attribuite. La relazione illustra in dettaglio gli aspetti qualificanti e gli esiti dell’azione di prevenzione antiriciclaggio e antiterrorismo e fornisce al Parlamento informazioni sui numeri complessivi espressi dal sistema, anche in termini statistici, e sulle attività svolte nell’anno solare precedente nell’ambito delle funzioni di vigilanza, supervisione e controllo²²⁷.

²²⁶ Nel sistema antiriciclaggio l’istanza politica mantiene fermo e preminente il proprio ruolo di titolare e garante dell’indirizzo politico, di conformazione dell’assetto regolamentare e operativo, di coordinamento e riconduzione a unità di competenze di prevenzione e contrasto “diffuse” tra una pluralità di soggetti specializzati.

²²⁷ Nella relazione sono riportati, in particolare, i dati sulle segnalazioni di operazioni sospette ricevute dalla UIF e sul relativo seguito, sui casi e i soggetti investigati dalla Guardia di Finanza e dalla Direzione Investigativa Antimafia, sulle persone indagate o sottoposte a procedimento di prevenzione, condannate per reati di riciclaggio, di autoriciclaggio o di finanziamento del terrorismo, sugli importi e sulla tipologia dei beni sequestrati e confiscati nell’ambito dei relativi procedimenti, sui congelamenti disposti ai sensi del D.lgs. 109/2007.

Ai sensi dell'art. 4, comma 3, del medesimo D.lgs. 231/2007, spetta inoltre al Ministro il compito di stabilire, su proposta del Comitato di sicurezza finanziaria, l'esenzione dall'osservanza degli obblighi antiriciclaggio per i soggetti che esercitano in modo occasionale o su scala limitata un'attività finanziaria che implichi scarsi rischi di riciclaggio o di finanziamento del terrorismo²²⁸.

L'ulteriore ambito di competenze del Ministro disciplinato dal D.lgs. 109/2007 riguarda la prevenzione del finanziamento del terrorismo e dell'attività di paesi che minacciano la pace e la sicurezza internazionale. Con le modalità e nei termini previsti da tale decreto, infatti, su proposta del Comitato di sicurezza finanziaria, il Ministro stabilisce con proprio decreto: a) le misure di congelamento dei fondi e delle risorse economiche detenuti, anche per interposta persona, da soggetti designati e le eventuali esenzioni, secondo i criteri e le procedure stabiliti da risoluzioni del Consiglio di sicurezza delle Nazioni Unite o da un suo Comitato; b) la designazione, a livello nazionale, di persone fisiche, di persone giuridiche, gruppi o entità che pongono in essere o tentano di porre in essere una o più delle condotte con finalità di terrorismo secondo quanto previsto dalle leggi penali e le misure per il congelamento dei fondi e delle risorse economiche detenuti, dai medesimi, anche per interposta persona; c) le misure di congelamento, a seguito di richiesta proveniente da uno Stato terzo, ai sensi della risoluzione n. 1373/2001 del Consiglio di sicurezza delle Nazioni Unite.

1.2. Il Ministero dell'economia e delle finanze

L'art. 5 del D.lgs. 231/2007 assegna al Ministero dell'economia, e in particolare agli uffici incardinati nel Dipartimento del Tesoro²²⁹, una serie di compiti di attuazione delle politiche di prevenzione. Il Ministero promuove innanzitutto la collaborazione e il raccordo tra le autorità²³⁰ e tra le amministrazioni e gli organismi interessati nonché tra i soggetti pubblici e il settore privato, anche tenuto conto degli standard internazionali in materia, delle analisi dei rischi di riciclaggio e di finanziamento del terrorismo elaborate dal Comitato di sicurezza finanziaria e, a livello sovranazionale, dalla Commissione europea. Tale collaborazione, che l'art. 5 lega strettamente all'attuazione delle politiche in materia, si esplica anche sul piano internazionale, con le omologhe autorità di altri paesi e con gli organismi internazionali di settore. Il Dipartimento del Tesoro cura infatti i rapporti con le istituzioni europee e gli organismi internazionali deputati all'elaborazione delle politiche e degli standard in materia di prevenzione dell'utilizzo del sistema finanziario e di quello economico per fini di riciclaggio e di finanziamento del terrorismo, assicurando l'adempimento degli obblighi derivanti dalla partecipazione dell'Italia ai tavoli internazionali. Fornisce, inoltre, il proprio contributo alla predisposizione di provvedimenti normativi a livello internazionale e coordina le delegazioni inter-istituzionali che rappresentano l'Italia nei vari *fora* nei quali si discute di temi connessi con la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo.

Fermi restando i poteri ispettivi assegnati alle altre autorità del sistema, il Ministero ha facoltà di effettuare proprie ispezioni presso i soggetti obbligati, al fine di acquisire elementi utili allo svolgimento dei procedimenti rientranti nelle proprie competenze istituzionali in materia di prevenzione²³¹.

Il ruolo del Ministero nel sistema di prevenzione si traduce anche nella predisposizione degli schemi dei provvedimenti necessari per dare attuazione alla legislazione antiriciclaggio e nella risoluzione delle

²²⁸ Lo stesso art. 4 rende espliciti i requisiti che tale attività deve presentare ai fini dell'esenzione. Essa, infatti, deve essere limitata in termini assoluti (cioè con un fatturato complessivo non eccedente una data soglia pure individuata dal CSF), deve essere limitata in base alle operazioni (cioè non eccedente una soglia massima per cliente e singola operazione, individuata dal CSF), non deve costituire l'attività principale, ma essere accessoria e direttamente collegata a quella principale, non deve essere una delle attività cui si applica la normativa europea antiriciclaggio (indicate all'art. 2, par. 1, della direttiva (UE) 2015/849) ad eccezione dei soggetti diversi dai professionisti e dagli operatori non finanziari, i quali negozino beni con pagamenti in contanti pari o superiore a euro 10.000), deve essere prestata solo ai clienti dell'attività principale e non offerta al pubblico in generale.

²²⁹ In particolare, presso la Direzione V, preposta alla prevenzione dei reati finanziari.

²³⁰ Si tratta, in particolare, del Ministero dell'Economia, delle Autorità di vigilanza di settore, della UIF, della Direzione Investigativa Antimafia, del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (cfr. art. 21, comma 2, lett. a), del D.lgs. 231/2007).

²³¹ In tale ambito, gli ispettori possono chiedere o rilevare ogni notizia o risultanza esistente presso i soggetti ispezionati. La previsione di un autonomo potere ispettivo in capo al Ministero pone un delicato tema di coordinamento con i poteri ispettivi pure assegnati alle altre autorità antiriciclaggio (tra cui, in particolare, la UIF e la Guardia di Finanza).

questioni emerse in sede operativa nell'ambito di applicazione delle suddette leggi. In tale ambito il Ministero promuove la collaborazione e il confronto delle autorità tecniche coinvolte nell'azione di prevenzione e contrasto, quali la Banca d'Italia, la UIF e la GdF. Il Ministero utilizza altresì i dati forniti dalle autorità del sistema antiriciclaggio ai fini dell'analisi nazionale del rischio (art. 14, comma 2, del D.lgs. 231/2007), assicurandone la trasmissione alla Commissione europea.

Per assicurare il rispetto della normativa antiriciclaggio al Ministero sono riconosciute competenze in materia di sanzioni amministrative pecuniarie. La potestà sanzionatoria amministrativa del Ministero prevista per alcune fattispecie di violazione della normativa antiriciclaggio può essere attivata dall'Unità di informazione finanziaria per l'Italia, dalle autorità di vigilanza di settore, dalle amministrazioni interessate, dalla Guardia di Finanza e dalla Direzione Investigativa Antimafia (DIA), le quali accertano, in relazione ai loro compiti e nei limiti delle loro attribuzioni, le violazioni e provvedono alla contestazione degli addebiti agli incolpati, trasmettendo poi gli atti al Ministero nei casi in cui il medesimo è competente per l'irrogazione delle sanzioni, ai sensi dell'art. 65 del D.lgs. 231/2007.

Il procedimento sanzionatorio, soggetto a rigorosi termini di decadenza e di prescrizione, comprende una fase istruttoria, audizioni personali e relazioni illustrative, la predisposizione del relativo decreto, la gestione del contenzioso, la fase esecutiva e la rappresentanza in giudizio dell'Amministrazione²³².

Infine, ai sensi dell'art. 51, D.lgs. 231/2007, il Ministero è destinatario delle comunicazioni da parte dei soggetti obbligati sulle infrazioni della normativa in materia di limitazioni all'utilizzo del contante (art. 49, commi 1, 5, 6, 7 e 12 e art. 50 del D.lgs. 231/2007), da inviare entro trenta giorni per la contestazione e gli ulteriori adempimenti previsti dalla legge.

2. Il Comitato di Sicurezza Finanziaria (*I. Borrello e V. Tusini Cottafavi*)

Il CSF è stato istituito con DL 12 ottobre 2001, n. 369, convertito, con modificazioni, dalla legge 14 dicembre 2001, n. 431, nell'ambito delle iniziative assunte a livello internazionale per il contrasto al terrorismo internazionale. Le sue competenze, disciplinate congiuntamente dal D.lgs. 231/2007 e dal D.lgs. 109/2007, si incentrano nella prevenzione dell'utilizzo del sistema finanziario ed economico per fini di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo nonché nel contrasto dell'attività dei paesi che minacciano la pace e la sicurezza internazionale. Il Comitato è inoltre l'autorità italiana responsabile per l'attuazione delle misure di congelamento dei fondi e delle risorse economiche di persone fisiche, giuridiche, gruppi o entità disposte dalle Nazioni unite e dall'Unione europea per contrastare e reprimere il finanziamento del terrorismo nonché per il contrasto dell'attività dei paesi che minacciano la pace e la sicurezza internazionale.

Il CSF è presieduto dal Direttore Generale del Tesoro e ha una composizione molto ampia e variegata, comprendendo rappresentanti del Ministero dell'Economia e delle Finanze, del Ministero dell'Interno, del Ministero della Giustizia, del Ministero degli Affari Esteri, della Banca d'Italia, della Commissione nazionale per le società e la borsa, dell'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo, dell'Unità di informazione finanziaria, della Guardia di Finanza, della Direzione Investigativa Antimafia, dell'Arma dei Carabinieri e della Direzione Nazionale Antimafia. Il CSF è inoltre integrato da rappresentanti designati, rispettivamente, dal Ministero dello Sviluppo Economico e dall'Agenzia delle Dogane ai fini dello svolgimento dei compiti relativi al contrasto della proliferazione delle armi di distruzione di massa.

Il presidente può altresì invitare a partecipare alle riunioni, senza diritto di voto, rappresentanti di altri enti o istituzioni, inclusi rappresentanti dei servizi per la informazione e la sicurezza, secondo le materie all'ordine del giorno e, ove sia necessario per acquisire pareri ed elementi informativi, rappresentanti dei consigli nazionali degli ordini professionali e delle associazioni private di categoria.

Il funzionamento del CSF è regolato dal decreto del Ministero dell'economia del 22 aprile 2022, n. 59. Questa norma disciplina anche le categorie di documenti, formati o comunque rientranti nella

²³² Per dettagli sul procedimento si rinvia alla specifica trattazione della materia contenuta nel presente volume.

disponibilità del Comitato, sottratti al diritto di accesso ai documenti amministrativi ai sensi dell'art. 24, commi 1, lett. a), e 2, della legge 7 agosto 1990, n. 241.

Il CSF si riunisce su iniziativa del presidente ovvero su richiesta di uno dei suoi componenti²³³, su convocazione della segreteria tecnica (le cui funzioni sono assicurate dalla Direzione V del Dipartimento del Tesoro del Ministero) previo invio dell'ordine del giorno²³⁴.

Il Comitato si avvale, per lo svolgimento delle proprie attività, di una "rete di esperti" che lo coadiuva e supporta nelle questioni di cui è competente. La rete, composta da rappresentanti designati dalle amministrazioni che compongono il Comitato, svolge un'attività di analisi, coordinamento e sintesi sulle questioni all'ordine del giorno delle riunioni, raccoglie informazioni a supporto dei lavori ed esamina ulteriori argomenti su richiesta dello stesso Comitato.

2.1. Le funzioni e il ruolo del CSF

Nell'ambito dell'azione di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, il CSF contribuisce alla definizione delle politiche in materia, presenta una relazione annuale con valutazioni e proposte, esercita funzioni di coordinamento e analisi, formula pareri.

I compiti del Comitato sono richiamati dall'art. 5, comma 5, del D.lgs. 231/2007 e successive modifiche, in base al quale il CSF esercita i poteri e le funzioni previsti dal [D.lgs. 109/2007](#), recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei paesi che minacciano la pace e la sicurezza internazionale, elabora le strategie di prevenzione del riciclaggio e di finanziamento del terrorismo e coordina le misure di contenimento del relativo rischio da parte delle autorità antiriciclaggio. L'art. 5, comma 6, del D.lgs. 231/2007 elenca poi nel dettaglio tali compiti, stabilendo che il CSF:

- a) elabora l'analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo;
- b) propone al Ministro dell'Economia, ai fini dell'adozione dei relativi decreti, le misure nazionali di designazione e congelamento dei fondi e delle risorse economiche detenuti, anche per interposta persona, da persone fisiche, persone giuridiche, gruppi o entità che commettono, o tentano di commettere, atti di terrorismo;
- c) propone al Ministro dell'Economia l'esenzione di taluni soggetti dall'osservanza degli obblighi antiriciclaggio, al ricorrere dei presupposti di cui all'art. 4, comma 3 (limitatezza dell'attività finanziaria in termini assoluti o per numero di operazioni, carattere non principale dell'attività finanziaria);
- d) formula pareri e proposte e fornisce consulenza al Ministro dell'Economia e delle finanze in materia di prevenzione del riciclaggio e di finanziamento del terrorismo.

In base alle richiamate disposizioni, le competenze del CSF possono essere ricondotte a due distinti ambiti: quello connesso con la legislazione antiriciclaggio e quello relativo all'attuazione degli obblighi internazionali in materia di prevenzione e contrasto del finanziamento del terrorismo. Nel primo, in particolare, il CSF rappresenta l'organo di raccordo e coordinamento del contributo dei vari attori del sistema. Questo ruolo trova due importanti momenti di sintesi nell'analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo e nella relazione annuale sulla valutazione dell'attività di prevenzione, dei relativi risultati e delle proposte per renderla più efficace.

La posizione del CSF, se analizzata in relazione a quella del Ministro dell'Economia, si rivela centrale nell'apparato antiriciclaggio, poiché in essa si sostanzia una fondamentale istanza di coordinamento e di garanzia di funzionalità dell'intero sistema. In numerosi e rilevanti snodi del funzionamento del sistema, infatti, poteri decisionali o consultivi sono assegnati al Comitato invece che al Ministro, anche se

²³³ Il CSF è regolarmente costituito quando sono presenti almeno i due terzi delle amministrazioni ivi rappresentate e delibera a maggioranza dei presenti. Il Comitato può altresì assumere decisioni e deliberare attraverso scambio di messaggi di posta elettronica certificata, su proposta del presidente.

²³⁴ Ciascuna amministrazione rappresentata nel Comitato designa preventivamente un supplente, da nominarsi con decreto del Ministro dell'Economia, che sostituisce il membro effettivo in caso di impedimento e partecipa alle riunioni con diritto al voto.

l'interazione tra i due soggetti istituzionali evidenzia i caratteri di una forte integrazione organizzativa e funzionale. Il CSF è la sede per il raccordo tra le amministrazioni e gli enti operanti nel campo della prevenzione, per l'emanazione dei pareri previsti dalla legge e per la valutazione dell'efficienza e dell'efficacia dell'azione antiriciclaggio. Il Comitato è anche dotato di poteri particolarmente penetranti, come quello di acquisire informazioni in possesso delle amministrazioni in esso rappresentate, anche in deroga al segreto d'ufficio, ai fini della predisposizione dell'analisi nazionale del rischio²³⁵. Inoltre secondo quanto previsto dall'art. 3, comma 7, del D.lgs. 109/2007 con riguardo alla prevenzione e contrasto del finanziamento del terrorismo, gli enti rappresentati nel Comitato comunicano allo stesso, "in deroga ad ogni disposizione vigente in materia di segreto di ufficio le informazioni riconducibili alle materie di competenza del Comitato medesimo". Infine, per le finalità di cui allo stesso D.lgs. 109/2007, il Comitato ha la facoltà di chiedere accertamenti agli enti in esso rappresentati, tenuto conto delle rispettive attribuzioni²³⁶.

Il ruolo del CSF, come definito dalle norme, risponde all'esigenza di ricondurre a sintesi e unità l'elevata articolazione e specializzazione delle competenze coinvolte nel sistema, garantendo altresì che autorità di diversa estrazione (politica, tecnica, investigativa e giudiziaria) possano far sentire la propria voce nella definizione delle politiche e nell'esercizio delle rispettive competenze²³⁷.

A tale scopo sembrano rispondere, in modo particolare, sia la funzione consulenziale, volta a inquadrare attività ed esigenze specifiche in una visione unitaria rispondente alla logica complessiva e sistematica imposta dalla normativa, sia l'analisi dei rischi e l'elaborazione della relazione annuale (contenente anche la valutazione dell'attività di prevenzione e le proposte dirette a renderla più efficace), atti nei quali vengono composti in una sintesi organica gli apporti tecnico/specialistici delle varie autorità presenti nel Comitato, allo scopo di restituire una immagine unitaria del sistema e delle politiche che lo governano.

Assume specifico significato, nel caso del CSF, il modello di coordinamento analizzato fin dagli anni '50 del secolo scorso da Vittorio Bachelet con riferimento all'amministrazione pubblica dell'economia²³⁸, quale formula organizzatoria in grado di rispondere all'allora crescente complessità e disarticolazione dell'assetto organizzativo dei pubblici poteri, fornendo una sorta di "collante giuridico" alle esigenze di prontezza e flessibilità dell'azione²³⁹.

Si realizza, nel Comitato, la composizione di interessi di diversa estrazione e natura, la riconduzione a unità delle politiche pubbliche in tema di prevenzione e contrasto secondo l'indirizzo definito dal Ministro dell'economia, nonché la riduzione di possibili "asimmetrie informative" in funzione dell'allineamento e della condivisione dei dati utili per assumere ogni decisione. Ne deriva una forma di coordinamento tecnico/politico "plurilaterale", essenziale per dare impulsi univoci e condurre a coerenza la complessità, pur salvaguardando l'autonomia e la specializzazione delle istanze e delle funzioni che ne sono espressione.

²³⁵ Cfr. art. 14, comma 3.

²³⁶ In tali casi è stato giustamente notato come sia ipotizzabile una "formidabile eccezione alla natura meramente consultiva e/o deliberativa del consesso antiterrorismo, giacché il conferimento *ope legis* da parte delle istituzioni e degli organismi di propri rappresentanti all'interno del CSF ... determina una vera e propria soggezione, ossia un *pacti* rispetto alle istanze di accertamento che l'organo collegiale abbia ad articolare" (così A. Cisterna, *La convergenza del molteplice. Cooperazione istituzionale e organizzazione delle Istituzioni*, in GNOSIS, n. 1/2010).

²³⁷ Il che rappresenta uno scostamento rispetto all'assetto dell'ordinamento finanziario, per molto tempo dominato dal dibattito dottrinale circa la natura (politica o amministrativa) del CICR, risolto nei termini di una mera legittimazione (o copertura) politica rispetto ad atti di regolazione e controllo del mercato sostanzialmente riferibili all'autorità tecnica indipendente della Banca d'Italia. La tesi della natura politica del CICR individuava nel Comitato una formula organizzatoria per il coordinamento dell'attività di governo e di deconcentrazione del Consiglio dei ministri, assegnando all'organo funzioni e competenze di vero e proprio indirizzo politico. Sul ruolo politico del CICR cfr. F. Merusi, *Le direttive governative nei confronti degli enti di gestione*, Milano, 1965; Id., *Commento all'art. 2*, in F. Capriglione (a cura di), *Commentario al Testo Unico delle Leggi in materia bancaria e creditizia*, 4^a ed., Padova, 2018; G. Quadri, *Diritto pubblico dell'economia*, Padova, 1980; S. Merlini, *Struttura del governo e intervento pubblico nell'economia*, Firenze, 1979; A. Mattioni, *Comitati interministeriali*, in *Enc. giur.*, IV, *ad vocem*, Milano, 1988; F. Capriglione, *L'ordinamento finanziario verso la neutralità*, Padova, Cedam, 1994.

²³⁸ V. Bachelet, *L'attività di coordinamento nell'amministrazione pubblica dell'economia*, Milano, 1957, in *Scritti giuridici*, vol. III, *Interessi sociali e intervento pubblico nell'economia*, Milano, 1981, p. 83. V. Bachelet, *Coordinamento*, in *Enc. Dir.*, Milano, 1962, vol. X, p. 632. V. anche M. D'Alberti, *Coordinamento amministrativo: immagini per la ricerca del concetto*, in G. Amato e G. Marongiu (a cura di), *L'amministrazione della società complessa*, Padova, 1982, p. 57.

²³⁹ Cfr., in particolare, G. Di Gaspare, *Indirizzo e coordinamento nell'ordinamento repubblicano nel pensiero di Vittorio Bachelet*, in *Amministrazioni in cammino*, luglio 2022.

2.2. L'analisi nazionale dei rischi e la relazione annuale

Il Comitato di sicurezza finanziaria, nell'esercizio delle competenze in materia di prevenzione, analizza e valuta il rischio nazionale di riciclaggio di denaro e di finanziamento del terrorismo, individuando le minacce più rilevanti e le vulnerabilità del sistema nazionale di prevenzione, di investigazione e di repressione, i metodi e i mezzi di svolgimento di tali attività e i settori maggiormente esposti al rischio. L'analisi ha cadenza triennale, salva la facoltà del CSF di procedere al relativo aggiornamento quando insorgono nuovi rischi e ogni qualvolta lo ritenga opportuno. Essa persegue l'obiettivo di identificare, analizzare e valutare le minacce di riciclaggio e di finanziamento del terrorismo, individuando quelle più rilevanti, i metodi di svolgimento di tali attività criminali, le vulnerabilità del sistema nazionale di prevenzione, di investigazione e di repressione di tali fenomeni e, quindi, i settori maggiormente esposti a tali rischi²⁴⁰.

L'analisi nazionale dei rischi, condotta nel rispetto dei principi internazionali in materia e dei risultati della relazione periodica sui rischi che gravano sul mercato europeo redatta dalla Commissione europea, tiene altresì conto dei dati quantitativi e statistici forniti dalle autorità che compongono il sistema antiriciclaggio, dalle amministrazioni e organismi interessati e dagli organismi di autoregolamentazione²⁴¹.

L'analisi può essere integrata dal contributo di rappresentanti della Presidenza del Consiglio dei ministri e di altre amministrazioni con competenze specifiche su temi di interesse e può avvalersi della collaborazione di studiosi e rappresentanti del mondo accademico e delle associazioni private rappresentative delle categorie interessate.

Le conclusioni riflettono la valutazione condivisa dei fenomeni, delle minacce e delle vulnerabilità, raggiunta da tutte le autorità coinvolte nel sistema antiriciclaggio partendo da informazioni, dati e valutazioni provenienti da patrimoni informativi eterogenei. Esse costituiscono la base per un effettivo coordinamento strategico delle *policy* in materia.

I risultati dell'analisi, con le modalità e nei termini stabiliti dal Comitato, sono resi disponibili ai soggetti obbligati e agli organismi di autoregolamentazione ai fini della valutazione, da parte dei medesimi, dei rischi di riciclaggio e di finanziamento del terrorismo cui sono esposti nell'esercizio della propria attività e della predisposizione di misure proporzionali e adeguate al rischio rilevato. I risultati sono altresì comunicati alla Commissione europea, alle autorità di vigilanza europee e alle autorità rilevanti di altri Stati membri che ne facciano richiesta.

L'art. 5, comma 7, del D.lgs. 231/2007 prevede che il Comitato presenti al Ministro dell'economia, entro il 30 maggio di ogni anno, per il successivo inoltro al Parlamento, una relazione contenente la valutazione dell'attività di prevenzione del riciclaggio e del finanziamento del terrorismo, dei relativi risultati e delle proposte dirette a renderla più efficace. Tale documento, pure riferito dalla legge alla competenza del CSF, raccoglie i dati statistici e le informazioni sulle attività svolte, nell'anno solare precedente, nell'ambito delle funzioni di vigilanza, supervisione e controllo, dalla UIF, dalle autorità di vigilanza di settore, dalle amministrazioni e organismi interessati, dagli organismi di autoregolamentazione, dalla Guardia di finanza e dalla Direzione Investigativa Antimafia (a questo fine tali autorità forniscono al CSF i dati di propria competenza entro il 30 marzo di ogni anno).

Ancorché la legge ascriva sia l'analisi dei rischi sia la relazione alle competenze del CSF, occorre sottolineare che tali documenti appaiono piuttosto il frutto di un'azione comune e congiunta tra le autorità del sistema, che il CSF favorisce, coordina e sintetizza e da cui il Ministro può trarre significative indicazioni di policy per il miglioramento del quadro normativo e delle strategie di prevenzione e contrasto.

²⁴⁰ L'esercizio, condotto per la prima volta nel 2014 in applicazione della Raccomandazione n. 1 del GAFI e aggiornato nel 2018, intende favorire l'elaborazione di linee di intervento per la mitigazione dei rischi, secondo un approccio *risk-based* nell'attività di contrasto al riciclaggio e al finanziamento del terrorismo, ispirato al principio di proporzionalità delle politiche e delle misure rispetto ai rischi da fronteggiare.

²⁴¹ Tali autorità, in particolare, forniscono al Comitato ogni informazione utile, anche in deroga al segreto d'ufficio, riferiscono periodicamente sugli esiti delle analisi di rispettiva competenza, anche al fine di individuare tipologie di clientela, prodotti, operazioni che per caratteristiche operative o geografiche necessitano di specifici interventi, utilizzano l'analisi ai fini della definizione delle priorità e della distribuzione delle risorse necessarie a migliorare il sistema nazionale di prevenzione e contrasto e a ottimizzare l'esercizio delle proprie competenze in funzione del livello di rischio. Le stesse autorità, in occasione della relazione annuale, riferiscono al CSF delle misure e dei presidi adottati al fine di mitigare i rischi riscontrati in sede di analisi.

2.3. I poteri di proposta, decisionali e consultivi

Il CSF è inoltre titolare di poteri di proposta, decisionali e consultivi, la cui previsione è contenuta in singole disposizioni della normativa antiriciclaggio. Quanto ai poteri propositivi, rileva quello previsto dall'art. 4, comma 3, del decreto, che il CSF esercita nei confronti del MEF al fine di stabilire, in base a criteri pure individuati dal CSF²⁴², l'esenzione dall'osservanza degli obblighi antiriciclaggio per taluni soggetti che esercitano un'attività finanziaria in modo occasionale o su scala limitata.

I poteri decisorii riguardano essenzialmente i doveri antiriciclaggio a carico delle pubbliche amministrazioni previsti dall'art. 10 del decreto. In tale ambito, infatti, il CSF, in funzione del rischio di riciclaggio o di finanziamento del terrorismo e anche sulla base dell'analisi nazionale del rischio, può escludere talune categorie di attività amministrative dagli obblighi previsti dalle norme, ovvero individuare procedimenti amministrativi ulteriori rispetto a quelli previsti, ai quali applicare gli obblighi antiriciclaggio (art. 10, comma 2). Il CSF, inoltre, elabora linee guida per la mappatura e la valutazione dei rischi di riciclaggio e finanziamento del terrorismo cui gli uffici delle pubbliche amministrazioni sono esposti nell'esercizio della propria attività istituzionale.

Infine, il CSF svolge un diffuso ruolo consultivo, che permea tutti gli snodi più rilevanti dell'azione antiriciclaggio posta in essere dalle autorità che compongono il sistema.

La legge prevede che la UIF senta il CSF prima dell'emanazione o dell'aggiornamento degli indicatori di anomalia volti ad agevolare l'individuazione delle operazioni sospette (art. 6, comma 4), nonché prima dell'adozione delle istruzioni alle pubbliche amministrazioni sui dati e sulle informazioni da trasmettere, le modalità e i termini della relativa comunicazione nonché gli indicatori per agevolare la rilevazione delle operazioni sospette (art. 10, comma 4). Il CSF esprime il proprio parere anche sulle regole tecniche adottate dagli organismi di autoregolamentazione, nonché in materia di procedure e metodologie di analisi e valutazione del rischio al quale sono esposti i professionisti, di controlli interni, di adeguata verifica e di conservazione (art. 11, commi 2 e 4-*bis*).

La UIF informa tempestivamente il CSF delle attività e degli strumenti con cui provvede alla disseminazione delle informazioni relative alle proprie analisi strategiche e fornisce al CSF, con cadenza semestrale, una relazione sintetica che informa in ordine al numero e alla tipologia delle informazioni disseminate e fornisce riscontro sulle attività intraprese a seguito del loro utilizzo.

La UIF sente il CSF in occasione della definizione dei criteri per l'approfondimento finanziario delle segnalazioni di operazioni sospette (art. 40, comma 1). Inoltre, la stessa UIF, la Guardia di Finanza e la Direzione Investigativa Antimafia sentono il CSF in vista dell'adozione, anche sulla base di protocolli d'intesa, delle misure necessarie ad assicurare la riservatezza dell'identità dei segnalanti ovvero di coloro che sono tenuti a fornire ulteriori informazioni utili ai fini dell'analisi delle segnalazioni e dell'approfondimento investigativo (art. 40, comma 3). La UIF sente il CSF anche prima dell'emanazione di istruzioni volte a individuare le operazioni, i dati e le informazioni in materia di comunicazioni oggettive (art. 47, comma 3). L'Agenzia delle dogane e dei monopoli, nell'esercizio delle proprie competenze e attribuzioni istituzionali nel comparto del gioco pubblico, verifica l'osservanza degli adempimenti cui, ai sensi del presente articolo, i concessionari sono tenuti e, previa presentazione al Comitato di sicurezza finanziaria, emana linee guida ad ausilio dei concessionari, adottando ogni iniziativa utile a sanzionarne l'inosservanza (art. 52, comma 4).

2.4. Le proposte di designazione e le procedure di congelamento

Una specifica disciplina è dettata con riferimento all'attività che il CSF svolge attraverso proposte indirizzate alle competenti autorità delle Nazioni unite e dell'Unione europea per la designazione o per la cancellazione di individui o entità dalle apposite liste, per l'attività di valutazione delle istanze di esenzione dal congelamento di fondi e risorse economiche e per la ricezione dei provvedimenti di irrogazione delle sanzioni per le violazioni degli obblighi previsti in materia (artt. da 4-*ter* a 4-*septies* del D.lgs. 109/2007).

²⁴² La proposta di esenzione fa riferimento ai seguenti requisiti: a) l'attività finanziaria è limitata in termini assoluti (cioè con fatturato complessivo non eccedente la soglia determinata dallo stesso CSF); b) l'attività finanziaria è limitata a livello di operazioni (cioè non eccede una soglia massima per cliente e singola operazione, individuata, in funzione del tipo di attività finanziaria, dal CSF); c) l'attività finanziaria non è l'attività principale (cioè il relativo fatturato non eccede il 5 per cento del fatturato complessivo); d) l'attività finanziaria è accessoria e direttamente collegata a quella principale; e) l'attività principale non è menzionata nella direttiva, ovvero l'attività finanziaria è prestata solo ai clienti dell'attività principale e non è offerta al pubblico in generale.

Il Comitato, sulla base delle informazioni fornite dalle forze di polizia²⁴³, di quelle provenienti da autorità internazionali e Stati esteri, ovvero altrimenti acquisite²⁴⁴, può formulare alle competenti autorità internazionali delle Nazioni unite e dell'Unione europea, proposte motivate di designazione di individui o entità da inserire nelle relative liste. A tal fine, il Comitato può tenere conto di elementi di fatto che indichino una partecipazione attiva o di supporto ad attività terroristiche, dell'esistenza di procedimenti penali, della idoneità degli elementi informativi ad assicurare la corretta identificazione dei soggetti, di eventuali relazioni con individui o entità già inseriti nelle liste, dell'adozione di altre misure sanzionatorie nei confronti dello stesso soggetto, nonché di ogni informazione rilevante in suo possesso.

Tramite il Ministero degli affari esteri, il Comitato può contattare lo Stato o gli Stati di cittadinanza e residenza di individui o entità di cui intende proporre l'inserimento nelle liste, al fine di ottenere informazioni aggiuntive rispetto a quelle già in suo possesso. Inoltre, al fine di assicurare il coordinamento internazionale, il Comitato può condividere le proprie proposte con gli organismi che svolgono simili funzioni negli altri paesi.

L'avvenuto inserimento nelle liste è notificato agli interessati²⁴⁵ e comunicato, a cura della Segreteria del Comitato, a tutte le amministrazioni rappresentate nel Comitato stesso.

L'Unità di informazione finanziaria agevola la diffusione dell'inserimento nelle liste dei soggetti sia presso gli intermediari finanziari sia presso i collegi e gli ordini professionali.

Il Comitato, di propria iniziativa o su richiesta motivata del soggetto interessato ovvero nell'ambito delle procedure internazionali, può anche formulare (dandone comunicazione allo Stato designante) proposte di cancellazione dalle liste internazionali di individui o entità, tenendo conto dell'esito dell'eventuale procedimento penale e di ogni altro elemento rilevante che indichi l'assenza di un coinvolgimento attuale in qualsiasi attività che abbia finalità di terrorismo²⁴⁶.

Infine, il Comitato è destinatario di istanze motivate e documentate volte a richiedere esenzioni dal congelamento e individua le relative modalità di autorizzazione.

3. Unità di informazione finanziaria per l'Italia (C. Clemente e I. Borrello)

L'Unità di informazione finanziaria per l'Italia (UIF) costituisce il nodo nazionale della rete mondiale delle *Financial Intelligence Unit (FIU)*, da intendersi come "unità centrali nazionali che, al fine di combattere il riciclaggio e il finanziamento del terrorismo, sono incaricate di ricevere (e, se consentito, di richiedere), analizzare e trasmettere alle competenti autorità le segnalazioni di informazioni relative a presumibili proventi di reato o a ipotesi di finanziamento del terrorismo ovvero richieste da leggi o regolamenti nazionali"²⁴⁷.

²⁴³ Le forze di polizia, d'intesa con l'autorità giudiziaria quando necessario, trasmettono la propria proposta motivata di segnalazione di soggetti al Comitato indicando: a) i fatti accertati e i riscontri emersi nell'attività di indagine; b) il ruolo, i capi di imputazione e l'impianto probatorio a carico di ciascun indagato; c) le fonti e le tecniche di finanziamento dell'attività terroristica; d) gli elementi utili per la corretta identificazione dei soggetti segnalati; e) ogni altro elemento indiziario o probatorio che ritengano opportuno.

²⁴⁴ Per ogni segnalazione pervenuta, il Comitato può attivare la Guardia di Finanza per l'acquisizione dei precedenti fiscali e sviluppare gli accertamenti riguardanti la posizione economica, finanziaria e patrimoniale dei soggetti in via di designazione.

²⁴⁵ Comunicando altresì: a) la parte pubblica dei motivi che sono a fondamento della decisione di inserimento; b) le misure di congelamento loro imposte; c) gli effetti delle misure di congelamento e le sanzioni per la loro inosservanza; d) i casi in cui è possibile chiedere la cancellazione dalle liste; e) l'autorità, nazionale ed internazionale, competente a ricevere la richiesta di cancellazione; f) i presupposti e le modalità per richiedere l'autorizzazione in deroga; g) le autorità, nazionali, ed internazionali, competenti a ricevere i ricorsi avverso i provvedimenti adottati. Il Comitato riesamina periodicamente e sulla base di quanto stabilito dagli organismi internazionali, la posizione dei soggetti inseriti nelle liste internazionali al fine di assicurare l'aggiornamento delle informazioni e verificare la permanenza delle condizioni che hanno determinato l'inserimento dei loro nominativi.

²⁴⁶ In caso di cancellazione dalle liste, il Comitato provvede alla restituzione delle risorse economiche secondo quanto previsto dall'art. 12, comma 12 del decreto legislativo 22 giugno 2007, n. 109. La UIF cura la diffusione della cancellazione dalle liste dei soggetti di cui al comma 1 sia presso gli intermediari finanziari sia presso i collegi e gli ordini professionali.

²⁴⁷ Si fa qui riferimento alla nozione ufficiale di FIU, elaborata nel 1996 dal Gruppo Egmont, organismo internazionale che riunisce le FIU di tutto il mondo, creato nel 1995 per promuoverne lo sviluppo, stimolarne la collaborazione e il reciproco scambio di informazioni, elaborare standard e pratiche comuni. La definizione di FIU adottata da Egmont è ampia e flessibile, poiché tesa a favorire la cooperazione, a livello internazionale, tra autorità di diversa natura e con diversa organizzazione in ogni Stato. Per un quadro d'insieme sulle caratteristiche istituzionali e le funzioni delle FIU, si veda International Monetary Fund-World Bank, *Financial Intelligence Units: an overview*, IMF Legal Dept., Monetary and Financial Systems Dept, World Bank, Financial Market Integrity Div., Washington, D.C., 2004.

Questa nozione di FIU, recepita in numerosi consessi internazionali²⁴⁸, ha trovato una consacrazione definitiva negli standard del GAFI²⁴⁹ e, in particolare, nella Raccomandazione n. 29, che individua nella FIU l'istituzione centrale del sistema preventivo antiriciclaggio e antiterrorismo e ne definisce le relative funzioni: “*a national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly*”. Inoltre, le FIU rientrano tra le “*competent authorities*” che, in base alla Raccomandazione n. 40, devono poter scambiare informazioni in modo costruttivo ed efficace e cooperare a livello internazionale, in modo spontaneo o su richiesta, attraverso canali dedicati e sicuri²⁵⁰.

I caratteri essenziali, i requisiti e i poteri delle FIU sono stati confermati dal diritto europeo²⁵¹, che qualifica le FIU come autorità “centrali nazionali” nel sistema di prevenzione. Alla definizione di “FIU” si ricollegano le funzioni di “ricezione” delle segnalazioni di operazioni sospette (ma anche di altre comunicazioni utili per gli approfondimenti), di “analisi” finanziaria dei casi di effettivo interesse e di “disseminazione”, spontanea o su richiesta, dei risultati delle analisi effettuate.

In base alla nozione appena illustrata, tra gli elementi che accomunano le FIU vi sono almeno i seguenti: la specializzazione delle funzioni, che qualifica le FIU quali centri nazionali di convergenza delle informazioni su operazioni sospette, di analisi e approfondimento finanziario di tali informazioni, di trasmissione e condivisione delle stesse informazioni - e dei risultati delle analisi - con altre autorità nazionali e con omologhe autorità estere; la posizione centrale a livello nazionale, che implica che ogni Stato - anche a ordinamento federale - abbia un'unica struttura nazionale incaricata di ricevere e analizzare le segnalazioni e di rappresentare il Paese nelle sedi della cooperazione internazionale²⁵²; l'autonomia e l'indipendenza dal punto di vista operativo, che rappresentano condizioni essenziali per preservare l'efficacia delle funzioni istituzionali da indebite influenze o interferenze²⁵³; la capacità di cooperare, a livello domestico e internazionale, in modo da assicurare il costante coordinamento e la condivisione di principi e obiettivi con le altre autorità coinvolte nel sistema nazionale antiriciclaggio (autorità di settore, organi investigativi, autorità giudiziaria), e garantire efficaci scambi di informazioni con le FIU di altri paesi, per l'analisi di operazioni che presentano caratteristiche transnazionali²⁵⁴.

Gli *standard* internazionali e le disposizioni del diritto europeo (in particolare, la terza e la quarta direttiva antiriciclaggio), individuano come vincolo essenziale, per l'efficace svolgimento dell'attività di una FIU, l'integrazione di informazioni eterogenee (di natura amministrativa, finanziaria, investigativa o giudiziaria), da acquisire presso organismi e soggetti diversi: le FIU devono pertanto godere di poteri informativi sufficientemente incisivi, accedere a informazioni “multidisciplinari”, richiedere agli stessi segnalanti “tutte le informazioni necessarie” per la propria attività di analisi delle operazioni segnalate. Oltre alle operazioni sospette, alle FIU possono essere segnalate anche altre informazioni (ad esempio,

²⁴⁸ Tra cui la Convenzione di Palermo delle Nazioni Unite sulla criminalità organizzata transnazionale del 2000 e la Convenzione di Merida delle Nazioni Unite contro la corruzione del 2003.

²⁴⁹ Nella più recente edizione, risultante dall'aggiornamento complessivo effettuato nel 2012. Cfr. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>.

²⁵⁰ La nota interpretativa alla stessa Raccomandazione n. 40, stabilisce, in particolare, che le FIU dovrebbero scambiare informazioni con le proprie controparti straniere, indipendentemente dalla loro natura istituzionale (“*regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature*”), con un'adeguata base legale che le ponga in grado di effettuare e soddisfare richieste di cooperazione accedendo al più ampio ambito di informazioni disponibili e utilizzando canali sicuri ed efficaci per gli scambi.

²⁵¹ In particolare, la direttiva (UE) 2015/849(UE) e la direttiva 2018/843, rispettivamente del 27 maggio 2015 e del 30 maggio 2018.

²⁵² La peculiare posizione istituzionale nonché l'indipendenza e l'autonomia consentono a ogni FIU nazionale, a prescindere dalla natura, di fungere da elemento di raccordo fra le diverse autorità nazionali (di polizia, giudiziarie, di vigilanza finanziaria) coinvolte a vario titolo nella prevenzione e nel contrasto del riciclaggio (*clearing house function*), nonché di svolgere un delicato ruolo di coordinamento sia dell'attività interna sia di quella concernente la cooperazione internazionale con le altre FIU. Cfr. IMF-WB, *Financial Intelligence Units: an overview*, cit.

²⁵³ Tra i fattori che rilevano, al riguardo, vi sono la collocazione istituzionale, che deve assicurare una chiara separazione delle funzioni della FIU, i meccanismi di nomina dei vertici, l'obbligo di rendere conto del proprio operato e dei risultati conseguiti.

²⁵⁴ Le oltre 160 FIU appartenenti al Gruppo Egmont, connesse da sistemi telematici di comunicazione, danno vita a una rete particolarmente vasta e capillare per lo scambio di informazioni, che spesso consente di individuare fondi di provenienza illecita collocati in altri paesi, di ricostruire la titolarità effettiva degli interessi coinvolti, di acquisire elementi rilevanti per lo svolgimento efficace della cooperazione giudiziaria internazionale, alla quale molto spesso la collaborazione tra le FIU risulta propedeutica. Cfr. Egmont Group of Financial Intelligence Units, *Principles for Information Exchange between Financial Intelligence Units*, 2013.

su operazioni in contanti, bonifici, transazioni di valore superiore a soglie determinate, trasferimenti transfrontalieri al seguito di denaro, ecc.).

Purché sia assicurata la presenza delle caratteristiche e degli elementi di centralità appena citati, gli *standard* internazionali lasciano agli Stati la facoltà di scegliere la soluzione istituzionale e organizzativa più idonea per la propria FIU. L'osservazione comparata rivela come nel panorama internazionale le FIU abbiano collocazioni e connotazioni istituzionali differenti, che consentono di ascriverle a diversi "modelli", di tipo investigativo, giudiziario, amministrativo ovvero misto, a seconda del differente approccio nazionale.

Se la collocazione di una FIU all'interno di strutture di polizia (*law enforcement model*) o del sistema giudiziario (*judicial model*) presenta il vantaggio della maggiore fluidità con cui le informazioni finanziarie dovrebbero giungere agli organi investigativi o alla magistratura, consentendo - almeno in astratto - un sollecito avvio delle fasi di investigazione e repressione dei reati, l'istituzione presso autorità amministrative, quali ad esempio ministeri o banche centrali (*administrative model*), pone maggiore enfasi sulla preliminare valutazione della fondatezza della segnalazione, sull'arricchimento della stessa con ulteriori dati rilevanti per l'analisi, sulla costruzione di un patrimonio informativo destinato a dare impulso e orientamento alla successiva attività di indagine. Questa soluzione istituzionale assicura quindi una netta distinzione tra la vera e propria attività di prevenzione (nella quale l'*intelligence* finanziaria consente di isolare i casi effettivamente rilevanti)²⁵⁵ e quella incentrata sulla investigazione e repressione dei reati. Evita, inoltre, il coinvolgimento diretto dei segnalanti in attività investigative e, al contrario, incentiva la dialettica tra essi e l'autorità pubblica destinataria delle segnalazioni.

Vi sono anche paesi che si sono orientati per l'istituzione di FIU caratterizzate da differenti combinazioni dei modelli descritti in precedenza. Questa tipologia "ibrida" tenta di combinare gli elementi e le caratteristiche di tipo amministrativo, di polizia e giudiziario, al fine di beneficiare dei vantaggi rivenienti da ciascun modello, ma rischia di attenuare i vantaggi della specializzazione che connota ciascuno di essi. Riflessioni compiute su come l'adozione dei diversi modelli si riflette sulle caratteristiche delle FIU²⁵⁶, talune recenti riforme introdotte in paesi europei e la stessa natura del nuovo Meccanismo europeo di coordinamento e supporto delle FIU tendono a privilegiare il modello amministrativo.

3.1. Il modello italiano: dall'UIC alla UIF

La legge 5 luglio 1991, n. 197, che introdusse nell'ordinamento italiano il primo sistema di prevenzione e contrasto del riciclaggio basato sulla collaborazione attiva degli intermediari bancari e finanziari²⁵⁷, prevedeva che le segnalazioni di operazioni sospette fossero inviate alle questure; il Nucleo speciale di polizia valutaria della Guardia di Finanza (NSPV) aveva il compito di effettuare i successivi approfondimenti investigativi.

Pochi anni dopo, il legislatore perveniva a una radicale modifica del meccanismo di segnalazione con l'adozione di un modello amministrativo di FIU. Il D.lgs. del 26 maggio 1997, n. 153, infatti accentrava le funzioni di ricezione delle segnalazioni presso l'Ufficio Italiano dei Cambi (UIC), prevedendo l'interposizione di tale Ufficio tra i soggetti tenuti alle segnalazioni e gli organi investigativi. La riforma intendeva favorire lo sviluppo della collaborazione attiva degli intermediari, prevedendo anche appositi presidi volti a tutelare la riservatezza dell'identità delle persone fisiche segnalanti.

Con la riforma del 1997, ispirata dal convincimento che nel contrasto al riciclaggio fosse opportuno separare la fase preventiva da quella repressiva, si posero inoltre le basi per lo sviluppo della funzione di analisi finanziaria, quale fonte di arricchimento delle segnalazioni di operazioni sospette. In particolare, il D.lgs. 153/1997 attribuì all'UIC la facoltà di acquisire ulteriori informazioni presso i soggetti segnalanti; utilizzare archivi e dati in proprio possesso o comunque ad esso accessibili; effettuare approfondimenti

²⁵⁵ Cfr. M. Van de Broek, *Preventing Money Laundering*, Eleven, 2015.

²⁵⁶ Cfr. D. Bartolozzi, M. Gara, D.J. Marchetti, D. Masciandaro, *La governance delle autorità nazionali antiriciclaggio (FIU): teoria, istituzioni ed evidenze empiriche*, Working Paper dell'Università Bocconi n. 126, dicembre 2019.

²⁵⁷ La legge includeva tra i soggetti obbligati alla segnalazione, oltre alle banche e agli altri intermediari finanziari, anche gli uffici della pubblica amministrazione.

coinvolgendo le competenze delle autorità di vigilanza di settore²⁵⁸; scambiare informazioni con omologhe autorità antiriciclaggio estere, anche attraverso la sottoscrizione di appositi *memoranda of understanding*²⁵⁹.

Nel 1998 - nell'ambito del processo di adeguamento della normativa nazionale in materia di gestione delle riserve valutarie al Sistema europeo delle Banche Centrali, - il D.lgs. 319, qualificava l'UIC come *ente strumentale* della Banca d'Italia, con specifici presidi di autonomia e indipendenza, attribuendo all'Ufficio, "a titolo principale e diretto", i compiti antiriciclaggio, da esercitare sotto l'"alta vigilanza" del Ministro del Tesoro.

Nel 2000, la legge 388 (legge finanziaria per il 2001), riconobbe all'UIC la qualifica di Unità di informazione finanziaria per l'Italia (artt.150 e 151). Il medesimo provvedimento rafforzò la posizione dell'UIC, attribuendo a tale Ufficio nuovi poteri, come l'emanazione di "*indicazioni*" per la rilevazione di operazioni sospette e l'archiviazione delle segnalazioni manifestamente infondate. Tali poteri, oltre a rappresentare un significativo potenziamento del ruolo di filtro tra segnalanti e autorità investigative, abbinati alla prevista "*informazione di ritorno*" al segnalante (c.d. *feedback negativo*), erano suscettibili di migliorare la qualità della collaborazione degli intermediari, favorendo l'individuazione di comportamenti ai quali ricollegare ipotesi di riciclaggio²⁶⁰.

Nel 2007, il D.Lgs 231 di recepimento della terza direttiva antiriciclaggio²⁶¹ istituiva l'Unità di Informazione Finanziaria (UIF), collocandola presso la Banca d'Italia in posizione di indipendenza e autonomia funzionale. L'Unità subentrava pertanto all'UIC, contestualmente soppresso, nelle funzioni di ricezione, analisi e trasmissione alle competenti autorità investigative delle informazioni sulle ipotesi di riciclaggio o finanziamento del terrorismo.

Gli interventi normativi di recepimento delle successive direttive europee emanate in materia (decreti legislativi n. 90/2017 e n. 125/2019) hanno mantenuto fondamentalmente intatte le caratteristiche essenziali dell'apparato di prevenzione del 2007, consolidando comunque il ruolo della UIF quale autorità di raccordo tra la platea dei segnalanti e le autorità investigative e giudiziaria.

Le principali disposizioni sulla UIF sono contenute negli artt. 6, 13-*bis* e 40 del D.lgs. 231/2007 e successive modifiche e integrazioni. Tali articoli definiscono le caratteristiche istituzionali, le funzioni e i poteri, la capacità di collaborazione internazionale, l'analisi e lo sviluppo delle segnalazioni di operazioni sospette. Le disposizioni tendono a recepire le prescrizioni contenute nelle direttive europee antiriciclaggio che, a loro volta, riflettono le indicazioni contenute nei principi internazionali sulla posizione istituzionale, sulle funzioni e sull'organizzazione delle *Financial Intelligence Units* (FIU). Andrebbero tuttavia compiuti ulteriori passi verso una maggiore adesione ai principi stabiliti dalle norme europee, in particolare in materia di estensione del perimetro delle collaborazioni con le diverse autorità e di accesso alle informazioni, aspetti che, peraltro, sono stati affrontati in più occasioni anche in sede parlamentare²⁶².

²⁵⁸ All'UIC erano altresì assegnate, d'intesa con le autorità preposte alla vigilanza di settore, funzioni ispettive sull'osservanza da parte degli intermediari bancari e finanziari sia delle norme restrittive in materia di trasferimento di valori sia di quelle in materia di segnalazione delle operazioni sospette.

²⁵⁹ L'attribuzione all'UIC del potere di sospendere - anche su richiesta degli Organi investigativi - l'esecuzione delle operazioni segnalate, rendeva evidente come l'interposizione di un'autorità specializzata tra i segnalanti e gli Organi investigativi consentisse l'utilizzo di canali di comunicazione informale con i primi, volti anche a garantire la necessaria tempestività degli interventi.

²⁶⁰ L'accentramento delle funzioni antiriciclaggio presso l'UIC ha consentito, nel tempo, a nuovi soggetti inseriti tra i destinatari degli obblighi antiriciclaggio (come ad esempio, i professionisti, ad opera del D.lgs. 56/2004, di recepimento della seconda direttiva) di sviluppare, anche per il tramite delle rispettive associazioni di categoria, un proficuo dialogo finalizzato a chiarire i problemi applicativi e a far emergere diversi profili di criticità.

²⁶¹ La normativa, nel confermare i tradizionali presidi di prevenzione, fondati sull'imposizione di obblighi di adeguata verifica della clientela, di registrazione delle transazioni finanziarie e di segnalazione delle operazioni sospette in capo a un'ampia platea di operatori economici qualificati, li ascriveva alla generale finalità di tutela dell'integrità del sistema economico e finanziario e della correttezza dei comportamenti e stabiliva la necessità di coordinamento tra l'azione di prevenzione e quella repressione, considerate in modo distinto ma poste in stretta correlazione.

²⁶² Si veda, al riguardo, Camera dei Deputati, XVII Legislatura, *Atto del Governo n. 389, Schema di decreto legislativo recante attuazione della direttiva (UE) 2015/849, Parere favorevole delle Commissioni riunite II (Giustizia) e VI (Finanze) con condizioni e osservazioni*, recante esplicite indicazioni sull'opportunità di estendere il novero di autorità con cui la UIF può scambiare informazioni, indicazioni poi non recepite dal Governo. Per osservazioni e considerazioni di dettaglio sul punto, cfr. anche C. Clemente, *Andizione del Direttore dell'Unità di Informazione Finanziaria per l'Italia davanti alle Commissioni riunite II (Giustizia) e VI (Finanze) della Camera dei Deputati*, Roma, 27 marzo 2017.

3.2. La UIF: inquadramento istituzionale e aspetti organizzativi

Nel collocare l'Unità di informazione finanziaria nella Banca d'Italia, il legislatore ha confermato la preferenza per un modello di autorità amministrativa le cui funzioni beneficiano anche dello *status* di indipendenza caratteristico della Banca centrale. Tale collocazione garantisce inoltre la piena autonomia nella gestione delle segnalazioni di operazioni sospette, poiché valorizza e distingue l'approfondimento finanziario delle stesse rispetto all'analisi investigativa; pone l'accento sulla funzione di collegamento e di filtro assegnata alla FIU, a tutela dell'integrità del sistema finanziario ed economico; distingue il momento della prevenzione da quello della successiva repressione del reato; fa leva sulla collaborazione tra la FIU e i soggetti segnalanti, incardinata in un vero e proprio rapporto fiduciario tutelato dal segreto d'ufficio. La scelta sottolinea inoltre l'intenzione di valorizzare il patrimonio delle informazioni contenuto nelle segnalazioni di operazioni sospette attraverso l'utilizzo delle specifiche competenze di carattere finanziario presenti nella Banca centrale, presupposto per lo sviluppo delle capacità di *intelligence* dell'Unità.

Si tratta di un approccio coerente con la missione affidata alla UIF, che non è la repressione dei reati (spettante invece all'insieme delle forze di polizia), bensì lo svolgimento di un'azione di prevenzione diretta a tutelare anche l'integrità del sistema finanziario ed economico e a favorire la correttezza dei comportamenti²⁶³.

Complementare alla posizione di indipendenza e autonomia è la previsione di un dovere di rendicontazione dell'attività svolta: in base all'art. 6, comma 8, del D.lgs. 231/2007, entro il 30 maggio di ogni anno il Direttore della UIF trasmette al Ministro dell'economia, per il tramite del CSF, un rapporto sull'attività svolta, unitamente a una relazione della Banca d'Italia in merito ai mezzi finanziari e alle risorse attribuite all'Unità. Tale documentazione è allegata alla relazione sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, elaborata dal Comitato di sicurezza finanziaria (art. 5, comma 7), e presentata dal Ministro dell'economia al Parlamento, entro il 30 giugno di ogni anno (art. 4, comma 2).

La soggettività della UIF è fortemente ancorata alle funzioni ad essa assegnate dall'ordinamento²⁶⁴: l'Unità non ha personalità giuridica e la sua organizzazione e il suo funzionamento sono disciplinati con un regolamento del Governatore della Banca d'Italia²⁶⁵. In base alla legge (art. 6, comma 1) e al regolamento, la stessa Banca attribuisce alla UIF mezzi finanziari, beni strumentali, risorse umane e tecniche per l'efficace perseguimento degli scopi istituzionali, in coerenza con il principio internazionale di adeguatezza delle risorse a disposizione delle FIU.

Al Direttore della UIF, nominato con provvedimento del Direttorio della Banca d'Italia, su proposta del Governatore della Banca, tra persone dotate di adeguati requisiti di onorabilità, professionalità e conoscenza del sistema finanziario²⁶⁶, compete in autonomia la responsabilità della gestione dell'Unità, di

²⁶³ Sul punto v. C. Clemente, *L'Unità di Informazione Finanziaria per l'Italia nel sistema di prevenzione del riciclaggio*, Intervento al convegno su "Legalità e buon funzionamento del sistema finanziario", Roma, Banca d'Italia, 4 febbraio 2014; Id., *Prevention and Suppression of Money Laundering. The Evolution in Italy and the Role of the UIF*, in M. Ventura, A. Palmieri, R. Pavoni, G. Milani (ed.), *Boosting European Security Law and Policy*, Edizioni Scientifiche Italiane, Collana: Studi «Pietro Rossi» Napoli 2021.

²⁶⁴ La specificità di queste ultime, oltre a giustificare l'indipendenza e autonomia accordate dalla legge, fa della UIF un centro di imputazione, coordinamento e canalizzazione di dati e informazioni di rilevante interesse pubblico. Così G. Castaldi, *L'Unità di informazione finanziaria (UIF): funzioni e organizzazione*, Intervento del Direttore dell'UIF al convegno "Normativa antiriciclaggio. Evoluzione del quadro regolamentare e connessi aspetti procedurali e operativi", Sassari, Camera di Commercio, 17 aprile 2009; Id., *L'Unità di informazione finanziaria (UIF) nel "sistema" italiano antiriciclaggio: l'attività svolta; i problemi aperti*, Intervento del Direttore dell'UIF al seminario "Normativa antiriciclaggio a tutela del mercato", Napoli, 2 luglio 2009; C. Clemente, *L'Unità di Informazione Finanziaria per l'Italia nel sistema di prevenzione del riciclaggio*, cit.; Id., *L'Unità di Informazione Finanziaria per l'Italia nel sistema di contrasto alla criminalità economica e al riciclaggio*, Audizione davanti alla Commissione parlamentare d'inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali anche straniere, Roma, 11 giugno 2014; Id., *L'azione di prevenzione e contrasto del riciclaggio*, Testimonianza del Direttore dell'Unità di Informazione Finanziaria davanti alla Commissione Parlamentare d'inchiesta sul fenomeno della mafia, Roma, 28 giugno 2011.

²⁶⁵ Il primo regolamento fu emanato il 21 dicembre 2007 (G.U. 9 gennaio 2008, n. 7); esso è stato rinnovato il 29 gennaio 2019 (G.U. 28 maggio 2019, n. 123) e, da ultimo, il 2 novembre 2022 (G.U. 11 novembre 2022, n. 264).

²⁶⁶ In particolare, il Direttore non deve essere stato sottoposto a misure di prevenzione né condannato per delitti non colposi e deve aver maturato una adeguata esperienza professionale e di conoscenza del sistema finanziario. Egli può essere sollevato dall'incarico con le medesime modalità prescritte per la nomina, solo se non soddisfa più alle condizioni richieste per l'espletamento delle sue funzioni o si è reso colpevole di gravi mancanze. Il mandato ha la durata di cinque anni ed è rinnovabile una sola volta.

cui definisce gli indirizzi e pianifica, dirige e controlla l'attività, assicurandone una conduzione integrata e unitaria. Egli adotta gli atti e i provvedimenti attribuiti dalla legge alla competenza dell'UIF e sovrintende al funzionamento della struttura, esercitando il coordinamento tra le unità che la compongono. Il Direttore della UIF è coadiuvato da un Vice Direttore (nominato dal Governatore, sentito il Direttorio e il Direttore della UIF, tra i dirigenti centrali della Banca d'Italia), che lo affianca e lo sostituisce in caso di assenza o impedimento.

Presso la UIF è costituito un "Comitato di esperti", composto dal Direttore della UIF, che lo presiede, e da quattro membri nominati con decreto del Ministro dell'economia e delle finanze, sentito il Governatore della Banca d'Italia (art. 6 comma 3). Il Comitato svolge funzioni di consulenza e ausilio a supporto dell'azione della UIF e, a tal fine, segue l'attività dell'Unità e fornisce contributi di riflessione sulle principali attività istituzionali. Il Comitato cura la redazione di un parere sull'azione dell'UIF che forma parte integrante della documentazione trasmessa dal Ministro dell'Economia, per il tramite del Comitato di Sicurezza Finanziaria, al Parlamento, in allegato alla relazione sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo (D.lgs. 231/2007, art. 4, comma 2).

3.3. I compiti della UIF

Nell'apparato antiriciclaggio, la UIF svolge un ruolo di raccordo tra i soggetti privati, sui quali grava l'obbligo delle segnalazioni (intermediari finanziari, professionisti e operatori non finanziari) e l'autorità investigativa e giudiziaria. Questo ruolo si sostanzia nell'esercizio di compiti di analisi operativa e strategica, ispettivi, regolatori e di collaborazione istituzionale, sia con le autorità di vigilanza nazionali e con gli altri soggetti coinvolti a vario titolo nell'attività di prevenzione, sia con le omologhe strutture di informazione finanziaria degli altri Stati²⁶⁷.

Come si è detto, l'attività principale e caratteristica dell'Unità, quale FIU per l'Italia, è quella di ricezione delle segnalazioni di operazioni sospette, di analisi e approfondimento finanziario delle stesse segnalazioni e di conseguente disseminazione di quelle rilevanti per il seguito investigativo e giudiziario.

Il processo di analisi finanziaria si articola in una serie di attività volte a selezionare le segnalazioni di operazioni sospette meritevoli di approfondimento, valutarne l'effettivo grado di rischio e definirne il trattamento con il ricorso a una pluralità di fonti informative²⁶⁸. Le segnalazioni sono trattate e selezionate tramite sistemi automatici, arricchite attraverso la consultazione di archivi e di fonti aperte, classificate in base al rischio e alla tipologia di operazione, valutate in base alla rilevanza e, infine, "disseminate" alle competenti autorità investigative. Questa sequenza, in cui si sostanzia il "ciclo" dell'*intelligence* finanziaria, costituisce il fulcro dell'attività della UIF, tesa ad ampliare l'originario contesto segnalato, identificare soggetti e legami oggettivi, ricostruire i flussi finanziari sottostanti all'operatività descritta, individuando operazioni e contesti riconducibili a finalità di riciclaggio o di finanziamento del terrorismo²⁶⁹. Si tratta di un'attività di carattere conoscitivo²⁷⁰, che si inserisce all'interno di una fase che precede l'eventuale attività investigativa. A seguito della segnalazione, infatti, la UIF procede a un esame dei fatti riferiti, mediante un'attività amministrativa di verifica che non rappresenta esercizio del potere-dovere di

²⁶⁷ Per un inquadramento generale delle funzioni della UIF cfr. G. Castaldi, *L'Unità di informazione finanziaria (UIF) nel "sistema" italiano antiriciclaggio: l'attività svolta; i problemi aperti*, Napoli, 2 luglio 2009; Id., *L'azione di prevenzione e contrasto del riciclaggio*, Audizione alla Commissione Parlamentare d'inchiesta sul fenomeno della mafia e sulle altre associazioni criminali anche straniere, Roma, 28 giugno 2011; I. Borrello, *Financial Intelligence Unit (FIU)*, in D. Siclari (ed.), *Italian Banking and Financial Law, Vol. I, Supervisory Authorities and Supervision*, Palgrave Macmillan, 2015, pp. 295 ss.; C. Clemente, *L'Unità di Informazione Finanziaria per l'Italia nel sistema di prevenzione del riciclaggio*, cit.; C. Clemente, *L'Unità di Informazione Finanziaria per l'Italia nel sistema di contrasto alla criminalità economica e al riciclaggio*, 11 giugno 2014, Audizione alla Commissione d'inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali anche straniere, Senato della Repubblica, Roma, 2014; UIF, *Rapporto annuale sull'attività svolta*, Roma, anni vari.

²⁶⁸ Nel corso dell'approfondimento delle segnalazioni la UIF può acquisire ulteriori informazioni presso i segnalanti, utilizzare informazioni e dati in proprio possesso, avvalersi degli archivi ai quali ha accesso, scambiare informazioni con omologhe autorità antiriciclaggio estere. L'approfondimento, che può estendersi a operazioni sospette non segnalate di cui la UIF venga comunque a conoscenza, è svolto secondo un approccio basato sul rischio di riciclaggio. G. Castaldi, *La segnalazione delle operazioni sospette all'Unità di informazione finanziaria (UIF). Obblighi e responsabilità*, Intervento al convegno "Legalità, antiriciclaggio e rischi professionali: il fenomeno, il ruolo delle imprese e degli operatori del settore finanziario", Castelnovo del Garda, 31 gennaio 2012.

²⁶⁹ La segnalazione consente anche di valutare la capacità dello stesso segnalante di riconoscere operazioni anomale, di valutarne il rischio in termini di riciclaggio e di dotarsi di assetti organizzativi, procedure e controlli atti a consentire il presidio dei rischi e la tempestiva intercettazione di fenomeni anomali. Cfr. C. Clemente, *L'attività dell'Unità di Informazione Finanziaria per l'Italia*, Audizione alla 6^a Commissione (Finanze e Tesoro) del Senato della Repubblica, Roma, 18 settembre 2018.

²⁷⁰ J.F. Thony, *Processing Financial Information in Money Laundering Matters: the Financial Intelligence Units*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 3, pp. 257-282, 1996.

provvedere, né si inserisce all'interno di un contesto formalmente procedimentalizzato²⁷¹ secondo i tradizionali canoni del diritto amministrativo²⁷².

In relazione all'esito delle proprie analisi, la UIF trasmette le segnalazioni al Nucleo speciale di polizia valutaria della Guardia di finanza (NSPV) e alla Direzione Investigativa Antimafia (DIA), che ne informano il Procuratore nazionale antimafia qualora siano attinenti alla criminalità organizzata. Comunica altresì all'Autorità giudiziaria i fatti di possibile rilevanza penale²⁷³.

In base all'art. 6, comma 4, lett. c, del D.lgs. 231/2007, la UIF può anche sospendere operazioni sospette per un massimo di cinque giorni lavorativi, d'iniziativa o su richiesta del NSPV, della DIA, dell'Autorità giudiziaria o di un'altra FIU, sempre che ciò non pregiudichi il corso delle indagini. Il provvedimento di sospensione è adottato in stretto coordinamento con le autorità inquirenti²⁷⁴. I profili di urgenza e indifferibilità, in uno con la spiccata finalità preventiva²⁷⁵, sembrano consentire di ricondurre tale potere al più generale "potere cautelare" della pubblica amministrazione. Inoltre, la natura fortemente limitativa della sfera giuridica degli interessati ne evidenzia il contenuto marcatamente precettivo.

Il D.lgs. 231/2007 assegna alla UIF anche poteri ispettivi (art. 6, comma 4, lett. f), e comma 5, lett. a); art. 40, comma 1, lett. a), del D.lgs. 231/2007). L'attività ispettiva della UIF è tesa ad accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione, ad acquisire dati e informazioni presso i soggetti obbligati, ad approfondire, sotto il profilo finanziario, le segnalazioni ricevute e le ipotesi di operazioni sospette non segnalate di cui l'Unità venga a conoscenza²⁷⁶.

Al fine di promuovere condizioni di efficace collaborazione attiva da parte dei segnalanti, l'art. 6, comma 4, lett. d), assegna alla UIF il compito di emanare istruzioni sul contenuto delle segnalazioni di operazioni sospette, da pubblicarsi in Gazzetta Ufficiale²⁷⁷.

²⁷¹ Ciò, tuttavia, non esclude che l'attività che precede la trasmissione della relazione tecnica possa essere preventivamente disciplinata e regolata dall'UIF. Si tratterebbe, comunque, di una disciplina idonea ad introdurre vincoli flessibili e, comunque, derogabili ogni qualvolta ciò venga imposto dalla particolare complessità degli approfondimenti istruttori o da particolari esigenze di celerità nella prevenzione della fattispecie di riciclaggio.

²⁷² Il carattere "pre-istruttorio" dell'analisi finanziaria rende difficilmente applicabili ad essa talune garanzie tipiche dell'azione amministrativa (come quelle partecipative e di termine del procedimento previste dalla legge n. 241/1990): nella fase di analisi, infatti, non vale l'obbligo di fissare un termine, né vale il termine di novanta giorni in caso di mancata fissazione; inoltre, l'unico interesse qualificato del segnalante, lungi dal consentirgli alcun accesso ai documenti o di pretendere il necessario avvio dell'analisi, è quello di conoscere se la UIF decida o meno di trasmettere la segnalazione alle autorità investigative, al fine di stabilire il rapporto più adeguato con il cliente segnalato: ma tale interesse trova già tutela autonoma grazie alla norma contenuta nell'art. 41, comma 2, D.lgs. 231/2007, che prevede che la UIF, con modalità idonee a garantire la tutela della riservatezza, comunichi al segnalante gli esiti delle segnalazioni, anche tenendo conto delle informazioni ricevute dalla DIA e dal NSPV.

²⁷³ I compiti di analisi sono meglio specificati dall'art. 40, comma 1, lett. a), del D.lgs. 231/2007, secondo cui la UIF effettua, "avvalendosi dei risultati delle analisi e degli studi compiuti nonché delle risultanze della propria attività ispettiva, approfondimenti sotto il profilo finanziario delle segnalazioni ricevute nonché delle ipotesi di operazioni sospette non segnalate" di cui comunque viene a conoscenza. A tal fine, ai sensi delle lett. b), c), d) ed e), la UIF "effettua, sulla base di protocolli d'intesa, approfondimenti che coinvolgono le competenze delle autorità di vigilanza di settore", "trasmette alla Direzione Nazionale Antimafia e Antiterrorismo i dati relativi alle segnalazioni delle operazioni sospette ricevute, per la verifica dell'eventuale attinenza a procedimenti giudiziari in corso", "trasmette, senza indugio, le segnalazioni che presentano un rischio di riciclaggio o di finanziamento del terrorismo e i risultati delle analisi svolte, incluse le informazioni ad esse pertinenti relative ai reati presupposto associati, alla DIA e al Nucleo speciale di polizia valutaria della Guardia di Finanza, che ne informano il Procuratore nazionale antimafia e antiterrorismo, qualora siano attinenti alla criminalità organizzata". In base allo stesso comma, lett. f), la UIF mantiene evidenza per dieci anni delle segnalazioni non trasmesse, mediante procedure che consentano, sulla base di protocolli d'intesa, la consultazione agli Organi investigativi.

²⁷⁴ Per un'analisi generale del potere di sospensione nel contesto dei poteri di una FIU cfr. K. Stroligo, H. Intscher, S. Davis-Crockwell, *Suspending Suspicious Transactions*. World Bank, Washington, DC. 2014.

²⁷⁵ La sospensione è infatti volta a evitare che lo svolgimento dell'operazione sospetta possa configurare una definitiva "consumazione" dell'attività di riciclaggio, con conseguente svuotamento dell'effettività dell'azione istituzionale di prevenzione propria della UIF. La misura della sospensione è funzionale all'adozione del sequestro giudiziario e presuppone l'attivazione dell'Autorità Giudiziaria anche al fine di evitare che il provvedimento possa ostacolare l'attività investigativa.

²⁷⁶ Rispetto a funzioni ispettive formalizzate e "normate" (come, ad esempio, quelle tributarie), l'attività ispettiva della UIF non viene direttamente disciplinata dalle norme attributive del potere. Essa trova fondamento sostanziale nella più generale funzione di controllo che il D.lgs. 231/2007 attribuisce alla stessa UIF: da questo punto di vista, le relative ispezioni trovano un limite precipuo nella pertinenza dell'oggetto ispezionato all'attività da controllare.

²⁷⁷ La UIF ha dato attuazione a questa norma con il provvedimento del 4 maggio 2011. Cfr. Unità di Informazione Finanziaria per l'Italia, *Istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette*, 4 maggio 2011, in G.U. n. 269 del 19 novembre 2018. Le Istruzioni perseguono l'obiettivo del miglioramento qualitativo delle segnalazioni, assicurando alle stesse completezza e tempestività.

Ai poteri di regolazione appena richiamati possono essere assimilati anche quelli che attribuiscono alla UIF il compito di elaborare ed emanare “indicatori di anomalia” (comma 4, lett. e) dell’art. 6), volti a richiamare l’attenzione degli operatori su tipiche e ricorrenti situazioni e condotte che potrebbero risultare sospette²⁷⁸. Un ulteriore ausilio per agevolare l’individuazione delle operazioni da segnalare, complementare agli indicatori, è offerto dai modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario (art. 6, comma 7, lett. b), D.lgs. 231/2007), attraverso i quali la UIF, con proprie comunicazioni, porta all’attenzione degli operatori possibili anomalie emergenti in specifici settori dell’attività economica o relative a specifiche categorie di transazioni.

Accanto all’analisi operativa, tra le funzioni istituzionali della UIF rientra anche l’individuazione e la valutazione di fenomeni e tendenze, nonché di punti di debolezza del sistema antiriciclaggio previsti dall’art. 6, comma 7, lett. a), del D.lgs. 231/2007. Attraverso questa tipologia di analisi (analisi strategica), che gli standard internazionali pongono tra le attività tipiche e qualificanti di ogni FIU, la UIF elabora e raccorda le informazioni derivanti dall’approfondimento delle segnalazioni di operazioni sospette, dall’analisi di dati aggregati, dall’attività operativa, dalla collaborazione con autorità nazionali e internazionali e dagli accertamenti ispettivi, al fine di indirizzare la propria azione istituzionale, programmare le attività, selezionare gli obiettivi prioritari da perseguire. Tra le finalità dell’analisi strategica rientra anche la valutazione del rischio di coinvolgimento in operazioni di riciclaggio e finanziamento del terrorismo del sistema economico-finanziario nel suo complesso o di aree geografiche, mezzi di pagamento e settori economici specifici, nonché l’individuazione di situazioni e contesti che possono essere oggetto di approfondimenti mirati²⁷⁹.

Le funzioni di analisi sono arricchite dalla disponibilità di flussi informativi ulteriori rispetto a quelli rivenienti dalle segnalazioni, di cui la UIF è pure destinataria in base alla normativa nazionale antiriciclaggio. L’art. 47 del D.lgs. 231/2007 prevede infatti che la UIF riceva dai soggetti obbligati, con cadenza periodica, dati e informazioni individuati in base a criteri oggettivi concernenti operazioni a rischio di riciclaggio o di finanziamento del terrorismo.

Anche le Pubbliche amministrazioni che svolgono specifiche funzioni nell’ambito di segmenti di attività esplicitamente richiamati dalla legge (quali procedimenti autorizzativi o concessori, scelta del contraente nei contratti pubblici, concessione di finanziamenti, ausili o sovvenzioni) sono tenute a comunicare alla UIF dati e informazioni concernenti operazioni sospette di cui vengono a conoscenza (art. 10, D.lgs. 231/2007).

3.4. La collaborazione a livello nazionale e internazionale

La collocazione della UIF al centro di una efficiente rete nazionale e internazionale per lo scambio di informazioni è essenziale per l’efficacia complessiva del sistema di prevenzione e contrasto del riciclaggio, che - in ossequio al principio cardine della complementarità tra prevenzione e repressione - esige il coordinamento tra la UIF, i soggetti incaricati di compiti di supervisione e controllo, gli organi investigativi e l’Autorità giudiziaria, basato sul rafforzamento degli strumenti conoscitivi e sulla condivisione di principi e obiettivi²⁸⁰. La configurazione organizzativa e funzionale dell’Unità, coerente con i principi e le regole internazionali ed europei, è pertanto preordinata a sviluppare un sistema di relazioni istituzionali basato su significative sinergie.

Oltre ai rapporti che si potrebbe definire “fisiologici” con la Guardia di finanza e con la DIA, incentrati sulla disseminazione delle segnalazioni di operazioni sospette e delle relative analisi finanziarie (art. 40, lett. d), del D.lgs. 231/2007), la UIF collabora con la magistratura inquirente²⁸¹, trasmettendo su richiesta informazioni utili per lo sviluppo di indagini e

²⁷⁸ Non si tratta evidentemente di poteri di regolazione in senso proprio, poiché gli indicatori costituiscono una mera guida per la valutazione delle operazioni potenzialmente sospette e vanno considerati come uno strumento di mero indirizzo, da interpretare e integrare alla luce dell’intero patrimonio informativo a disposizione del segnalante.

²⁷⁹ In base alla legge, pertanto, la UIF conduce studi su singole anomalie, su settori dell’economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realtà economiche territoriali. La principale fonte a disposizione dell’Unità per lo svolgimento di tali compiti è rappresentata dalle Segnalazioni AntiRiciclaggio Aggregate (“flussi S.A.R.A.”), trasmesse mensilmente dagli intermediari ai sensi dell’art. 33 del D.lgs. 231/2007, che rappresentano il mezzo per l’individuazione di fenomeni anomali di rilevanza “sistemica”, ovvero per approfondimenti da svolgere a livello complessivo e strutturale.

²⁸⁰ Viene in considerazione il principio di “leale collaborazione” di rango costituzionale, affermato in più occasioni dalla Corte costituzionale e incentrato sull’affermazione di doveri di correttezza nei rapporti reciproci tra le istituzioni e di rispetto “dell’altrui autonomo ruolo” (Corte Cost., sentt. n. 379 del 27 luglio 1992, n. 92 del 26 marzo 1999 e n. 98 del 13 aprile 2000). Su tali aspetti, cfr. A. Cisterna, *La convergenza del molteplice. Cooperazione istituzionale e organizzazione delle Istituzioni*, in Gnosis. Rivista italiana di intelligence, n. 1/2010.

²⁸¹ Resta in ogni caso fermo l’obbligo di denuncia ai sensi dell’art. 331 c.p.p. per le notizie di reato di cui la UIF venga a conoscenza nell’esercizio delle proprie funzioni.

supportando, in tal modo, procedimenti penali attraverso analisi e approfondimenti di carattere finanziario (art. 12, comma 3, del D.lgs. 231/2007)²⁸².

Specifiche forme di collaborazione intercorrono con la Direzione Nazionale Antimafia e Antiterrorismo (DNA), alla quale la UIF trasmette i dati anagrafici contenuti nelle SOS ricevute per consentire l'incrocio con i nominativi presenti nelle basi dati della Direzione (art. 8, comma 1, lett. a), del D.lgs. 231/2007).

Un ulteriore arricchimento delle forme di collaborazione tra la UIF e l'Autorità Giudiziaria proviene, da ultimo, dalla collaborazione con l'*European Public Prosecutor's Office* (EPPO), istituito dal regolamento UE/2017/1939 quale organo titolare dell'azione penale per il perseguimento dei reati che ledono gli interessi finanziari dell'Unione europea e delle conseguenti condotte di riciclaggio²⁸³. Lo scambio informativo tra le due Autorità consente all'Unità di fornire un supporto di analisi in merito ai reati di competenza dell'Ufficio europeo.

Per quanto riguarda la cooperazione con le autorità di settore, gli scambi della UIF con la funzione di vigilanza della Banca d'Italia, con la Commissione nazionale per le società e la borsa (Consob) e con l'Istituto per la vigilanza sulle assicurazioni (Ivass) sono finalizzati a fissare criteri e modalità di proficuo svolgimento dei rispettivi compiti, a coordinare le attività di controllo, scambiare informazioni, condividere analisi e studi; nell'ambito dei rapporti con la Banca d'Italia, inoltre, la UIF ha la possibilità di consultare dati rilevanti contenuti nei numerosi archivi dell'Istituto.

La legislazione nazionale conferma la spiccata proiezione internazionale come una caratteristica qualificante dell'attività della UIF. Ciò è coerente con regole internazionali, che assegnano alle FIU compiti di scambio informativo con le controparti estere, essenziali per l'analisi di flussi finanziari che oltrepassano i confini nazionali, interessando una pluralità di giurisdizioni²⁸⁴.

La materia è disciplinata dall'art. 13-*bis* del D.lgs. 231/2007, secondo cui la UIF, previa richiesta ovvero di propria iniziativa, può, a condizioni di reciprocità, anche per quanto riguarda la riservatezza, scambiare informazioni e collaborare con le FIU per il trattamento o l'analisi di informazioni collegate al riciclaggio o al finanziamento del terrorismo e ai soggetti coinvolti, indipendentemente dalla tipologia e dall'accertamento delle fattispecie di reato presupposto. In tal modo, lo scambio di informazioni con FIU estere diviene in molti casi propedeutico all'individuazione di fondi di provenienza illecita collocati in altri paesi da soggetti indagati in Italia.

A seguito delle modifiche al D.lgs. 231/2007 apportate in occasione del recepimento della quarta e della quinta direttiva europea antiriciclaggio, l'art. 13-*bis* disciplina ora anche la partecipazione della UIF, con le FIU degli Stati membri dell'Unione, ad analisi congiunte dei casi di carattere transfrontaliero e la trasmissione alle medesime FIU delle informazioni su segnalazioni di operazioni sospette che riguardano tali Stati, individuate tenendo conto degli indirizzi formulati dalla Piattaforma delle FIU dell'Unione europea. In base alle modifiche introdotte dalle cennate direttive, la UIF è, per converso, destinataria delle informazioni relative alle operazioni sospette concernenti l'Italia e, in particolare, di quelle provenienti da soggetti finanziari che operano sul territorio nazionale in libera prestazione di servizi.

La spiccata proiezione internazionale della UIF, infine, si traduce anche nella partecipazione attiva ai lavori svolti dagli organismi comunitari e dalle organizzazioni internazionali dediti all'attività di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo (GAFI, MoneyVal, Gruppo Egmont), nonché all'attività di altre organizzazioni internazionali pure incentrate sui temi della prevenzione e del contrasto di specifici reati finanziari.

3.5. I compiti in materia di contrasto del finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa

Il sistema internazionale di prevenzione e contrasto al finanziamento del terrorismo e all'attività dei paesi che minacciano la pace e la sicurezza internazionale, basato sull'applicazione delle misure di

²⁸² Sui rapporti tra autorità preposte alla vigilanza creditizia e alla tutela dell'integrità e autorità giudiziaria, si vedano gli atti del convegno "Legalità e buon funzionamento del sistema finanziario", Banca d'Italia, Roma, 4 febbraio 2014 e, in particolare, gli interventi di C. Clemente, *L'Unità di Informazione Finanziaria per l'Italia nel sistema di prevenzione del riciclaggio*, cit., M. Perassi, *Ruolo della Banca d'Italia e della Autorità Giudiziaria nel preservare l'integrità del sistema economico finanziario*, e C. Barbagallo, *Collaborazione informativa e coordinamento*.

²⁸³ Su tale organismo, cfr., per tutti, S. Allegrezza, 2022, *A European Public Prosecutor Office to Protect Common Financial Interests: A Milestone for the EU Integration Process*, in K. Ambos, P. Rackow (eds), *Cambridge Companion on European Criminal Justice*, CUP, 2022.

²⁸⁴ L'esigenza di collaborazione internazionale consistente nello scambio di informazioni su operazioni sospette costituisce dunque una delle stesse ragioni d'essere della "FIU". Si veda P. Lagerwaard, *Following Suspicious Transactions in Europe. Comparing the Operations of European Financial Intelligence Units (FIUs)*, Research Report, 2018. Cfr. anche F. Mouzakiti, *Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive*, *New Journal of European Criminal Law*, vol. 11, no. 3, 2020, pp. 351-374.

"congelamento" di fondi e risorse economiche detenute dai soggetti "designati" ai sensi del D.lgs. 109/2007 prevede una serie di adempimenti informativi nei confronti della UIF.

I destinatari degli obblighi antiriciclaggio sono infatti tenuti a comunicare alla UIF le misure di congelamento applicate ai soggetti designati, indicando i nominativi coinvolti, l'ammontare e la natura dei fondi o delle risorse economiche²⁸⁵. La UIF riceve anche comunicazioni relative a operazioni o rapporti, nonché ogni altra informazione disponibile riconducibili ai soggetti designati ovvero a quelli in via di designazione, anche sulla base delle indicazioni fornite dal Comitato di Sicurezza Finanziaria (art. 7, comma 2, del D.lgs. 109/2007).

Le attribuzioni della FIU italiana venivano inoltre estese dall'art. 10 del D.lgs. 109/2007 al contrasto al finanziamento del terrorismo e dei programmi di proliferazione delle armi di distruzione di massa. Attribuzioni poi confermate dal nuovo quadro normativo antiriciclaggio introdotto dal D.lgs. 231/2007, che ha esteso le misure di prevenzione antiriciclaggio, incluso l'obbligo di segnalazione delle operazioni sospette²⁸⁶, anche a tali fattispecie criminose. Al fine di agevolare l'assolvimento degli obblighi in materia di congelamenti e di segnalazioni, la UIF diffonde, mediante la pubblicazione dei rispettivi link, le liste dei soggetti designati dal Consiglio di Sicurezza dell'ONU e dall'Unione europea (art. 10, comma 2, del D.lgs. 109/2007).

La UIF, inoltre, diffonde ulteriori liste predisposte da altre istituzioni ed enti coinvolti nel contrasto del terrorismo internazionale, come quella dell'Office of Foreign Asset Control (OFAC) del Dipartimento del Tesoro degli Stati Uniti, atta a supportare eventuali segnalazioni, ma in relazione alle quali non sussistono obblighi di congelamento dei fondi.

3.6. L'evoluzione del ruolo delle FIU nel quadro internazionale ed europeo

Le FIU sono istituite, in ciascun paese, indipendentemente da considerazioni politico-istituzionali e dai connotati giuridici e amministrativi della giurisdizione di riferimento, secondo caratteristiche tipiche e in base a uno *status*, risultante dagli *standard* internazionali, che le qualifica come agenzie nazionali centrali e autonome, responsabili per la ricezione e l'analisi delle segnalazioni e delle altre informazioni relative a casi di riciclaggio, reati presupposto associati, finanziamento del terrorismo, nonché per la disseminazione dei risultati dell'analisi finanziaria alle autorità competenti.

In questo ruolo, le FIU, oltre ad assicurare il raccordo tra i soggetti obbligati alla segnalazione e le autorità investigative, sono al centro di reti di collaborazione inter-istituzionali a livello domestico e responsabili di scambi di informazioni finanziarie a livello internazionale con le controparti estere.

Pur tenendo conto delle differenze ancora esistenti, nei vari paesi, nella natura e nella collocazione istituzionale, le FIU sono ormai riconosciute come "attori-chiave" dei sistemi nazionali di prevenzione per la loro funzione, eminentemente tecnica, di valutazione e diffusione di informazioni finanziarie di rilevante interesse pubblico, per le caratteristiche di riservatezza e confidenzialità dell'attività di *intelligence* svolta, per la specifica attitudine alla cooperazione e allo scambio di informazioni a livello nazionale e internazionale.

Questi elementi sono considerati, dalla comunità internazionale, di significativa importanza per assicurare l'efficacia della prevenzione anche al di fuori del sistema antiriciclaggio con una crescente attenzione per il possibile utilizzo delle competenze delle FIU e delle potenzialità informative che esse esprimono, ai fini della prevenzione e del contrasto di specifici reati.

²⁸⁵ L'art. 7, comma 1, D.lgs. 109/2007 fissa il termine per l'effettuazione della comunicazione in 30 giorni decorrenti dall'entrata in vigore dei regolamenti comunitari, delle decisioni degli organismi internazionali e dell'Unione europea (il termine decorre dalla data di detenzione dei fondi e delle risorse economiche, se successiva).

²⁸⁶ Gli obblighi di comunicazione di cui al D.lgs. 109/2007 sono distinti e autonomi rispetto a quelli di segnalazione delle operazioni sospette; essi pertanto devono essere assolti anche nel caso in cui le medesime informazioni siano portate a conoscenza della UIF mediante l'invio di segnalazioni di operazioni sospette nelle quali risultino coinvolti soggetti designati nelle liste. Peraltro, la presenza di operazioni cui prendono parte, anche come controparti, nominativi destinatari delle misure di congelamento o soggetti ad essi contigui costituisce uno degli indicatori di anomalia per l'invio di una segnalazione di operazioni sospette alla UIF.

In materia fiscale, da tempo la *Task Force on Tax Crime* dell'OCSE dedica attenzione ai benefici derivanti dalla cooperazione tra FIU e agenzie fiscali, nel quadro di un approccio c.d. *"whole of government"*²⁸⁷.

Con riferimento alle iniziative internazionali per la prevenzione e il contrasto della corruzione, i più importanti esercizi di valutazione dei sistemi nazionali²⁸⁸ tengono conto sistematicamente del contributo delle FIU, riconoscendo che la corruzione può essere combattuta con maggiore successo attraverso un approccio globale e *multi-stakeholder*²⁸⁹, nel quale le FIU e le agenzie specializzate anticorruzione possano scambiare dati e informazioni in modo sicuro.

Il ruolo e le competenze delle FIU sono analizzati e considerati di valore in settori specifici quali l'*asset tracing* e la lotta al crimine organizzato²⁹⁰.

Nell'Unione europea il progressivo rafforzamento della cooperazione e degli scambi di informazioni di natura finanziaria e investigativa prende in considerazione le attività, i poteri e la cooperazione delle FIU anche oltre l'ambito della lotta al riciclaggio e al finanziamento del terrorismo. La direttiva (UE) 2019/1153²⁹¹ ha ribadito la centralità dell'informazione finanziaria sviluppata e posseduta dalle FIU e il valore che essa assume se condivisa e utilizzata dalle "autorità competenti" a fini di prevenzione, accertamento, indagine o perseguimento di reati gravi²⁹². Il regolamento (UE) 2018/1672 prevede inoltre che le autorità doganali trasmettano regolarmente alla FIU le dichiarazioni del loro paese riguardanti il trasporto di valori di importo pari o superiore a 10.000 euro, segnalando alla stessa FIU le informazioni sui casi sospetti rilevati, senza limiti di soglia, nonché le denunce di violazione dell'obbligo di dichiarazione emerse durante i controlli²⁹³.

La prossima riforma del sistema antiriciclaggio europeo, che allocherà in una nuova autorità europea le funzioni di coordinamento e supporto della loro attività, va nella direzione della maggiore uniformità dei poteri²⁹⁴ e degli strumenti di analisi a disposizione delle FIU e della più chiara definizione delle fonti di informazione da esse accessibili: l'autonomia e l'indipendenza delle FIU riceveranno una rinnovata declinazione sui versanti complementari dell'operatività e dell'organizzazione; saranno definite nel dettaglio le tipologie di fonti di natura finanziaria, amministrativa e investigativa cui esse avranno accesso; la collaborazione tra le FIU sarà favorita dall'uniformità dei formati e dei contenuti delle segnalazioni *cross-border* e dal rafforzamento della base legale e delle direttrici di sviluppo tecnologico dell'infrastruttura europea dedicata agli scambi di informazioni.

²⁸⁷ Tale organismo ha raccomandato ai paesi la più ampia e fluida condivisione di informazioni tra le amministrazioni fiscali e le FIU, con particolare riferimento alla previsione, in capo alle prime, di doveri di condivisione di informazioni con le FIU del proprio paese. Inoltre, al fine di massimizzare l'uso del sistema della segnalazione di operazioni sospette, con la salvaguardia di tutte le garanzie di riservatezza, si prefigura anche il possibile accesso delle stesse amministrazioni fiscali alle informazioni contenute nelle segnalazioni. Si veda, al riguardo, OECD, *Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes*, 3^a ed., OECD Pub. Paris, 2019; OECD's Task Force on Tax Crimes and Other Crimes, *Improving Co-operation between Tax and Anti-Money Laundering Authorities: Access by tax administrations to information held by financial intelligence units for criminal and civil purposes*, OECD Pub., Paris, 2015; Id., *Fighting Tax Crime: The Ten Global Principles*, OECD Pub., Paris, 2017.

²⁸⁸ Si fa riferimento, in particolare, agli esercizi periodici condotti dal *Groupe d'Etats contre la Corruption* presso il Consiglio d'Europa, dall'UNODC e dal *Working Group on Bribery* presso l'OCSE.

²⁸⁹ Merita di essere richiamata l'esperienza italiana del Tavolo inter-istituzionale di coordinamento anticorruzione presso il MAECI, al quale partecipa anche la UIF, riconosciuto come *best practice* a livello internazionale.

²⁹⁰ Quale autorità di prevenzione antiriciclaggio specializzata nell'analisi finanziaria delle segnalazioni di operazioni sospette, la UIF ha contribuito ai lavori del Gruppo di Lavoro Anticorruzione (ACWG) del G20. La Presidenza italiana di tale Foro globale per il 2021 ha condotto ad approvazione rilevanti documenti presentati in attuazione delle proprie priorità e, tra l'altro, gli "Alti Principi" in materia di rapporti tra corruzione, riciclaggio e crimine organizzato, corruzione e sport, corruzione in contesti di emergenza oltre la crisi pandemica.

²⁹¹ Direttiva (UE) 2019/1153 del 20 giugno 2019, che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati, e che abroga la decisione 2000/642/GAI del Consiglio.

²⁹² Secondo la direttiva, infatti, le "informazioni finanziarie" e i risultati delle analisi delle FIU possono essere utilizzate dalle "autorità competenti" preposte al perseguimento dei "reati gravi" (la definizione comprende non solo i reati economici, ma anche varie altre tipologie, quali i reati contro la persona e il traffico illecito ambientale, oltre al riciclaggio, ai reati presupposto e al finanziamento del terrorismo). È inoltre stabilito che le FIU debbano avere accesso alle informazioni investigative in possesso delle stesse autorità, per rafforzare la loro azione e rendere più efficace la loro collaborazione. Purtroppo, il recepimento in Italia della norma europea (con il D.lgs. 8 novembre 2021, n. 186) ha adottato un approccio restrittivo che di fatto non consente di sfruttare pienamente le opportunità offerte dalla direttiva per accrescere l'utilità delle informazioni detenute dalla UIF.

²⁹³ Regolamento (UE) 2018/1672 del 23 ottobre 2018, relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione e che abroga il regolamento (CE) n. 1889/2005, in GUUE L 284 del 12 novembre 2018.

²⁹⁴ Le FIU vedranno confermati i tratti qualificanti del proprio ruolo, incentrati sulla ricezione, sull'analisi e sulla disseminazione delle segnalazioni di operazioni sospette, con importanti elementi aggiuntivi legati all'assegnazione all'AMLA del compito di emanare "orientamenti indirizzati alle FIU sulla natura delle caratteristiche e sugli obiettivi dell'analisi operativa e strategica".

Il modello di FIU che risulterà dall'evoluzione appena illustrata, assumendo valenza comune in tutta Europa, è quello di un'agenzia nazionale con poteri estesi, ampia disponibilità di informazioni, elevata capacità di collaborare con le autorità nazionali, attitudine a produrre *intelligence* di qualità, utilizzabile per la prevenzione dei più importanti e diffusi fenomeni di criminalità finanziaria che abbiano il riciclaggio di denaro come fattore comune.

L'autonoma valorizzazione delle capacità analitiche e dei prodotti delle FIU rende ancora più netta l'esigenza di distinguere l'attività di analisi finanziaria da quella investigativa e di contrasto. La separazione tra prevenzione e repressione, pur legate da un rapporto di stretta complementarità, può essere oggi considerata alla stregua di un principio fondamentale per un moderno ed efficace sistema nazionale antiriciclaggio²⁹⁵.

Tali aspetti inducono a considerare con rinnovata attenzione anche i criteri in base ai quali si può valutare l'efficacia complessiva dell'azione di una FIU. È infatti evidente che tale valutazione non può essere condotta con criteri esclusivamente quantitativi, basati sul numero di investigazioni e di condanne per il reato di riciclaggio, ma, come richiesto dagli stessi *standard* internazionali, deve guardare: alla capacità della FIU di stimolare nel sistema un adeguato grado di sensibilità rispetto ai tentativi di infiltrazione criminale, favorendo la loro intercettazione e pronta segnalazione; al valore aggiunto che le segnalazioni - e l'analisi finanziaria prodotta - apportano alle indagini e alle azioni penali volte a individuare e perseguire non solo il riciclaggio, ma anche gli altri reati presupposto²⁹⁶; alla misura in cui la collaborazione con altre autorità a livello nazionale e internazionale contribuisce a creare un modello di prevenzione e repressione della criminalità finanziaria fondato su un "sistema" coordinato di relazioni istituzionali, sullo scambio di esperienze e su una "cultura" condivisa della legalità e dell'integrità.

Tali caratteri sembrano trovare piena e compiuta espressione nel modello amministrativo di FIU, rispetto al quale il grado elevato di indipendenza e autonomia operativa, la specializzazione nell'analisi finanziaria, la vicinanza al settore privato e l'attitudine alla cooperazione appaiono predominanti.

Le caratteristiche istituzionali e le funzioni della UIF italiana, riconosciute conformi alle disposizioni internazionali ed europee²⁹⁷, sono in linea con questo modello. C'è da auspicare che, quando saranno esauriti i ripetuti impulsi rivenienti dal recepimento delle regole europee e sarà stato definito l'assetto del sistema antiriciclaggio comune dell'Unione, il quadro normativo nazionale consolidi il ruolo dell'Unità come autorità indipendente e autonoma, con poteri e compiti definiti e una riconosciuta attitudine alla proficua interazione con gli enti segnalanti, con le autorità investigativa e giudiziaria, ma anche con le altre istituzioni a vario titolo responsabili della prevenzione e della protezione dell'integrità di importanti settori dell'economia. Si tratta di un presupposto essenziale perché il potenziale che il sistema antiriciclaggio italiano può esprimere, anche in Europa, possa essere sfruttato pienamente.

4. Le Autorità di vigilanza di settore (*R. Cercione*)

Uno dei pilastri su cui poggia la forza del dispositivo antiriciclaggio²⁹⁸, almeno nell'esperienza italiana, è senza dubbio l'integrazione della risposta istituzionale: autorità amministrative, giudiziarie, Organi investigativi concorrono, ciascuno per la propria competenza, all'azione di prevenzione e di contrasto, attraverso ormai sperimentati meccanismi di collaborazione e di coordinamento. I rapporti tra gli attori istituzionali sono consolidati da una consuetudine di cooperazione e coordinamento reciproci, che è talvolta suggellata da protocolli bilaterali che regolano le forme e le modalità dello scambio di informazioni e del coordinamento operativo.

²⁹⁵ Cfr. I. Borrello, *The FIU's role in the AML/CTF system. The supranational scenario and the Italian experience*, in M. Ventura, A. Palmieri, R. Pavoni, G. Milani (ed.), *Boosting European Security Law and Policy*, Edizioni Scientifiche Italiane, Collana: Studi «Pietro Rossi» Napoli 2021.

²⁹⁶ Vale la pena notare che negli ultimi anni una percentuale crescente di segnalazioni trasmesse dalla UIF agli Organi investigativi sono state ritenute meritevoli di rilievi istruttori e molte di esse hanno generato procedimenti penali, non solo per riciclaggio ma anche relativi ad altri reati presupposto.

²⁹⁷ Nella *Mutual Evaluation* del sistema antiriciclaggio italiano, condotta nel 2016, il GAFI ha evidenziato, tra l'altro, che la UIF è una struttura "ben funzionante", che produce analisi strategiche e operative di alta qualità, le quali aggiungono valore alle segnalazioni. Oltre alla qualità degli output prodotti dalla UIF, il Rapporto ha messo in evidenza le risorse e competenze della UIF, le metodologie avanzate utilizzate nell'analisi operativa e strategica e gli strumenti per la gestione delle attività e dei processi di lavoro. Particolare enfasi è stata posta sulla necessità di garantire l'accesso della UIF alle informazioni investigative per le sue analisi e di ampliare la disseminazione ad altri Organi investigativi e autorità interessate, tra cui quella anticorruzione.

²⁹⁸ Il termine è da intendersi comprensivo dell'attività di prevenzione e contrasto al finanziamento del terrorismo.

Tra gli attori di questo processo le autorità di vigilanza di settore richiamate dall'art. 7 del decreto antiriciclaggio (Banca d'Italia, Consob e IVASS) svolgono compiti di supervisione antiriciclaggio con riguardo agli operatori sui quali esercitano poteri di vigilanza "settoriale" (sostanzialmente gli intermediari bancari, finanziari, assicurativi). Nel prosieguo si tratteggeranno le caratteristiche e le interazioni di tali autorità nell'esercizio della funzione di vigilanza antiriciclaggio e i processi evolutivi che le hanno interessate e che le interesseranno in un futuro non lontano, con particolare riferimento all'ambito sovranazionale.

4.1 Le autorità di vigilanza di settore nell'ordinamento nazionale

Nel definire i compiti delle autorità di settore, il decreto, anche sulla scorta delle direttive europee in materia, mostra di seguire il modello di controllo sugli intermediari che le stesse autorità hanno sviluppato e applicano nell'esercizio della vigilanza settoriale, imperniato sui poteri di regolamentazione secondaria, di supervisione e di intervento, come stabilito nei testi unici bancario e della finanza e nel codice delle assicurazioni private.

I poteri di supervisione antiriciclaggio si esprimono nei – tradizionali, per la vigilanza settoriale – ambiti della vigilanza informativa e ispettiva e degli interventi correttivi; prevedono una serie articolata di iniziative di crescente pervasività sugli intermediari, che giungono fino alla sospensione dell'attività ("nuove operazioni") e all'irrogazione di sanzioni amministrative pecuniarie²⁹⁹.

L'attribuzione alle autorità di settore di questi poteri modellati su quelli delle funzioni di vigilanza settoriale ha favorito la crescita nel tempo della capacità operativa delle autorità nel campo dell'antiriciclaggio e l'interazione orizzontale, all'interno delle autorità stesse. L'incontro con la cultura e il metodo della vigilanza settoriale, affinati in decenni di evoluzione, ha influenzato e plasmato anche l'attività di supervisione antiriciclaggio, che si è evoluta in una vera e propria funzione (di regolamentazione, controllo e intervento).

Con la vigilanza settoriale l'antiriciclaggio condivide ormai principi e metodologie: la proporzionalità e l'approccio in base al rischio³⁰⁰, lo sviluppo di un modello di analisi del rischio di riciclaggio³⁰¹, la correlazione tra gli esiti delle verifiche cartolari e ispettive e gli interventi, la stessa tipologia degli interventi, presi a prestito da quelli della vigilanza settoriale.

Il decreto non attribuisce i poteri di intervento in tutta l'estensione che ad essi è concessa nell'ambito della vigilanza settoriale; mancano i poteri più incisivi, di rimozione individuale o collettiva degli esponenti aziendali, di avvio della procedura di amministrazione straordinaria degli intermediari e di proposta al Ministro dell'economia e delle finanze della liquidazione coatta amministrativa degli stessi.

Questo però non significa che tali misure non possano essere adottate per ragioni legate alle anomalie in materia di antiriciclaggio, implica solo che devono essere assunte dalle autorità in funzione e sulla base dei poteri di vigilanza settoriali attribuiti dai testi unici e dal codice sopra citati e non di quelli attribuiti dal decreto antiriciclaggio, implica cioè che queste

²⁹⁹ Nel richiamare "ispezioni e controlli" delle autorità di settore in materia di antiriciclaggio il decreto (art.7, comma 2, lett. b)) indica i seguenti poteri: di acquisizione informativa (...tutti i documenti, gli atti e [di] ogni altra informazione utili all'espletamento delle funzioni di vigilanza e controllo.); "di convocare i componenti degli organi di direzione, amministrazione e controllo e il personale dei soggetti obbligati rispettivamente vigilati" e di "richiedere l'invio, ..., di segnalazioni periodiche rilevanti per finalità di prevenzione del riciclaggio e di finanziamento del terrorismo"; di ordinare ovvero, in caso di inottemperanza all'ordine di convocare, di convocare direttamente "gli organi di amministrazione, direzione e controllo dei soggetti obbligati rispettivamente vigilati, fissandone l'ordine del giorno e proponendo l'assunzione di specifiche decisioni."; di adottare "provvedimenti aventi ad oggetto il divieto di nuove operazioni nelle ipotesi di gravi carenze o violazioni, riscontrate a carico dei soggetti obbligati rispettivamente vigilati"; di "irrogare, ..., le sanzioni previste per l'inosservanza degli obblighi di cui al presente decreto, e delle relative disposizioni di attuazione, da parte dei soggetti obbligati rispettivamente vigilati".

³⁰⁰ Le autorità basano la frequenza e l'intensità dei controlli e delle ispezioni di vigilanza in funzione del profilo di rischio, delle dimensioni e della natura del soggetto obbligato vigilato (art. 7, comma 2, lett. a). Cfr. anche *Orientamenti sulla vigilanza basata sul rischio*, reperibile sul sito dell'EBA (Eu. Banking Authority).

³⁰¹ Le autorità "definiscono procedure e metodologie per la valutazione del rischio di riciclaggio e finanziamento del terrorismo cui gli intermediari rispettivamente vigilati sono esposti nell'esercizio della propria attività" (art. 7, comma 1, lett. c).

misure possono essere assunte dalla funzione di vigilanza settoriale se le violazioni e le irregolarità riscontrate nel settore dell'antiriciclaggio siano tali da integrare i presupposti di gravità richiesti per l'adozione di quelle misure³⁰².

Le ragioni dell'integrazione tra le due funzioni stanno non solo nella similitudine di poteri, metodologie e strumenti di azione, ma anche nella insistenza di tali attribuzioni sostanzialmente sugli stessi intermediari e sugli stessi specifici aspetti dell'organizzazione aziendale: pensiamo al convergente interesse alla funzionalità della *governance* e dei sistemi di controllo interno, evidentemente rilevante sia per la vigilanza settoriale che per la supervisione antiriciclaggio³⁰³. Pertanto, una stretta cooperazione è, per ciascuna delle due funzioni, prima ancora che frutto di previsioni legislative, conseguenza naturale ed esigenza irrinunciabile per la forte interconnessione, pena un'azione che rischia di essere inefficace, se non incoerente, per entrambe le funzioni³⁰⁴.

4.2 La dimensione sovranazionale e la prospettiva europea.

Ai processi di integrazione orizzontale sopra indicati (delle autorità di settore con gli altri attori istituzionali operanti nell'antiriciclaggio e, all'interno delle autorità, tra funzioni di vigilanza settoriale e di supervisione antiriciclaggio) corrisponde poi un'integrazione verticale, che ha riguardato gli intermediari bancari. Con l'avvento del Meccanismo di Vigilanza Unico sulle banche (*Single Supervisory Mechanism*), infatti, si spezza l'unità formale tra autorità antiriciclaggio e autorità di vigilanza settoriale: per le banche di maggiore dimensioni (cosiddette "significative") la funzione di vigilanza settoriale emigra presso il Comitato di Sorveglianza (*Single Supervisory Board*) costituito nell'ambito della Banca centrale europea, mentre le competenze in materia di antiriciclaggio restano a livello nazionale. Non diminuisce naturalmente, anzi aumenta, il fabbisogno di scambio informativo e coordinamento operativo tra le due funzioni, considerato che la funzione di supervisione antiriciclaggio nazionale si interfaccia verticalmente con la Vigilanza europea (per le banche significative) e orizzontalmente, come si è detto, con la Vigilanza nazionale (per le banche non significative). L'uniformità delle interlocuzioni verticali è consacrato nell'accordo multilaterale del 2019 che fissa il quadro di riferimento per lo scambio informativo tra la Banca centrale europea e le autorità antiriciclaggio nazionali³⁰⁵.

Un ulteriore processo, di integrazione orizzontale, si è sviluppato nei rapporti tra gli ordinamenti. La crescita progressiva della cooperazione internazionale accelera le interazioni tra le autorità dei vari Stati nazionali competenti per la supervisione antiriciclaggio. In questo settore, permanevano approcci nazionali diversificati e frammentati, prassi di vigilanza differenti e lacune nella collaborazione internazionale; aspetti che la Commissione europea mette a fuoco come problemi strutturali da risolvere con coerenti azioni riformatrici, in un rapporto del 2019 elaborato anche sull'onda di gravi fatti di riciclaggio che avevano coinvolto intermediari di paesi europei con una tradizione del contrasto al crimine organizzato, segnatamente finanziario, non consolidata, almeno nel confronto con l'Italia³⁰⁶.

³⁰² Su questa impostazione cfr. anche EBA, che delimita i ruoli delle due funzioni: "*The AML/CFT supervisor should provide to the prudential supervisor all relevant information and details on the identified serious breach(es) in order to allow the prudential supervisor to properly evaluate the information received and conduct its own assessment on whether withdrawal of the authorisation is appropriate.*" (*Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU*, reperibile sul sito dell'EBA ([Final AML-CFT Cooperation Guidelines.pdf](#) (europa.eu)).

³⁰³ Il decreto chiede alle autorità di settore di verificare "l'adeguatezza degli assetti organizzativi e procedurali dei soggetti obbligati rispettivamente vigilati" (art. 7, comma 1, lett b).

³⁰⁴ L'ambito di questa collaborazione copre tutto l'arco della vita e delle evenienze degli intermediari: "*The guidelines explain how AML/CFT supervisors, prudential supervisors and financial intelligence units should cooperate and exchange information throughout the supervisory life cycle covering authorisations, ongoing supervision including the risk assessment and the imposition of supervisory measures and sanctions, including the withdrawal of the authorization*" (*Guidelines on cooperation and information exchange*, cit., p. 3).

³⁰⁵ Cfr. *Multilateral Agreement on the practical modalities for exchange of information on AML/CFT between the ECB and CAs.*, messo a punto congiuntamente dalle tre autorità di vigilanza europee (EBA, ESMA, EIOPA).

³⁰⁶ Cfr. *Report from the Commission to the EU Parliament and the Council on the assessment of recent alleged money laundering cases involving EU credit institutions*, approvato dalla Commissione il 24 luglio 2019. In particolare cfr. le considerazioni finali (pp. 22-23): "*The different approaches ... by credit institutions and to its supervision by national authorities are the consequence of minimum harmonisation at Union level. The integration of anti-money laundering/ countering the financing of terrorism concerns in prudential supervision especially in cross-border situations is not yet sufficiently well articulated in the prudential framework. This results in a degree of regulatory and supervisory fragmentation... Weak links pose threats to the integrity of the Union's financial system as a whole and will continue to exist unless it is ensured that all entities implement in a coherent and effective manner common rules and are*

Il rapporto imprime una forte accelerazione alla revisione del quadro ordinamentale e istituzionale. Di qui, tra l'altro, il rafforzamento del ruolo di indirizzo, coordinamento e supervisione dell'EBA (che vede ampliati dal 2020 i propri compiti)³⁰⁷, l'enfasi sull'esigenza di sviluppare un approccio consolidato sui gruppi con operatività internazionale³⁰⁸, la spinta ad elevare il livello di armonizzazione normativa in sede europea, il maggiore coinvolgimento della funzione di vigilanza settoriale nella valutazione del rischio di riciclaggio, lo sviluppo delle interazioni tra le autorità nazionali dei vari Stati.

Questo processo si consolida nell'istituzionalizzazione delle sedi di confronto, con la formazione di appositi collegi permanenti di supervisione antiriciclaggio, regolati da Linee guida elaborate dalle tre autorità di vigilanza europee³⁰⁹, che ne prevedevano la prima riunione entro il 2021. I collegi erano destinati a riunire periodicamente le autorità di settore degli Stati interessati dall'attività di uno stesso intermediario; essi dovevano costituire il momento centrale dello scambio informativo e del coordinamento operativo internazionale, conferendo così carattere strutturale e continuità ai rapporti di collaborazione delle autorità dei vari Stati membri³¹⁰. Inoltre, ha preso quota l'armonizzazione operativa promossa dall'EBA, attraverso l'emanazione di norme secondarie e linee guida standardizzate.

Tuttavia, il momento decisivo che corona questo processo evolutivo dei rapporti tra le autorità di settore nazionali è la scelta di passare dall'integrazione e dalla cooperazione sovranazionale alla centralizzazione della funzione antiriciclaggio in un'autorità unica europea. Non basta più l'omogeneità delle regole, ma è necessaria l'unicità dell'autorità che le applica.

Un passaggio epocale, che affonda le sue radici in fattori contingenti, come l'allarme procurato dai richiamati fenomeni di criminalità finanziaria in Europa, e in fattori strutturali, come la portata internazionale delle attività di riciclaggio, favorita dal prorompente sviluppo tecnologico anche nell'attività finanziaria, il livello di integrazione interna raggiunto nell'area europea, la stessa creazione del Meccanismo di Vigilanza Unico per le banche, di cui il processo di definizione dell'autorità unica antiriciclaggio pare ripercorrere le orme, con gli aggiustamenti del caso.

Le autorità di settore saranno chiamate ad interagire con la nuova autorità unica, che si candida a rappresentare un punto di riferimento generale in materia di contrasto al riciclaggio nell'Unione europea e a cui spetterà di conseguire un elevato livello di protezione del sistema economico – finanziario, ma anche la sfida di non ostacolare lo sviluppo della finanzia digitale e di contenere gli oneri a carico degli attori del mercato (operatori e clienti), prestando la dovuta attenzione all'efficienza della regolamentazione, degli adempimenti e dei controlli.

5. La Direzione Nazionale Antimafia e Antiterrorismo (DNAA) (I. Borrello)

La Direzione Nazionale Antimafia e Antiterrorismo (DNAA) è stata istituita come “Direzione Nazionale Antimafia” con il decreto-legge 20 novembre 1991, n. 367, convertito con modificazioni dalla legge 20 gennaio 1992, n. 8, con il compito di coordinare, in ambito nazionale, le indagini delle Procure distrettuali relative alla criminalità organizzata. Successivamente, il decreto legge 18 febbraio 2015, n. 7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43, ha aggiunto alle competenze della Direzione la “trattazione di procedimenti in materia di terrorismo, anche internazionale”.

subject to supervision of the highest quality. This implies that the tasks of the various relevant authorities involved... should be clearly spelled out and appropriately attributed... at international level, cooperation with key third country authorities should be more structured and systematic, ... Consideration could be given to further harmonising the ... rulebook both as regards the obligations of credit institutions as well as the powers, duties and tools necessary for effective supervision. In particular, transformation of the Anti-Money Laundering Directive into a Regulation ... should be considered. ... in order to ensure high quality and consistent anti-money laundering supervision, seamless information exchange and optimal cooperation between all relevant authorities in the Union. This may require conferring specific anti-money laundering supervisory tasks to a Union body”.

³⁰⁷ Per una panoramica sulle attribuzioni e l'attività dell'EBA in materia antiriciclaggio cfr. *Anti-Money Laundering and Countering the Financing of Terrorism*, reperibile sul sito dell'EBA.

³⁰⁸ Sul punto il decreto antiriciclaggio contiene specifiche previsioni sulla collaborazione sovranazionale, che abilitano le autorità di settore a interagire con le corrispondenti autorità degli altri Stati membri, con riguardo agli intermediari che operano in più Stati membri. L'art. 7, nei commi da 4-bis a 4-quinquies, si occupa della collaborazione, specificamente per l'attività ispettiva.

³⁰⁹ EBA, ESMA (Eu. Securities and Markets Authority) e EIOPA (Eu. Insurance and Occupational Pensions Authority).

³¹⁰ Cfr. *Joint Guidelines on cooperation and information exchange on AML - CFT.pdf (europa.eu)*; per una sintetica descrizione dei collegi cfr. *European Banking Authority - Factsheet on AML/CFT colleges (europa.eu)*. Per quanto concerne il diritto interno, i collegi sono evocati espressamente nel decreto, al comma 4-sexies dell'art. 7, nell'ambito delle “forme di collaborazione e coordinamento” che le autorità di settore italiane sono chiamate a definire sulla base di accordi con le corrispondenti autorità di altri Stati, con la previsione anche della facoltà di concordare specifiche ripartizioni di compiti e deleghe di funzioni.

Tenuto conto della consolidata equiparazione della mafia a un'impresa criminale³¹¹, l'istituzione e l'attività della DNAA rispondono all'esigenza di sviluppare efficaci strategie di contrasto alle associazioni di stampo mafioso mediante strumenti di aggressione ai patrimoni e ai flussi economici illeciti riconducibili alla criminalità organizzata. Tali strumenti appaiono utili anche ai fini del contrasto al terrorismo e, in particolare, di quelle formazioni terroristiche internazionali che si connotano sempre più quali veri e propri "Stati-mafia"³¹², esprimendo, oltre al radicalismo ideologico e al ricorso alla violenza, anche capacità imprenditoriali e di dominio del territorio derivanti dall'accumulo di risorse economiche frutto di attività criminali di vasta portata (traffici di stupefacenti, di petroli, di opere d'arte, di armi, di tabacchi e di migranti, estorsioni e sequestri di persona, corruzione e riciclaggio dei proventi illeciti).

L'enfasi posta dal D.lgs. 231/2007 sulla prevenzione, declinata nelle forme del coordinamento, dell'ampio utilizzo dell'*intelligence* finanziaria e della pre-investigazione, ha giustificato l'inserimento della Direzione, con compiti sempre più definiti e pregnanti, nell'apparato antiriciclaggio nazionale, quale attore istituzionale centrale per l'impulso e il coordinamento delle indagini per mafia e terrorismo³¹³.

La DNAA è formalmente costituita nell'ambito della Procura generale presso la Corte Suprema di Cassazione³¹⁴ ed è diretta dal Procuratore nazionale antimafia e antiterrorismo, nominato dal Consiglio Superiore della Magistratura, di concerto con il Ministro della Giustizia, tra magistrati aventi qualifica non inferiore a quella di magistrato di Cassazione³¹⁵.

In base all'art. 371-bis c.p.p., il Procuratore Nazionale Antimafia, soggetto alla vigilanza del Procuratore Generale presso la Corte di Cassazione³¹⁶, ha funzioni di coordinamento, impulso e controllo delle indagini svolte dalle Procure distrettuali presso i tribunali dei 26 capoluoghi di distretto di Corte d'Appello, nei cui confronti può impartire direttive ed esercitare anche poteri di avocazione (in casi eccezionali di grave inerzia o di mancato coordinamento). Il Procuratore nazionale, attraverso i sostituti, mantiene un costante collegamento con ciascuna Direzione distrettuale per l'acquisizione e la successiva elaborazione di dati, notizie e informazioni relativi ai reati di competenza. Dispone inoltre l'applicazione temporanea degli stessi sostituti presso specifiche Direzioni Distrettuali a supporto di indagini di particolare complessità. Il Procuratore ha infine il compito di risolvere eventuali contrasti tra procuratori distrettuali che impediscano di promuovere o di rendere effettivo il coordinamento³¹⁷.

I sostituti procuratori nazionali esplicano l'attività di coordinamento presso ciascuna DDA, dove si recano periodicamente per seguire le indagini e riportare le informazioni in DNA, esprimono pareri nei casi previsti dalla legge³¹⁸, seguono le materie di interesse loro delegate³¹⁹, assumendo le necessarie informazioni sia direttamente, che attraverso le forze

³¹¹ In coerenza con le intuizioni di Giovanni Falcone circa la forte connotazione economico/finanziaria degli interessi criminali. Sull'evoluzione delle forme di condizionamento illecito dell'economia si vedano, tra gli altri, P. Arlacchi, *La mafia imprenditrice. L'etica mafiosa e lo spirito del capitalismo*, Il Mulino, 1983; E. Fantò, *L'impresa a partecipazione mafiosa*, Dedalo, 1999; N. Dalla Chiesa, *L'impresa mafiosa*, Cavallotti, 2012; G. Conzo e R. Vona, *L'impresa criminale. La metamorfosi aziendale delle attività malavite*, Fridericiana ed., 2017; F. Costantino, *L'impresa criminale*, Rubbettino, 2020.

³¹² Cfr. DNAA, *Relazione sulle attività svolte dal Procuratore nazionale e dalla Direzione nazionale antimafia e antiterrorismo nonché sulle dinamiche e strategie della criminalità organizzata di tipo mafioso nel periodo 1° luglio 2018 – 31 dicembre 2019*, Roma, 24 novembre 2020.

³¹³ Per una ricostruzione accurata e un inquadramento delle funzioni della DNAA, si veda M.V. De Simone e G. Russo (a cura di), *La Direzione Nazionale Antimafia e Antiterrorismo a 30 anni dalla sua istituzione*, Roma, 2022.

³¹⁴ Si veda l'art. 76-bis del R.D. 30 gennaio 1941, n. 12 (Ordinamento giudiziario), inserito dall'art. 6 del DL 20 novembre 1991, n. 367, convertito con modificazioni dalla legge 20 gennaio 1992, n. 8, e, successivamente, l'art. 103 del D.lgs. 6 settembre 2011, n. 159, recante "Codice delle leggi antimafia e delle misure di prevenzione", come sostituito dall'art. 10 del DL 18 febbraio 2015, n.7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43.

³¹⁵ Il Procuratore, in particolare, è scelto tra coloro che hanno svolto anche non continuativamente, per un periodo non inferiore a dieci anni, funzioni di pubblico ministero o giudice istruttore, sulla base di specifiche attitudini, capacità organizzative ed esperienze nella trattazione di procedimenti relativi alla criminalità organizzata. L'incarico ha durata di quattro anni e può essere rinnovato una sola volta.

³¹⁶ Che riferisce al Consiglio Superiore della Magistratura circa l'attività svolta e i risultati conseguiti dalla DNA e dalle direzioni distrettuali antimafia (DDA). Quello del Procuratore Generale si configura come un controllo di legalità: "questa sorveglianza comporta sicuramente un controllo di legalità che non può essere meramente formale. (...) Il Procuratore Generale della Cassazione non potrà dare delle direttive al Procuratore Nazionale Antimafia ma sicuramente avrà il diritto e dovere di essere informato tempestivamente e continuativamente dell'attività di questo organismo", G. Falcone, Audizione presso il Consiglio Superiore della Magistratura, Commissione per il conferimento degli uffici direttivi, Seduta del 24 febbraio 1992, riportato in G. Governale, *La Direzione Nazionale Antimafia e la Direzione Investigativa Antimafia: la visione di Giovanni Falcone*, Cross, vol.5, n. 2, 2019.

³¹⁷ Ai fini del coordinamento il Procuratore può avvalersi dei servizi centrali delle Forze di polizia quali la Direzione Investigativa Antimafia (DIA), il Raggruppamento operativo speciale dell'Arma dei Carabinieri (ROS), il Servizio Centrale di investigazione sulla criminalità organizzata della Guardia di Finanza (SCICO).

³¹⁸ Sui collaboratori di giustizia, sull'applicazione dell'art. 41-bis dell'ordinamento penitenziario (regime carcerario particolarmente severo), sul gratuito patrocinio per gli imputati di reati di mafia non abbienti.

³¹⁹ Le principali materie di interesse sono: mafia, camorra, 'ndrangheta, narcotraffico, tratta di esseri umani, riciclaggio, appalti pubblici, misure di prevenzione patrimoniali, ecomafie, contraffazione di marchi, operazioni finanziarie sospette, organizzazioni criminali straniere.

di polizia o altri organismi che istituzionalmente operano nel medesimo ambito. Essi curano inoltre l'inserimento degli atti processuali delle DDA nella Banca Dati Nazionale, e i rapporti con le autorità giudiziarie di alcuni paesi particolarmente sensibili nelle materie di competenza, secondo le deleghe impartite dal Procuratore nazionale.

5.1. Il ruolo della DNAA nel sistema italiano antiriciclaggio

Il sistema di prevenzione antiriciclaggio basato sulla segnalazione alla UIF delle operazioni sospette è ormai considerato tra gli strumenti più moderni per il contrasto patrimoniale alla criminalità organizzata e al terrorismo. Al fine di rendere ancora più efficace l'utilizzo delle informazioni rivenienti dalle segnalazioni di operazioni sospette nelle indagini coordinate dalla DNAA, conseguendo anche una più fluida e proficua interazione della stessa Direzione con la UIF, il D.lgs. 231/2007 ha conosciuto rilevanti modifiche in occasione del recepimento della quarta e della quinta direttiva UE antiriciclaggio, che hanno disegnato un ruolo importante e innovativo per la DNAA.

Tale ruolo è oggi codificato nell'art. 8 del D.lgs. 231/2007, come modificato dal D.lgs. 190/2017, dedicato esclusivamente alla DNAA e volto principalmente a disciplinare la collaborazione e lo scambio di informazioni che la Direzione intrattiene con la UIF, con l'Agenzia delle dogane e dei monopoli e con le Autorità di vigilanza di settore.

In base al comma 1, lett. a) della norma citata, la DNAA, nell'esercizio delle competenze e nello svolgimento delle funzioni di coordinamento delle indagini e di impulso investigativo ad essa attribuite, riceve tempestivamente dalla UIF, per il tramite del Nucleo speciale di polizia valutaria della Guardia di Finanza ovvero, per quanto attinente alle segnalazioni relative alla criminalità organizzata, per il tramite della Direzione Investigativa Antimafia, informazioni tratte dalle segnalazioni di operazioni sospette e relative ai dati anagrafici dei soggetti segnalati o collegati, necessari per la verifica della loro eventuale attinenza a procedimenti giudiziari in corso. La DNAA può inoltre richiedere ogni altro elemento informativo e di analisi che ritenga di proprio interesse, anche ai fini della potestà di impulso attribuita al Procuratore Nazionale.

A questi fini, la legge consente alla DNAA la stipula di appositi protocolli tecnici con la UIF, la Guardia di finanza e la Direzione Investigativa Antimafia, volti a stabilire le modalità e la tempistica dello scambio di informazioni, assicurando l'adozione di ogni accorgimento idoneo a tutelare il trattamento in forma anonima dei dati anagrafici, necessari per la verifica della loro eventuale attinenza a procedimenti giudiziari in corso e la riservatezza dell'identità del segnalante.

L'obiettivo perseguito dalle disposizioni richiamate è quello di consentire alla DNAA di intervenire nella primissima fase dell'analisi delle operazioni sospette, confrontando le informazioni da queste rivenienti con quelle contenute nelle proprie banche dati³²⁰ allo scopo di migliorare la qualità degli approfondimenti investigativi. Un primo confronto avviene attraverso una procedura di "matching" anagrafico che consente di confrontare le informazioni contenute nelle segnalazioni con i registri concernenti i procedimenti penali iscritti presso le Procure Distrettuali per i reati previsti dall'art. 51 terzo comma *bis* c.p.p. nonché per i reati di terrorismo e con quelli concernenti le misure di prevenzione in materia di criminalità organizzata e terrorismo³²¹. Questo confronto permette di isolare le segnalazioni di operazioni sospette che riguardano processi in corso ovvero misure di prevenzione, affinché siano immediatamente trasmesse alla Procura Distrettuale procedente, omettendo qualsiasi ulteriore approfondimento e lasciando alla stessa autorità inquirente ogni valutazione circa il possibile utilizzo dell'informazione a fini investigativi. Un secondo confronto riguarda le segnalazioni di operazioni sospette che, pur non essendo riferibili a soggetti indagati, siano collegabili a persone fisiche o giuridiche presenti nella banca dati SIDNA. In questo caso le segnalazioni vengono approfondite all'interno della stessa DNA per l'eventuale trasmissione alla Direzione Distrettuale competente, anche mediante l'esercizio del potere di impulso attribuito al Procuratore Nazionale Antimafia e Antiterrorismo dall'art. 371-*bis* c.p.p.³²².

Oltre a garantire la speditezza, l'economicità e l'efficacia delle investigazioni che costituiscono il fondamento della attività di coordinamento attribuita alla Direzione, le tipologie di confronto dei dati sopra illustrate forniscono anche alla UIF indicazioni essenziali sulle possibili connessioni delle operazioni sospette con contesti di criminalità o di finanziamento del

³²⁰ Su cui cfr. F. Roller e F. Polino, *Il sistema SIDDA-SIDNA*, in M.V. De Simone e G. Russo (a cura di), *La Direzione Nazionale Antimafia e Antiterrorismo* cit., pp. 123 ss.

³²¹ Si tratta, rispettivamente, degli archivi "REGE/SICP" concernenti i procedimenti penali iscritti presso le Procure Distrettuali, e "SIPPI", relativo alle misure di prevenzione.

³²² Cfr. A. Laudati e A. Marandola, *Sviluppo e perfezionamento degli strumenti di contrasto antimafia: il ruolo della DNA*, in M.V. De Simone e G. Russo (a cura di), *La Direzione Nazionale Antimafia e Antiterrorismo* cit., pp. 63 ss.

terrorismo, utili per valutare la rischiosità delle relative segnalazioni, decidere le priorità di lavorazione, orientare la propria attività di analisi finanziaria, calibrandone la profondità.

Per l'attuazione pratica delle disposizioni di legge, il 7 maggio 2018, il 12 marzo 2021 e il 30 dicembre 2022 la UIF e la DNAA hanno sottoscritto e aggiornato un Protocollo d'Intesa volto a disciplinare i principali aspetti della collaborazione reciproca. Il nuovo accordo, in particolare, mira ad accrescere la tempestività dei flussi informativi tra la Direzione e l'Unità e la quantità dei dati oggetto di *matching* anagrafico (estesi anche ad alcune tipologie di comunicazioni di FIU estere), per consentire un più immediato utilizzo delle informazioni contenute nelle segnalazioni di operazioni sospette e nelle comunicazioni della FIU estere da parte della magistratura e favorire la profondità delle analisi finanziarie svolte dalla UIF³²³.

Un ulteriore aspetto della collaborazione tra UIF e DNAA trova specifica disciplina nell'art. 8, comma 1, lett. d), del D.lgs. 231/2007, che consente alla DNAA di chiedere alla UIF l'analisi dei flussi finanziari ovvero analisi e studi su singole anomalie, riferibili a ipotesi di utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività della criminalità organizzata o di finanziamento del terrorismo, su specifici settori dell'economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realtà economiche territoriali. Si tratta di una norma volta a sfruttare il patrimonio di dati di carattere generale pure a disposizione della UIF per consentire alla DNAA di effettuare analisi a spettro esteso e di orientare particolari tipologie di indagini. Dalla disponibilità di dati di carattere generale traggono spunto alcune attività sviluppate dalla DNAA nell'ambito del polo di interesse dedicato al contrasto patrimoniale alla criminalità organizzata e al terrorismo.

Un apposito "tavolo tecnico", del quale fanno parte, oltre alla DNAA, la UIF, l'Agenzia delle dogane e monopoli, la DIA, la Polizia postale, lo SCICO e il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e il ROS dell'Arma dei Carabinieri si occupa delle tematiche relative alle valute virtuali, allo scopo approfondire i sistemi di pagamento elettronici e l'uso delle "cripto-valute" a fini illeciti. Anche in questo caso l'attività mira a sfruttare il potenziale informativo a disposizione della Direzione (*in primis*, le segnalazioni di operazioni sospette) e la collaborazione con gli intermediari in chiave preventiva al fine di ricostruire possibili reti di collegamento criminale sul territorio nazionale³²⁴.

L'art. 8 disciplina anche ulteriori flussi informativi che hanno al centro la DNAA. La lett. b) dispone che la Direzione riceva dall'Agenzia delle dogane e dei monopoli i dati e le informazioni necessari all'individuazione di possibili correlazioni tra flussi merceologici a rischio e flussi finanziari sospetti. Anche in questo caso, le modalità e le tempistiche degli scambi di informazioni sono regolate nel concreto sulla base di protocolli tecnici stipulati con la medesima Agenzia.

In particolare, il Protocollo sottoscritto il 2 marzo 2018 tra la Direzione e l'Agenzia prevede la centralizzazione della raccolta, dell'elaborazione e dell'analisi dei dati utili alla prevenzione e alla repressione di illeciti quali i traffici transfrontalieri di rifiuti, sostanze stupefacenti, materiali strategici o prodotti agroalimentari, al fine, da un lato, di supportare le prerogative di impulso e coordinamento investigativo da parte della DNA, dall'altro, di rinforzare le procedure di controllo doganale e quelle di contrasto ai fenomeni illegali da parte dell'Agenzia.

La lett. e), inoltre, consente alla DNAA l'accesso alle informazioni sul titolare effettivo di persone giuridiche e trust, contenute nell'apposita sezione del registro delle imprese, ai sensi dell'art. 21 del D.lgs. 231/2007, e di chiedere alle autorità di vigilanza di settore ogni altra informazione utile all'esercizio delle proprie attribuzioni. Anche tali flussi di informazioni consentono alla DNAA di accrescere la propria capacità di coordinamento e orientamento informativo delle indagini sul territorio.

Infine, alcune disposizioni dell'art. 8 riguardano i flussi di ritorno che la DNAA è tenuta a indirizzare ai propri interlocutori. In particolare, ferme le disposizioni vigenti in materia di tutela del segreto investigativo, la Direzione fornisce alla UIF e all'Agenzia delle dogane e dei monopoli tempestivo riscontro in ordine all'utilità delle informazioni ricevute. Come si è detto, tale feedback è essenziale per consentire alle istituzioni destinatarie di orientare la propria attività, di decidere priorità di trattazione, di gestire ogni utile approfondimento.

³²³ Sulla collaborazione tra UIF e DNAA, con particolare riguardo alla condivisione delle informazioni tratte dalle segnalazioni di operazioni sospette connesse con l'emergenza sanitaria, si veda C. Clemente, *Audizione del Direttore dell'Unità di Informazione Finanziaria per l'Italia sull'attività di prevenzione e contrasto dei fenomeni di criminalità finanziaria connessi con l'emergenza da Covid-19*, Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere, Roma, 16 luglio 2020.

³²⁴ Altre iniziative riguardano i rapporti con l'ABI, il monitoraggio dei beni confiscati e del Fondo Unico Giustizia.

Nel contesto della complessiva rendicontazione pubblica dei risultati dell'azione di prevenzione e contrasto, anche la DNAA è tenuta a fornire al Comitato di sicurezza finanziaria, nel rispetto del segreto di indagine, i dati in proprio possesso, utili all'elaborazione dell'analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo e le proprie valutazioni sui risultati dell'attività di contrasto del riciclaggio e del finanziamento del terrorismo, necessarie per l'elaborazione della Relazione annuale trasmessa dal Ministero dell'economia e delle finanze al Parlamento ai sensi dell'art. 5, comma 7, del D.lgs. 231/2007.

5.2. Il ruolo di coordinamento della DNAA nel sistema di prevenzione antiriciclaggio

Il modello organizzativo e operativo seguito dalla DNAA fin dalla sua istituzione è quello di una struttura funzionale al coordinamento delle indagini per mafia e terrorismo svolte sul territorio, all'analisi delle caratteristiche strutturali e territoriali dei fenomeni criminali, all'acquisizione e all'utilizzo di strumenti informativi di tipo preventivo.

Questo modello è stato inizialmente concepito e successivamente declinato secondo un coordinamento "di tipo orizzontale"³²⁵, teso a escludere l'assunzione da parte della DNAA di qualsivoglia posizione gerarchica rispetto alle Procure distrettuali e a costituire, invece, una "cabina di regia" con compiti di "impulso, di promozione del collegamento e del coordinamento investigativo, da realizzarsi anche attraverso l'utilizzo di strumenti informatici, la promozione dei rapporti internazionali e l'analisi dei fenomeni attinenti alla criminalità organizzata"³²⁶.

L'evoluzione degli ultimi anni ha rafforzato progressivamente la posizione e le funzioni della DNAA, ben oltre il ruolo di mera "cabina di regia", favorendo lo sviluppo di una capacità di analisi completa e aggiornata dei fenomeni criminali, l'elaborazione di strategie integrate di contrasto, la costruzione di un "sapere investigativo specializzato e unitario"³²⁷, a beneficio dell'azione delle Direzioni Distrettuali, poste in condizioni di dare una risposta giudiziaria "non frammentata" ai crimini di mafia³²⁸.

In questo contesto, la sempre più netta connotazione in senso preventivo dei poteri informativi della DNAA e del conseguente coordinamento delle indagini sul territorio trova una conferma significativa nella posizione che il legislatore ha assegnato alla Direzione nel sistema antiriciclaggio. Rilevo peculiare hanno assunto, infatti, l'acquisizione e l'elaborazione di crescenti quantità di dati e informazioni di diversa fonte³²⁹ sulla criminalità organizzata e sul terrorismo, utili a consentire "una "radiografia" dei fenomeni su basi territoriali più estese e collegate" e funzionali a un impulso essenzialmente informativo a "vaste operazioni investigative di contrasto con esiti processuali conseguenti".

Il D.lgs. 231/2007, come modificato dal D.lgs. 190/2017, ha ulteriormente valorizzato le reti inter-istituzionali su cui si fonda il sistema nazionale antiriciclaggio, coinvolgendo anche la DNAA (e in misura ben più rilevante rispetto al passato) negli scambi di flussi informativi, nelle attività di confronto dei dati, nella collaborazione operativa. Essenziale, da questo punto di vista, è il peso assegnato alla condivisione delle informazioni sulle segnalazioni di operazioni sospette tra la Direzione e la UIF. Le segnalazioni, infatti, benché rappresentative di meri sospetti (ben lontani, pertanto, dal poter assumere immediata evidenza giudiziaria), sono ormai riconosciute come la principale fonte di arricchimento informativo a disposizione della DNAA, idonea a imprimere un forte impulso ad attività investigative e giudiziarie, orientandone significativamente lo svolgimento³³⁰. Si alimenta, in tal modo, quell'azione preventiva di

³²⁵ Così G. Falcone, *Audizione cit.*

³²⁶ In base anche al decreto del Ministero dell'Economia e delle finanze dell'11 marzo 2022, n. 55, *Regolamento recante disposizioni in materia di comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di trust produttivi di effetti giuridici rilevanti ai fini fiscali e di istituti giuridici affini al trust*, in G.U. n.121 del 25 maggio Così G. Falcone, *Audizione cit.*

³²⁷ G. Canzio, S. Liotta, F. Spiezia, *La Direzione Nazionale Antimafia e il coordinamento cit.*

³²⁸ G. Canzio, S. Liotta, F. Spiezia, *La Direzione Nazionale Antimafia e il coordinamento cit.*

³²⁹ Segnalazioni di collaboratori di giustizia, segnalazioni di operazioni sospette, comunicazioni di FIU estere, interdittive antimafia, informazioni rivenienti dal canale rogatorio e dall'EPPO, comunicazioni del CSF e del DAP, oltre al notevole patrimonio sulle indagini contenuto nell'archivio SIDNA.

³³⁰ "Tra gli strumenti più moderni per il contrasto patrimoniale alla criminalità organizzata e al terrorismo vi è il meccanismo del sistema antiriciclaggio e delle SOS così come delineato dall'impianto della legge 231/2007". Così F. Cafiero De Raho, *Comunicazione della Commissione relativa a un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del*

analisi e coordinamento informativo in cui si sostanzia il ruolo principale della stessa Direzione, sintetizzabile nel concetto di “pre-investigazione”³³¹.

Questo ruolo colloca dunque la DNAA al crocevia tra i due poli dell’azione di contrasto, quello preventivo e quello dell’individuazione e repressione dei reati, con il compito di massimizzare il valore delle informazioni finanziarie ai fini dell’orientamento e dell’arricchimento di ogni successiva attività di indagine.

6. Amministrazioni e organismi interessati (S. Pace)

Le amministrazioni e gli organismi interessati rientrano tra le Autorità con competenze rilevanti per la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo in quanto presiedono alla verifica sul rispetto degli obblighi da parte dei soggetti non sottoposti al controllo delle Autorità di vigilanza di settore³³².

Essi sono coinvolti, in generale, nelle attività di prevenzione promosse dal MEF, contribuiscono alla stesura della relazione annuale del Comitato di Sicurezza Finanziaria (CSF)³³³, sono competenti ad accertare e contestare alcune violazioni amministrative della disciplina antiriciclaggio³³⁴ e sono parte attiva della collaborazione e dello scambio di informazioni tra Autorità nazionali³³⁵, anche se non rientrano nel circuito delle Autorità nei confronti delle quali il segreto di ufficio è derogabile³³⁶.

6.1. Amministrazioni interessate

Le amministrazioni interessate non sono puntualmente individuate ma vengono richiamate in diverse norme e astrattamente indicate come titolari di poteri di controllo ovvero competenti al rilascio di concessioni, autorizzazioni, licenze o altri titoli abilitativi. Per le esclusive finalità di cui al D.lgs. 231/2007, sono considerate tali il Ministero dell’economia e delle finanze (MEF), quale autorità preposta alla sorveglianza dei revisori legali e delle società di revisione legale senza incarichi di revisione legale su enti di interesse pubblico o su enti sottoposti a regime intermedio, e il Ministero dello sviluppo economico (MISE), quale autorità preposta alla sorveglianza delle società fiduciarie non iscritte nell’albo di cui all’art. 106 TUB.

Tra le amministrazioni interessate è compresa, per il suo ruolo di supervisione nel settore del gioco, l’Agenzia delle Dogane e dei Monopoli (ADM). Pur non ricevendo dal D.lgs. 231/2007 la qualifica di

terrorismo, Audizione del Procuratore Nazionale antimafia e antiterrorismo alle Commissioni riunite II (Giustizia) e VI (Finanze) della Camera dei Deputati, Roma, 13 ottobre 2020. Pochi mesi prima, lo stesso Procuratore aveva affermato che “vanno potenziati monitoraggio e controllo delle segnalazioni per individuare soggetti potenzialmente pericolosi. Bisogna puntare sulla normativa antiriciclaggio, che ha già dimostrato la sua efficacia, e sulla segnalazione di operazioni sospette”, F. Cafiero De Raho, *Audizione informale del Procuratore Nazionale Antimafia e Antiterrorismo*, Commissioni Riunite Finanze e Attività Produttive della Camera dei Deputati, Esame relativo alla conversione in legge del c.d. “Decreto Liquidità”, Roma, 29 aprile 2020.

³³¹ “In un momento storico in cui l’emergenza terrorismo ha messo in crisi la distinzione tra l’*intelligence* e l’*evidence*, l’unico strumento che appare efficace è quello della pre-investigazione”. Così DNAA, *Relazione sulle attività svolte* cit., par. 8.5.2. *Le attività di contrasto in materia di finanziamento del terrorismo*, p. 489.

³³² Ai sensi dell’art. 1, comma 2, lett. a), del D.lgs. 231/2007, per “Amministrazioni e organismi interessati” si intendono: “*le amministrazioni, ivi comprese le agenzie fiscali, titolari di poteri di controllo ovvero competenti al rilascio di concessioni, autorizzazioni, licenze o altri titoli abilitativi comunque denominati, nei confronti dei soggetti obbligati e gli organismi preposti alla vigilanza sul possesso dei requisiti di professionalità e onorabilità, prescritti dalla pertinente normativa di settore nei confronti dei predetti soggetti*”.

³³³ Le amministrazioni e gli organismi interessati forniscono al CSF, entro il 30 marzo di ogni anno, i dati statistici e le informazioni sulle attività rispettivamente svolte, nell’anno solare precedente, nell’ambito delle funzioni di vigilanza, supervisione e controllo (art. 5, comma 7, del D.lgs. 231/2007).

³³⁴ Cfr. art. 12, comma 2, del D.lgs. 231/2007.

³³⁵ Le amministrazioni e gli organismi interessati collaborano per agevolare l’individuazione di ogni circostanza in cui emergono fatti e situazioni la cui conoscenza può essere comunque utilizzata per prevenire l’uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo (art. 12, comma 1, del D.lgs. 231/2007).

³³⁶ Cfr. art. 12, commi 1 e 1-bis e comma 8 del D.lgs. 231/2007, come modificato dal DL 4/2022 (c.d. Sostegni-ter) convertito dalla legge 28 marzo 2022, n. 25. Tale circostanza rischia di influire negativamente sull’efficacia delle azioni che, in coordinamento con le altre Autorità antiriciclaggio, potrebbero essere intraprese per ottenere proficua collaborazione attiva da soggetti non strettamente “vigilati”, operanti in settori a rischio.

“Autorità di vigilanza di settore”, l’ADM è infatti titolare di poteri di controllo e competente al rilascio di concessioni e autorizzazioni ai soggetti in possesso dei requisiti prescritti dalla normativa di settore³³⁷.

All’ADM sono poi attribuite funzioni di regolamentazione, indirizzo, coordinamento e controllo attraverso: l’elaborazione di standard tecnici, anche sulla base dell’analisi nazionale del rischio di riciclaggio e di finanziamento del terrorismo elaborata dal CSF³³⁸; l’emanazione, previa presentazione al CSF, di linee guida ad ausilio dei concessionari, in ordine alle procedure e ai sistemi di controllo volti a mitigare e gestire i rischi di riciclaggio e finanziamento del terrorismo; la verifica dell’osservanza da parte dei concessionari degli adempimenti previsti a loro carico³³⁹; il riscontro dell’autenticità dei dati contenuti nei documenti presentati dai richiedenti l’apertura dei conti di gioco³⁴⁰; l’adozione di protocolli d’intesa con il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, volti ad assicurare lo scambio di informazioni necessario a garantire il coordinamento, l’efficacia e la tempestività delle attività di controllo dell’adeguatezza dei sistemi di prevenzione e contrasto del riciclaggio di denaro e di finanziamento del terrorismo, adottati dai prestatori di servizi di gioco³⁴¹.

In assenza di una normativa antiriciclaggio specifica, per i soggetti non sottoposti al controllo delle Autorità di vigilanza, un ruolo significativo è svolto anche da iniziative di autoregolamentazione (es. linee guida) promosse dalle associazioni di categoria per i rispettivi settori di attività. In tal senso si richiama, ad esempio, la “Guida all’Antiriciclaggio” elaborata dall’UNIREC (Unione Nazionale Imprese a Tutela del Credito) che ha disciplinato alcuni profili applicativi degli obblighi antiriciclaggio per le società di recupero crediti.

6.2. Organismi di autoregolamentazione

Il D.lgs. 231/2007, come modificato dal D.lgs. 90/2017, attribuisce agli organismi di autoregolamentazione³⁴² poteri normativi, di contributo per l’analisi e la valutazione del rischio, di controllo e sanzionatori e di formazione, oltre che di possibile interposizione nei rapporti con la UIF per l’inoltro delle segnalazioni di operazioni sospette³⁴³.

Agli organismi di autoregolamentazione spettano l’elaborazione e l’aggiornamento di regole tecniche, previo parere del Comitato di sicurezza finanziaria (CSF), in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui i professionisti sono esposti nell’esercizio della propria attività, di controlli interni, di adeguata verifica, anche semplificata, della clientela e di conservazione³⁴⁴.

Gli organismi individuano, inoltre, i requisiti dimensionali e organizzativi in base ai quali i soggetti obbligati controllati debbono adottare specifici presidi, controlli e procedure per la valutazione e gestione del rischio di riciclaggio e di finanziamento del terrorismo nonché per l’introduzione di una funzione antiriciclaggio, ivi comprese, se adeguate rispetto alle dimensioni e alla natura dell’attività, la nomina di un responsabile della funzione antiriciclaggio e la previsione di una funzione di revisione indipendente per la verifica delle politiche, dei controlli e delle procedure³⁴⁵.

Le regole tecniche forniscono ai professionisti, in applicazione dell’approccio basato sul rischio³⁴⁶, istruzioni operative sulle modalità da seguire nell’assolvimento degli obblighi antiriciclaggio, tenuto conto

³³⁷ Si ha altresì presente che l’Agenzia delle Dogane e dei Monopoli è espressamente inclusa fra le “agenzie fiscali” (istituite dall’art. 57 del D.lgs. 30 luglio 1999, n. 300, e richiamate dal medesimo art. 1, comma 2, lett. a), del decreto antiriciclaggio).

³³⁸ Cfr. art. 54, comma 1, del D.lgs. 231/2007.

³³⁹ Cfr. art. 52, comma 4, del D.lgs. 231/2007. L’ADM, nell’esercizio delle proprie competenze e attribuzioni istituzionali nel comparto del gioco pubblico, ha emanato, nel febbraio 2019, apposite linee guida ad ausilio dei concessionari di gioco in materia di antiriciclaggio e per la mitigazione del rischio.

³⁴⁰ Cfr. art. 53, comma 4, del D.lgs. 231/2007.

³⁴¹ Cfr. art. 54, comma 2, del D.lgs. 231/2007.

³⁴² Ai sensi dell’art. 1, comma 2, lett. aa), del D.lgs. 231/2007 per “organismo di autoregolamentazione” si intende “l’ente esponenziale, rappresentativo di una categoria professionale, ivi comprese le sue articolazioni territoriali e i consigli di disciplina cui l’ordinamento vigente attribuisce poteri di regolamentazione, di controllo della categoria, di verifica del rispetto delle norme che disciplinano l’esercizio della professione e di irrogazione, attraverso gli organi all’uopo predisposti, delle sanzioni previste per la loro violazione”.

³⁴³ Cfr. artt. 11, 15 e 37 del D.lgs. 231/2007.

³⁴⁴ Cfr. art. 11, comma 2, del D.lgs. 231/2007.

³⁴⁵ Cfr. art. 16, comma 2, del D.lgs. 231/2007.

³⁴⁶ L’adozione di tale approccio mira a favorire l’abbandono di logiche burocratiche nell’adempimento degli obblighi, promuovendo invece la concentrazione sulle situazioni più esposte al rischio.

delle specificità delle varie categorie professionali e, in generale, della diversità del mondo delle professioni, in termini di scala e dimensioni, rispetto agli intermediari bancari e finanziari³⁴⁷.

In attuazione di quanto previsto dal riformato D.lgs. 231/2007, il Consiglio Nazionale del Notariato (CNN), il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC), il Consiglio Nazionale Forense (CNF) e il Consiglio Nazionale dei Consulenti del Lavoro (CNOCDL) si sono dotati, dopo il rilascio dei rispettivi pareri del CSF³⁴⁸, di propri corpi di regole tecniche in materia di adeguata verifica della clientela e di conservazione dei dati, documenti e informazioni, a beneficio delle rispettive categorie di professionisti³⁴⁹.

Le regole tecniche del CNN individuano alcune attività notarili per le quali sono da intendersi esclusi gli obblighi di adeguata verifica e si soffermano sulla disciplina applicabile dopo la riforma del 2017. Sono fornite, altresì, indicazioni in tema di adeguata verifica semplificata, in particolare con riferimento a fattori di basso rischio relativi a tipologie di clienti, nonché riguardo alle modalità di acquisizione di informazioni su scopo e natura della prestazione. Ulteriori regole riguardano l'identificazione del cliente ovvero dell'esecutore e del titolare effettivo, i tempi di svolgimento dell'adeguata verifica e le modalità di conservazione dei dati e delle informazioni³⁵⁰.

Le regole tecniche approvate dal CNDCEC forniscono indicazioni per l'adempimento degli obblighi in materia di valutazione del rischio, adeguata verifica della clientela e conservazione dei documenti, dei dati e delle informazioni agli iscritti all'Albo dei Dottori Commercialisti e degli Esperti Contabili di cui al D.lgs. 28 giugno 2005, n. 139³⁵¹. Il medesimo organismo di autoregolamentazione ha altresì approvato, in data 16 maggio 2019, delle "Linee guida per la valutazione del rischio, adeguata verifica, conservazione dei documenti, dei dati e delle informazioni ai sensi del D.lgs. 231/2007", aventi valenza meramente esemplificativa, relative alle predette regole tecniche³⁵².

Le regole tecniche emanate dal CNF sono tese a escludere l'applicazione della normativa di prevenzione con riguardo a talune attività svolte dagli avvocati, a fornire chiarimenti sulla disciplina applicabile dopo la riforma del 2017 e istruzioni in materia di valutazione del rischio, adeguata verifica e conservazione. Alle regole tecniche è allegato un corposo documento contenente i criteri e le metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo, con particolare riferimento all'adeguata verifica semplificata.

Le regole tecniche del CNOCDL riportano indicazioni in merito all'analisi e valutazione dei rischi connessi all'attività professionale dei consulenti del lavoro, alle misure di adeguata verifica della clientela, all'adeguata verifica rafforzata da attuare in presenza di persone politicamente esposte (PEP) nonché in materia di identificazione della clientela, di identificazione del titolare effettivo e di corretto adempimento dell'obbligo di conservazione della documentazione³⁵³.

³⁴⁷ La natura giuridica di tali regole è discussa. Secondo uno studio del Consiglio Nazionale del Notariato si sarebbe di fronte a "fonti normative integrative della norma primaria, non a norme regolamentari subordinate e neppure ad ipotesi di *soft law*", in quanto sarebbe la legge primaria a prevedere una delega, attribuendo a tali fonti il compito di completare la normazione da essa prodotta, configurando un rinvio, mancando il quale la stessa legge sarebbe incompleta ed inapplicabile" (Cfr. "*Le Regole tecniche elaborate dagli organismi di autoregolamentazione nella rete delle fonti del diritto*", studio del CNN n. 1-2018/B, novembre 2018).

³⁴⁸ Le regole tecniche sono state rispettivamente approvate dal CNN in data 16 ottobre 2018, dal CNDCEC in data 16 gennaio 2019, dal CNF in data 20 settembre 2019 e dal CNOCDL in data 27 maggio 2022. Il CSF ha statuito che tali regole, se adeguate ai contenuti del parere e applicate in senso ad esso conforme, costituiscono idonee modalità semplificate di adempimento degli obblighi di adeguata verifica della clientela e di conservazione prescritti dalla vigente normativa.

³⁴⁹ Nella definizione delle regole tecniche si è tenuto conto della "Metodologia per la mappatura dei rischi dei professionisti" approvata dal CSF in data 27 marzo 2018, a supporto dell'attività richiesta agli organismi di autoregolamentazione, per agevolare la mappatura e classificazione dei rischi di riciclaggio e finanziamento del terrorismo. In particolare, nella Metodologia vengono descritte le operazioni che il professionista deve compiere per attribuire la classe di rischio effettiva alla prestazione o all'operazione e, conseguentemente, le rispettive misure di adeguata verifica da adottare; ciò sulla base di una valutazione congiunta del "rischio inerente" (rischio proprio delle attività svolte dal professionista, considerate per categorie omogenee, in termini oggettivi ed astratti e tenuto conto delle peculiarità tipiche della professione) e del "rischio specifico" (rischio proprio dell'atto o dell'operatività costituente oggetto della prestazione professionale, per come in concreto definita in occasione del conferimento dell'incarico).

³⁵⁰ Tali regole sono state integrate da un successivo documento approvato dal CNN e trasmesso al Ministero dell'Economia e delle finanze (MEF) per il prescritto parere del CSF ("Regole tecniche per l'analisi e la valutazione del rischio di riciclaggio").

³⁵¹ In particolare, il CNDCEC ha classificato le principali prestazioni rese da commercialisti ed esperti contabili in base al rischio inerente alle stesse, fornendo dettagli applicativi, soprattutto in tema di adeguata verifica ordinaria, semplificata e rafforzata, nonché di adempimento degli obblighi di conservazione.

³⁵² Le soluzioni operative proposte nelle Linee guida sono frutto di orientamenti interpretativi maturati in assenza di specifiche indicazioni da parte delle Autorità competenti, per cui vengono periodicamente aggiornate in conformità alle interpretazioni ufficiali diffuse da tali Autorità su specifici aspetti.

³⁵³ In particolare, il testo si compone di sei regole tecniche e di un'appendice contenente l'elenco delle categorie di persone politicamente esposte e dei Paesi terzi con regimi deboli di lotta contro il riciclaggio e il finanziamento del terrorismo e una scheda per la valutazione del rischio specifico.

Gli organismi di autoregolamentazione sono chiamati ad applicare, attraverso propri organi all'uopo predisposti, sanzioni disciplinari dirette a punire eventuali violazioni gravi, ripetute o sistematiche ovvero plurime degli obblighi antiriciclaggio e delle relative disposizioni tecniche di attuazione cui i propri iscritti sono tenuti³⁵⁴. A tal fine il MEF informa gli organismi in caso di violazioni qualificate della Legge antiriciclaggio, ai fini dell'adozione di ogni atto idoneo ad intimare ai responsabili di porre termine alle violazioni e di astenersi dal ripeterle³⁵⁵. Gli organismi, a loro volta, debbono comunicare annualmente al MEF e al Ministero della Giustizia i dati attinenti il numero dei procedimenti disciplinari avviati o conclusi dagli ordini territoriali.

Il potere di controllo degli organismi nei confronti dei propri iscritti non è esclusivo, ma concorre con quello esercitato dal Nucleo speciale di polizia valutaria della Guardia di Finanza (NSPV) che, nel quadro degli obiettivi e priorità strategiche individuati annualmente dal MEF, esegue i controlli sull'osservanza delle disposizioni dettate dalla Legge antiriciclaggio da parte dei soggetti obbligati non vigilati dalle Autorità di vigilanza di settore³⁵⁶.

Gli organismi di autoregolamentazione collaborano inoltre con le altre Autorità, amministrazioni e organismi interessati, nonché con l'Autorità giudiziaria e gli organi delle indagini per agevolare l'individuazione di ogni circostanza da cui emergano fatti e situazioni la cui conoscenza può essere comunque utilizzata per prevenire l'uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo.

In tale ambito, particolarmente significativa è la collaborazione con il Comitato di sicurezza finanziaria (CSF), al quale gli organismi, ai fini dell'analisi nazionale del rischio di riciclaggio e di finanziamento del terrorismo svolta dallo stesso Comitato con cadenza triennale, devono fornire i dati quantitativi e statistici sulla dimensione e importanza dei settori rientranti nell'ambito di applicazione del D.lgs. 231/2007, tra cui il numero dei soggetti vigilati e l'importanza economica di ciascun settore nonché i dati statistici e le informazioni sulle attività svolte, nell'anno solare precedente, nell'ambito delle funzioni di vigilanza, supervisione e controllo³⁵⁷.

Gli organismi di autoregolamentazione sono altresì investiti di poteri consultivi, nel rapporto di collaborazione con l'UIF, in quanto debbono essere sentiti ai fini dell'adozione e dell'aggiornamento degli indicatori di anomalia di cui all'art. 6, comma 4, lett. e), del D.lgs. 231/2007³⁵⁸. Infine, agli organismi è attribuita la responsabilità di formare e aggiornare i propri iscritti in materia di politiche e strumenti di prevenzione del riciclaggio e di finanziamento del terrorismo.

7. Organi investigativi: NSPV e DIA (W. Negrini)

Nella filiera delle Autorità coinvolte nella prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo, il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (NSPV) e la Direzione Investigativa Antimafia (DIA) sono gli Organi di polizia deputati in Italia a ricevere gli esiti delle analisi finanziarie condotte dalla UIF sulle segnalazioni di operazioni sospette, per lo sviluppo investigativo delle successive indagini.

³⁵⁴ Cfr. art. 11, comma 3, del D.lgs. 231/2007. L'obbligo di acquisire previamente il parere del Comitato di sicurezza finanziaria (CSF) conferisce alle regole tecniche elaborate dagli organismi quel valore giuridico che ne giustifica la sanzionabilità sul piano disciplinare.

³⁵⁵ Per il compimento di tali violazioni gli organismi di autoregolamentazione (consigli di disciplina) applicano le sanzioni disciplinari, ai sensi e per gli effetti dei rispettivi ordinamenti, fermo restando che l'eventuale interdizione dallo svolgimento della funzione, dell'attività o dell'incarico non può essere inferiore a due mesi e superiore a cinque anni.

³⁵⁶ Art. 9, comma 1, del D.lgs. 231/2007.

³⁵⁷ Ai sensi dell'art. 11, comma 4-*bis*, del D.lgs. 231/2007 gli organismi di autoregolamentazione sono altresì tenuti a pubblicare, dandone preventiva informazione al CSF, una relazione annuale contenente: a) il numero dei decreti sanzionatori e delle altre misure sanzionatorie, suddivisi per tipologia di infrazione, adottati dalle competenti autorità, nei confronti dei rispettivi iscritti, nell'anno solare precedente; b) il numero di segnalazioni di operazioni sospette ricevute dall'organismo di autoregolamentazione, per il successivo inoltro alla UIF; c) il numero e la tipologia di misure disciplinari, adottate nei confronti dei rispettivi iscritti a fronte di violazioni gravi, ripetute, sistematiche ovvero plurime degli obblighi in materia di controlli interni, di adeguata verifica della clientela, di conservazione e di segnalazione di operazioni sospette.

³⁵⁸ In merito alla possibilità per gli organismi di autoregolamentazione di ricevere le segnalazioni di operazioni sospette dei propri iscritti, per il successivo inoltro alla UIF, si rinvia all'Appendice.

L'art. 40, comma 1, lett. d), del D.lgs. 231/2007 stabilisce infatti che, fermo restando l'obbligo di denuncia delle notizie di reato ai sensi dell'art. 331 c.p.p., la UIF trasmette senza indugio a NSPV e DIA le segnalazioni di operazioni sospette che presentano un rischio di riciclaggio o di finanziamento del terrorismo e i risultati delle analisi svolte, incluse le informazioni ad esse pertinenti relative ai reati presupposto associati, nonché le comunicazioni di operazioni sospette provenienti dalle Pubbliche amministrazioni e le relative analisi³⁵⁹. Per converso, il NSPV e la DIA devono a loro volta informare la UIF, anche sulla base di appositi protocolli d'intesa, degli esiti investigativi dell'approfondimento delle segnalazioni di operazioni sospette, fatte salve le norme sul segreto di indagine³⁶⁰.

Il NSPV opera sia come organismo investigativo di polizia sia nella qualità di organo amministrativo di controllo del rispetto degli obblighi antiriciclaggio. Con riguardo alla prima funzione, il D.lgs. 231/2007 esplicita che l'autorità giudiziaria può chiedere al NSPV i risultati degli approfondimenti investigativi svolti sulle segnalazioni di operazioni sospette³⁶¹; per quanto concerne, invece, la funzione di organi di controllo, l'art. 9 del D.lgs. 231/2007 stabilisce una generale competenza del NSPV a eseguire i controlli sul rispetto degli obblighi da parte dei soggetti non vigilati nonché quelli ulteriori effettuati, in collaborazione con la UIF che ne richieda l'intervento a supporto dell'esercizio delle funzioni di propria competenza. Ulteriori verifiche possono essere eseguite, previa intesa con le Autorità di vigilanza di settore, su alcune specifiche categorie di soggetti vigilati³⁶².

La frequenza e l'intensità dei controlli e delle ispezioni è definita in funzione del profilo di rischio, della natura e delle dimensioni dei soggetti obbligati e dei rischi nazionali e transfrontalieri di riciclaggio e di finanziamento del terrorismo. Nello svolgimento delle verifiche il NSPV utilizza i poteri attribuiti al Corpo dalla normativa valutaria³⁶³ e acquisisce dati e informazioni presso i soggetti obbligati.

Il NSPV e la DIA accertano e contestano (ovvero trasmettono alle Autorità di vigilanza di settore) le violazioni degli obblighi antiriciclaggio riscontrate nell'esercizio dei propri compiti. È inoltre espressamente specificato che i "dati e le informazioni acquisite nell'ambito delle attività svolte [...] sono utilizzabili ai fini fiscali, secondo le disposizioni e le attribuzioni vigenti"³⁶⁴.

³⁵⁹ NSPV e DIA, a loro volta, provvedono alla trasmissione di tali segnalazioni nei confronti del Procuratore nazionale antimafia e antiterrorismo qualora siano attinenti alla criminalità organizzata o al terrorismo (art. 40, comma 1, lett. d), del D.lgs. 231/2007). All'interno del Nucleo è stato istituito, con determinazione del Comandante Generale della Guardia di Finanza n. 237345/3102 del 30 luglio 2016, il Gruppo investigativo finanziamento del terrorismo (G.I.F.T.), con competenze precise di analisi e indagine in materia di finanziamento del terrorismo; in argomento, cfr. M. Carbone, P. Bianchi, V. Vallefucio, *Le nuove regole antiriciclaggio. Obblighi antiriciclaggio a carico di professionisti, intermediari bancari e finanziari e operatori non finanziari*, cit., p. 406-407. NSPV e DIA sono inoltre tempestivamente informati dalla UIF nei casi di dati e informazioni comunicati agli Organismi di informazione per la sicurezza della Repubblica ai sensi dell'art. 40, comma 1, lett. e), del D.lgs. 231/2007.

³⁶⁰ Art. 41, comma 1, del D.lgs. 231/2007. Ai sensi del successivo comma 4, la UIF, la GdF e la DIA forniscono altresì al CSF informazioni sull'esito delle segnalazioni ripartito per categoria dei segnalanti, tipologia delle operazioni e aree territoriali.

³⁶¹ Analoga richiesta, per quanto attiene alla criminalità organizzata, può essere avanzata nei confronti della DIA. D'altra parte, ai sensi del comma 3 del medesimo art. 12, fermo quanto disposto dall'art. 40 in materia di analisi e sviluppo investigativo della segnalazione di operazione sospetta, l'autorità giudiziaria, nell'ambito di indagini relative all'esistenza di reati di riciclaggio, di autoriciclaggio, di reati a essi presupposti ovvero di attività di finanziamento del terrorismo e ogni qualvolta lo ritenga necessario per lo svolgimento di un procedimento penale, può richiedere alla UIF, con le garanzie di cui all'art. 38, i risultati delle analisi e qualsiasi altra informazione pertinente.

³⁶² Si tratta di: istituti di pagamento, istituti di moneta elettronica e relative succursali; punti di contatto centrale, designati dagli istituti di moneta elettronica o dai prestatori di servizi di pagamento con sede legale e amministrazione centrale in un altro Stato membro, che operano, senza succursale, sul territorio nazionale tramite i soggetti convenzionati e gli agenti; società fiduciarie e intermediari iscritti all'albo previsto dall'art. 106 T.u.b.; i soggetti eroganti micro-credito ai sensi dell'art. 111 T.u.b., i confidi e gli altri soggetti di cui all'art. 112 del medesimo Testo Unico; - succursali insediate sul territorio della Repubblica di intermediari bancari e finanziari e di imprese assicurative aventi sede legale e amministrazione centrale in un altro Stato membro o in uno Stato terzo; intermediari assicurativi di cui all'art. 109, comma 2, lett. a), b) e d), D.lgs. 209/2005 (CAP), che operano nei rami di attività di cui all'art. 2, comma 1, del medesimo Codice; revisori legali e società di revisione legale con incarichi di revisione legale su enti di interesse pubblico o su enti sottoposti a regimi intermedio; soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'art. 134 TULPS, salve le competenze in materia di pubblica sicurezza attribuite dal medesimo Testo Unico.

³⁶³ I medesimi poteri sono attribuiti ai militari appartenenti ai reparti della Guardia di Finanza ai quali il NSPV delega le ispezioni e i controlli (art. 9, comma 4, lett. a), del D.lgs. 231/2007. Ai sensi della successiva lett. b), con i medesimi poteri il NSPV svolge gli approfondimenti investigativi delle informazioni ricevute ai sensi dell'art. 13 e delle segnalazioni di operazioni sospette trasmesse dalla UIF ai sensi dell'art. 40.

³⁶⁴ Art. 9, comma 9, del D.lgs. 231/2007.

Il medesimo NSPV ha inoltre poteri specifici di controllo con riguardo ai soggetti convenzionati e agenti di cui all'art. 1, comma 2, lett. nn), del D.lgs. 231/2007³⁶⁵, e ai distributori ed esercenti di gioco³⁶⁶ di cui si avvalgono i prestatori di servizi di gioco ai sensi dell'art. 3, comma 6, dello stesso decreto³⁶⁷.

Nell'esercizio delle rispettive funzioni, sia il NSPV sia la DIA³⁶⁸ hanno accesso all'anagrafe tributaria³⁶⁹, al registro dei titolari effettivi di persone giuridiche e trust nonché all'anagrafe immobiliare³⁷⁰; tali database, elencati nell'art. 9 del D.lgs. 231/2007, non sono comunque gli unici ai quali gli Organi investigativi in questione accedono a fini antiriciclaggio e sono da menzionare in aggiunta, per esempio, il registro dei distributori ed esercenti tenuto dall'ADM ai sensi dell'art. 52-*bis*³⁷¹ nonché il registro presso l'OAM dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale di cui all'art. 17-*bis* del D.lgs. 141/2010.

Il NSPV e la DIA accedono altresì alle diverse forme di collaborazione e scambio di informazioni che si svolgono sul piano nazionale e internazionale, ai sensi degli artt. 12 e 13 del D.lgs. 231/2007, e che sono richieste in modo efficace e integrato per il buon funzionamento dell'intero sistema di prevenzione nazionale.

Entrambi gli Organi investigativi rientrano, in particolare, nel novero ristretto di autorità tra le quali è prevista la collaborazione in deroga al segreto d'ufficio³⁷². Sul piano della cooperazione internazionale, collaborano con la UIF e la DNA, anche mediante la definizione di appositi protocolli d'intesa, volti a disciplinare il processo di tempestiva condivisione delle informazioni ottenute nell'ambito della predetta cooperazione. Inoltre, al fine di facilitare le attività comunque connesse all'approfondimento investigativo delle segnalazioni di operazioni sospette, il NSPV e la DIA scambiano, anche direttamente, a condizioni di reciprocità ed in deroga all'obbligo del segreto d'ufficio, dati ed informazioni di polizia con omologhi organismi esteri e internazionali³⁷³.

Le disposizioni contenute nel D.lgs. 231/2007 testimoniano che il legislatore nazionale ha tenuto ben distinte le fasi dell'analisi, rispettivamente, finanziaria e investigativa delle segnalazioni di operazioni sospette; la prima tipologia di analisi è stata affidata alla UIF quale FIU amministrativa istituita presso la Banca d'Italia in posizione di autonomia e indipendenza operativa; la seconda è stata affidata invece a

³⁶⁵ Le violazioni accertate nei confronti dei soggetti convenzionati e agenti rilevano ai fini dell'applicazione delle sanzioni di cui all'art. 61 del D.lgs. 231/2007 nonché ai fini delle comunicazioni all'OAM nei casi previsti dalla medesima disposizione.

³⁶⁶ Con riguardo ai controlli svolti nel comparto del gioco, si evidenzia che, ai sensi dell'art. 54, comma 2, del D.lgs. 231/2007, il NSPV e l'ADM, *“nel rispetto delle proprie attribuzioni e competenze, adottano protocolli d'intesa, volti ad assicurare lo scambio di informazioni necessario a garantire il coordinamento, l'efficacia e la tempestività delle attività di controllo e verifica dell'adeguatezza dei sistemi di prevenzione e contrasto del riciclaggio di denaro e di finanziamento del terrorismo, adottati dai prestatori di servizi di gioco”*.

³⁶⁷ Si vedano anche, per i soggetti convenzionati e agenti di cui all'art. 1, comma 2, lett. nn), l'art. 61 del D.lgs. 231/2007; per i distributori ed esercenti nel comparto del gioco gli artt. 54 e 64 del medesimo D.lgs. 231/2007.

³⁶⁸ Per la DIA l'art. 9, comma 7, del D.lgs. 231/2007 fa salva l'applicabilità, in quanto compatibili, delle disposizioni di cui agli artt. 1, comma 4, e 1-*bis*, commi 1 e 4, del DL 629/1982 convertito, con modificazioni, dalla legge 12 ottobre 1982, n. 726. Si tratta delle norme che disciplinano i poteri di accesso e accertamento presso pubbliche amministrazioni, enti pubblici anche economici e soggetti di cui al Titolo I, Capo I, del decreto antiriciclaggio; il potere di richiedere dati e informazioni ai funzionari responsabili e presidenti degli organi di controllo su atti e documenti in loro possesso, nonché ogni altra notizia utile; il potere di ordinare ai soggetti citati di effettuare ispezioni nell'ambito di uffici e servizi posti alle loro dipendenze, oppure verifiche sulle procedure amministrative e sull'esecuzione di appalti di opere e forniture e delle concessioni di opere e servizi, nonché sull'impiego di finanziamenti pubblici, mutui agevolati e contributi comunitari.

³⁶⁹ Art. 7, commi 6 e 11 del decreto del Presidente della Repubblica 29 settembre 1973, n. 605, come modificato dall'art. 37, comma 4, del decreto-legge 4 luglio 2006, n. 223, convertito, con modificazioni, dalla legge 4 agosto 2006, n. 248.

³⁷⁰ Art. 19 del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122.

³⁷¹ Solo la Guardia di Finanza, unitamente alla Banca d'Italia e alla UIF, è invece abilitata ad accedere alla sottosezione del registro dei soggetti convenzionati e agenti di prestatori di servizi di pagamento e IMEL di cui all'art. 45, comma 2, del D.lgs. 231/2007, che contiene l'indicazione delle cessazioni dei rapporti di convenzionamento o di mandato per motivi non commerciali.

³⁷² Per la condivisione delle informazioni inerenti alle comunicazioni oggettive si veda l'art. 47, comma 2, del D.lgs. 231/2007. Il comma 8 del citato art. 12 stabilisce poi che *“Salvo quanto previsto dal comma 1-bis e fuori dai casi di cooperazione tra le forze di polizia di cui all'articolo 16 della legge 1° aprile 1981, n. 121, tutte le informazioni, in possesso delle autorità di cui all'articolo 21, comma 2, lett. a), e rilevanti per l'esercizio delle attribuzioni di cui al presente decreto, sono coperte da segreto d'ufficio. Il segreto non può essere opposto all'autorità giudiziaria ovvero alle forze di polizia di cui al primo periodo, quando le informazioni siano necessarie per lo svolgimento di un procedimento penale, nonché ai servizi centrali di cui all'art. 12 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, nei casi in cui sia necessario disporre, con assoluta urgenza, di informazioni finanziarie o analisi finanziarie della UIF per la prevenzione, l'accertamento, l'indagine o il perseguimento di condotte riconducibili ai delitti contro la personalità dello Stato previsti dagli articoli da 270 a 270-septies del codice penale”*.

³⁷³ Art. 13 del D.lgs. 231/2007.

Organi investigativi specializzati³⁷⁴ che, nel quadro del rigoroso segreto d'ufficio previsto in materia antiriciclaggio, sono divenuti i destinatari unici delle informazioni derivanti dalle segnalazioni di operazioni sospette, con l'unica eccezione costituita dall'autorità giudiziaria e (per effetto della recente Legge n. 25/2022) dalle forze di polizia per la prevenzione, l'accertamento, l'indagine o il perseguimento di condotte riconducibili a taluni delitti contro la personalità dello Stato e connessi con finalità di terrorismo.

La scelta in questione è stata ribadita in occasione del recepimento nell'ordinamento nazionale della direttiva UE/2019/1153, con la quale sono stati disciplinati nuovi canali di collaborazione domestica e internazionale a fini di prevenzione, accertamento, indagine o perseguimento di reati cosiddetti "gravi", con particolare riguardo alle informazioni sui conti bancari, alle informazioni e alle analisi finanziarie della UIF nonché alle informazioni in materia di contrasto che l'Unità ha diritto di acquisire. In tale ambito, sebbene in argomento fossero state espresse opinioni diverse³⁷⁵, è stato infatti confermato che il NSPV e la DIA sono le sole autorità nazionali che possono richiedere e ricevere informazioni finanziarie o analisi finanziarie dalla UIF. In sede di recepimento della direttiva in questione non è stata, quindi, colta l'opportunità di una più ampia indicazione del novero di autorità che avrebbero potuto beneficiare dei predetti scambi e, in particolare, di provvedere al coinvolgimento dell'*Asset Recovery Office*, delle autorità fiscali e anticorruzione³⁷⁶.

Tale impostazione appare non collimare perfettamente con le indicazioni della direttiva europea³⁷⁷, del GAFI e della Commissione europea. L'art. 49 della direttiva richiede, in particolare, agli Stati membri di provvedere affinché le "autorità di indirizzo, le FIU, le autorità di vigilanza e le altre autorità competenti che operano nell'AML/CFT, nonché le autorità fiscali e le autorità di contrasto" cooperino e si coordinino a livello nazionale per l'elaborazione e l'attuazione delle politiche e nell'attività di contrasto al riciclaggio e al finanziamento del terrorismo. Nel 2015-2016, in occasione della *Mutual Evaluation* del sistema italiano, il GAFI ha rilevato la necessità di riconoscere espressamente alla FIU italiana la possibilità di scambiare informazioni in modo ampio e flessibile con tutti gli Organi investigativi³⁷⁸. Analoghe indicazioni sono giunte dalla Commissione europea nell'ambito

³⁷⁴ La presenza di organi specificamente deputati alla conduzione di analisi di carattere investigativo è caldeggiata anzitutto a livello sovranazionale, rientrando nella previsione di cui alla Raccomandazione GAFI n. 30 e relativa nota interpretativa. *FATF Recommendations*, n. 30: "Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations within the framework of national AML/CFT policies. At least in all cases related to major proceeds-generating offences, these designated law enforcement authorities should develop a pro-active parallel financial investigation when pursuing money laundering, associated predicate offences and terrorist financing". Nota interpretativa: "There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, predicate offences and terrorist financing are properly investigated through the conduct of a financial investigation".

³⁷⁵ Il Direttore della UIF, Claudio Clemente, in occasione dell'*Audizione resa il 13 ottobre 2020* dinanzi alle Commissioni riunite II e VI della Camera dei Deputati, aveva affermato che "Per realizzare un'autentica circolarità delle informazioni rilevanti per la prevenzione e il contrasto, in linea con quanto indicato dal GAFI e ribadito con forza nella citata direttiva 1153 e nel Piano d'Azione, occorrerebbe – come ho recentemente richiamato nell'audizione di luglio 2020 presso la Commissione Antimafia – inserire nella legge di delegazione europea 2019 un criterio direttivo che, senza alterare il vigente assetto istituzionale e di competenze in materia di antiriciclaggio, consenta al Governo di designare un ampio novero di autorità con cui la UIF potrebbe instaurare proficui scambi informativi". Analogamente si era espresso il Sottocapo di Stato Maggiore del Comando Generale dell'Arma dei Carabinieri, Gen. D. Mario Cinque nell'ambito dell'*Audizione* del 20 ottobre 2020 dinanzi alle citate Commissioni riunite II e VI della Camera dei Deputati: "A proposito del recepimento della direttiva 1153 desidero evidenziare come questa costituisca altresì occasione imperdibile per l'individuazione, seppur nel rispetto delle prerogative e competenze della polizia valutaria, di una procedura di collaborazione istituzionale con la UIF, la cui "resura" (specie con riguardo alle informazioni provenienti dall'estero) sta già incidendo sulla tempestività, coraltà ed efficacia dell'azione di contrasto al terrorismo, da sempre attribuita alla competenza concorrente di tutte le Forze di polizia". In senso contrario all'ampliamento della condivisione delle informazioni in possesso della UIF si erano invece espressi il Comandante Generale della Guardia di Finanza, Gen. C.A. Giuseppe Zafarana, nel corso dell'*Audizione tenutasi sempre il 20 ottobre 2020* ("[...] le modifiche introdotte per effetto del d.lgs. 125/2019 incentivano ed accrescono le opportunità per la cooperazione interistituzionale, evitando, nel contempo, il rischio di una "indiscriminata diffusione" di dati e notizie connotati da elevata rilevanza e delicatezza"; a proposito del recepimento della direttiva (UE) 2019/1153 "occorre considerare come il nostro ordinamento giuridico soddisfi ampiamente gli obiettivi di tutela penale che il legislatore europeo si è prefissato") il Capo della Polizia, Direttore Generale della Pubblica Sicurezza, Franco Gabrielli, nel corso dell'*Audizione del 3 novembre 2020* ("Il pregio del nostro sistema "anti-riciclaggio", infatti, è dato dal rigoroso meccanismo, sulla base del quale i soggetti obbligati individuano le operazioni sospette e le segnalano a Autorità individuate dalla legge in ragione di competenze e specializzazioni. [...] L'inserimento di informazioni generate al di fuori di questi presidi rischierebbe di introdurre un elemento di difformità, suscettibile di indebolire l'affidabilità del sistema") nonché il Direttore della Direzione Investigativa Antimafia, Maurizio Vallone, nel corso dell'*Audizione del 10 novembre 2020* ("Il sistema di prevenzione risulta ben bilanciato nella cura dei molteplici interessi che coinvolgono anche diritti soggettivi tutelati dalla nostra Carta Costituzionale, quali la libertà economica e la privacy, garantendo solo a soggetti qualificati e normativamente individuati la gestione delle informazioni in assenza di una delega dell'AG").

³⁷⁶ In argomento si veda il *Rapporto annuale della UIF per il 2021*, p. 111.

³⁷⁷ Direttiva (UE) 2015/849 come modificata dalla direttiva (UE) 2018/843.

³⁷⁸ Cfr. GAFI, *Mutual Evaluation Report – Italy*, 2016, in relazione all'IO6, *key findings and recommended actions*: "Enable the UIF to disseminate selected information and the results of its analysis beyond the DIA and GdF NSPV to additional LEAs and concerned agencies", p. 37. Più in particolare, a p. 44 del report si legge che una disseminazione diretta delle relazioni tecniche predisposte dall'UIF ad altre forze di polizia dovrebbe garantire che tali nuclei e le forze di polizia siano tempestivamente allertati circa eventuali reati, consentendo loro di adottare le azioni necessarie con maggiore velocità. Inoltre, nei casi di sospetti reati tributari e/o corruzione, la disseminazione delle relazioni tecniche all'Agenzia delle Entrate e ad ANAC le aiuterebbe a focalizzare le rispettive attività di auditing e di altro genere. Ciò rafforzerebbe il regime italiano in materia di prevenzione, rivestendo una particolare importanza alla luce del rischio elevato di reati tributari e di corruzione.

dell'articolato rapporto pubblicato nel luglio 2019 sulla cooperazione delle FIU. Tale rapporto ha tra l'altro ribadito la necessità di assicurare la collaborazione delle FIU con tutte le Autorità pubbliche, inclusi gli organi di polizia, quelli doganali e fiscali, gli uffici antifrode e di recupero dei beni provenienti da reato (ARO)³⁷⁹.

La richiamata L. 25/2022 può essere perciò considerata un passo avanti verso le sopra riportate indicazioni³⁸⁰, sebbene manchino ancora nel decreto antiriciclaggio riferimenti completi agli ulteriori rapporti di collaborazione che la UIF potrebbe instaurare con altre autorità e organismi con compiti di controllo su settori di rilievo anche a fini antiriciclaggio (oltre al citato ARO, l'ADM, l'ANAC, l'OAM, l'Organismo dei consulenti finanziari), seguendo un'impostazione analoga a quella riguardante le relazioni dell'Unità con le autorità di vigilanza di settore³⁸¹.

8. I rapporti della UIF con le altre Autorità (A.M.A. Carriero e R. Circosta)

Il principio della collaborazione tra i soggetti preposti al sistema antiriciclaggio trova espressione sia a livello sovranazionale³⁸² sia europeo ed è stato accolto anche nella normativa nazionale³⁸³. Il D.lgs. 231/2007, infatti, dedica alla disciplina della collaborazione tra le Autorità preposte al sistema antiriciclaggio l'art. 12, al fine di *“agevolare l'individuazione di ogni circostanza che possa essere utilizzata per prevenire l'uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo”*³⁸⁴, nel rispetto delle reciproche prerogative istituzionali e del criterio di biunivocità degli scambi.

Nella disciplina delle relazioni tra le Autorità preposte al sistema antiriciclaggio particolare attenzione è rivolta ai rapporti tra UIF e Autorità giudiziaria, al fine di realizzare la massima sinergia³⁸⁵ tra attività di prevenzione e attività di repressione nella lotta al peculiare fenomeno del riciclaggio.

³⁷⁹ Nel *report*, p. 3, si legge: “FIUs also have to cooperate and exchange information with other public authorities, including law enforcement authorities, customs and tax authorities, Anti-Fraud Office, and Asset Recovery Offices”.

³⁸⁰ In questo senso aveva espresso un auspicio il Direttore della UIF nell'ambito dell'*Audizione resa il 27 marzo 2017* dinanzi alla Camera dei Deputati, Commissioni riunite 2^a Giustizia e 6^a Finanze, sullo schema di decreto legislativo di recepimento della quarta direttiva europea. In tale occasione era stata indicata la necessità di *“introdurre una previsione, rispettosa delle sensibilità istituzionali, che - pur confermando il canale ordinario della disseminazione di informazioni e analisi della UIF al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e alla Direzione Investigativa Antimafia - consenta all'Unità di ampliare, in casi di specifico interesse (come ad esempio per il contrasto finanziario del terrorismo), lo scambio anche con le altre forze di polizia”*. Il Direttore della UIF è tornato in argomento nell'*Audizione resa il 18 settembre 2019* dinanzi alle Commissioni congiunte della Camera dei Deputati (II, VI e XIV) e del Senato della Repubblica (2^a, 6^a e 14^a) sullo schema di decreto legislativo di recepimento della quinta direttiva europea.

³⁸¹ In argomento si vedano le richiamate Audizioni del Direttore della UIF del 27 marzo 2017 e 18 settembre 2019.

³⁸² Le principali fonti internazionali sul punto sono le *FATF Recommendations*. La Raccomandazione n. 2, p. 10 – 11 statuisce *“Countries should ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction”*. Rilevante anche la nota interpretativa alla Raccomandazione n. 2, p. 37 *“Countries should establish appropriate inter-agency frameworks for cooperation and coordination with respect to combating money laundering, terrorist financing and the financing of proliferation. These may be a single framework or different frameworks for ML, TF and PF respectively. Such frameworks should be led by one or more designated authorities, or another mechanism that is responsible for setting national policies and ensuring co-operation and co-ordination among all the relevant agencies. Inter-agency frameworks should include the authorities relevant to combating ML, TF and PF. Depending on the national organization of functions, authorities relevant to such frameworks could include: a) The competent central government departments (e.g. finance, trade and commerce, home, justice and foreign affairs); b) Law enforcement, asset recovery and prosecution authorities; c) Financial intelligence unit; d) Security and Intelligence agencies; e) Customs and border authorities; f) Supervisors and self-regulatory bodies; g) Tax authorities; h) Import and export control authorities; i) Company registries, and where they exist, beneficial ownership registries; and j) Other agencies, as relevant. Countries should ensure that there are mechanisms in place to permit effective operational cooperation, and where appropriate, co-ordination and timely sharing of relevant information domestically between different competent authorities for operational purposes related to AML, CFT and CPF, both proactive and upon request. These could include: (a) measures to clarify the role, information needs and information sources of each relevant authority; (b) measures to facilitate the timely flow of information among relevant authorities (e.g. standard formats and secure channels), and (c) practical mechanisms to facilitate inter-agency work (e.g. joint teams or shared data platforms)”*.

³⁸³ Su questo fronte, a parte le enunciazioni programmatiche, la disciplina nazionale ha subito ingiustificati arretramenti. Ciò è un visibile passo indietro se si pensa che nel corso del 2015 il Gruppo di Azione Finanziaria Internazionale ha approvato il Rapporto di *“Mutual Evaluation”* del sistema antiriciclaggio italiano, in cui si riconosceva che il sistema italiano *“è caratterizzato [...] da un adeguato grado di cooperazione e coordinamento tra le autorità cardine del sistema”*.

³⁸⁴ Cfr. art. 12, comma 1, del D.lgs. 231/2007.

³⁸⁵ La collaborazione tra Autorità giudiziaria e UIF si esplica anche attraverso appositi Protocolli di intesa. Lo strumento non è previsto dal legislatore, ma in concreto può essere un utile stimolo alla crescita della cooperazione. I Protocolli, infatti, hanno il vantaggio di racchiudere le migliori prassi emerse nei rapporti con l'Autorità giudiziaria, in relazione allo scambio di informative di specifico interesse, all'individuazione di aree tematiche per l'analisi congiunta di fatti e informazioni, a iniziative periodiche di formazione reciproca, alle modalità di scambio delle informazioni. Attualmente sono stati stipulati protocolli con le Procure di Milano (gennaio 2017), Roma (maggio 2017), Napoli (aprile 2018) e Firenze (luglio 2018).

Più nel dettaglio, fermo restando l'obbligo di denuncia ai sensi dell'art. 331 c.p.p.³⁸⁶ per le notizie di reato di cui la UIF venga a conoscenza nell'esercizio delle proprie funzioni, l'Autorità giudiziaria può avanzare richieste finalizzate a ottenere i risultati delle analisi finanziarie svolte dall'Unità e qualsiasi altra informazione ritenuta necessaria per lo svolgimento di un procedimento penale oppure utile nell'ambito di indagini relative all'esistenza di reati di riciclaggio, autoriciclaggio, reati presupposto o attività di finanziamento del terrorismo.

Nei casi maggiormente rilevanti o complessi la collaborazione richiesta alla UIF dagli organi inquirenti può sostanziarsi nella ricostruzione dei flussi finanziari riconducibili a nominativi e/o rapporti d'interesse. I risultati degli approfondimenti svolti confluiscono generalmente in una relazione della UIF che può costituire una linea di orientamento delle successive attività di indagine.

L'Autorità giudiziaria può chiedere all'Unità, a determinate condizioni³⁸⁷, di effettuare il monitoraggio di rapporti riconducibili ai soggetti di interesse investigativo oppure richiedere l'acquisizione di informazioni nella disponibilità di FIU estere³⁸⁸, anche al fine di adottare misure patrimoniali conservative; in alcuni casi può domandare la canalizzazione di richieste dati e informazioni a determinati destinatari; inoltre, il giudice può chiedere che siano eseguite ispezioni mirate, volte a integrare le informazioni acquisite in sede di analisi delle segnalazioni o a rispondere a esigenze derivanti da rapporti di collaborazione intrattenuti con la stessa Autorità giudiziaria, con gli Organi investigativi e le Autorità di vigilanza di settore.

La collaborazione con l'Autorità giudiziaria risulta essenziale anche nell'esercizio del potere di sospensione delle operazioni sospette di riciclaggio o di finanziamento del terrorismo di cui all'art. 6, comma 4, lett. c), del D.lgs. 231/2007³⁸⁹: il coordinamento con gli organi interessati, infatti, consente di appurare che la misura non sia di pregiudizio alle indagini, di acquisire informazioni sull'eventuale emanazione di provvedimenti cautelari giudiziari per la migliore efficacia degli stessi e di evitare che i fondi oggetto dell'operazione sospetta siano sottratti al provvedimento del giudice competente.

Da parte sua, l'Autorità giudiziaria informa la UIF – e le Autorità di vigilanza competenti – quando ha fondato motivo di ritenere che riciclaggio, autoriciclaggio, impiego di disponibilità di origine illecita o attività preordinate al finanziamento del terrorismo siano avvenuti attraverso intermediari vigilati. Le notizie comunicate sono coperte dal segreto d'ufficio e la relativa comunicazione può essere ritardata quando possa deriverne pregiudizio alle indagini. Le Autorità di vigilanza di settore e la UIF comunicano all'Autorità giudiziaria le iniziative assunte³⁹⁰.

Le informazioni in possesso della UIF sono coperte dal segreto d'ufficio; il regime stringente del segreto d'ufficio tipico delle Autorità amministrative che compongono il sistema, insieme agli obblighi di riservatezza rafforzata che assistono le segnalazioni di operazioni sospette, costituisce una condizione essenziale per il buon funzionamento del sistema di prevenzione. Negli scambi con l'Autorità giudiziaria il segreto subisce una rilevante deroga al fine di garantire la massima collaborazione possibile³⁹¹.

Nell'ambito dei rapporti con l'Autorità giudiziaria rientrano anche la collaborazione e il supporto prestati dalla UIF nelle analisi inerenti a fattispecie di competenza dell'*European Public Prosecutor Office (EPPO)* - Ufficio del Procuratore europeo.

³⁸⁶ L'art. 331 c.p.p., comma 1 stabilisce “[...] i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito”.

³⁸⁷ In casi eccezionali e di estrema rilevanza, per periodi temporali circoscritti e fornendo le informazioni di contesto, può essere richiesto il monitoraggio della movimentazione di specifici rapporti, al fine di attivare la procedura di sospensione delle operazioni sospette.

³⁸⁸ Le informazioni ottenute dalle altre FIU sono condivisibili “previo consenso” e solo per approfondimenti investigativi.

³⁸⁹ Si fa riferimento al potere di sospendere, anche su richiesta dell'autorità giudiziaria (oltre che del NSPV, della DIA o di un'altra FIU), per un massimo di cinque giorni lavorativi, operazioni sospette, dandone immediata notizia a tali organi.

³⁹⁰ Si veda l'art. 12, comma 7, del D.lgs. 231/2007 che riprende - adeguandolo al nuovo contesto - il contenuto della disposizione originaria presente nell'art. 4 del DL 8/1991 (convertito, con modificazioni, dalla legge 82/1991), relativo ai rapporti tra l'autorità giudiziaria e la Banca d'Italia in materia antiriciclaggio. Questa disposizione introdusse per prima l'obbligo per l'autorità giudiziaria di informare il Governatore della Banca d'Italia quando vi fosse fondato motivo di ritenere che reati di riciclaggio, impiego di denaro o di beni di provenienza illecita fossero avvenuti attraverso operazioni bancarie, secondo alcuni commentatori (cfr. L. Donato e D. Masciandaro, *Criminalità e intermediazione finanziaria*, Roma, 1996, p. 451) al fine di “confrontare gli elementi informativi propri delle indagini penali con le risultanze dell'attività di vigilanza”. L'obiettivo di coniugare il momento repressivo con quello preventivo accomuna la norma appena descritta anche al vecchio art. 5, comma 13, della legge 197/91 (“Qualora le irregolari operazioni di trasferimento di valori siano state effettuate per il tramite di enti creditizi ovvero di altri intermediari abilitati iscritti in albi o soggetti ad autorizzazione amministrativa, i provvedimenti con i quali sono state irrogate le sanzioni amministrative pecuniarie previste dal presente decreto sono comunicati alle autorità vigilanti e, se del caso, agli ordini professionali per le iniziative di rispettiva competenza”).

³⁹¹ Art. 12, comma 8, del D.lgs. 231/2007.

L'organo è stato istituito dal regolamento UE/2017/1939, quale titolare dell'azione penale per il perseguimento dei reati che ledono gli interessi finanziari dell'Unione e delle conseguenti condotte di riciclaggio, ed è entrato in funzione nel giugno del 2021. Nel giugno 2022 la UIF ha sottoscritto un protocollo d'intesa con questo ente per agevolare lo scambio di informazioni di reciproco interesse in attuazione del quadro normativo europeo e nazionale. L'accordo, inoltre, richiama i presidi di riservatezza delle informazioni trattate e prevede l'individuazione di aree tematiche per l'analisi congiunta di fatti e informazioni nonché iniziative di formazione reciproca.

8.1. La collaborazione con MEF, CSF e Autorità di vigilanza

La UIF collabora con il Ministero dell'economia e delle finanze, contribuendo alla definizione delle politiche di prevenzione e all'elaborazione della normativa di settore, partecipando agli organismi internazionali, prestando il proprio supporto anche in materia sanzionatoria³⁹².

L'Unità partecipa, poi, ai lavori del Comitato di Sicurezza Finanziaria (CSF), istituito presso il Ministero dell'economia e delle finanze con funzioni di analisi e coordinamento in materia di prevenzione dell'utilizzo del sistema finanziario e di quello economico a scopo di riciclaggio e di finanziamento del terrorismo. Cura, inoltre, l'attuazione delle misure sanzionatorie internazionali.

In tale ambito, la UIF partecipa ai lavori della rete di esperti di cui si avvale il CSF, in particolare fornendo supporto nell'elaborazione di risposte ai quesiti posti da operatori commerciali e intermediari finanziari riguardanti l'applicazione di sanzioni finanziarie derivanti da regolamenti europei e contribuendo al consolidamento di orientamenti interpretativi e allo sviluppo di prassi operative in materia.

La forte complementarità tra gli obiettivi generali perseguiti (integrità del sistema finanziario, correttezza dei comportamenti, sana e prudente gestione dei soggetti vigilati e osservanza delle disposizioni in materia creditizia, finanziaria e assicurativa) e la contiguità tra le aree di rispettiva competenza in materia antiriciclaggio rendono indispensabile uno stretto coordinamento nella redazione della normativa, nella programmazione ispettiva, in materia di controlli e sanzioni tra la UIF e le Autorità di vigilanza di settore.

La collaborazione tra Autorità di vigilanza e UIF negli ambiti di rispettiva competenza in materia antiriciclaggio è disciplinata dal D.lgs. 231/2007. Gli interventi di riforma del 2017 sembravano aver indebolito la cooperazione tra l'Unità e le stesse autorità considerate nella loro veste di soggetti competenti per la vigilanza prudenziale³⁹³. I dubbi sono stati tuttavia fugati da recenti interventi della normativa europea che hanno rimosso gli ostacoli allo scambio informativo e alla collaborazione tra Autorità di vigilanza AML e autorità prudenziali, anche su base transnazionale³⁹⁴ e hanno attribuito all'EBA il compito di adottare apposite *guidelines*³⁹⁵ che specifichino le modalità attraverso cui il predetto scambio informativo può realizzarsi³⁹⁶.

L'attuazione della richiamata normativa europea ha comportato la modifica del decreto antiriciclaggio, che prevede ora l'obbligo per tutte le Autorità di vigilanza antiriciclaggio di collaborare su base transfrontaliera con le autorità estere, antiriciclaggio, prudenziali (compresa la BCE) e di risoluzione e la possibilità di concludere accordi di collaborazione con le stesse³⁹⁷.

³⁹² Il D.lgs. 231/2007 prevede un articolato sistema di sanzioni amministrative pecuniarie, che si aggiungono alle sanzioni penali previste per le violazioni più gravi. Tranne nelle ipotesi relative a sanzioni nei confronti di soggetti vigilati, nel sistema antiriciclaggio la potestà sanzionatoria è attribuita al MEF e la UIF – insieme ad altre Autorità competenti – accerta le violazioni e provvede alla contestazione degli addebiti ai soggetti interessati, trasmettendo poi gli atti al MEF, competente per l'irrogazione della sanzione.

³⁹³ La formulazione dell'art. 12, comma 1, del D.lgs. 231/2007, come modificato dal D.lgs. 90/2017, collega la collaborazione alle esigenze di prevenzione del riciclaggio e del finanziamento del terrorismo in modo più netto della precedente (contenuta nel previgente art. 9, comma 2, del D.lgs. 231/2007), che collegava gli scambi alla più ampia finalità "di agevolare l'esercizio delle rispettive funzioni".

³⁹⁴ Cfr. direttiva UE 2018/843 (cosiddetta quinta direttiva antiriciclaggio).

³⁹⁵ L'EBA ha adottato le linee guida il 16 dicembre 2021. Le stesse prevedono, tra l'altro, forme di scambio informativo tra le autorità di vigilanza e le unità di informazione finanziaria, sia nazionali sia di altri Stati membri; le FIU, poi, dovrebbero essere coinvolte in alcune fattispecie autorizzative/valutative, laddove emergessero rischi ML/TF.

³⁹⁶ L'attuazione degli Orientamenti EBA non dovrebbe comportare modifiche rilevanti a livello nazionale, poiché l'insieme degli accordi in tema di scambi di informazione siglati dalla Banca d'Italia con la UIF e con la BCE sono sufficienti a soddisfarne le previsioni.

³⁹⁷ Si fa riferimento al contenuto dell'art 13-ter, del D.lgs. 231/2007, introdotto dal D.lgs. 125/2019.

Il necessario coordinamento tra autorità competenti per la vigilanza prudenziale e autorità responsabili del rispetto delle norme antiriciclaggio, inoltre, è stato ribadito e rafforzato attraverso una modifica normativa in materia di vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che ha interessato specificatamente la collaborazione tra Banca d'Italia e UIF: il D.lgs. 385/1993 (c.d. Testo Unico Bancario - TUB), infatti, è stato integrato con una disposizione che richiama espressamente la collaborazione tra la Banca d'Italia – quale autorità di vigilanza prudenziale – e l'Unità, in deroga al segreto d'ufficio e per agevolarne le rispettive funzioni³⁹⁸.

La necessità di valorizzare l'area degli scambi informativi tra FIU e Autorità di vigilanza è emersa con forza nei casi di crisi di banche europee; a livello nazionale la collaborazione, che è stata una costante anche in ragione della natura amministrativa della UIF e della sua collocazione in seno alla Banca centrale, ha consentito l'adozione di iniziative congiunte o complementari in vari ambiti, e anche in campo ispettivo, che hanno portato, in alcuni casi, all'adozione di misure correttive e, in particolare, di provvedimenti di rigore o inibitori da parte delle Autorità competenti italiane o estere³⁹⁹.

Anche questi rapporti di collaborazione, come quelli tra la UIF e l'Autorità giudiziaria, si svolgono in deroga al segreto d'ufficio⁴⁰⁰. Lo scambio può avere ad oggetto anche informazioni relative a segnalazioni di operazioni sospette; in questo caso, le comunicazioni si realizzano con modalità idonee a garantire la tutela della riservatezza⁴⁰¹.

8.2. La collaborazione tra UIF e DNA

La UIF ha sempre intrattenuto stretti rapporti di collaborazione con la Direzione Nazionale Antimafia e Antiterrorismo (DNA). A partire dal 2008 le due Autorità hanno cooperato per l'individuazione dei requisiti della “Piattaforma informatica per la conduzione di indagini patrimoniali”, volta alla costituzione di un sistema informativo di ausilio agli accertamenti di carattere finanziario e patrimoniale⁴⁰².

L'esigenza di intensificare la collaborazione ha portato, nell'ambito della riforma del decreto antiriciclaggio attuata dal D.lgs. 90/2017, a disciplinare espressamente i rapporti tra UIF e DNA con il nuovo art. 8 che ha istituito scambi informativi sistematici⁴⁰³. La norma, infatti, prevede che la DNA riceva dalla UIF – per il tramite del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e della DIA – i dati anagrafici in forma crittografata dei soggetti segnalati e che, in caso di incrocio con le proprie basi dati, possa richiedere ai fini dell'esercizio dei poteri di coordinamento e di impulso del Procuratore Nazionale Antimafia, altri elementi informativi e di analisi.

La DNA, poi, fermo restando il segreto investigativo, fornisce alla UIF riscontro in ordine all'utilità delle informazioni ricevute. Lo scambio in questione, di reciproca utilità per entrambe le istituzioni, ha posto le basi per un significativo rafforzamento dell'azione di prevenzione e contrasto della criminalità organizzata e dei casi di finanziamento del terrorismo. La UIF viene messa in grado di elevare le capacità di individuazione delle segnalazioni attinenti al fenomeno della criminalità organizzata e realizzare di conseguenza approfondimenti mirati; la DNA viene agevolata nell'attività di impulso e coordinamento attraverso la conoscenza di sospetti di natura finanziaria legata ai soggetti di interesse.

In generale, va considerato che la DNA ha avuto un ruolo cruciale per l'utilizzo delle informazioni acquisite e analizzate dalla UIF nell'ambito delle indagini nel contesto normativo delineato dalla normativa del 2015 in materia di repressione del terrorismo⁴⁰⁴; le due Autorità collaborano anche per l'elaborazione di informazioni sui flussi finanziari correlati a possibili fenomeni criminali assieme ad altri organismi pubblici.⁴⁰⁵

³⁹⁸ Art. 7, comma 5, del TUB, come modificato dal D.lgs. 182/2021, di recepimento della citata direttiva UE 2019/878.

³⁹⁹ Cfr. in proposito Rapporto annuale della UIF per il 2016, p. 91. Oltre agli esiti della campagna ispettiva specifica sui *money transfer*, si pensi al caso della succursale della AS PrivatBank nei cui confronti è stato adottato un provvedimento di chiusura motivato da gravi violazioni della normativa antiriciclaggio con rischio di reiterazione delle irregolarità ([Comunicato Banca d'Italia del 9 agosto 2016](#)).

⁴⁰⁰ Art. 12, comma 1 e 8, del D.lgs. 231/2007.

⁴⁰¹ Art. 38, comma 6, del D.lgs. 231/2007.

⁴⁰² Cfr. Rapporto annuale della UIF per il 2009, p. 67.

⁴⁰³ Gli scambi sono regolati, più in dettaglio, da due Protocolli d'intesa, stipulati rispettivamente il 5 ottobre 2017 e il 7 maggio 2018, aggiornato con un nuovo Protocollo concluso il 12 marzo 2021.

⁴⁰⁴ Si fa riferimento al DL 7/2015, convertito dalla legge 43/2015, con cui sono stati estesi al settore dei procedimenti per i delitti di terrorismo anche di matrice internazionale le funzioni e i compiti di coordinamento del Procuratore nazionale antimafia, in precedenza già svolti in materia di contrasto della criminalità mafiosa, al fine di sopperire alla carenza di coordinamento nelle indagini.

⁴⁰⁵ Si veda Rapporto annuale della UIF per il 2015, p. 88.

8.3. Le novità del quadro regolamentare nazionale alla luce del decreto di recepimento della direttiva UE/2018/843

I D.lgs. 90/2017 e 125/2019 emanati, rispettivamente, in attuazione della quarta e della quinta direttiva antiriciclaggio hanno inciso in maniera significativa sulla disciplina della collaborazione tra Autorità nazionali e internazionali contenuta nel D.lgs. 231/2007, senza peraltro accogliere talune indicazioni formulate in occasione delle *Mutual evaluation* condotta nel 2015-2016 dal GAFI e dal Fondo Monetario Internazionale sul sistema di prevenzione italiano. Le modifiche sono state realizzate nel contesto di principi direttivi che - invece - imponevano una conferma del vigente assetto istituzionale e di competenze in materia antiriciclaggio⁴⁰⁶ all'esito della *Mutual evaluation* condotta nel 2015-2016.

Il D.lgs. 90/2017 ha rivisto i rapporti istituzionali nazionali, enunciando il principio generale della collaborazione tra le diverse Autorità impegnate nell'antiriciclaggio⁴⁰⁷. Le disposizioni in materia - prima della riforma intervenuta nel 2019 - precisavano che dette collaborazioni si svolgevano in deroga al segreto d'ufficio⁴⁰⁸. La riforma del 2017 aveva anche novellato la disciplina della cooperazione internazionale, in particolare quella tra la UIF e le FIU estere⁴⁰⁹, recependo solo in parte le disposizioni della direttiva europea⁴¹⁰.

La riforma operata con il D.lgs. 125/2019, che avrebbe dovuto realizzare una revisione meno ampia di quella del 2017⁴¹¹, è tornata a modificare le disposizioni sulla collaborazione tra Autorità con previsioni che rischiano di ridurre in maniera significativa il raggio degli scambi che la UIF può effettuare sul versante interno e internazionale.

8.3.1. La collaborazione tra Autorità nazionali secondo il decreto antiriciclaggio

Oltre gli scambi informativi con l'Autorità giudiziaria già enunciati in precedenza, l'art. 12 del D.lgs. 231/2007 stabilisce che l'Unità, le altre Autorità di cui all'art. 21, comma 2, lett. a)⁴¹², le amministrazioni e gli organismi interessati e gli organi delle indagini collaborano per agevolare l'individuazione di ogni circostanza in cui emergono fatti e situazioni la cui conoscenza possa essere comunque utilizzata per prevenire l'uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo. È poi previsto che, per le finalità del decreto antiriciclaggio, la UIF, il NSPV e la DIA, il MEF e le Autorità di vigilanza di settore collaborano tra loro scambiando informazioni, anche in deroga all'obbligo del segreto d'ufficio. Il segreto non può essere opposto, inoltre, all'Autorità giudiziaria e alle

⁴⁰⁶ Cfr. art. 15, comma 2, lett. f), della legge 170/2016.

⁴⁰⁷ L'art. 12, comma 1, del D.lgs. 231/2007 stabilisce che “le autorità di cui all'articolo 21, comma 2, lett. a), le amministrazioni e gli organismi interessati, l'autorità giudiziaria e gli organi delle indagini collaborano per agevolare l'individuazione di ogni circostanza in cui emergono fatti e situazioni la cui conoscenza può essere comunque utilizzata per prevenire l'uso del sistema finanziario e di quello economico a scopo di riciclaggio o di finanziamento del terrorismo”.

⁴⁰⁸ Il previgente comma 8 dell'art. 12 recitava “Fermo quanto disposto dal presente articolo, tutte le informazioni, rilevanti ai fini del presente decreto, in possesso delle autorità di cui all'articolo 21, comma 2, lett. a), delle amministrazioni e organismi interessati e degli organismi di autoregolamentazione, sono coperte da segreto d'ufficio anche nei confronti della pubblica amministrazione. Il segreto non può essere opposto all'autorità giudiziaria, quando le informazioni siano necessarie per le indagini o per lo svolgimento di un procedimento penale”.

⁴⁰⁹ Art. 13 del D.lgs. 231/2007.

⁴¹⁰ In proposito l'Italia è stata oggetto di procedura d'infrazione avviata dalla Commissione europea; la disciplina italiana è stata quindi integrata in argomento in occasione della riforma del 2019.

⁴¹¹ Per la ricostruzione in argomento si consideri che la direttiva UE/2018/843 figura tra quelle inserite nell'allegato A della legge 117/2019 (Legge di delegazione europea per il 2018), in relazione alle quali non sono stati dettati principi e criteri direttivi specifici per il recepimento; ne consegue l'applicazione dei criteri generali contenuti negli artt. 31 e 32 della legge 234/2012, a cui fa rinvio l'art. 1 della citata legge 117/2019. Rileva, più in particolare, il disposto dell'art. 32, comma 1, lett. e) della L. 234/2012, secondo cui “al recepimento di direttive o all'attuazione di altri atti dell'Unione europea che modificano precedenti direttive o atti già attuati con legge o con decreto legislativo si procede, se la modificazione non comporta ampliamento della materia regolata, apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione della direttiva o di altro atto modificato”.

⁴¹² Si tratta di Ministero dell'Economia e delle finanze, Direzione Investigativa Antimafia e Nucleo speciale di polizia valutaria della Guardia di Finanza.

forze di polizia di cui all'art. 16 della L. 121/1981⁴¹³ quando le informazioni siano necessarie per lo svolgimento di un procedimento penale. Le predette forze di polizia, però, possono cooperare tra loro in ogni caso, rafforzando così il loro circuito di scambi informativi a detrimento delle possibilità di collaborazione diretta con la UIF.

Più recentemente, il DL 4/2022 (c.d. *Sostegni-ter*), convertito dalla L. 25/2022, ha modificato la disposizione di cui all'art. 12, comma 8, del D.lgs. 231/2007, introducendo un'ulteriore ipotesi di deroga al segreto di ufficio. È previsto, infatti, che lo stesso non possa essere opposto ai servizi centrali della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della Guardia di finanza, nei casi in cui sia necessario disporre, con assoluta urgenza, di informazioni finanziarie o analisi finanziarie della UIF⁴¹⁴ per la prevenzione, l'accertamento, l'indagine o il perseguimento di condotte riconducibili ai delitti contro la personalità dello Stato previsti dagli artt. da 270 a 270-*septies* del codice penale⁴¹⁵. La formulazione della norma induce a ritenere che gli scambi informativi descritti potranno instaurarsi, nei soli nei casi previsti, a prescindere dallo svolgimento di un procedimento penale e prima dell'avvio di quest'ultimo, per finalità di prevenzione di specifici reati che attengono al terrorismo. Lo scambio, inoltre, potrà instaurarsi solo su richiesta dei servizi centrali richiamati dalla norma, segnando, quindi, una differenza rispetto alla "disseminazione" di segnalazioni di operazioni sospette di cui all'art. 40, comma 1, lett. d), del D.lgs. 231/2007 – rivolta dalla UIF in via esclusiva al NSPV e alla DIA – e alla comunicazione dei risultati delle analisi che la UIF è chiamata a effettuare, nei casi di specifico interesse, nei confronti degli Organismi di informazione per la Sicurezza ai sensi della lett. d), del predetto art. 40.

Al di fuori delle eccezioni richiamate, la UIF è tenuta al segreto su tutte le informazioni rilevanti per l'esercizio delle sue attribuzioni. La disciplina descritta, anche a seguito delle modifiche più recenti, disvela un quadro non del tutto coerente con le corrispondenti disposizioni della normativa europea⁴¹⁶ e degli standard internazionali⁴¹⁷ in materia di prevenzione e rivela un'interna contraddizione sul piano sistematico a livello domestico. Infatti, emerge un'incongruenza tra le disposizioni, meramente programmatiche, che enunciano la più ampia collaborazione tra tutte le Autorità con competenze rilevanti per la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo⁴¹⁸ e quelle che limitano la collaborazione in deroga al segreto d'ufficio soltanto nell'ambito di una cerchia ristretta di Autorità, contraddicendo il principio generale sancito e rendendo, in concreto, impossibile lo scambio di informazioni tra la UIF, ad esempio, e le c.d. amministrazioni interessate⁴¹⁹.

⁴¹³ L'art. 16 della legge 121/1981 stabilisce che "[...] oltre alla Polizia di Stato sono forze di polizia, fermi restando i rispettivi ordinamenti e dipendenze: a) l'Arma dei carabinieri, quale forza armata in servizio permanente di pubblica sicurezza; b) il Corpo della Guardia di Finanza, per il concorso al mantenimento dell'ordine e della sicurezza pubblica. Fatte salve le rispettive attribuzioni e le normative dei vigenti ordinamenti, sono altresì forze di polizia e possono essere chiamati a concorrere nell'espletamento di servizi di ordine e sicurezza pubblica il Corpo degli agenti di custodia e il Corpo forestale dello Stato. Le forze di polizia possono essere utilizzate anche per il servizio di pubblico soccorso".

⁴¹⁴ La nuova disposizione non chiarisce se la deroga sia applicabile alle sole informazioni già in possesso della UIF o possa essere estesa anche a quelle "acquisibili" mediante attività di analisi e ricerca. Nell'interpretazione della norma si deve tenere presente che il nuovo art. 12, comma 8 è stato formulato riproponendo locuzioni (informazioni finanziarie e analisi finanziarie) già presenti nella direttiva (UE) 2019/1153 e nel relativo D.lgs. di recepimento 186/2021. In particolare, ai sensi dell'art. 2, comma 1, lett. c) e d), del citato D.lgs. 186/2021 sono definite informazioni finanziarie "qualsiasi tipo di informazioni o dati, quali dati su attività finanziarie, movimenti di fondi o relazioni finanziarie commerciali, già detenuti dalle unità di informazione finanziaria(FIU)" e analisi finanziarie "i risultati delle analisi operative e strategiche già condotte dalle FIU nello svolgimento dei compiti alle stesse attribuiti". Tra le due possibili opzioni ermeneutiche, a parere di chi scrive, sembrerebbe preferibile la prima, sia dal punto di vista sistematico sia perché più coerente con le ragioni di urgenza poste a fondamento della deroga, oltre che con le istanze garantiste che rendono necessaria la sussistenza di un procedimento penale perché possa essere avviata una collaborazione con la UIF ai sensi dell'art. 12, comma 3, del D.lgs. 231/2007.

⁴¹⁵ Cfr. art. 28-*quinquies* della legge 25/2022.

⁴¹⁶ L'art. della direttiva (UE) 2015/849 statuisce infatti che "gli Stati membri provvedono affinché le autorità di indirizzo, le FIU, le autorità di vigilanza e le altre autorità competenti che operano nell'AML/CFT dispongano di meccanismi efficaci, tali da consentire loro di cooperare e coordinarsi a livello nazionale nell'elaborazione e nell'attuazione delle politiche e attività di lotta al riciclaggio e al finanziamento del terrorismo".

⁴¹⁷ In esito alla *Mutual Evaluation* del 2015-2016 il GAFI e il FMI hanno sollecitato la disseminazione diretta delle relazioni tecniche redatte dalla UIF alle forze di polizia (per allertarle circa eventuali reati, consentendo loro di intervenire più velocemente) e all'Agenzia delle entrate e all'ANAC, alla luce dell'elevato rischio di corruzione e evasione.

⁴¹⁸ Cfr. art. 12, comma 1, del D.lgs. 231/2007.

⁴¹⁹ Cfr. art. 12, comma 1-*bis* e 8, del D.lgs. 231/2007.

Il dato letterale lascerebbe intendere che non sono sottoposti a segreto solo gli scambi informativi tra UIF, MEF, Autorità di vigilanza di settore, NSPV e DIA, con l'Autorità giudiziaria e con le forze di polizia diverse da NSPV e DIA allorché esse agiscano nell'ambito di un procedimento penale, nonché quelli con i servizi centrali della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della Guardia di finanza per la prevenzione di specifici reati che attengono al terrorismo. Se si accogliesse questa opzione interpretativa, il principio della collaborazione perderebbe gran parte del proprio effettivo contenuto applicativo; sarebbero preclusi, infatti, gli scambi informativi diretti con Organi investigativi diversi da NSPV e DIA, come l'Arma dei Carabinieri e la Polizia di Stato⁴²⁰, a meno che non sussistano i presupposti previsti dalla norma (procedimento penale, prevenzione di specifici reati di terrorismo).

Inoltre, i rapporti di collaborazione potrebbero svolgersi in maniera ampia con le Autorità di vigilanza, ma non con "amministrazioni e organismi interessati" con compiti di controllo su soggetti non vigilati, tra cui il MEF sui revisori legali, il Ministero dello Sviluppo economico (MISE) sulle società fiduciarie non iscritte nell'albo di cui all'art. 106 TUB e le Agenzie fiscali, non rientrando il secondo gruppo di autorità pubbliche nel circuito di quelle per le quali il segreto è derogabile. Tale circostanza rischia di incidere negativamente sull'efficacia delle azioni che, in coordinamento con le sopra richiamate Autorità, potrebbero essere intraprese per ottenere proficua collaborazione attiva da soggetti non strettamente "vigilati", operanti in settori a rischio.

Sembra quindi rendersi necessario uno sforzo interpretativo che sia orientato a principi e logiche generali di leale cooperazione tra autorità. Un'impostazione restrittiva appare priva di *ratio* logico-giuridica se letta in chiave di preclusione di rapporti di scambio informativo diretto tra autorità che perseguono analoghi obiettivi d'interesse generale, adottando adeguati presidi di riservatezza.

8.3.2. *L'attuazione della direttiva UE 2019/1153: il D.lgs. 186/2021 e i nuovi canali di collaborazione*

L'importanza della collaborazione tra tutte le Autorità impegnate nella lotta al riciclaggio è confermata anche dalla direttiva UE 2019/1153. Il provvedimento mira a realizzare una piena condivisione delle informazioni tra soggetti preposti al perseguimento di "reati gravi", sul presupposto che l'impossibilità di accedere tempestivamente a conti bancari, informazioni e analisi finanziarie comprometta l'efficacia di indagini e azioni penali e, allo stesso, tempo l'assenza di meccanismi di accesso alle informazioni in materia di contrasto pregiudichi l'utilità dell'azione preventiva.

Per queste ragioni la direttiva prevede che le informazioni sui conti bancari, quelle finanziarie e i risultati delle analisi delle FIU debbano poter essere utilizzati da tutte le autorità coinvolte e che le FIU, a loro volta, possano accedere alle informazioni in materia di contrasto per prevenire il riciclaggio, i reati presupposto associati e il finanziamento del terrorismo, nonché per favorire la cooperazione tra Unità estere.

Ogni Stato membro è tenuto a designare le autorità competenti che svolgano funzioni di prevenzione, accertamento, indagine o perseguimento di "reati gravi". In continuità con i principi più volte richiamati, la direttiva individua un ampio novero di soggetti da includere negli scambi informativi, ricomprendendo anche "gli uffici per il recupero dei beni", nonché le autorità fiscali e quelle anticorruzione nella misura in cui anche queste siano competenti in materia di prevenzione, accertamento, indagine o perseguimento di reati ai sensi del diritto nazionale⁴²¹.

Al fine di dare attuazione alla normativa europea, il legislatore nazionale ha adottato il D.lgs. 186/2021. In linea con le finalità perseguite dalla direttiva, il decreto ha disciplinato nuovi canali di collaborazione domestica e internazionale a fini di prevenzione, accertamento, indagine o perseguimento di reati, riservando particolare attenzione alle informazioni sui conti bancari, alle informazioni e alle analisi finanziarie della UIF nonché alle informazioni in materia di contrasto che l'Unità ha diritto di acquisire.

Le questioni relative all'accesso alle informazioni e analisi finanziarie della UIF sono strettamente legate al tema delle collaborazioni dell'Unità. La direttiva UE 2019/1153, pur non riguardando direttamente le previsioni che definiscono obiettivi, attori e obblighi del sistema antiriciclaggio, estende il novero di autorità che possono accedere alle informazioni finanziarie e alle analisi delle FIU e, quindi, avrebbe potuto essere un'occasione per compiere scelte diverse in termini di ampiezza negli scambi informativi e per superare le limitazioni previste dalla normativa antiriciclaggio.

⁴²⁰ Si pensi, ad esempio, alla collaborazione fornita dall'Unità ai ROS dei Carabinieri a fronte di richieste urgenti di informative di tipo finanziario volte a rilevare l'eventuale presenza di presunti terroristi e di reti relazionali sul territorio nazionale; oppure alle informative, riconducibili ad attività di commercio di materiale pedopornografico condivise con il Centro Nazionale per il Contrasto alla Pedopornografia della Polizia di Stato.

⁴²¹ Cfr. considerando 9, 10 e 11 della direttiva (UE)/2019/1153.

Tuttavia, il decreto di attuazione non ha realizzato l'ampliamento sperato, mantenendo intatto il novero delle autorità coinvolte nello scambio informativo; in particolare, mentre è esteso l'elenco di autorità nazionali abilitate ad accedere al registro centralizzato dei conti bancari⁴²², è stabilito che solo il NSPV e la DIA possono richiedere e ricevere informazioni finanziarie o analisi finanziarie dalla UIF⁴²³. Si deve sottolineare, però, che la modifica dell'art. 12, comma 8, del D.lgs. 231/2007 ad opera del citato decreto Sostegni - *ter* consente all'Arma dei Carabinieri e alla Polizia di Stato di superare il limite informativo derivante dalla circostanza di non essere state incluse tra le autorità nazionali abilitate ai sensi della direttiva, sebbene limitatamente ai reati di terrorismo.

La UIF - quando risulti necessario per l'esercizio delle proprie funzioni - può chiedere, caso per caso, "informazioni materia di contrasto"⁴²⁴ al NSPV e alla DIA, i quali forniscono tempestiva risposta, nel rispetto del segreto delle indagini⁴²⁵.

Inoltre, ai sensi dell'art. 8 del D.lgs. 186/2021, la cooperazione tra la UIF e le altre FIU europee è estesa agli scambi di informazioni connessi con il terrorismo o la criminalità organizzata associata al terrorismo. In base alla medesima disposizione, la UIF trasmette tempestivamente le informazioni ricevute alla DNA e, tramite il NSPV e la DIA, al Comitato di analisi strategica antiterrorismo (C.A.S.A.).

Ciò implica che informative della specie saranno portate a conoscenza dei servizi centrali della Polizia di Stato e dell'Arma dei Carabinieri, grazie alla loro partecipazione al C.A.S.A., senza che possano verificarsi asimmetrie informative, anche nell'ipotesi in cui manchino richieste espresse ai sensi del nuovo art. 12, comma 8, del D.lgs. 231/2007.

9. L'AMLA (*Anti-Money Laundering Authority europea*) (P. Costanzo)

La proposta di regolamento "AMLA", presentata dalla Commissione europea nell'AML Package del 20 luglio 2021, prospetta l'istituzione di una *Anti-Money Laundering Authority* quale agenzia europea competente per lo svolgimento di nuovi compiti antiriciclaggio sovranazionali in due distinti comparti: la supervisione, il supporto e il coordinamento delle FIU. L'istituzione di un nuovo soggetto giuridico è stata preferita all'allocazione delle funzioni presso agenzie esistenti⁴²⁶.

La proposta di istituire un'autorità antiriciclaggio sovranazionale prende le mosse dalle istanze di rafforzamento dell'azione e della collaborazione delle FIU. Il "Mapping Exercise and Gap Analysis on FIUs' Powers and Obstacles for Obtaining and Exchanging Information", elaborato dalla Piattaforma delle FIU nel 2016, svolge un'ampia disamina dei limiti esistenti e indica espressamente la necessità di forme di coordinamento sovranazionale per le FIU. Nel *Commission Staff Working Document "On improving cooperation between EU Financial Intelligence units"* (26 giugno 2017) vengono articolate alcune policy per dare seguito al Mapping Exercise che trovano un primo riscontro legislativo nella quinta direttiva antiriciclaggio (UE) 2018/843, ove la Commissione è chiamata a valutare "la possibilità di istituire un meccanismo di coordinamento e supporto delle FIU". Il Meccanismo è prefigurato nel Rapporto su "Assessing the framework for cooperation between Financial Intelligence Units" (24 luglio 2019) e ulteriori dettagli vengono elaborati nel Piano d'Azione del 2020 che prelude alla presentazione delle proposte legislative dell'AML Package⁴²⁷.

⁴²² Si tratta delle seguenti autorità: Ufficio nazionale per il recupero dei beni (ARO); autorità giudiziaria e ufficiali di polizia giudiziaria delegati dal pubblico ministero; servizi centrali e interprovinciali per il contrasto della criminalità organizzata; Ministro dell'Interno; Capo della polizia - direttore generale della pubblica sicurezza; questori; direttore della Direzione Investigativa Antimafia (art. 3, D.lgs. 186/2021).

⁴²³ Si veda l'art. 5, del D.lgs. 186/2021 che, peraltro, fa salvi gli artt. 8 e 12 del D.lgs. 231/2007.

⁴²⁴ Ai sensi dell'art. 2, lett. g), del D.lgs. 186/2021 si tratta di "informazioni o dati già detenuti dalle autorità di cui agli articoli 3 e 5 [Autorità nazionali competenti abilitate ad accedere al registro nazionale centralizzato dei conti bancari e che possono richiedere e ricevere informazioni finanziarie o analisi finanziarie dalla UIF] o alle stesse accessibili, nel contesto della prevenzione, dell'accertamento, dell'indagine o del perseguimento dei reati".

⁴²⁵ Art. 7 del D.lgs. 186/2021.

⁴²⁶ L'alternativa fu prospettata dalla Commissione nel "Piano d'Azione" *For a comprehensive Union policy on preventing money laundering and terrorist financing* (13 maggio 2020). Sugli sviluppi precedenti cfr. J. Kirschenbaum, N. Véron, *A Better European Architecture to Fight Money Laundering*, Bruegel Policy Contribution, Issue 19, October 2018.

⁴²⁷ Con le *Council Conclusions* del 5 novembre 2020 gli Stati membri hanno espresso sostegno a queste linee di sviluppo, invitando la Commissione a procedere con il piano di riforme e con l'istituzione del Meccanismo. Inoltre, un "Joint Position Paper" su "Enhancing FIUs' cooperation. The 'Coordination and Support Mechanism' for EU FIUs" è stato adottato il 16 dicembre 2020 da otto Paesi (tra cui l'Italia) con indicazioni che hanno poi trovato riscontro nel Package.

L'istituzione di un'Autorità europea consolida l'apparato antiriciclaggio quale sistema organico, completo e separato rispetto a comparti collegati (ad esempio quello della vigilanza prudenziale nel *Single Supervisory Mechanism* e quelli delle indagini penali, nei quali operano Europol, Eurojust, lo *European Public Prosecutor Office*). Tuttavia, l'Autorità presenta caratteristiche peculiari nel panorama delle agenzie dell'Unione. Nella sua unitarietà soggettiva, sancita dalla personalità giuridica (art. 3), ad essa sono imputate due funzioni distinte e separate, sul piano operativo e su quello organizzativo. L'AMLA agisce disgiuntamente, in conformità a diversi statuti normativi, quale Supervisore e quale Meccanismo delle FIU; devono applicarsi le prerogative di autonomia e indipendenza previste per queste ultime nelle regole europee e negli standard internazionali.

L'art. 5 della proposta di regolamento enuncia le materie che rientrano nel mandato dell'Autorità⁴²⁸. Il comma 1 è dedicato a compiti di carattere generale, non circoscritti all'una o all'altra delle due aree di responsabilità. L'AMLA svolge il monitoraggio dei rischi di riciclaggio e finanziamento del terrorismo, elaborando informazioni acquisite nella propria attività ovvero ottenute dai supervisori nazionali. Tale ruolo si inserisce nel complessivo sistema di valutazione sovranazionale dei rischi ricondotto, nella sesta direttiva, alla responsabilità della Commissione attraverso la predisposizione del *Supra-National Risk Assessment*. Sembrano da chiarire le modalità con le quali i supervisori nazionali e le FIU contribuiscono alla valutazione sovranazionale: collaborando direttamente con la Commissione (cfr. art. 7, comma 5, della sesta direttiva) ovvero fornendo elementi all'AMLA per il contributo che questa è a sua volta chiamata a fornire alla Commissione (art. 5 del regolamento).

9.1. L'AMLA quale supervisore antiriciclaggio europeo

L'AMLA, nel regolamento, è il fulcro di un sistema integrato di supervisione antiriciclaggio articolato sul piano sovranazionale e su quello nazionale. Il regolamento segna il passaggio da un insieme frammentato di sistemi nazionali giustapposti, disciplinati da regole della direttiva di limitata armonizzazione e da variegate disposizioni di recepimento, a un sistema europeo.

A un "sistema di supervisione AML/CFT" fa esplicito riferimento l'art. 7; di esso fanno parte le autorità nazionali competenti, molteplici e diversificate, e l'AMLA, "responsabile del funzionamento efficace e coerente". All'Autorità europea spettano compiti di coordinamento dei supervisori nazionali e funzioni di supervisione diretta, diversi a seconda del comparto (finanziario o non finanziario) e del livello di rischio (determinato in base a un'apposita metodologia).

Il sistema si fonda su una segmentazione dei soggetti obbligati in tre comparti ("selezionati", "non selezionati", "non finanziari") e su una ripartizione di compiti tra il livello sovranazionale dell'AMLA e quello delle autorità nazionali secondo tre regimi distinti di supervisione (diretta, indiretta, sorveglianza). Entro queste coordinate fissate in termini prescrittivi, la supervisione si articola poi in modalità di intervento flessibili, secondo un approccio basato sul rischio nel quale si tiene conto, ad esempio, di fattori geografici, comparti operativi, caratteristiche di soggetti e attività.

9.1.1. Attività di coordinamento

Con l'obiettivo di ricondurre a coerenza un sistema europeo eterogeneo, segnato da marcate differenze nelle modalità e nell'intensità della supervisione tra paesi e tra settori, l'AMLA elabora una comune "metodologia di supervisione antiriciclaggio" (art. 8 del regolamento). In coerenza con gli standard del GAFI, la metodologia deve "descrivere in dettaglio l'approccio basato sul rischio per la supervisione". Essa deve tenere conto ("come minimo") dell'esposizione dei soggetti obbligati nei diversi comparti, classificandoli in classi di rischio omogenee; deve anche fare riferimento alla "autovalutazione" cui è tenuto ciascun soggetto obbligato sulla propria esposizione, alle "politiche e procedure interne" alla base dei presidi organizzativi e di adeguata verifica, a fattori di rischio connessi alla clientela, alle tipologie e alle aree geografiche di operatività.

All'AMLA è anche affidato il compito di favorire lo svolgimento uniforme e coerente, da parte delle autorità nazionali, di "verifiche tematiche" (art. 9, comma 1). Queste consistono nella ricognizione dei rischi di riciclaggio e finanziamento del terrorismo, o di profili particolari di tali rischi, cui sono esposti congiuntamente più soggetti obbligati. Le autorità nazionali devono presentare piani di lavoro annuali

⁴²⁸ Poi riprese in dettaglio in sezioni dedicate e in altre parti del Package (cfr. ad esempio gli artt. 17 ss. della proposta di sesta direttiva antiriciclaggio, relativi a compiti di supporto all'analisi domestica e alla collaborazione delle FIU).

all'AMLA, che ne svolge una ricognizione complessiva e compila una programmazione generale europea, nella quale sono indicati l'ambito di ciascuna iniziativa (categorie e numerosità dei soggetti coinvolti), la durata prevista, gli strumenti e le modalità.

L'AMLA, sebbene non abbia poteri di modifica o integrazione, svolge un incisivo ruolo di coordinamento: le verifiche tematiche di rilievo europeo (*union-wide*), individuate dal Consiglio Generale tra quelle elencate nel documento di programmazione, devono essere svolte in forma congiunta dalle autorità nazionali con il coordinamento dell'AMLA. Questa acquisisce informazioni dai soggetti sottoposti alla propria supervisione diretta, senza l'intermediazione delle rispettive autorità nazionali (pur coinvolte nelle verifiche cui si riferiscono le richieste stesse). La prevalenza del livello sovranazionale si manifesta anche nella circostanza che le verifiche congiunte conseguono automaticamente alla valutazione del Consiglio sul rilievo "Union-wide", con l'"attrazione" dell'iniziativa alla sfera di coordinamento dell'AMLA, e che la partecipazione dei supervisori dei paesi interessati appare obbligatoria⁴²⁹. Gli esiti sono approvati dal Consiglio e pubblicati.

All'AMLA è affidata la definizione di "strumenti pratici e di convergenza per promuovere approcci e prassi comuni in materia di supervisione" (art. 10). Strumenti comuni, unitamente alla "metodologia" di supervisione basata sul rischio, dovranno favorire la condivisione di prassi efficaci e la coerenza tra sistemi ed esperienze differenziati, tra paesi e tra settori. Spesso, infatti, gli approcci nazionali e settoriali alla supervisione non sono commisurati alle peculiarità degli obiettivi e dei soggetti e sono condizionati dalla scarsità delle risorse e del livello di specializzazione, con significativi dislivelli e deficit di efficacia. Per favorire la convergenza l'AMLA fornisce assistenza e supporto alle autorità nazionali; a fronte di richieste circostanziate, "compie ogni sforzo per prestare l'assistenza (...), anche mobilitando risorse umane proprie e assicurando la mobilitazione di risorse presso le autorità di supervisione su base volontaria"⁴³⁰.

Presso l'AMLA viene collocato l'"hub" informativo che accentra dati sulle attività di supervisione antiriciclaggio, a beneficio dell'AMLA stessa e delle autorità nazionali (art. 11). Le informazioni da acquisire riguardano sia le caratteristiche "strutturali" dei sistemi nazionali sia gli interventi effettuati. A fronte dell'obbligo per le autorità nazionali di fornire i dati, l'AMLA assicura l'accesso delle stesse autorità alla base dati europea, in circostanze di comprovata necessità; svolge inoltre analisi di tali informazioni, rendendo disponibili i risultati a supporto della supervisione nazionale.

9.1.2. Supervisione diretta

L'AMLA esercita supervisione diretta, in sostituzione dei supervisori nazionali, nei confronti di "soggetti obbligati selezionati" (art. 2, comma 1) per verificare la *compliance* rispetto alle regole europee del rulebook antiriciclaggio e l'adeguatezza dei presidi a fronte dei rischi (art. 5, comma 2).

La supervisione diretta viene svolta per mezzo di "gruppi di supervisione congiunti", uno per ogni soggetto obbligato selezionato, formati da personale dell'AMLA e dei "supervisori del settore finanziario competenti (...) a livello nazionale". L'AMLA istituisce e coordina i gruppi; questi svolgono "revisioni e valutazioni della supervisione", effettuano ispezioni *in loco* proponendo eventuali "misure di supervisione", partecipano alla preparazione delle decisioni del Consiglio e del Comitato Esecutivo, intrattengono rapporti con i supervisori nazionali (art. 15, comma 3).

L'AMLA può anche svolgere "indagini generali" (*general investigations*) nei confronti di soggetti obbligati selezionati, laddove necessarie per "svolgere i compiti che le sono conferiti" dal regolamento⁴³¹. I poteri esercitabili, particolarmente incisivi, comprendono l'accesso a informazioni e la possibilità di "ottenere spiegazioni" e "organizzare audizioni".

Alle competenze di supervisione diretta e ai connessi poteri si associa la capacità di adottare misure e provvedimenti specifici di diretta applicazione nei confronti dei soggetti obbligati selezionati. Ad esempio, l'AMLA può imporre particolari presidi o contromisure rispetto a rischi non ben governati o a debolezze nella *compliance*, disporre modifiche nella *governance*, adottare provvedimenti "di rigore" per restringere o limitare le attività, applicare requisiti specifici in comparti determinati, proporre la revoca dell'autorizzazione⁴³². Tali estesi poteri sono completati dalla possibilità di irrogare sanzioni pecuniarie per la violazione delle regole europee o di decisioni dell'AMLA stessa (art. 21).

⁴²⁹ Poiché il Consiglio Generale decide secondo meccanismi di maggioranza (semplice o qualificata), la partecipazione a verifiche tematiche congiunte sembra dovuta anche per le autorità nazionali che, nel Consiglio, si sono espresse in senso contrario sul rilievo dell'iniziativa in sede di esame e approvazione del documento di programmazione.

⁴³⁰ Art. 10, commi 3 e 5.

⁴³¹ Art. 17. Le "indagini" possono riguardare anche "qualsiasi persona fisica o giuridica impiegata da un soggetto obbligato selezionato o appartenente a esso".

⁴³² Art. 20, comma 2. Il provvedimento resta di competenza dell'autorità (nazionale) che ha concesso l'autorizzazione.

I “soggetti obbligati selezionati” sono definiti nell’art. 2, comma 1, del regolamento e vanno poi individuati in base ai molteplici criteri enunciati nell’art. 13. Il novero è circoscritto a intermediari finanziari: la definizione fa riferimento a un “ente creditizio, ente finanziario o gruppo” di tali enti. Si tratta di una delimitazione rigida, uno “sbarramento” all’ambito della supervisione diretta dell’AMLA fondato su una presunzione, non modificabile in concreto, di maggiore rischiosità del settore finanziario⁴³³. Prevale un’esigenza pratica di fattibilità, perseguita con l’applicazione di criteri di natura oggettiva.

L’individuazione concreta degli intermediari che soddisfano la definizione normativa di “obbligati selezionati” è, invece, direttamente fondata sulla considerazione dei rischi (art. 12). Questa selezione di “secondo livello” è svolta secondo una “metodologia” predisposta dall’AMLA nella quale devono essere declinati numerosi parametri⁴³⁴.

9.1.3. Supervisione indiretta su intermediari non “selezionati”

L’AMLA esercita la supervisione indiretta nei confronti di intermediari finanziari diversi da quelli “selezionati” (artt. 28 ss.). Anche per tale segmento l’ambito dei soggetti non è individuato in base al rischio concreto e risulta, in termini “deterministici”, dalla sottrazione dei soggetti selezionati dalla compagine degli enti creditizi, enti finanziari e relativi gruppi (art. 2, comma 1, n. 1).

Nella supervisione indiretta l’AMLA non si sostituisce alle autorità nazionali; si raccorda con esse per forme di intervento che solo indirettamente si riverberano sui soggetti obbligati non selezionati. Per questi, dunque, la supervisione antiriciclaggio si articola in due livelli: controlli diretti dei supervisori nazionali⁴³⁵; controlli indiretti dell’AMLA nei confronti delle autorità nazionali.

L’AMLA valuta la supervisione sui soggetti obbligati non selezionati verificando l’applicazione della metodologia europea “risk-based” per la convergenza degli approcci nazionali (art. 20, “Valutazioni dello stato di convergenza della supervisione”). A conclusione della valutazione possono essere formulate “misure specifiche di follow-up” che i supervisori “devono adottare”⁴³⁶.

Nella supervisione indiretta l’AMLA coordina collegi di supervisori nazionali⁴³⁷. Ad essa, inoltre, vanno notificate le “circostanze in cui la situazione di qualsiasi soggetto obbligato non selezionato (...) si deteriora rapidamente e significativamente”, con riguardo alla *compliance* ovvero all’esposizione a rischi. In presenza di “violazioni rilevanti” l’AMLA indirizza al supervisore nazionale istruzioni su iniziative o misure da adottare, con valore cogente; qualora l’autorità nazionale resti inerte o non dia altrimenti seguito all’impulso ricevuto, l’AMLA può promuovere una procedura di avocazione dell’intervento diretto nei confronti dei soggetti obbligati interessati. Spetta alla Commissione europea decidere se trasferire all’Autorità le prerogative nazionali, conferendo a questa un ruolo di supervisione diretta in sostituzione dell’autorità nazionale inerte o inadempiente⁴³⁸.

⁴³³ I rischi di riciclaggio e finanziamento del terrorismo, diversi da quelli “prudenziali”, connessi alla stabilità di intermediari e del sistema finanziario e in linea di massima maggiormente dipendenti dalle dimensioni e dalla natura “finanziaria” dell’attività, possono manifestarsi con intensità pari o superiore in comparti non finanziari o per specifiche imprese operanti in tali comparti, sia per la gravità e l’intensità di particolari minacce sia per la possibile relativa debolezza delle misure di mitigazione (nella compliance, nella governance o nell’organizzazione).

⁴³⁴ In particolare, sono sottoposti a supervisione diretta i gruppi bancari stabiliti in almeno sette Stati membri, ovvero che presentino un rischio alto in almeno quattro Paesi, ovvero che siano stati oggetto di un’azione di vigilanza intensa e rafforzata in almeno uno di questi Stati nei tre anni precedenti la valutazione. Rientrano nel perimetro anche i gruppi non bancari attivi in almeno dieci Stati membri, con uno stabilimento in un altro Stato e in libera prestazione negli altri, ovvero che presentino un rischio alto in almeno cinque degli Stati di operatività (artt. 12 e 13). In una posizione comune del febbraio 2022 sei Paesi, tra cui l’Italia, hanno proposto modifiche di tali criteri per definire un perimetro di supervisione dell’AMLA più aderente alla considerazione dei rischi di riciclaggio e di finanziamento del terrorismo, diversi da quelli prudenziali e non necessariamente inferiori nei settori non finanziari. Secondo la posizione comune, il perimetro includerebbe: banche, intermediari e CASP con operatività cross-border ed esposti a rischi maggiori; banche, intermediari e CASP attivi in almeno sette Paesi membri. L’AMLA dovrebbe in ogni caso esercitare la supervisione diretta nei confronti di almeno un soggetto obbligato in ciascuno Stato membro.

⁴³⁵ Le competenze e i poteri delle autorità nazionali di supervisione sono disciplinati nella sesta direttiva con disposizioni di limitata portata armonizzante, oggetto di recepimento nazionale con regole locali anche significativamente eterogenee.

⁴³⁶ Cfr. tuttavia l’art. 28 comma 4: tali misure possono consistere in “orientamenti o raccomandazioni” che i supervisori nazionali “compiono ogni sforzo per rispettare”.

⁴³⁷ Previsti e regolati nell’art. 36 della sesta direttiva. L’Autorità europea assicura che i collegi “siano istituiti e funzionino in modo uniforme” nei diversi Stati membri interessati; è dotata a questo fine di poteri incisivi per la diretta istituzione dei collegi, la loro convocazione, l’organizzazione di piani di supervisione, la raccolta e la condivisione di informazioni, l’impulso e il controllo delle attività poste in essere da supervisori nazionali (art. 29, comma 1).

⁴³⁸ La procedura di avocazione è dettagliatamente regolata, nelle fasi e nei presupposti, nei commi da 4 a 7 dell’art. 30.

9.1.4. La “sorveglianza” sul settore non finanziario

Nella graduazione delle forme di supervisione, il terzo comparto comprende le imprese e i professionisti che svolgono attività non finanziarie. I soggetti non finanziari⁴³⁹ costituiscono un coacervo eterogeneo, ampio e con esposizione a rischi diversificata (non necessariamente inferiore a quella del comparto finanziario)⁴⁴⁰. Non sono possibili forme efficaci di supervisione accentrata sovranazionale; i controlli restano in capo alle autorità nazionali, diverse e con poteri disomogenei, e sono esclusi interventi e contatti diretti dell'AMLA con soggetti non finanziari.

Nel suo ruolo di “sorveglianza” (*oversight*) l'AMLA compie una “mappatura” delle autorità nazionali competenti (art. 31 ss.) e predispone una metodologia comune per favorire convergenza ed efficacia. Essa esercita controlli nei confronti dei supervisori nazionali⁴⁴¹ coordinando comitati di valutazione composti dagli stessi; le conclusioni, pubblicate, indicano misure di “follow-up” e sono impiegate dalla Commissione per finalità di policy⁴⁴².

L'Autorità svolge inoltre verifiche sulla corretta applicazione delle regole europee antiriciclaggio e delle connesse disposizioni nazionali da parte dei supervisori del comparto non finanziario. Esse vengono attivate nei casi in cui informazioni disponibili all'AMLA ovvero fornite da autorità nazionali o da altri soggetti pongano in evidenza violazioni del diritto dell'Unione da parte di un supervisore nazionale. L'AMLA può formulare “raccomandazioni” per il riallineamento alle regole.

9.2. L'AMLA quale “Meccanismo” sovranazionale delle FIU

Diversamente dal comparto della supervisione, nella veste di Meccanismo per le FIU l'AMLA non assume compiti operativi in sostituzione di queste. La ricezione di segnalazioni di operazioni sospette, l'analisi, la disseminazione, la collaborazione restano radicati nelle FIU nazionali⁴⁴³. Il Meccanismo si concentra su formati, contenuti e indicatori uniformi per le segnalazioni (incluse quelle “cross-border”), su metodi per la convergenza degli approcci nazionali nell'analisi, su strumenti avanzati per la collaborazione internazionale, su “analisi congiunte” per casi di rilievo transfrontaliero.

Le competenze dell'AMLA nelle materie delle FIU sono delineate nell'art. 5, comma 5, del regolamento e riprese, per alcuni aspetti, negli artt. da 33 a 37, raccolti nella Sezione 6 del Capo II (“Meccanismo di sostegno e coordinamento delle FIU”)⁴⁴⁴. Altri compiti sono richiamati nel regolamento AMLR (formulazione di regole applicative su contenuti e formati delle operazioni sospette e delle segnalazioni: art. 50) e nella direttiva (specie artt. 22 ss. sulla collaborazione tra FIU).

⁴³⁹ Individuati nel regolamento con un mero rinvio ai “soggetti obbligati elencati nell'art. 3 [del regolamento AMLR] che non sono enti creditizi e enti finanziari”. I riferimenti nell'art. 3, a loro volta, non giungono a “tipizzare” i soggetti non finanziari che, a differenza di quelli finanziari, sono privi di discipline europee di settore; vengono semplicemente richiamate le attività rilevanti, regolate poi in ciascun Paese al di fuori di un quadro armonizzato.

⁴⁴⁰ Come osservato, la “segmentazione” non segue, se non per larga approssimazione, una logica *risk-based* che associ le forme più intense di supervisione ai soggetti più esposti a rischi. Essa si basa su presupposti rigidi (*rule-based*) connessi alla natura e alle attività dei soggetti obbligati, per ragioni di “convenienza” e fattuale praticabilità. Il sistema europeo di supervisione prevede così forme più incisive di intervento per un insieme relativamente ristretto di intermediari, maggiormente regolato e uniforme (soggetti obbligati selezionati e non selezionati).

⁴⁴¹ In termini simili alla supervisione indiretta ma, diversamente da questa, senza la previsione di ipotesi di avocazione. Le verifiche (*peer review*) sull'attività di supervisori nazionali tengono conto sia delle informazioni acquisite ai sensi del regolamento (cfr. ad esempio l'art. 11) sia dei risultati di analoghe valutazioni svolte da organismi internazionali (art. 31; ad esempio, le Mutual Evaluation del GAFI e di MoneyVal).

⁴⁴² Ovvero quando emerga la necessità di “un'ulteriore armonizzazione delle norme dell'Unione applicabili ai soggetti obbligati del settore non finanziario o ai supervisori del settore non finanziario”.

⁴⁴³ L'istituzione di una vera e propria “EU FIU” (sostenuta in alcune occasioni dal Parlamento europeo), dotata delle funzioni essenziali secondo la definizione elaborata dal Gruppo Egmont e ripresa dalle regole europee, non è praticabile per ragioni giuridiche e pratiche. In virtù della definizione, la FIU è un'unità centrale statale da istituire su base nazionale; nazionali sono anche le funzioni; un accentramento sovranazionale della ricezione di segnalazioni di operazioni sospette, con le relative conseguenze su lingue e procedure per la vastissima platea di soggetti obbligati in ciascun Paese, oltre a non essere realisticamente praticabile e inefficiente, sarebbe in contrasto con le regole europee e gli standard del GAFI.

⁴⁴⁴ A questa Sezione fa rinvio l'art. 49 del regolamento per determinare l'ambito delle competenze decisionali del Consiglio Generale nella composizione “FIU”. Deve ritenersi tuttavia, per evitare lacune o contraddizioni, che tali competenze comprendano tutte le materie relative alle FIU nelle quali l'AMLA interviene, segnatamente quelle richiamate nell'art. 5 e in altre parti del “Package” (ad esempio, nel Capo III della direttiva, rubricato “FIU”), anche se non esplicitamente richiamate nella Sezione 6 del Capo II del regolamento cui fa rinvio l'art. 49.

Le disposizioni su mandato, compiti e poteri dell'AMLA nelle materie delle FIU sono dunque distribuite e non raccolte in un'unica *sedes materiae*. Tali "plessi" normativi non appaiono omogenei nei contenuti, talora duplicati o difformi; ne è necessaria una considerazione congiunta per ricavare il sistema delle competenze del Meccanismo e, in esso, ricostruire la disciplina, ad esempio, dell'analisi congiunta, della segnalazione di operazioni sospette, della collaborazione tra FIU⁴⁴⁵.

Nell'art. 5, comma 5, vengono individuati i seguenti compiti: supporto allo svolgimento di analisi congiunte, cui vengono dedicate tre lettere (con una certa ridondanza) sul ruolo dell'AMLA per l'individuazione di casi, lo sviluppo di metodi, l'impulso a esercizi concreti; elaborazione di metodi e procedure per il "rilevamento, l'analisi e la disseminazione" di operazioni sospette (materie ampie e complesse, cui viene riferito uno stringato richiamo comune nella lett. f)⁴⁴⁶; sviluppo di strumenti tecnologici avanzati a supporto delle FIU "per la condivisione sicura delle informazioni"⁴⁴⁷; prestazione di generiche forme di supporto e assistenza alle FIU, articolata in ben tre lettere⁴⁴⁸. Un ulteriore riferimento, nella lett. i), riguarda un ruolo dell'AMLA per "preparare e coordinare" le valutazioni delle FIU sui rischi di riciclaggio e finanziamento del terrorismo. Tale disposizione non fa che richiamare le competenze dell'AMLA nel *Supra-National Risk Assessment* coordinato dalla Commissione, al quale anche le FIU in ogni caso partecipano.

Rispetto al generale mandato dell'AMLA di cui all'art. 5, comma 5, gli artt. da 33 a 37 si rivolgono a tre sole materie: analisi congiunte, assistenza alla cooperazione tra FIU (limitatamente ad alcuni profili non operativi), gestione di FIU.net.

L'art. 36 del regolamento prevede compiti di "assistenza reciproca nel settore della cooperazione tra FIU": si fa riferimento a "programmi di formazione", "scambi di personale", "scambi di prassi", senza in realtà aggiungere dettagli al richiamo generale di cui all'art. 5, comma 5. Dalla lettura congiunta di tali disposizioni sembra dunque evincersi che l'Autorità erogherà formazione specialistica e supporto finanziario alle FIU; faciliterà i rapporti tra queste e i soggetti obbligati mediante formazione a questi ultimi, con particolare riguardo alla rilevazione e segnalazione di operazioni sospette⁴⁴⁹.

A fronte degli estesi compiti di elaborazione normativa previsti nel regolamento, la direttiva attribuisce all'Autorità europea, nelle materie "FIU", competenze di attuazione limitate ad alcuni aspetti della collaborazione internazionale: standard sui formati da utilizzare per gli scambi; "orientamenti" (non vincolanti) su criteri di selezione delle segnalazioni cross-border, trasmissione, feedback.

Mancano inoltre, nella Sezione 6, dettagli sui compiti del Meccanismo per la convergenza di attività, metodi e procedure delle FIU, essenziale per la maggiore efficacia. Tale obiettivo di convergenza resta solo enunciato, senza che seguano disposizioni sulle modalità per perseguirlo.

Quanto ai poteri esercitabili dall'AMLA nella veste di Meccanismo delle FIU, l'art. 6, comma 3, del regolamento enuncia un catalogo minimo, da leggere congiuntamente, e integrare, con previsioni specifiche in altre parti del Package. In generale, l'Autorità può richiedere "dati e analisi" alle FIU ai fini della valutazione dei rischi sovranazionali, raccogliere dati statistici su compiti e attività delle FIU, emanare orientamenti e raccomandazioni; può anche ottenere e trattare informazioni e dati necessari per il coordinamento delle analisi congiunte (art. 30).

⁴⁴⁵ Differenze nella terminologia e nel livello di dettaglio vanno risolte in via interpretativa per evitare discontinuità e incertezze, considerato anche che le disposizioni in esame possiedono efficacia diretta e, per questo, dovrebbero definire un quadro certo delle competenze e dei poteri dell'AMLA quale "Meccanismo".

⁴⁴⁶ L'art. 5, su questo punto, va letto congiuntamente con l'art. 50, commi da 3 a 5, del regolamento AMLR ove è previsto che l'AMLA elabori *Regulatory Technical Standards* per la segnalazione di operazioni sospette. Tale competenza, tuttavia, appare circoscritta alla specificazione del "formato" delle segnalazioni; sul restante contenuto dell'art. 5, comma 5, lett. f) (rilevamento, analisi, disseminazione) non si rinviengono dettagli sull'esercizio delle competenze dell'AMLA.

⁴⁴⁷ "Anche attraverso l'*hosting* di FIU.net". I contenuti di tale compito non sono organicamente individuati in altre disposizioni del Package (cfr. art. 37 del regolamento sulle attività relative a FIU.net).

⁴⁴⁸ Su cooperazione reciproca, assistenza tecnica e finanziaria, interazione con i soggetti obbligati. Si tratta di riferimenti sintetici da cui è difficile desumere iniziative concrete da assumere. Anche in tal caso, poi, se si eccettuano alcuni (parziali) riferimenti nella direttiva ad aspetti della collaborazione tra FIU, non si leggono nel Package indicazioni su interventi dell'AMLA nelle materie elencate nelle lett. a), g), h) dell'art. 5, comma 5. Si può richiamare l'art. 36, comma 2, del regolamento su attività di assistenza tecnica (ma non anche quella finanziaria) alle FIU.

⁴⁴⁹ Non sono precisate le possibili forme di sostegno finanziario (prestiti, erogazioni a fondo perduto) e non è chiaro come l'Autorità possa erogare formazione su materie per le quali è priva di compiti specifici.

9.2.1. Le analisi congiunte. Limiti e prospettive

La disciplina delle analisi congiunte e il ruolo in esse del Meccanismo si ricavano dalla considerazione combinata degli artt. 33, 34 e 35 del regolamento e degli artt. da 22 a 28 della direttiva.

Il disegno complessivo dei presupposti, della procedura e dei compiti degli organi coinvolti, al livello sovranazionale e a quello nazionale, non sembra emergere con chiarezza, a discapito dell'efficace attuazione di una delle principali innovazioni della riforma. Le disposizioni principali riguardano, con duplicazioni e possibili incoerenze tra regolamento e direttiva, l'avvio degli esercizi, la condivisione di informazioni, il ruolo di "delegati nazionali delle FIU" e di "squadre di analisi congiunta" (*Joint Analysis Teams*), il feedback dalle FIU all'AMLA su metodi e risultati.

L'Autorità fornisce supporto per l'identificazione e la selezione di casi di portata cross-border suscettibili di essere sottoposti ad analisi congiunta; sviluppa inoltre una metodologia per tali analisi, necessaria per riconciliare nell'attività congiunta diversi approcci nazionali. L'AMLA è chiamata poi ad avviare, coordinare, organizzare e facilitare lo svolgimento di specifici esercizi di "joint analysis". Ad essa non viene attribuito un ruolo di centro sovranazionale di impulso e coordinamento di analisi congiunte e nemmeno di partecipazione al loro svolgimento⁴⁵⁰; queste restano incentrate su iniziative e decisioni nazionali, secondo dinamiche che restano multilaterali, in termini simili a quelli dello "status quo" nella Piattaforma delle FIU, con rischi di inefficienza e appesantimento burocratico.

L'iniziativa di avviare le analisi congiunte è riservata alle FIU⁴⁵¹. Ognuna può discrezionalmente "lanciare" procedure congiunte proponendo l'istituzione di "team" di analisti. Le FIU conservano piena discrezionalità e possono in ogni caso declinare l'invito con un mero onere di motivazione⁴⁵². L'AMLA ha accesso a "informazioni necessarie", non specificate, in ogni caso previo "esplicito consenso" delle FIU interessate⁴⁵³. Essa non prende parte alle analisi, restando al di fuori dei "joint team". Alcune previsioni riguardano la condivisione dei risultati e forme di feedback; nulla è invece specificato sulla "disseminazione" all'esito degli esercizi.

Le disposizioni in esame non giungono quindi a configurare un "terreno" sovranazionale di svolgimento delle analisi congiunte, con l'attribuzione all'AMLA di un ruolo di impulso. Gli esercizi conservano, come nel regime attuale, caratteristiche multilaterali: le FIU decidono i casi da trattare (unilateralmente, in assenza di un sistema di condivisione preventiva), confermano o rifiutano la partecipazione entro stretti termini, determinano volta per volta le informazioni da condividere e i limiti di utilizzo, curano gli approfondimenti e l'elaborazione di documenti e rapporti. Le FIU potrebbero non avere incentivi per promuovere e partecipare ad analisi congiunte di interesse europeo se non quando questo coincida con propri interessi e priorità nazionali.

9.3. Governance e organizzazione

La caratteristica dell'AMLA di "sintetizzare" due funzioni distinte in un soggetto giuridico unitario richiede particolari accorgimenti per la configurazione di un assetto di *governance* e di procedure decisionali in grado di conciliare unicità soggettiva e duplicità dei ruoli. Al modello di riferimento fornito dalle Autorità Europee di Vigilanza vengono apportate modifiche per contenere due spinte "centrifughe": la coesistenza di due funzioni separate e indipendenti; la coesistenza del livello sovranazionale dell'AMLA e di sistemi nazionali non armonizzati e diversificati.

Gli organi decisionali e gestionali comprendono un Presidente (*Chair*) che coordina le attività interne e rappresenta l'AMLA all'esterno, un Consiglio Generale (*General Board*), organo collegiale cui partecipano a seconda delle materie rappresentanti dei supervisor o delle FIU nazionali, un Comitato Esecutivo

⁴⁵⁰ Per contrasto, si veda l'approccio invece seguito nella disciplina delle "verifiche tematiche congiunte": all'AMLA nella veste di supervisore vengono attribuiti compiti di programmazione, impulso e coordinamento, con effetti vincolanti rispetto ai supervisor nazionali, nei casi di verifiche di interesse europeo.

⁴⁵¹ La direttiva indica generici criteri di rilevanza, attinenti alla natura complessa e transnazionale del caso, tale da rendere necessario un approccio congiunto (art. 25, comma 3: "a) le analisi operative della FIU richiedono analisi difficili e impegnative che presentano collegamenti con altri Stati membri; b) alcune FIU stanno conducendo analisi operative in cui le circostanze del caso richiedono un'azione coordinata e concertata negli Stati membri interessati").

⁴⁵² Entro un termine di 5 giorni, difficilmente sufficiente per la valutazione e un'eventuale riallocazione di priorità e risorse.

⁴⁵³ Art. 33, comma 3.

(*Executive Board*), organo collegiale non rappresentativo delle autorità nazionali con compiti esecutivi e di organizzazione interna, un Direttore Esecutivo (*Executive Director*) responsabile delle attività operative, una Commissione Amministrativa del Riesame (*Board of Appeal*) che riceve e decide ricorsi avverso decisioni dell'AMLA.

La linearità del modello viene alterata con geometrie organizzative e di *governance* “irregolari” per allocare nel medesimo organismo competenze e procedure eterogenee e separate per la supervisione e per il Meccanismo. La distribuzione dei ruoli tra gli organi non è simmetrica; alcuni hanno competenza in entrambi i comparti (Presidente), con una sorta di “ibridazione”, altri operano in uno (*Executive Board*, nella supervisione), altri ancora assumono diverse configurazioni in ciascuno dei due (Consiglio Generale), con una sorta di “sdoppiamento” funzionale, se non soggettivo. Anche le procedure decisionali sono diversamente strutturate a seconda che riguardino materie dell'uno o dell'altro comparto ovvero questioni di rilievo comune: in questo secondo caso, il Comitato esecutivo delibera per l'AMLA nel suo complesso e l'organo collegiale “ibrido” di vertice (Consiglio Generale) adotta, in sessioni disgiunte nelle due composizioni, due decisioni convergenti.

Il Consiglio Generale è convocato dal Presidente. Nella *Supervisory Composition* vi partecipano il Presidente, i Capi dei supervisori nazionali (uno per Paese), un rappresentante della Commissione (senza diritto di voto). A causa dell'eterogenea allocazione delle responsabilità di supervisione antiriciclaggio nei diversi paesi e nei diversi settori, conseguenza di sistemi non armonizzati, partecipano al Consiglio autorità di volta in volta diverse, sia per i singoli Stati membri (a seconda delle materie) sia tra gli Stati stessi. Nella *FIU Composition* fanno parte del Consiglio il Chair, i Capi delle FIU, un rappresentante della Commissione (senza diritto di voto).

Il Consiglio può ammettere membri osservatori e istituire “comitati interni” (art. 47); è indipendente da ogni soggetto terzo e definisce le proprie regole di funzionamento. Esso adotta *draft regulatory* e *implementing technical standards*, pareri, raccomandazioni e linee-guida. Nel comparto della supervisione, assume decisioni in particolare nelle materie della collaborazione di vigilanza, della metodologia di supervisione, delle verifiche tematiche; nella “*FIU composition*”, è competente per le decisioni in tutte le materie del Meccanismo (artt. 30-42).

Il Comitato Esecutivo svolge compiti specifici, con membri impegnati a tempo pieno. Ne fanno parte il Chair dell'Autorità, cinque membri nominati dal Consiglio Generale nelle due composizioni, un rappresentante della Commissione (senza diritto di voto). Il Comitato è competente per la pianificazione complessiva delle attività dell'AMLA; assume decisioni relative alla supervisione diretta; non svolge invece un ruolo specifico nel Meccanismo delle FIU. È inoltre competente per le decisioni in materie non attribuite al Consiglio Generale.

Il Presidente rappresenta l'Autorità e istruisce le attività del General Board e dell'Executive Board, predisponendo l'ordine del giorno e presiedendo le riunioni. Assegna ai membri dell'Executive Board specifiche aree di responsabilità. Il Direttore Esecutivo è responsabile della gestione ordinaria (“day-to-day”), dell'attuazione delle decisioni del Comitato Esecutivo, della preparazione e attuazione del documento di programmazione, del budget previsionale e del rapporto periodico sull'attività.

9.3.1. Prime osservazioni sulla governance

La complessa architettura dell'AMLA, robusta nel suo disegno statico, dovrà mostrarsi nel funzionamento dinamico idonea a sostenere una dialettica articolata. Nonostante lo sforzo “creativo” nel definire un sistema di *governance* in grado di adattarsi al contesto antiriciclaggio europeo, possono essere individuati alcuni punti critici, specie nella prospettiva del Meccanismo delle FIU.

Un primo punto riguarda la non piena separatezza organizzativa tra le due funzioni. L'AMLA racchiude due ruoli in un medesimo apparato. L'esigenza di separatezza, se spinta alle conseguenze più rigorose, reagirebbe sulla unicità stessa dell'Autorità, conducendo a una scissione lungo la linea di confine tra la supervisione e il Meccanismo delle FIU; nel regolamento, la tensione tra unicità soggettiva e duplicità funzionale è affrontata con l'istituzione di un unico organo di vertice “monocratico” e di organi di *governance* in parte differenziati, nella natura o nella composizione.

Spicca la separazione tra le due configurazioni del Consiglio Generale, organo di vertice sia del supervisore sia del Meccanismo. La separazione si riscontra anche per il Comitato Esecutivo che, semplicemente, si occupa solo di materie di supervisione (oltre che di aspetti di auto-organizzazione dell'AMLA nel suo complesso). Tuttavia, la linea di distinzione tra la *governance* del supervisore e quella del Meccanismo si interrompe nell'organo apicale: il Chair presiede il Consiglio Generale in entrambe le sue composizioni, lo convoca, esercita il diritto di voto. Tale organo assomma quindi due ruoli e in esso si “confondono” il supervisore antiriciclaggio e il Meccanismo delle FIU, venendo meno distinzione e separatezza, presupposto dell'indipendenza secondo le regole europee.

La soluzione basata su un unico responsabile per due comparti organizzativi va ponderata alla luce delle regole europee e degli standard internazionali che pongono presidi di indipendenza e separatezza dei compiti e dell'organizzazione della FIU. Nell'art. 17, comma 4, della sesta direttiva antiriciclaggio è anzitutto richiamata l'indipendenza operativa: la FIU "ha l'autorità e la capacità di svolgere liberamente le sue funzioni" di ricezione, analisi e disseminazione; inoltre, "è esente da indebite interferenze o ingerenze politiche, governative o del settore" privato. L'autonomia operativa e l'indipendenza da influenze esterne presuppongono adeguati presidi organizzativi e di *governance*; all'indipendenza organizzativa è dedicata la seconda parte del comma 4: "quando la FIU è situata all'interno della struttura esistente di un'altra autorità, le funzioni fondamentali della FIU sono indipendenti e operativamente separate dalle altre funzioni dell'autorità ospitante". Dunque, l'indipendenza operativa presuppone quella organizzativa che, a sua volta, presuppone la "separatezza" della FIU rispetto alla "autorità ospitante" nella quale essa è collocata.

Come detto, occorre cautela nel trasporre tali requisiti e vincoli, dettati per la FIU quale autorità nazionale e in relazione alle funzioni sue proprie, sul diverso piano sovranazionale dell'AMLA quale Meccanismo delle FIU, incaricato di compiti diversi. Ad ogni modo, appare legittimo attendersi che i presupposti di autonomia e separatezza siano rispecchiati sul versante sovranazionale nel quale le FIU ora si trovano a operare. Non sarebbe congruo applicare standard di indipendenza diversi sul piano domestico e su quello sovranazionale, con la conseguenza che le FIU, organizzativamente autonome e separate da altre autorità nei rispettivi paesi, opererebbero nella sede europea in un contesto di "commistione". È ciò che accade nel Consiglio Generale, nel quale i capi delle FIU incontrano un limite alle proprie prerogative nella figura del *Chair*, titolare di competenze decisionali proprie in entrambi i comparti dell'AMLA.

La configurazione "due corpi, una testa" e l'imperfetta separatezza, con gli assetti del supervisore e del Meccanismo che si congiungono nel *Chair*, comportano commistioni di funzioni e informazioni.

Nella sua duplice veste il *Chair* si occupa allo stesso tempo, ad esempio, di interventi di supervisione diretta su intermediari "selezionati" e di analisi congiunte. Queste ultime possono riguardare casi emersi nell'operatività degli intermediari o informazioni provenienti da essi; può anche verificarsi che attività sottoposte ad analisi congiunta coinvolgano intermediari sottoposti a supervisione diretta. In tali casi, gli obiettivi e gli "interessi" del supervisore e del Meccanismo (nonché delle FIU) possono divergere, con vari gradi di intensità. La commistione può riguardare, oltre alle funzioni e agli obiettivi, anche le informazioni. Sul *Chair* convergono sia gli elementi di supervisione disponibili al Consiglio nella relativa composizione sia quelli sottoposti al Consiglio delle FIU nelle materie del Meccanismo.

Nella prospettiva delle FIU l'indipendenza e la separatezza costituiscono presidi di protezione da influenze e deviazioni dagli obiettivi, incondizionati, di rilevazione e analisi di attività illecite. Occorre per questo valutare con attenzione le caratteristiche della *governance* dell'AMLA, nel suo concreto funzionamento, e il duplice ruolo del *Chair*. Può essere utile riflettere su correttivi di *checks and balances* quali ipotesi di astensione o limitazioni nell'impiego di dati e documenti, idonei a minimizzare rischi di conflitto e asimmetrie informative e valorizzare opportunità di collegamento tra supervisione e analisi di operazioni sospette.

Nella supervisione le competenze sono distribuite tra il Consiglio Generale e l'Executive Board (art. 53). Nel Meccanismo, invece, le valutazioni e le decisioni sono tutte affidate al *General Board* nella relativa composizione. Le FIU, nell'ambito della Piattaforma, hanno promosso una posizione comune, accolta nei negoziati presso il Consiglio europeo, con proposte sulla *governance* del Meccanismo.

Si prospetta la creazione di uno *Standing Committee* con compiti di iniziativa e proposta a supporto del Consiglio Generale in composizione FIU. Il Comitato conferirebbe maggiore peso alle FIU, contenendo gli oneri "esecutivi" che, in assenza di un ruolo dell'Executive Board, incomberebbe sul Consiglio e verrebbe gestito prevalentemente dal *Chair* (quale organo "permanente"). Lo *Standing Committee* si interporrebbe, con compiti di coordinamento e impulso, tra l'articolazione organizzativa dell'Autorità e il Consiglio; questo si concentrerebbe su aspetti decisionali e strategici, ferma la possibilità di istituire, ai sensi dell'art. 47, Comitati Interni ai quali delegare attività specifiche.

CAPITOLO 3

Adeguate verifica, profilazione, conservazione

(a cura di G. Castaldi)

1. Analisi, valutazione e mitigazione del rischio (W. Negrini e L. La Rocca)

Il sistema nazionale di prevenzione del riciclaggio e del finanziamento del terrorismo (AML/CFT), in coerenza con quanto stabilito dalle Raccomandazioni del GAFI⁴⁵⁴ e dalle direttive europee⁴⁵⁵, si fonda sul c.d. “*risk based approach*”, sul presupposto che il rischio di realizzazione dei predetti reati non sia lo stesso in ogni caso⁴⁵⁶; esso è da considerarsi mutevole a seconda della realtà operativa del soggetto obbligato e deve essere mitigato sulla base di processi decisionali basati su evidenze fattuali; si deve quindi procedere alla valutazione concreta del predetto rischio e alla predisposizione di adeguati presidi organizzativi, la cui articolazione va modulata alla luce della normativa primaria e secondaria in materia, della specificità dell’attività svolta dai destinatari degli obblighi di prevenzione e delle relative dimensioni organizzative, al fine di assicurare un corretto adempimento dei medesimi obblighi e un efficace governo dei rischi⁴⁵⁷.

Sulla base della disciplina vigente, le attività di analisi e valutazione del rischio sono svolte a un triplice livello: *i)* sovranazionale; *ii)* nazionale e *iii)* da parte di ciascun soggetto obbligato. Più in dettaglio, a livello europeo, secondo quanto stabilito dalla quarta direttiva che rispetto alla terza ha ampliato il *risk-based approach*, la Commissione effettua ogni due anni (o, se del caso, anche prima dello scadere del biennio) la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo che gravano sul mercato interno e relativi alle attività transfrontaliere; sono presi in considerazione i rischi associati a ciascun settore e i mezzi più diffusi cui ricorrono i criminali per riciclare proventi illeciti, anche alla luce dei pareri formulati dalle Autorità europee di supervisione. La Commissione formula, inoltre, raccomandazioni agli Stati membri con riguardo alle misure idonee ad affrontare i rischi individuati e, qualora decidano di non applicare le predette raccomandazioni nei rispettivi sistemi nazionali, gli Stati membri sono tenuti a darne notizia motivata alla Commissione⁴⁵⁸.

Sono state finora pubblicate tre relazioni sulla valutazione sovranazionale dei rischi di riciclaggio e di finanziamento del terrorismo: la prima nel giugno del 2017⁴⁵⁹, la seconda nel luglio del 2019⁴⁶⁰ e la terza

⁴⁵⁴ Cfr., in primo luogo, la Raccomandazione n. 1 e la relativa nota interpretativa sul tema “Assessing risks and applying a risk-based approach”. Riferimenti al risk-based approach si rintracciano anche in altre Raccomandazioni, ad esempio n. 10, n. 12 e n. 13 per la graduazione delle misure di customer due diligence. Sul tema in generale si veda P. Fratangelo, *L’approccio basato sul rischio nella normativa antiriciclaggio*, in *Bancaria* n. 2/2009, pp. 70 e ss., nonché più recentemente G. Barbato, *La valutazione del rischio nella disciplina preventiva antiriciclaggio: profili sistematici e procedurali*, in *IANUS Diritto e Finanza*, n. 2/2019, pp. 167 e ss. e G. Castaldi, *Le misure antiriciclaggio tra norme inderogabili e valutazioni discrezionali*, in *Bancaria*, n. 9/2022, pp. 80 e ss.

⁴⁵⁵ Si vedano la direttiva 2005/60/CE (c.d. terza direttiva), nonché la direttiva (UE) 2015/849 (c.d. quarta direttiva) come modificata dalla direttiva (UE) 2018/843 (c.d. quinta direttiva). Va inoltre considerato che, ai sensi della citata Raccomandazione n. 1 del GAFI “Countries should also identify, assess, and understand the proliferation financing risks for the country. In the context of Recommendation 1, “proliferation financing risk” refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7”.

⁴⁵⁶ Si vedano i considerando (22), rispettivamente, della terza e della quarta direttiva.

⁴⁵⁷ Si veda P. Fratangelo, *Intermediari bancari e gestione del rischio di riciclaggio*, in *Bancaria* n. 5/2016, pp. 59 e ss.

⁴⁵⁸ Art. 6 della quarta direttiva come modificato dalla quinta.

⁴⁵⁹ Commissione europea, COM(2017) 340 final.

⁴⁶⁰ Commissione europea, COM(2019) 370 final. La relazione è stata pubblicata il 24 luglio 2019, in occasione della pubblicazione di una Comunicazione della Commissione al Parlamento e al Consiglio in cui sono stati richiamati i risultati ottenuti con l’adozione: *i)* della quinta direttiva antiriciclaggio; *ii)* delle norme sulla collaborazione e lo scambio di informazioni tra i supervisori (prudenziali e antiriciclaggio, europei e nazionali) e le FIU; *iii)* della direttiva (UE) 2018/1673 per l’armonizzazione della fattispecie penale di riciclaggio; *iv)* delle disposizioni tese ad agevolare l’accesso delle autorità nazionali designate alle informazioni finanziarie e rafforzare lo scambio di informazioni tra le autorità investigative e le FIU. Oltre alla richiamata relazione contenente la nuova valutazione dei rischi sovranazionali di riciclaggio e finanziamento del terrorismo, sono stati pubblicati un Rapporto inerente alle FIU, un Rapporto su casi di riciclaggio che hanno coinvolto alcune banche europee e un Rapporto relativo al tema dell’interconnessione dei registri nazionali dei conti bancari.

nell'ottobre 2022⁴⁶¹. In quest'ultima – alla luce della revisione del quadro giuridico dell'Unione in materia di AML/CFT, degli effetti della pandemia COVID-19 e delle sanzioni imposte a Russia e Bielorussia – sono stati valutati nuovamente tutti i settori trattati dagli esercizi precedenti e sono state aggiornate le informazioni contenute nella relazione del 2019⁴⁶². Per i settori o i prodotti in cui sono stati rilevati mutamenti rilevanti, la valutazione ha comportato un ricalcolo dei livelli di rischio (ad esempio, le cripto-attività e il gioco d'azzardo online, due settori in cui il rischio oggi è più elevato).

A livello nazionale l'analisi e la valutazione dei rischi ML/TF è richiesta a ciascuno Stato membro, che è chiamato a designare un'Autorità o a istituire un meccanismo attraverso il quale coordinare la risposta nazionale ai rischi individuati. L'*assessment* nazionale è utilizzato per migliorare il sistema AML/CFT, in particolare indicando i settori in cui i soggetti obbligati sono tenuti ad applicare misure rafforzate e, se del caso, specificando le misure da adottare. Sono precisati i settori o le aree di minore o maggiore rischio anche al fine di agevolare la distribuzione e la definizione delle risorse da destinare al contrasto del riciclaggio e del finanziamento del terrorismo e gli adempimenti da parte dei soggetti obbligati. Ciascuno Stato membro è tenuto, inoltre, a redigere una relazione sulla struttura istituzionale e sulle principali procedure del proprio sistema di prevenzione nonché sulle attività e sulle risorse nazionali destinate al contrasto dei predetti fenomeni criminali⁴⁶³.

In Italia, in attuazione della Raccomandazione n. 1 del GAFI, il primo *risk assessment* a livello nazionale è stato realizzato in via sperimentale nel 2014 dalle Autorità partecipanti al Comitato di Sicurezza Finanziaria (CSF) e con i contributi ricevuti da amministrazioni ed esperti del settore. Le minacce per l'economia nazionale sono state giudicate molto significative, anche in relazione alla gravità delle condotte che producono proventi da riciclare (corruzione; reati fallimentari, societari e fiscali; usura; criminalità organizzata dedita ad attività di narcotraffico; gioco d'azzardo; gestione del traffico illecito di rifiuti; sfruttamento sessuale; traffico di esseri umani). Sono state considerate le incidenze negative derivanti dall'utilizzo del contante e dall'economia sommersa; anche per il finanziamento del terrorismo, il rischio è stato reputato abbastanza significativo⁴⁶⁴.

Nel 2017, in occasione del recepimento della quarta direttiva europea, il legislatore ha modificato il D.lgs. 231/2007 e ha affidato formalmente al Comitato di Sicurezza Finanziaria (CSF) il compito di analizzare e valutare il rischio nazionale di riciclaggio di denaro e di finanziamento del terrorismo.

L'analisi ha cadenza triennale, salva la facoltà del CSF di effettuarne l'aggiornamento quando insorgono nuovi rischi e ogniqualvolta il Comitato lo ritenga opportuno; essa viene svolta nel rispetto dei criteri internazionali, delle indicazioni contenute nel *supra national risk assessment* della Commissione europea nonché sulla base dei dati e delle informazioni fornite dagli attori coinvolti nel sistema di prevenzione; in primo luogo il Ministero dell'economia e delle finanze, le Autorità di vigilanza di settore, l'Unità di informazione finanziaria per l'Italia, la Guardia di finanza e la Direzione Investigativa Antimafia, ma anche le amministrazioni e gli organismi interessati, gli organismi di autoregolamentazione e i rappresentanti della Presidenza del Consiglio dei ministri e di altre amministrazioni con competenze specifiche su temi di interesse. Il CSF può altresì avvalersi della collaborazione di studiosi e rappresentanti del mondo accademico e delle associazioni private rappresentative delle categorie interessate⁴⁶⁵. La nuova analisi nazionale condotta ai sensi di tale previsione normativa è stata pubblicata nel giugno del 2019, sulla base dei dati riferiti al periodo 2014-2018. È emerso un quadro sostanzialmente in linea con la rilevazione effettuata nel 2014, con un rischio di riciclaggio molto significativo e di finanziamento del terrorismo (di matrice sia nazionale sia internazionale) abbastanza significativo. Nel suo complesso, il sistema di prevenzione e contrasto è apparso adeguatamente rispondente rispetto alla minaccia che proventi di attività criminali possano essere inseriti nel sistema finanziario ed economico. Le modifiche normative e il rafforzamento dei presidi hanno consentito di evidenziare l'esistenza

⁴⁶¹ Commissione europea, COM(2022) 554 final. Per il dettaglio delle valutazioni sui singoli settori esaminati cfr. *Commission Staff Working Document* che accompagna la relazione sulla valutazione dei rischi del 2022.

⁴⁶² Nella relazione del 2019 erano stati individuati, in particolare, rischi connessi con prodotti nuovi e non regolamentati come le cripto-attività e settori da esplorare quali il calcio professionistico, i porti franchi, i programmi di soggiorno e di cittadinanza per gli investitori. Vulnerabilità comuni avevano riguardato, fra l'altro, l'anonimato nelle operazioni finanziarie, l'identificazione dei titolari effettivi e i rischi derivanti dallo sviluppo del FinTech.

⁴⁶³ Art. 7 della quarta direttiva, come modificato dalla quinta.

⁴⁶⁴ La relazione contenente gli esiti della prima analisi nazionale dei rischi condotta in Italia è consultabile alla pagina https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Sintesi_NRA_divulgabile_a_soggetti_obbligati_2_dicembre_2014.pdf. In argomento si veda P. Fratangelo, *Intermediari bancari e gestione del rischio di riciclaggio*, cit., p. 61-62.

⁴⁶⁵ Art. 14 del D.lgs. 231/2007 come modificato dal D.lgs. 90/2017.

di un impianto potenziato e migliorato. La collaborazione tra le Autorità italiane è considerata un punto di forza del sistema mentre la cooperazione internazionale presenta ancora margini di miglioramento. Sono state indicate alcune linee di intervento e compiuti focus tematici sul rischio di abuso di valute virtuali e sulle criticità emerse in esito all'attività ispettiva della UIF presso istituti di pagamento e IMEL italiani e comunitari⁴⁶⁶.

I rischi individuati a livello sovranazionale e nazionale sono funzionali all'adempimento dell'analogo obbligo di *assessment* posto a carico dei soggetti obbligati, i quali sono tenuti ad adottare procedure oggettive e coerenti per l'analisi e la valutazione dei rischi cui essi sono esposti nello svolgimento della propria attività; a tal fine, essi tengono conto dei fattori di rischio associati alla tipologia di clientela, all'area geografica di operatività, ai canali distributivi e ai prodotti e ai servizi offerti e utilizzano i criteri e le metodologie definiti dalle Autorità di vigilanza di settore e dagli organismi di autoregolamentazione di riferimento per ciascuna categoria di soggetti obbligati⁴⁶⁷. In argomento occorre in particolare considerare le disposizioni emanate, rispettivamente, da Banca d'Italia, IVASS e Consob, per i soggetti rispettivamente vigilati, nonché le regole tecniche e le relative linee guida elaborate dagli organismi di autoregolamentazione per le distinte categorie professionali⁴⁶⁸.

La valutazione così condotta deve essere documentata, periodicamente aggiornata e messa a disposizione delle Autorità (MEF, Autorità di vigilanza, UIF, NSPV e DIA) e degli organismi di autoregolamentazione, ai fini dell'esercizio delle loro funzioni e poteri in materia di prevenzione del riciclaggio e di finanziamento del terrorismo. I soggetti obbligati adottano, inoltre, i presidi e attuano i controlli e le procedure, adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi individuati. In caso di gruppi, la capogruppo adotta un approccio globale al rischio di riciclaggio e di finanziamento del terrorismo secondo le modalità stabilite dalle Autorità di vigilanza di settore (art. 16 del D.lgs. 231/2007).

Il *risk based approach* caratterizza quindi concretamente l'attività AML/CFT e per essere efficace attiene al *risk assessment* condotto da ciascun soggetto obbligato, al fine di valutare i rischi cui esso è esposto, al conseguente adeguamento delle politiche e procedure interne nonché alla graduazione nell'adempimento degli obblighi, in particolare in materia di adeguata verifica⁴⁶⁹. I destinatari del D.lgs.

⁴⁶⁶ La relazione contenente gli esiti della seconda analisi nazionale dei rischi di riciclaggio e di finanziamento del terrorismo è consultabile alla pagina http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Analisi_dei_rischi_di_riciclaggio_e_di_finanziamento_del_terrorismo_2018_-_Sintesi.pdf.

⁴⁶⁷ Art. 7 della quarta direttiva come modificato dalla quinta e art. 15 del D.lgs. 231/2007. Inoltre, ai sensi del comma 3 del predetto art. 15, le autorità di vigilanza di settore individuano, informandone il Comitato di sicurezza finanziaria, le categorie di soggetti obbligati, rispettivamente vigilati, per i quali le disposizioni di cui al presente articolo non trovano applicazione, in considerazione dell'irrelevanza del rischio di riciclaggio e di finanziamento del terrorismo dell'attività svolta ovvero dell'offerta di prodotti e servizi che presentano caratteristiche di rischio tipizzate.

⁴⁶⁸ Per il dettaglio sia consentito rinviare, con riguardo alla Banca d'Italia, alle [disposizioni del 27 marzo 2019](#) per gli intermediari bancari e finanziari nonché alle [disposizioni del 4 febbraio 2020](#) in materia di adeguata verifica della clientela e di conservazione dei dati e delle informazioni per gli operatori non finanziari iscritti nell'elenco di cui all'art. 8 del decreto-legge 25 settembre 2001, n. 350; in ambito bancario e finanziario vanno altresì considerati gli [Orientamenti dell'Autorità Bancaria europea del 1° marzo 2021](#), che hanno assunto il valore di orientamenti di vigilanza in virtù di quanto disposto dalla Banca d'Italia (cfr. [Nota n. 15 del 4 ottobre 2021](#)) e che attengono ai fattori che da prendere in considerazione nella valutazione del rischio ML/TF correlato all'attività dell'intermediario e ai rapporti o alle operazioni con la clientela, nonché le modalità con cui graduare le misure di adeguata verifica in modo commisurato al rischio. Per le imprese e gli intermediari assicurativi si ha inoltre riguardo alle indicazioni dell'IVASS e, in particolare, al [Regolamento n. 44](#) del 12 febbraio 2019 e al successivo [Regolamento n. 111](#) del 13 luglio 2021 recante disposizioni sulle procedure di mitigazione del rischio di riciclaggio e modifiche al predetto regolamento n. 44; per i revisori legali e le società di revisione sottoposte alla vigilanza della Consob si veda la [Delibera n. 20570](#) del 4 settembre 2018 recante adozione del regolamento di attuazione del D.lgs. 231 del 2007. Con riguardo ai dottori commercialisti ed esperti contabili, si rinvia alle Regole tecniche del gennaio 2019 e alle [Linee guida](#) del maggio dello stesso anno elaborate dal Consiglio Nazionale Dottori Commercialisti ed Esperti Contabili (CNDCEC) e inerenti agli obblighi di valutazione del rischio, adeguata verifica della clientela, conservazione dei documenti, dei dati e delle informazioni. Per gli avvocati si vedano i documenti pubblicati nel settembre 2019 dal Consiglio Nazionale Forense (CNF) e recanti le [Regole tecniche](#) nonché i [Criteri e le metodologie](#) per l'analisi e la valutazione del rischio. Per i notai si rinvia alle [Regole tecniche](#) pubblicate dal Consiglio Nazionale del Notariato (CNN) nel settembre 2018. Infine, per i consulenti del lavoro il Consiglio Nazionale dei Consulenti del Lavoro (CNCL) ha pubblicato le Regole tecniche nel giugno 2022.

⁴⁶⁹ G. Castaldi, *Le misure antiriciclaggio tra norme inderogabili e valutazioni discrezionali*, cit., p. 86, ha osservato che agli "obbligati si chiede di prendere in considerazione un elevato numero di circostanze ed elementi di giudizio, dalla cui valutazione emergono spesso indicazioni divergenti circa il livello di rischio dei singoli clienti [...] lo spazio lasciato al criterio del risk based approach, espressione dell'autonomia degli intermediari – per il cui tramite il legislatore sembra consentire un adeguamento della regolamentazione generale alle diverse realtà dimensionali e operative dei destinatari degli obblighi – rischia di risultare eccessivamente compresso da numerose norme inderogabili. Tra fattori di rischio da prendere comunque in considerazione, fattispecie sottoposte inderogabilmente ad adeguata verifica rafforzata e misure obbligatorie di mitigazione del rischio, non molto margine sembra, infatti, residuare per un'autoregolamentazione ispirata al principio di proporzionalità. [...] Il documento di policy antiriciclaggio costituisce lo strumento più efficace a disposizione degli intermediari per tentare di adattare razionalmente e motivatamente alle proprie peculiarità dimensionali e operative le misure antiriciclaggio, modulandone l'estensione e l'intensità secondo il grado di rischio associato ai singoli clienti, in applicazione del criterio dell'approccio commisurato al rischio".

231/2007: *i*) identificano i rischi (cc.dd. “inerenti”) attuali e potenziali cui sono esposti in base alla natura e all’estensione dell’attività svolta; *ii*) analizzano l’adeguatezza dell’assetto organizzativo e dei presidi rispetto ai rischi precedentemente identificati, al fine di individuare eventuali vulnerabilità; *iii*) determinano il livello di adeguatezza delle procedure e implementano le stesse per renderle idonee a mitigare i rischi⁴⁷⁰. Ne deriva che l’attività di antiriciclaggio è destinata ad assumere un ruolo centrale nel sistema di *risk management* e che la definizione di metodologie per la gestione dei rischi garantisce la correttezza dei comportamenti e contribuisce a rendere immune la struttura aziendale da infiltrazioni di origine criminale⁴⁷¹.

In funzione del profilo di rischio, della natura e delle dimensioni dei soggetti obbligati e dei rischi nazionali e transfrontalieri di riciclaggio e di finanziamento del terrorismo sono d’altra parte definite la frequenza e l’intensità delle verifiche da parte delle Autorità di controllo antiriciclaggio⁴⁷². In questo modo si consente di assicurare una più elevata efficacia dei controlli, in coerenza con il criterio di efficienza nell’uso delle risorse, di proporzionalità dell’azione di vigilanza, nonché di minimizzazione degli oneri a carico dei destinatari⁴⁷³.

2. Profilazione del rischio del cliente (F. Berghella)

Lo sviluppo della normativa, con il D.lgs. 21 novembre 2007 n. 231, pose l’approccio basato sul rischio al centro degli adempimenti, con misure da adottare graduate e commisurate all’entità del rischio di riciclaggio o di finanziamento del terrorismo, e la correlata necessità di valutare la clientela anche per segmenti omogenei. Alle nozioni di “probabilità” e “dinamicità” del rischio, che caratterizzavano la precedente normativa, si aggiunsero quelle di “gradualità” delle misure e di “segmentazione” della clientela⁴⁷⁴.

La logica sottostante alla profilazione degli eventi di rischio si è consolidata nel tempo, assumendo un ruolo rilevante nella prevenzione della criminalità economica mediante il controllo costante del rapporto d’affari e delle operazioni effettuate dai clienti, ed è confermata dagli orientamenti relativi ai fattori di rischio emanati dall’Autorità bancaria europea il 1° marzo 2021, che definiscono il rischio come la “probabilità” che abbiano luogo attività di ML/TF e le relative ripercussioni. La “natura mutevole” delle minacce del riciclaggio e del finanziamento del terrorismo, facilitata dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, e la conseguente necessità di un costante adattamento dei presidi di prevenzione e contrasto è richiamata dalle istruzioni di vigilanza emanate da Banca d’Italia e IVASS sull’autovalutazione dei rischi ML/TF.

⁴⁷⁰ S. Galmarini e C. Saba, *IV direttiva Antiriciclaggio e approccio basato sul rischio*, 2018, disponibile su dirittobancario.it.

⁴⁷¹ P. Fratangelo, *Intermediari bancari e gestione del rischio di riciclaggio*, cit., p. 62.

⁴⁷² Art. 7, comma 2, lett. a), e art. 9, comma 3, del D.lgs. 231/2007.

⁴⁷³ P. Fratangelo, *Intermediari bancari e gestione del rischio di riciclaggio*, cit., p. 65.

⁴⁷⁴ L’obbligo di profilare il rischio di riciclaggio della clientela origina con il DM 3 febbraio 2006, n.142 del Ministero dell’Economia e delle finanze, unitamente al Provvedimento 24 febbraio 2006 dell’Ufficio Italiano Cambi. Le istruzioni dell’UIC sulle procedure per la conoscenza e l’identificazione della clientela disposero che, per acquisire una conoscenza adeguata dei propri clienti, gli intermediari devono valutarne il profilo di rischio, inteso come la probabilità di esposizione a fenomeni di riciclaggio, da stimare in base alla conoscenza dei clienti e tenendo conto di aspetti oggettivi e soggettivi concernenti le caratteristiche delle attività svolte dai clienti, dalle operazioni da essi compiute, dagli strumenti utilizzati e da elementi connessi al rischio geografico. Venne così introdotto un metodo di valutazione e classificazione correlato ai concetti di probabilità e dinamicità del rischio, poiché i fattori che lo compongono, non essendo statici e mutando nel tempo, richiedono la valutazione nel continuo dell’attività dei clienti e l’aggiornamento del profilo di rischio assegnato. Nello stesso anno il sistema bancario si organizzò, con riunioni dedicate del Comitato antiriciclaggio ABI ARMA, progettando la metodologia da utilizzare per la profilazione del rischio di riciclaggio e alla raccolta di informazioni per la conoscenza del cliente, in applicazione al principio del *Know Your Customer*, con l’obiettivo di codificarle in una procedura informatica (GIANOS Gestione Profili di Rischio) che tenesse conto delle disposizioni dell’UIC e degli adempimenti indicati della terza direttiva AML/CFT. Nell’ottobre 2007, dopo un periodo di ampia sperimentazione, il nuovo programma venne integrato nel più ampio sistema denominato GIANOS 3D. Con questa decisione il sistema bancario italiano avviò la prima esperienza di classificazione del rischio della clientela (cfr. Lettere circolari ABI dell’8 agosto 2007, e del 13 marzo 2008). Il modello ispirò le applicazioni di altri intermediari e settori. Il provvedimento sull’adeguata verifica del 2013 attribuì dignità normativa alle soluzioni tecniche e organizzative adottate dal sistema bancario ed altri intermediari (cfr. G. Castaldi, *L’adeguata verifica della clientela bancaria e il recente provvedimento della Banca d’Italia*, *Bancaria* n.10/2013). Il GAFI, nel 2016, rilevò come “in gran parte del settore finanziario le procedure di adeguata verifica della clientela sono uniformi in modo impressionante”.

L'avvento dell'approccio basato sul rischio e il successivo ampliamento c.d. olistico operato dalla quarta e quinta direttiva, hanno generato un progressivo aumento di fattori da considerare per la profilazione del rischio dei clienti⁴⁷⁵, e un correlato maggior numero dei soggetti classificati a rischio alto da sottoporre a misure di adeguata verifica rafforzata, con la conseguente necessità di perfezionare frequentemente i contenuti, le funzionalità e le prestazioni delle applicazioni informatiche. Nel 2007, anno della prima profilazione, i soggetti con rischio elevato, nel sistema bancario, erano mediamente lo 0,02% della clientela; dopo i provvedimenti sull'adeguata verifica del 2013 lo 0,33%; in seguito alla quarta direttiva lo 0,74%; con i successivi provvedimenti di vigilanza del 2019 e delle linee guida ESAs raggiunsero l'1,6%⁴⁷⁶.

2.1. Criteri e modalità

La normativa vigente prescrive che il profilo di rischio attribuibile a ogni cliente avviene sulla base dei complessivi elementi di valutazione richiesti per l'adeguata verifica e dei fattori di rischio relativi al cliente, all'esecutore, al titolare effettivo, ai prodotti, ai servizi, alle operazioni, ai canali di distribuzione e ai rischi geografici.

I criteri per la profilazione del cliente sono specificati nei provvedimenti in materia di adeguata verifica emanati dalla vigilanza⁴⁷⁷, integrati dagli orientamenti EBA (GL/2021/02), recepiti con Nota della Banca d'Italia n. 15 del 4 ottobre 2021⁴⁷⁸. I singoli fattori di rischio sono ponderati sulla base della loro importanza relativa che, spesso, si traduce nell'assegnazione da parte delle imprese di "punti" ai diversi elementi. Il peso attribuito a ciascun fattore è suscettibile di variazione sulla base della tipologia di prodotto, cliente o categoria di cliente e impresa. La valutazione complessiva permette di includere ciascun cliente in una classe (o fascia) di rischio preventivamente definita (es. alto, medio, basso, irrilevante⁴⁷⁹; a volte tre o cinque livelli). L'elaborazione del profilo si basa, per quanto possibile, su algoritmi e procedure informatiche, con l'avvertenza che i destinatari assicurano che la classe di rischio proposta in automatico dai sistemi informatici sia coerente con la propria conoscenza del cliente e di poter applicare, con l'intervento umano, classi di rischio diverse. Nel caso la decisione comporti l'abbassamento del livello di rischio proposto (o dei controlli da parte degli operatori) la motivazione deve essere annotata, conservata e circoscritta a casi eccezionali. Se il sistema informatico utilizzato per la profilazione è fornito da soggetti esterni all'intermediario, i destinatari ne devono conoscere adeguatamente il funzionamento e i criteri utilizzati per determinare i punteggi e l'attribuzione della classe di rischio, poterli modificare ed essere in grado di dimostrarlo all'Autorità competente.

Nei gruppi la profilazione del cliente può essere accentrata o svolta dalle singole società del gruppo; quando non è accentrata ogni società calcola il rischio anche sulla base delle informazioni utilizzate dalle altre società del gruppo e, in ciascuna società, viene assunto per uno stesso cliente il profilo di rischio più elevato tra quelli assegnati; nel caso s'intenda attribuire un profilo di rischio più basso, le ragioni della scelta sono specificamente motivate per iscritto; se una società modifica la classe di rischio di un cliente ne dà comunicazione alle altre società interessate.

A ciascuna classe di rischio è associato un coerente livello di profondità ed estensione delle misure adottate nelle diverse aree dell'adeguata verifica. Per i rapporti continuativi è definita la frequenza ordinaria di aggiornamento della profilazione del

⁴⁷⁵ Ad esempio l'applicativo GIANOS per la profilazione del rischio ne comprende circa 800.

⁴⁷⁶ Dati numerici anonimi relativi al sistema bancario, rilevati dalla procedura GIANOSTAT.

⁴⁷⁷ In particolare, e in ordine cronologico: Banca d'Italia, Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del decreto legislativo 21 novembre 2007, n. 231. Roma, 3 aprile 2013; IVASS, regolamento n.5 del 21 luglio 2014; Provvedimento della Banca d'Italia 30 luglio 2019, Parte prima, Sezione III; e art.31 del regolamento IVASS n.44 del 12 febbraio 2019 (aggiornato il 13 luglio 2021, dal Provvedimento n. 111).

⁴⁷⁸ Le linee guida EBA sostituiscono le precedenti emanate congiuntamente dalle ESAs, e indirizzano su tre linee di valutazione: a) l'attività o la professione svolta dal cliente e dal suo titolare effettivo; b) la reputazione del cliente e del suo titolare effettivo; c) la natura e il comportamento del cliente e del suo titolare effettivo, compreso se ciò potrebbe indicare un aumento del rischio di finanziamento del terrorismo. Introducono quattro nuovi settori di business (crowdfunding, PISP-AISP, cambio valuta, corporate finance).

⁴⁷⁹ La decisione di adottare una fascia di rischio "irrilevante" venne adottata nelle riunioni del Comitato ABI-ARMA del 2006, per comprende i soggetti con probabilità di rischio marginale, (inconsistente, irrisorio) e consentire una migliore adesione ai principi di protezione dei dati personali. Il concetto di rischio irrilevante è utilizzato anche nelle classificazioni adottate in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (Cfr. D.lgs. 9 aprile 2008, n. 81).

cliente in coerenza con il suo livello di rischio, includendo i rischi nuovi o emergenti. La congruità della classe assegnata è verificata al ricorrere di eventi o circostanze che sono suscettibili di modificare il profilo di rischio (es. nel caso di assunzione o perdita della qualifica di Pep, di cambiamenti rilevanti dell'operatività del cliente o del titolare effettivo o della compagine societaria ovvero in occasione di una segnalazione di operazione sospetta o della presenza del soggetto in particolari liste).

2.2. Procedure informatiche

Un programma informatico per la profilazione del rischio del cliente dovrebbe possedere requisiti e funzionalità necessari alla gestione degli adempimenti, o comunque utili alle fasi di valutazione. In particolare, le capacità: a) di acquisire, memorizzare, organizzare ed elaborare i dati e le informazioni necessari per la conoscenza del cliente. Ad esempio, i questionari parametrizzabili per l'adeguata verifica fruibili anche in formato elettronico, l'importazione di dati afferenti da altri applicativi, da sottosistemi contabili e gestionali, da liste e banche dati interne ed esterne (titolari effettivi, persone politicamente esposte, soggetti segnalati, sistemi di conservazione, operazioni sottosoglia di registrazione, sistemi di selezione delle operazioni anomale, estrattori delle operazioni per le comunicazioni oggettive, paesi e aree geografiche a rischio elevato o non cooperativi o a fiscalità privilegiata, richieste ricevute dall'Autorità giudiziaria o dagli Organi investigativi, ecc.); b) di segmentare la clientela identificando *cluster* di clienti con bisogni e domanda di servizi omogenei, e permettere, con l'ausilio di tabelle decisionali, di definire per ogni fattore di rischio un peso relativo; c) di determinare e proporre automaticamente la classe di rischio attribuita a ciascun cliente sulla base delle condizioni preimpostate e di amministrare l'iter di approvazione, le personalizzazioni e le variazioni con l'intervento umano; e) di gestire la propagazione del rischio ai soggetti collegati stabilendone la misura; f) di armonizzare il rischio di un cliente tra tutte le società di un gruppo, trasferendo il valore di rischio più elevato e di conservare l'annotazione delle ragioni che motivano l'eventuale riduzione; g) di governare l'insieme delle informazioni con funzionalità che consentano la visione complessiva del rischio per ciascun cliente, le ricerche storiche, la generazione di evidenze, l'estrazione di statistiche, le verifiche, la modifica delle tabelle decisionali con i criteri per la valutazione e la frequenza dell'aggiornamento dei dati.

Nella preimpostazione delle tabelle decisionali e degli algoritmi per le condizioni di rischio, particolare attenzione è dedicata alla valutazione ponderata dei singoli fattori che concorrono alla valutazione complessiva, poiché lo stesso fattore può assumere valenze diverse in relazione alle caratteristiche soggettive e oggettive di ogni cliente.

Il trattamento dei dati personali per la profilazione del rischio, e le altre operazioni per l'esecuzione degli obblighi AML/CFR, avvengono nel rispetto delle prescrizioni e delle garanzie stabilite dal Codice in materia di protezione dei dati personali e del regolamento (UE) 2016/679. Quest'ultimo definisce la "profilazione" come qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica (in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica⁴⁸⁰) e dispone che i processi decisionali automatizzati e la profilazione basati su categorie particolari di dati personali sono consentiti solo a determinate condizioni⁴⁸¹.

2.3. Protezione dei dati trattati

La liceità del trattamento richiede che le misure tecniche e organizzative, per garantire un adeguato livello di sicurezza dei dati trattati nella profilazione del rischio del cliente, siano preventivamente definite e descritte in modo concreto, ed includano la protezione da ogni violazione di sicurezza che comporti

⁴⁸⁰ Art. 4 del regolamento (UE) 2016/679 (General Data Protection Regulation).

⁴⁸¹ I trattamenti di dati personali cui si riferisce la normativa antiriciclaggio riguardano patrimoni, comportamenti e disponibilità economiche delle persone e, per tale loro intrinseca delicatezza, nonché per gli effetti che essi possono comunque determinare, vanno ascritti fra quelli che presentano rischi per i diritti e le libertà fondamentali degli interessati riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, il cui art. 8 garantisce ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano (cfr. considerando 48 dir. n. 2005/60/Ce).

accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati⁴⁸².

Le misure di tutela dovrebbero comprendere⁴⁸³, se del caso: 1) l'analisi preventiva dei rischi che incombono sui dati individuando le minacce, le vulnerabilità e le fonti, con stima dell'impatto che gli eventi nocivi indesiderati potrebbero generare sui diritti e libertà fondamentali dei soggetti profilati; 2) le soluzioni per assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi; 3) la configurazione del sistema informatico con impostazioni di sicurezza predefinite (c.d. per *default*); 4) la qualità dei dati per garantirne l'esattezza; 5) la minimizzazione dei dati, trattando solo quelli necessari e pertinenti rispetto alle finalità; 6) l'identificazione dei soggetti autorizzati al trattamento in coerenza con il sistema di autenticazione e autorizzazione per l'accesso ai dati; 7) la cifratura e la pseudonimizzazione; 8) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico (regole di *backup* e piano di *business continuity*); 9) la protezione dei dati durante la trasmissione; 10) la conservazione protetta e limitata ai periodi temporali stabiliti dalla normativa; 11) la registrazione degli eventi (c.d. tracciabilità dei *log*); 12) la sicurezza fisica dei luoghi in cui è svolto il trattamento; 13) la possibilità che il programma informatico consenta interventi umani sui risultati delle elaborazioni automatiche; 14) le *policy* di gestione e *governance* della sicurezza informatica; le certificazioni e altre garanzie di processi e prodotti; 15) la portabilità dei dati e la garanzia di cancellazione; 16) le iniziative formative per rendere note al personale incaricato gli obblighi cui sono tenuti; 17) le specifiche tecniche e organizzative per il responsabile o sub-responsabile del trattamento, anche al fine di fornire assistenza al titolare; 18) le procedure di controllo per testare, verificare e valutare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; 19) le procedure idonee ad assicurare la massima riservatezza dell'identità delle persone che effettuano la segnalazione di operazioni sospette, di tutela del segreto d'ufficio, del segreto investigativo e d'indagine; 20) la tenuta di un registro dei trattamenti contenente tutte le informazioni prescritte all'art. 30 del regolamento (UE) 2016/679. I rischi ICT (*Information and Communication Technologies*) e di sicurezza sono valutati, unitamente agli altri rischi di conformità e frode, anche nel caso di utilizzo di mezzi tecnologici innovativi per scopi di identificazione e verifica dell'identità dei clienti, in particolare nelle situazioni a distanza⁴⁸⁴.

I trattamenti di dati personali per finalità di prevenzione del riciclaggio e del finanziamento del terrorismo sono riconosciuti di interesse pubblico da parte di tutti gli Stati membri dell'Unione europea, e ciò comporta la limitazione dell'esercizio di alcuni diritti del cliente, fermo restando il diritto di essere informato sull'esistenza di un processo decisionale automatizzato, compresa la profilazione, fornendo informazioni significative sulla logica utilizzata⁴⁸⁵ in ossequio al principio di trasparenza, e adottando particolari tutele e garanzie per i trattamenti relativi alle condanne penali e ai reati, o a connesse misure di sicurezza.

3. Adeguata verifica della clientela (*I. Cosenza e I. Cesarotto*)

Tra gli adempimenti antiriciclaggio che il D.lgs. 231/2007 pone a carico dei destinatari, l'adeguata verifica della clientela assolve una funzione fondamentale, rivestendo un ruolo centrale non soltanto nell'ambito della collaborazione passiva, ma anche ai fini della trasmissione delle segnalazioni di operazioni sospette all'Unità di Informazione Finanziaria (UIF): dall'identificazione del cliente e della sua operatività dipende, infatti, sia la correttezza della conservazione dei dati, sia la qualità del processo segnaletico delle operazioni sospette, che costituiscono, quindi, adempimenti derivati rispetto all'adeguata verifica⁴⁸⁶.

⁴⁸² Art.32, Sicurezza del trattamento, regolamento (UE) 2016/679.

⁴⁸³ Cfr. Allegato III alla Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021, relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'art. 28, par. 7, del regolamento (UE) 2016/679.

⁴⁸⁴ Cfr. EBA, Orientamenti relativi ai fattori di rischio di ML/TF, 1° marzo 2021, punto 4.32 e successivi.

⁴⁸⁵ Art. 2-*undecies* del D.lgs. 10 agosto 2018, n.101 e art.22 del regolamento (UE) 2016/679.

⁴⁸⁶ A tal proposito, si evidenzia la necessaria sinergia tra obblighi di collaborazione passiva e obblighi di collaborazione attiva previsti dal decreto antiriciclaggio, data la prodromicità dei primi rispetto ai secondi: soltanto attraverso il corretto adempimento degli obblighi di valutazione del rischio, adeguata verifica della clientela e conservazione dei dati, infatti, il soggetto obbligato acquisisce il corredo informativo necessario per l'individuazione del sospetto e, quindi, per la trasmissione delle segnalazioni di operazioni sospette alla UIF.

Attraverso lo strumento dell'adeguata verifica, in particolare, i soggetti obbligati possono intercettare e valutare il rischio di riciclaggio che essi assumono nell'instaurare rapporti con la clientela: la valutazione del rischio connesso con il cliente è infatti richiesto prima e in funzione dell'avvio dell'operatività e costituisce un'attività costante nel corso dell'intero rapporto⁴⁸⁷.

Quanto al contenuto dell'obbligo, l'art. 18 del D.lgs. 231/2007 descrive le attività nelle quali l'adeguata verifica della clientela si declina, recando così una definizione avente carattere eminentemente procedurale, che nulla rivela in merito alla finalità perseguita dall'adempimento: sotto questo profilo, è possibile affermare che le attività previste dalla normativa mirano all'acquisizione di un quadro conoscitivo del cliente per gli aspetti di natura economica e finanziaria, al fine di coglierne il profilo complessivo e predisporre le necessarie misure di protezione.

Secondo un approccio funzionale, l'adeguata verifica può essere quindi definita come quel complesso di attività attraverso le quali l'operatore si rappresenta il livello di esposizione del cliente al rischio di riciclaggio e individua il novero di informazioni da acquisire e da approfondire in relazione alle specificità del caso concreto. L'adeguata verifica si presenta pertanto come attività al contempo conoscitiva e valutativa; i due profili, per quanto distinti, risultano strettamente avvinti e destinati a influenzarsi reciprocamente. Le informazioni acquisite ai sensi dell'art. 18 del D.lgs. 231/2007 forniscono infatti i primi elementi di analisi, dalla valutazione dei quali può emergere l'esigenza di approfondire alcuni aspetti del profilo del cliente.

Emerge così anche il tenore discrezionale dell'adempimento: nella sua attuale configurazione l'adeguata verifica, pur conservando il nucleo originario dell'identificazione del cliente, è venuta ad arricchirsi di attività irriducibili a uno schema operativo predefinito, in quanto caratterizzate da una preminente esigenza di adattamento al caso concreto.

La discrezionalità del soggetto obbligato costituisce infatti un elemento coesistente al moderno assetto dei compiti antiriciclaggio. La nuova disciplina prevede il ricorso sistematico all'approccio basato sul rischio, principio cardine che orienta le modalità e la profondità delle analisi che i soggetti obbligati devono condurre per lo svolgimento degli obblighi di adeguata verifica: i controlli e le risorse vanno dunque calibrati sulle diverse situazioni, in funzione del rischio che ciascuna di esse presenta.

Il carattere discrezionale dell'obbligo di adeguata verifica richiede, dal punto di vista operativo, indicazioni che orientino i comportamenti dei destinatari, pur senza giungere ad automatismi che limiterebbero la flessibilità richiesta per aderire alle specificità del caso concreto: in tale contesto, accanto alla normativa primaria, vengono in ausilio dei soggetti obbligati le disposizioni di attuazione emanate in materia di organizzazione, procedure e controlli interni e adeguata verifica da parte delle Autorità di vigilanza di settore (cfr. art. 7, comma 2, del D.lgs. 231/2007).

3.1. Assetto normativo

Agli "Obblighi di adeguata verifica della clientela" il D.lgs. 231/2007 dedica il Titolo II ("Obblighi"), Capo I⁴⁸⁸: tale disciplina è stata sensibilmente modificata prima dal D.lgs. 90/2017, in attuazione della direttiva (UE) 2015/849 e, più recentemente, dal D.lgs. 125/2019, in attuazione della direttiva (UE) 2018/843.

⁴⁸⁷ A conferma del ruolo rivestito dall'adeguata verifica della clientela per l'intera durata del rapporto con il cliente, l'art. 42, comma 1, D.lgs. 231/2007 prevede che i soggetti obbligati che si trovino nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela, si astengono dall'instaurare, eseguire ovvero proseguire il rapporto, la prestazione professionale e le operazioni e valutano se trasmettere una segnalazione di operazione sospetta alla UIF. Nella stessa ottica, in base all'art. 22, comma 2, del decreto, viene posto a carico dei clienti l'obbligo fornire per iscritto, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire ai soggetti obbligati di adempiere agli obblighi di adeguata verifica.

⁴⁸⁸ Il Capo I è, a sua volta, suddiviso in 3 Sezioni: la Sezione I (artt. 17-22) reca disposizioni di carattere generale, sul contenuto e sulle modalità di adempimento degli obblighi di adeguata verifica, sulla titolarità effettiva e sugli obblighi del cliente; la Sezione II (artt. 23-25) disciplina le misure di adeguata verifica semplificate e rafforzate; la Sezione III (artt. 26-30) si occupa, infine, dell'esecuzione degli obblighi di adeguata verifica per il tramite di terzi.

In particolare, a seguito della riforma intervenuta nel 2017, le norme sull'adeguata verifica previste dal D.lgs. 231/2007, recano una regolamentazione molto dettagliata che recepisce a livello legislativo gran parte delle regole precedentemente contenute nelle previgenti disposizioni secondarie adottate dalle Autorità di vigilanza di settore. Si è cercato in questo modo di uniformare il più possibile l'applicazione degli obblighi di adeguata verifica alle diverse categorie di soggetti obbligati, ivi inclusi i soggetti non sottoposti alla vigilanza di Autorità di settore.

Come si avrà modo di vedere nel prosieguo, l'attuale disciplina antiriciclaggio mira a valorizzare nella maggior misura possibile il principio cardine dell'approccio basato sul rischio: basti pensare, tra le altre, alle novità introdotte in tema di titolare effettivo, adeguata verifica semplificata e rafforzata, adeguata verifica a distanza e tramite terzi.

Le richiamate norme di legge sono poi completate e integrate dalle disposizioni attuative emanate dalle Autorità di vigilanza di settore (art. 7, comma 1, lett. a) e dalle regole tecniche adottate dagli Organismi di autoregolamentazione (art. 11, comma 2).

A tal proposito, per quanto riguarda i soggetti vigilati, si ricorda il Provvedimento di Banca d'Italia del 30 luglio 2019 recante "Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo", che rappresenta un'evoluzione delle disposizioni dettate dal Provvedimento della Banca d'Italia 3 aprile 2013 del quale, per quanto possibile, è stata conservata invariata la struttura.

Si ricordano, inoltre, il Provvedimento di Banca d'Italia del 4 febbraio 2020, concernente "Disposizioni in materia di adeguata verifica della clientela e di conservazione dei dati e delle informazioni per gli operatori non finanziari", iscritti in un apposito elenco tenuto dalla Banca d'Italia, limitatamente all'attività di trattamento delle banconote in euro; il regolamento IVASS 44/2019 concernente "Disposizioni attuative volte a prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela"; il regolamento Consob 20570/2018, contenente le "disposizioni di attuazione del decreto legislativo 21 novembre 2007, n. 231 e successive modifiche ed integrazioni per i revisori legali e le società di revisione con incarichi di revisione su enti di interesse pubblico o su enti sottoposti a regime intermedio".

Considerato il carattere molto dettagliato delle riformate norme primarie, molte delle quali sono applicabili *ex se* e non necessitano di norme attuative, il margine di discrezionalità lasciato alle Autorità di vigilanza nella delineazione delle disposizioni secondarie è risultato ridotto rispetto al passato.

3.2. Disposizioni generali

L'art 17 del decreto antiriciclaggio reca disposizioni generali relative ai presupposti di applicazione degli obblighi di adeguata verifica, che si rivolgono alla totalità dei soggetti obbligati; ciò a differenza di quanto stabiliva la previgente versione del decreto, che prevedeva regole diverse per gli intermediari finanziari e gli altri operatori finanziari, per i professionisti e i revisori contabili e per gli altri operatori, rispettivamente agli artt. 15, 16 e 17.

Più in dettaglio, in base al comma 1 dell'art. 17, i soggetti obbligati sono tenuti ad effettuare l'adeguata verifica della clientela in occasione: a) dell'instaurazione di un rapporto continuativo o del conferimento dell'incarico per l'esecuzione di una prestazione professionale⁴⁸⁹; b) dell'esecuzione di un'operazione occasionale, disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con una operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata⁴⁹⁰ ovvero che consista in un trasferimento di fondi, come definito dall'art. 3,

⁴⁸⁹ In base all'art. 1, comma 2, del D.lgs. 231/2007, si intende: per rapporto continuativo, "un rapporto di durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione" (lett. ll); per conferimento dell'incarico, l'"attribuzione di un mandato, esplicito o implicito, anche desumibile dalle caratteristiche dell'attività istituzionalmente svolta dai soggetti obbligati, diversi dagli intermediari bancari e finanziari e dagli altri operatori finanziari, al compimento di una prestazione professionale, indipendentemente dal versamento di un corrispettivo o dalle modalità e dalla tempistica di corresponsione del medesimo" (lett. h); per prestazione professionale, una "prestazione intellettuale o commerciale resa in favore del cliente, a seguito del conferimento di un incarico, della quale si presume che abbia una certa durata" (lett. gg).

⁴⁹⁰ In base alle definizioni fornite dall'art. 1, comma 2, del D.lgs. 231/2007, si intende: per operazione occasionale, "un'operazione non riconducibile a un rapporto continuativo in essere; costituisce operazione occasionale anche la prestazione intellettuale o commerciale, ivi comprese quelle ad esecuzione istantanea, resa in favore del cliente" (lett. z); per operazioni collegate, le "operazioni tra loro connesse per il perseguimento di un unico obiettivo di carattere giuridico patrimoniale" (lett. u); per operazione frazionata, "un'operazione unitaria sotto il profilo del valore economico, di importo pari o superiore ai limiti stabiliti dal presente decreto, posta in essere attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi ed in un circoscritto periodo di tempo fissato in sette giorni, ferma restando la sussistenza dell'operazione frazionata quando ricorrano elementi per ritenerla tale" (lett. v).

par. 1, punto 9, del regolamento (UE) n. 2015/847 (ossia effettuato, almeno parzialmente, per via elettronica, per conto di un ordinante da un prestatore di servizi di pagamento, allo scopo di mettere i fondi a disposizione del beneficiario mediante un prestatore di servizi di pagamento) superiore a 1.000 euro⁴⁹¹.

Rientrano tra le operazioni occasionali anche i casi in cui le banche, gli istituti di moneta elettronica, gli istituti di pagamento o Poste Italiane S.p.A. agiscano da tramite o siano comunque parte nei trasferimenti di denaro contante o titoli al portatore effettuati a qualsiasi titolo tra soggetti diversi, di importo complessivo pari o superiore a 15.000 euro.

I limiti di importo non si applicano, ed è quindi sempre dovuta l'adeguata verifica: a) per tutte le operazioni occasionali effettuate da banche, istituti di moneta elettronica, istituti di pagamento e Poste Italiane S.p.A. a titolo di servizio di pagamento o di emissione e distribuzione di moneta elettronica tramite agenti in attività finanziaria ovvero mediante "soggetti convenzionati e agenti", come definiti dall'art. 1, comma 2, lett. nn), del decreto; b) con riferimento ai prestatori di servizi di gioco di cui all'art. 3, comma 6, in occasione del compimento di operazioni di gioco⁴⁹², anche secondo le specifiche disposizioni dettate per tali operatori economici dal Titolo IV (artt. 52-54).

Ai sensi del successivo comma 2 dell'art. 17, l'adeguata verifica del cliente e del titolare effettivo deve essere in ogni caso effettuata *"quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile"*⁴⁹³ oppure *"quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione"*.

I soggetti obbligati sono tenuti all'adempimento degli obblighi in materia di adeguata verifica nei confronti dei nuovi clienti nonché dei clienti già acquisiti, rispetto ai quali tale attività si renda opportuna in considerazione del mutato livello di rischio di riciclaggio o di finanziamento del terrorismo associato al cliente.

Sono escluse dall'applicazione degli obblighi di adeguata verifica le attività di mera redazione e trasmissione ovvero di sola trasmissione delle dichiarazioni derivanti da obblighi fiscali e degli adempimenti in materia di amministrazione del personale di cui all'art. 2, comma 1, della L. 12/1979.

Le disposizioni attuative adottate dalla Banca d'Italia e dall'IVASS chiariscono, inoltre, che non è richiesta l'adeguata verifica per le attività finalizzate o connesse all'organizzazione, al funzionamento e all'amministrazione dei destinatari, tenuto conto che esse non rientrano nelle attività istituzionali proprie dei destinatari e che, nel loro svolgimento, le controparti si configurano come prestatori di beni o servizi su iniziativa dei destinatari stessi, piuttosto che come clienti che richiedono di instaurare un rapporto continuativo o di effettuare un'operazione occasionale (es. forniture per l'acquisizione di materiali o beni strumentali propri; acquisizione e manutenzione degli immobili ove viene esercitata l'attività istituzionale; prestazioni acquisite da liberi professionisti per consulenze).

3.3. Contenuto e modalità di adempimento degli obblighi di adeguata verifica

Ai sensi dell'art. 18, comma 1, gli obblighi di adeguata verifica della clientela si attuano attraverso: a) l'identificazione del cliente (e dell'esecutore) e la verifica della sua identità; b) l'identificazione del titolare effettivo e la verifica della sua identità; c) l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale; d) il controllo costante del rapporto con il cliente, per tutta la sua durata⁴⁹⁴. L'estensione e la profondità delle verifiche, della valutazione e del controllo è commisurata al livello di rischio rilevato.

⁴⁹¹ Come precisato dalla relazione illustrativa sullo Schema di decreto legislativo recante attuazione della direttiva (UE) 2015/849, la previsione, risponde all'esigenza di garantire la piena tracciabilità di tali tipologie di operazioni al fine di contrastare i tentativi di immissione nel sistema finanziario di fondi provenienti da attività criminali ovvero destinati al finanziamento del terrorismo.

⁴⁹² Per operazione di gioco si intende *"un'operazione atta a consentire, attraverso i canali autorizzati, la partecipazione a uno dei giochi del portafoglio dell'Agenzia delle dogane e dei monopoli, a fronte del corrispettivo di una posta di gioco in denaro"* (art. 1, comma 3, lett. h).

⁴⁹³ A questo fine, i destinatari si avvalgono degli indicatori di anomalia e degli schemi rappresentativi di comportamenti anomali emanati dalla UIF, in base al decreto antiriciclaggio.

⁴⁹⁴ L'art. 19, comma 3, del D.lgs. 231/2007 richiede agli intermediari bancari e finanziari di applicare altresì misure di adeguata verifica del beneficiario della prestazione assicurativa, non appena individuato o designato, nonché dell'effettivo percipiente della prestazione liquidata e dei rispettivi titolari effettivi. Tali misure, consistono: a) nell'acquisizione del nome o della denominazione del soggetto specificamente individuato o designato quale beneficiario; b) nei casi di beneficiario designato in base a particolari caratteristiche o classi, nell'acquisizione di informazioni sufficienti a consentire al soggetto obbligato di stabilirne l'identità al momento del pagamento della prestazione.

Il primo passaggio dell'adeguata verifica consiste nelle attività di identificazione e verifica dell'identità, da condurre nei confronti: del cliente, definito come il *"soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede o ottiene una prestazione professionale a seguito del conferimento di un incarico"* (art. 1, comma 2, lett. f); dell'esecutore, definito quale *"soggetto delegato ad operare in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente"* (art. 1, comma 2, lett. p), rispetto al quale andranno anche verificate l'esistenza e l'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente.

L'esecutore è il soggetto che agisce in nome e per conto di terzi, in tutte le forme e con tutte le modalità con le quali ciò è possibile (in forza di specifica procura o di un generale potere di rappresentanza oppure sulla base dell'immedesimazione organica della persona fisica con la persona giuridica che rappresenta oppure ancora in forza di provvedimenti dell'autorità, come per i curatori fallimentari). Il cliente che agisce in nome proprio, ma per conto di un altro soggetto, non muta la sua natura di intestatario giuridico diretto dell'operatività e, quindi, resta sempre e comunque cliente, riassorbendo così, in tale veste, la circostanza che l'operatività benefici un soggetto terzo. In questo caso, spetterà al cliente stesso dichiarare se il rapporto continuativo è aperto, la prestazione professionale è richiesta o l'operazione occasionale è effettuata per conto di un altro soggetto nonché fornire tutte le indicazioni necessarie all'identificazione di questo soggetto e del suo eventuale titolare effettivo⁴⁹⁵.

La regolamentazione non sembra prendere in considerazione la figura del *nuncius*, ossia del soggetto che non si spinge a esprimere una sua volontà riferendone gli effetti direttamente al rappresentato (il cliente), ma si limita a trasmettere la volontà di quest'ultimo. A tale proposito, è stato evidenziato come l'utilizzo del *nuncius* vada circondato da precauzioni e cautele volte a verificare l'effettiva natura di messaggero della volontà del cliente. Situazioni in cui terzi agiscono da delegati senza averne i poteri, da un lato non sono raccomandabili nell'interesse della certezza delle relazioni tra intermediari e clienti, in quanto esposte al rischio di contestazioni per mancanza di delega e disconoscimento delle operazioni effettuate, dall'altra, offrono una comoda dimora in cui possono annidarsi fenomeni di schermatura e attività di prestanome, in cui il "delegato di fatto" sia il vero referente dell'operazione o del rapporto e il cliente formale solo la testa di legno da far figurare negli archivi informativi dell'intermediario⁴⁹⁶.

Accanto al cliente e all'esecutore, i soggetti obbligati sono poi tenuti all'identificazione e alla verifica dell'identità del titolare effettivo, definito dal decreto antiriciclaggio come *"la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita"* (art. 1, comma 2, lett. pp). L'identificazione del titolare effettivo viene normalmente effettuata in via indiretta, per il tramite del cliente, il quale è obbligato a fornire tutte le informazioni a tal fine necessarie.

In base all'art. 19, comma 1, lett. a) l'identificazione del cliente e del titolare effettivo è svolta in presenza del medesimo cliente ovvero dell'esecutore, anche attraverso dipendenti o collaboratori del soggetto obbligato, e consiste nell'acquisizione dei dati identificativi forniti dal cliente, previa esibizione di un documento d'identità in corso di validità, o altro documento di riconoscimento equipollente ai sensi della normativa vigente, del quale viene acquisita copia. La medesima disposizione elenca altresì i casi in cui l'obbligo di identificazione si considera assolto anche senza la presenza fisica del cliente⁴⁹⁷.

⁴⁹⁵ A questo riguardo, il Provvedimento della Banca d'Italia del 30 luglio 2019 chiarisce che le operazioni riconducibili a un rapporto continuativo si presumono effettuate nell'interesse del cliente-persona fisica intestatario del rapporto o, nel caso di cliente diverso da persona fisica, del titolare effettivo del rapporto, salva diversa indicazione del cliente. All'atto della costituzione del rapporto continuativo, i destinatari sono tenuti ad assicurare che il cliente si impegni a segnalare, nel corso del futuro svolgimento del rapporto, le eventuali operazioni occasionali effettuate per conto di terzi e a fornire tutte le indicazioni necessarie all'identificazione del titolare effettivo dell'operazione.

⁴⁹⁶ Cfr. R. Cercone, *L'adeguata verifica della clientela nel settore bancario e finanziario*, in G. Castaldi e G. Conforti (a cura di), *Manuale Antiriciclaggio*, Bancaria Editrice, 2013, pp. 153-154.

⁴⁹⁷ Più in dettaglio, in base all'art. 19, comma 1, lett. a), l'obbligo di identificazione si considera assolto anche senza la presenza fisica nei seguenti casi: 1) i dati identificativi del cliente risultano da atti pubblici, da scritture private autenticate o da certificati qualificati utilizzati per la generazione di una firma digitale associata a documenti informatici; 2) il cliente è in possesso di un'identità digitale (con livello di garanzia specificamente individuato dalla disposizione in commento) o di un certificato per la generazione di firma digitale; 3) i dati identificativi risultano da dichiarazione della rappresentanza diplomatica e dell'autorità consolare italiana; 4) il cliente è già stato identificato dal destinatario in relazione a un altro rapporto continuativo in essere, purché le informazioni esistenti siano aggiornate e adeguate rispetto allo specifico profilo di rischio del cliente e alle caratteristiche del nuovo rapporto che si intende avviare; 5) i dati identificativi del cliente sono acquisiti attraverso forme e modalità idonee, individuate dalle Autorità di vigilanza di settore. In base a tale

Ai sensi della successiva lett. b) dell'art. 19, la verifica dell'identità richiede il riscontro della veridicità dei dati identificativi contenuti nei documenti e delle informazioni acquisiti all'atto dell'identificazione, solo laddove, in relazione agli stessi, sussistano dubbi, incertezze o incongruenze. Tale riscontro può essere effettuato attraverso la consultazione del sistema pubblico per la prevenzione del furto di identità di cui al D.lgs. 64/2011⁴⁹⁸ ovvero attraverso il ricorso ad altre fonti attendibili e indipendenti, che si caratterizzano per la natura di terzietà rispetto al soggetto di cui va verificata l'identità, e di particolare affidabilità, in genere assicurata dalla riconducibilità ad autorità pubbliche⁴⁹⁹.

L'art. 27 del DL 76/2020 (c.d. decreto Semplificazioni, convertito con modificazioni dalla L. 120/2020) è intervenuto sulle modalità di adempimento degli obblighi di adeguata verifica al fine di favorire la digitalizzazione e snellire le procedure di identificazione della clientela per l'accesso ai servizi bancari.

In particolare, è stata eliminata dall'art. 18, comma 1, lett. a), la prescritta necessità di riscontrare in ogni caso il documento di identità e i suoi estremi: è quindi venuto meno l'obbligo del cliente di trasmettere la fotocopia del documento di identità o altro equipollente quando l'identificazione avviene a distanza, previa adeguata verifica identificativa secondo le condizioni di sicurezza e attendibilità imposte dagli standard nazionali ed europei. Inoltre, è stato modificato il comma 1, lett. a), n. 2) dell'art. 19, che prevedeva la possibilità di procedere all'adeguata verifica senza la presenza del cliente nel caso in cui questo fosse dotato di un'identità digitale di livello massimo di sicurezza nell'ambito del Sistema di cui all'art. 64, D.lgs. 82/2005, nonché di un'identità digitale di livello massimo di sicurezza o di un certificato per la generazione di firma digitale, rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'art. 9 del regolamento UE n. 910/2014 o identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale. Con le modifiche apportate dal decreto Semplificazioni, il livello massimo di sicurezza previsto per l'identità digitale del cliente è stato abbassato ad "almeno significativo". Il medesimo decreto ha infine introdotto una speciale modalità di identificazione e verifica a distanza dell'identità applicabile solo nel caso di instaurazione di rapporti continuativi relativi a carte di pagamento e dispositivi analoghi, nonché a strumenti di pagamento basati su dispositivi di telecomunicazione, digitali o informatici – con esclusione dei casi in cui tali carte, dispositivi o strumenti sono utilizzabili per generare l'informazione necessaria a effettuare direttamente un bonifico o un addebito diretto verso e da un conto di pagamento – che si realizza tramite l'esecuzione di un bonifico, disposto dallo stesso cliente da identificare, verso un conto di pagamento intestato al soggetto tenuto all'obbligo di identificazione, a condizione che il bonifico sia disposto previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'art. 4 del regolamento delegato (UE) 2018/389 della Commissione del 27 novembre 2017 (art. 19, comma 1, lett. a), n. 4bis). Come chiarito dalla relazione illustrativa al decreto, la previsione *"evita il ripetersi di inefficienti e non necessari adempimenti di identificazione dei clienti, essendo stati questi già svolti dal prestatore del servizio di radicamento del conto di provenienza del bonifico. In definitiva, le modifiche introdotte permettono di adempiere agli obblighi di adeguata verifica anche sfruttando le potenzialità del FinTech riducendo, così, notevolmente i rischi di collusione, induzione o costrizione dei soggetti preposti alla identificazione e verifica dell'identità dei clienti, nonché quelli connessi all'archiviazione e circolazione delle immagini digitali dei documenti di identità ovvero al loro facile riutilizzo per furti di identità o interposizione di persona"*⁵⁰⁰. Da ultimo, l'art. 3 del DL n. 228/221 (c.d. decreto Milleproroghe, convertito con modificazioni

ultima disposizione, il Provvedimento della Banca d'Italia del 30 luglio 2019 e il regolamento IVASS n. 44/2019 hanno introdotto specifiche disposizioni in materia di operatività "a distanza", ossia svolta senza la compresenza fisica, presso il destinatario, del cliente, dei dipendenti del destinatario o di altro personale incaricato dal destinatario (es., attraverso i sistemi di comunicazione telefonica o informatica). Rispetto a tale operatività, i destinatari sono chiamati a porre particolare attenzione, in considerazione dell'assenza di un contatto diretto e del rischio di frodi connesse al furto di identità, e sono tenuti a effettuare specifici riscontri sui dati acquisiti, secondo le modalità ritenute opportune in relazione al rischio associato al cliente. Si consente, inoltre, di effettuare l'identificazione del cliente-persona fisica in digitale da remoto secondo la procedura di registrazione audio/video, nel rispetto delle prescrizioni dettate dai Provvedimenti medesimi (cfr. Allegato 3 del Provvedimento della Banca d'Italia del 30 luglio 2019 e art. 39, commi 5 e ss. del regolamento IVASS n. 44/2019).

⁴⁹⁸ Si tratta dell'archivio c.d. SCIPAFI, che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento, attualmente quelle dell'Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei trasporti, INPS e INAIL.

⁴⁹⁹ Tra le quali rientrano le basi di dati, ad accesso pubblico o condizionato al rilascio di credenziali di autenticazione, riferibili ad una pubblica amministrazione nonché quelle riferibili a soggetti privati autorizzati al rilascio di identità digitali nell'ambito del sistema previsto dall'art. 64 del D.lgs. 82/2005 ovvero di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'art. 9 del regolamento EU n. 910/2014.

⁵⁰⁰ Al riguardo, è stato osservato come sia certamente un fine nobile quello di agevolare i rapporti a distanza; tuttavia, la disciplina vigente sembra determinare una disparità di trattamento tra professionisti e intermediari finanziari: mentre i soggetti obbligati sottoposti a vigilanza possono effettuare l'adeguata verifica anche con strumenti a distanza, i professionisti sono invece tenuti a un riscontro fisico, rapportandosi col cliente in studio o nella sede del cliente stesso, salvo ovviamente ricorrere alle procedure di adeguata verifica a distanza "classiche" previste dall'art. 19 del decreto antiriciclaggio (cfr. G. Sciarretta, *Antiriciclaggio: il decreto Semplificazioni facilita l'adeguata verifica a distanza*, in IPSOA, 29 settembre 2020). Si tratta di una disparità che è stata evidenziata anche dal CNN, che ha sottolineato inoltre come le diverse regole previste per le ipotesi di identificazione non in presenza (senza acquisizione del documento) e in presenza (con acquisizione del documento) appaiano peraltro incongrue, in quanto tendenti a semplificare l'identificazione quando non si è in presenza

dalla L. n. 15/2022) ha previsto un'ulteriore ipotesi di identificazione a distanza utilizzabile con riferimento ai rapporti relativi a servizi di disposizione di ordini di pagamento e a servizi di informazione sui conti previsti dal TUB, per i clienti già identificati da un soggetto obbligato, i quali, previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'art. 4 del regolamento delegato (UE) 2018/389 della Commissione (autenticazione forte che comporta la generazione di un codice di autenticazione), consentono al soggetto tenuto all'obbligo di identificazione di accedere alle informazioni relative agli estremi del conto di pagamento intestato al medesimo cliente presso il citato soggetto obbligato in uno Stato membro dell'Unione europea (art. 19, comma 1, lett. a), n. 4-ter).

Con riferimento ai clienti diversi dalle persone fisiche e ai fiduciari di *trust* espressi e alle persone che esercitano diritti, poteri e facoltà equivalenti in istituti giuridici affini, la verifica dell'identità del titolare effettivo impone l'adozione di misure, commisurate alla situazione di rischio, idonee a comprendere la struttura di proprietà e di controllo del cliente.

Le attività di identificazione e verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, devono essere svolte prima dell'instaurazione del rapporto continuativo o del conferimento dell'incarico per lo svolgimento di una prestazione professionale ovvero prima dell'esecuzione dell'operazione occasionale. La verifica dell'identità può essere posticipata a un momento successivo rispetto all'instaurazione del rapporto o al conferimento dell'incarico a due condizioni: 1) che sussista un basso rischio di riciclaggio o di finanziamento del terrorismo; 2) che tale posticipazione sia necessaria a consentire l'ordinaria gestione dell'attività oggetto del rapporto. In questa ipotesi, i soggetti obbligati provvedono comunque all'acquisizione dei dati identificativi e dei dati relativi alla tipologia e all'importo dell'operazione e completano le procedure di verifica dell'identità dei medesimi al più presto e, comunque, entro trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico⁵⁰¹.

Fermi gli obblighi di identificazione, il decreto esonera espressamente i professionisti dall'obbligo di verifica dell'identità del cliente e del titolare effettivo fino al momento di effettivo conferimento dell'incarico nei casi in cui siano chiamati a esaminare la posizione giuridica del cliente ovvero a espletare compiti di difesa o di rappresentanza del cliente in un procedimento innanzi a un'Autorità giudiziaria o in relazione a tale procedimento, compresa la consulenza sull'eventualità di intentarlo o evitarlo.

Effettuate le attività di identificazione e verifica dell'identità, i soggetti obbligati devono procedere all'acquisizione e alla valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale per tali intendendosi quelle relative all'instaurazione del rapporto, alle relazioni intercorrenti tra il cliente e l'esecutore, tra il cliente e il titolare effettivo e quelle relative all'attività lavorativa; è espressamente fatta salva la possibilità di acquisire, in funzione del rischio, ulteriori informazioni, ivi comprese quelle relative alla situazione economico-patrimoniale del cliente, acquisite o possedute in ragione dell'esercizio dell'attività. In presenza di un elevato rischio di riciclaggio e di finanziamento del terrorismo, i soggetti obbligati applicano la procedura di acquisizione e valutazione delle predette informazioni anche alle prestazioni o operazioni occasionali.

Le informazioni su scopo e natura del rapporto devono essere intese in senso ampio; lo spirito della disposizione è di acquisire sia elementi conoscitivi sulle caratteristiche dell'operatività richiesta dalla clientela e sullo scopo immediato cui quell'operatività è diretta – informazioni in larga parte intrinseche alla tipologia oggettiva dei servizi richiesti dal cliente stesso – sia ogni ulteriore dato che consenta di inquadrare quell'operatività nell'ambito del profilo economico finanziario del cliente. Questo adempimento consente di connettere l'operatività astratta desumibile dall'oggettività del servizio (es. apertura di un conto corrente, di un rapporto di custodia e amministrazione titoli, erogazione di un finanziamento) al cliente specifico, personalizzando il corredo informativo relativo a quell'operatività (ad esempio, risalendo all'uso cui il cliente destinerà il rapporto che sta aprendo, alla tipologia di movimentazione finanziaria che il rapporto accoglierà, ecc.).

fisica del cliente, situazione ritenuta più a rischio rispetto alla presenza fisica del cliente davanti al soggetto obbligato e sembrerebbero piuttosto frutto di un difetto di coordinamento normativo, difficilmente superabile sulla base di un'interpretazione sistematica in assenza di opportuno chiarimento da parte del legislatore (cfr. lo Studio 2Bis-2020/B, *L'identificazione non in presenza fisica nel contrasto al riciclaggio ed al terrorismo internazionale dopo il DL "Semplificazioni" n. 76/2020 convertito con legge n. 120/2020G*, di G. Arcella, L. Piffaretti e M. Manente, Approvato dalla Commissione Antiriciclaggio del CNN il 02.11.2020).

⁵⁰¹ Decorso tale termine, qualora riscontrino l'impossibilità oggettiva di completare la verifica dell'identità del cliente, i soggetti obbligati, si astengono ai sensi dell'art. 42 e valutano, sussistendone i presupposti, se effettuare una segnalazione di operazione sospetta ai sensi dell'art. 35.

Ai sensi dell'art. 19, comma 1, lett. c), occorrerà quindi verificare la compatibilità dei dati e delle informazioni fornite dal cliente con le informazioni acquisite autonomamente dai soggetti obbligati, anche avuto riguardo al complesso delle operazioni compiute in costanza del rapporto o di altri rapporti precedentemente intrattenuti nonché all'instaurazione di ulteriori rapporti.

Infine, è richiesto ai soggetti obbligati di mantenere il controllo costante del rapporto con il cliente, per tutta la sua durata, attraverso l'esame della complessiva operatività del cliente medesimo, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività di adeguata verifica.

La condizione dell'aggiornamento dei dati in forza del controllo costante è fondamentale in quanto consente, da un lato, di mantenere l'allineamento del profilo del cliente con l'operatività che viene concretamente svolta e, dall'altro, di esaminare e valutare le singole operazioni e la loro eventuale incoerenza rispetto alle caratteristiche del cliente da approfondire e valutare. Al riguardo, è stato osservato che, se l'attività di informazione e di valutazione sui soggetti (cliente, esecutore e titolare effettivo) e sull'oggetto dell'operatività (scopo e natura) possono vedersi come una "fotografia" del cliente, il controllo costante introduce un elemento evolutivo, trasformando l'immagine statica in una "sequenza di fotogrammi" che testimonia la storia del cliente e della sua operatività. Tale dinamismo impresso agli adempimenti serve ad assicurare l'aderenza delle informazioni e delle valutazioni rispetto all'effettiva situazione tempo per tempo⁵⁰².

L'art. 19, comma 1, lett. d), precisa che il controllo costante si attua attraverso l'analisi delle operazioni effettuate e delle attività svolte o individuate durante tutta la durata del rapporto, in modo da verificare che esse siano coerenti con la conoscenza che il soggetto obbligato ha del cliente e del suo profilo di rischio. Ove necessaria in funzione del rischio, è richiesta anche la verifica della provenienza dei fondi e delle risorse nella disponibilità del cliente, sulla base di informazioni acquisite o possedute in ragione dell'esercizio dell'attività.

Quanto agli effetti del controllo costante, l'emersione di elementi nuovi può condurre a un aggiornamento del quadro conoscitivo e del profilo di rischio del cliente, a effettuare specifici approfondimenti, ove ritenuti utili; ove risultino anomalie, queste andranno apprezzate ai fini delle iniziative da assumere, quali una eventuale segnalazione di operazione sospetta alla UIF fino a misure estreme, come la chiusura del rapporto.

Nel caso in cui l'adeguata verifica del cliente si renda necessaria a fronte di sospetti di riciclaggio o di finanziamento del terrorismo ovvero di dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'identificazione, la stessa può non avere portata generale e focalizzarsi sugli specifici aspetti che hanno generato il sospetto di riciclaggio ovvero che sono interessati da inadeguatezza, inattendibilità o da mancanza di veridicità. Ovviamente, va sempre verificato che anomalie circoscritte, e come tali risolubili in base a verifiche limitate, non siano rivelatrici di criticità a più ampio spettro, che suggeriscano di rinnovare verifiche e controlli su aree non direttamente interessate da sospetto o incertezza e finanche di ripercorrere l'intero processo di adeguata verifica.

L'adeguata verifica non va, inoltre, ripetuta quando sia già stata effettuata dall'intermediario in relazione a un rapporto in essere, a condizione che identificazione e verifica siano aggiornate nell'ambito del controllo costante.

4. Titolare effettivo (*R. Circosta*)

La definizione e la disciplina del titolare effettivo sono funzionali a garantire la riconducibilità di un'operazione alla persona fisica che, di fatto, ne trae vantaggio per evitare che altri soggetti e, in particolare, strutture giuridiche complesse – società e altri enti, *trust* e istituti giuridici affini – siano utilizzati come schermo per occultarne il reale beneficiario⁵⁰³ e realizzare finalità illecite (es. riciclaggio, corruzione, frode fiscale).

⁵⁰² Cfr. R. Cercone, *L'adeguata verifica della clientela nel settore bancario e finanziario*, in G. Castaldi e G. Conforti (a cura di), *Manuale Antiriciclaggio*, cit., p. 167.

⁵⁰³ In proposito, si veda l'analisi delle vulnerabilità connesse all'occultamento della titolarità effettiva contenuta nella relazione sulla valutazione dei rischi del 2022 della Commissione europea. In particolare, si sottolinea che "*L'anonimato continua a essere una vulnerabilità critica del sistema finanziario internazionale*" (COM(2022) 554 final, p. 11).

La normativa – primaria⁵⁰⁴ e secondaria⁵⁰⁵ – definisce la figura come la persona fisica o le persone fisiche, diverse dal cliente⁵⁰⁶, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è instaurato, la prestazione professionale è resa o l'operazione è eseguita⁵⁰⁷.

Al fine di evitare indebite sovrapposizioni nell'utilizzo dell'espressione "titolare effettivo", i Provvedimenti in materia di adeguata verifica della clientela emanati dalla Banca d'Italia distinguono il c.d. "titolare effettivo sub 1" – con cui si fa riferimento a una persona fisica che agisce in nome proprio, ma per conto di altra persona fisica o altre persone fisiche terze – dal "titolare effettivo sub 2", riferibile al caso in cui il soggetto per conto del quale è instaurato il rapporto continuativo o è realizzata l'operazione sia un'entità diversa da una persona fisica. Il secondo enunciato è applicabile al cliente persona giuridica o persona fisica che però agisce a sua volta per conto di una persona giuridica. In questo modo è sempre garantita piena trasparenza a prescindere dalla posizione assunta nei rapporti con gli intermediari.

L'identificazione e individuazione del titolare effettivo sono funzionali al corretto adempimento degli obblighi di adeguata verifica della clientela. Per la titolarità effettiva di persone giuridiche, *trust* e altri istituti e soggetti giuridici affini, in particolare, il legislatore richiama l'attenzione sulla necessità di adottare misure che "consentano di ricostruire, con ragionevole attendibilità, l'assetto proprietario e di controllo del cliente"; inoltre, tra le "informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale", che i soggetti obbligati sono chiamati ad acquisire e valutare, sono comprese anche quelle relative alle relazioni che intercorrono tra cliente e titolare effettivo⁵⁰⁸.

A livello europeo, l'EBA ha auspicato che gli intermediari, nell'ambito delle proprie politiche e procedure, disciplinino le modalità da seguire per identificare e, in funzione del rischio, verificare con certezza l'identità dei titolari effettivi.

Nel tentativo di agevolare il compito dei soggetti destinatari degli obblighi sopra menzionati l'art. 20 del D.lgs. 231/2007 prevede i criteri cui fare riferimento per individuare il titolare effettivo. Questi sono elencati secondo un ordine gerarchico, in modo che quelli riportati per ultimi siano residuali e, quindi, applicabili solo nel caso in cui risultino inutilizzabili i primi. La norma di cui all'art. 20, comma 1 statuisce che "il titolare effettivo di clienti diversi dalle persone fisiche⁵⁰⁹ coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo"⁵¹⁰. Il secondo comma, poi, specifica che nel caso in cui il cliente sia una società di capitali, il titolare effettivo deve essere identificato nella persona fisica che detiene –

⁵⁰⁴ Cfr. art. 1, comma 2, lett. pp) D.lgs. 231/2007, introdotto dall'art. 1 del D.lgs. 90/2017. In base alla direttiva UE/2015/849 "titolare effettivo" è "la persona o le persone fisiche che, in ultima istanza, possiedono o controllano il cliente e/o le persone fisiche per conto delle quali è realizzata un'operazione o un'attività". La bozza di nuovo regolamento europeo in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo, pur intervenendo in materia di titolarità effettiva, conferma la nozione già esistente nell'ordinamento europeo. Le definizioni discendono dall'adeguamento alle 40 Raccomandazioni del GAFI, che per prime hanno parlato di "beneficial owner", espressione con cui si fa riferimento alle persone fisiche che "infine" possiedono o controllano il cliente e/o la persona per la quale la transazione è effettuata, con ciò comprendendo i soggetti che esercitano, in ultima istanza, un controllo effettivo su una persona giuridica o su un accordo giuridico.

⁵⁰⁵ Si tenga presente, inoltre, che la Banca d'Italia ha adottato una nota (n. 15 del 4 ottobre 2021) per adeguarsi agli Orientamenti dell'EBA (European Banking Authority) in materia di adeguata verifica e relativi fattori di rischio (EBA/GL/2021/02). I predetti Orientamenti potrebbero integrare e, eventualmente, sostituire le disposizioni del provvedimento emanato dalla Banca il 30 luglio 2019.

⁵⁰⁶ Il cliente è "soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede o ottiene una prestazione professionale a seguito del conferimento di un incarico" (cfr. art. 1, comma 2, lett. f), del D.lgs. 231/2007).

⁵⁰⁷ Risulta chiara la differenza rispetto all'esecutore del cliente, il quale è definito dal già citato art. 1, comma 2, lett. p), del D.lgs. 231/2007 come "il soggetto delegato ad operare in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente".

⁵⁰⁸ Cfr. art. 18, comma 1, del D.lgs. 231/2007.

⁵⁰⁹ Si richiamano, ancora una volta, gli orientamenti EBA e, in particolare, il punto 4.12, lett. c) e d) in base al quale dovranno essere adottate "misure ragionevoli" rapportate al rischio per comprendere l'assetto proprietario e di controllo dei clienti diversi dalle persone fisiche.

⁵¹⁰ Nella direttiva UE/2015/849 si veda art. 3, par. 6, "j) la persona fisica o le persone fisiche che, in ultima istanza, possiedono o controllano il soggetto giuridico attraverso il possesso, diretto o indiretto, di una percentuale sufficiente di azioni o diritti di voto o altra partecipazione in detta entità, anche tramite azioni al portatore, o attraverso il controllo con altri mezzi, ad eccezione di una società ammessa alla quotazione su un mercato regolamentato e sottoposta a obblighi di comunicazione conformemente al diritto dell'Unione o a standard internazionali equivalenti che garantiscono una trasparenza adeguata delle informazioni sugli assetti proprietari".

direttamente o indirettamente – una partecipazione superiore al 25% del capitale sociale⁵¹¹. La disposizione impone di ricercare la titolarità effettiva in capo a una persona fisica. Ne deriva che, nel caso in cui la quota di capitale rilevante sia detenuta da una persona giuridica, si dovrà applicare il criterio della proprietà indiretta, risalendo la catena partecipativa fino alla persona fisica titolare della società apicale del gruppo che controlla il “cliente”⁵¹².

Nell'ipotesi in cui, tuttavia, la struttura dell'ente non consenta un'individuazione immediata del soggetto che ne abbia la proprietà diretta o indiretta, la titolarità effettiva della società dovrà essere riconosciuta a chi ne detiene il controllo, come definito dall'art. 2359 c.c. (alternativamente, controllo della maggioranza dei voti esercitabili in assemblea ordinaria; controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria; esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante)⁵¹³.

Nella disposizione appena analizzata non sono citate le società di persone. Un chiarimento sul punto si trova, però, nella normativa secondaria che estende l'applicabilità dei criteri sopra elencati anche a queste società, purché essi siano compatibili con la loro disciplina. Infatti, anche le società di persone – pur non avendo personalità giuridica – hanno autonomia patrimoniale e propria soggettività, motivo per cui potrebbero essere utilizzate come schermo.

Nel caso in cui il cliente sia una persona giuridica privata – associazioni, fondazioni e altre istituzioni di carattere privato⁵¹⁴ – l'art. 20, comma 4 prevede, invece, che i titolari effettivi siano cumulativamente i fondatori, ove in vita; i beneficiari, quando individuati o facilmente individuabili; i titolari di poteri di rappresentanza legale, direzione e amministrazione⁵¹⁵.

Non sono menzionate espressamente le organizzazioni prive di personalità giuridica (es. associazioni non riconosciute), ma le disposizioni secondarie stabiliscono che i criteri enunciati dalla norma siano applicabili anche ad altri soggetti giuridici – pubblici o privati – pure se privi di personalità giuridica.

Per *trust* e istituti giuridici affini⁵¹⁶ è necessario fare riferimento all'art. 22, comma 5, del D.lgs. 231/2007, ai sensi del quale i titolari effettivi si identificano cumulativamente nel costituente o nei costituenti (se ancora in vita), fiduciario o fiduciari, nel guardiano o guardiani ovvero in altra persona per conto del fiduciario, ove esistenti, nei beneficiari o classe di beneficiari (che possono essere beneficiari

⁵¹¹ Cfr. considerando n. 12 direttiva UE/2015/849 “Sebbene il riscontro di una precisa percentuale di partecipazione azionaria o altra partecipazione non comporti automaticamente l'individuazione del titolare effettivo, ciò dovrebbe costituire un elemento probatorio da tenere in considerazione, assieme ad altri. Tuttavia, gli Stati membri dovrebbero poter stabilire che una percentuale inferiore sia indicativa della titolarità o del controllo”.

⁵¹² L'inserimento di questa disposizione ha determinato l'abrogazione dell'allegato tecnico precedentemente vigente in materia, che aveva determinato varie incertezze interpretative riguardo alle modalità di applicazione della soglia del 25% più uno. Per una ricostruzione del dibattito, si veda: P. Iemma e N. Cuppini, *Antiriciclaggio: la babele del titolare effettivo*, in *Diritto Bancario online*, 2020. Anche a seguito delle modifiche apportate alla norma, tuttavia, non vi è uniformità di vedute sulle modalità di applicazione della soglia del 25%. Secondo una prima ricostruzione la quota andrebbe calcolata avendo come base il capitale della sola società cliente. Tale lettura sembrerebbe avallata dalla normativa europea: infatti l'art. 3, par. 6, della direttiva UE/2015/849 statuisce che “una percentuale di azioni del 25% più una quota o altra partecipazione superiore al 25% del capitale di un cliente, detenuta da una società, controllata da una o più persone fisiche, ovvero da più società, controllate dalla stessa persona fisica, costituisce indicazione di proprietà indiretta”. Prima dell'emanazione del D.lgs. 90/2017, la Banca d'Italia nelle proprie FAQ aveva adottato un diverso orientamento, preferendo l'impostazione per cui la soglia del 25% dovesse applicarsi a tutti i livelli della catena partecipativa. La stessa soluzione è stata adottata anche dalle Linee Guida emanate a maggio 2019 dal CNDCEC, *Casi di controllo*, p. 39 ss. A ciò si aggiunga che, in contrasto con quanto fatto nel 2013, la Banca d'Italia non ha fornito un'interpretazione su quale metodo sia preferibile, sul presupposto che l'inserimento di criteri sulla titolarità effettiva nella legge renda più opportuno che sia il MEF a intervenire per fornire indicazioni interpretative. A livello nazionale, quindi, non vi sono ulteriori indicazioni sul tema. Sulla materia potrebbe avere un ruolo incisivo la ridefinizione della disciplina antiriciclaggio da parte del c.d. “AML Package”. L'art. 42 della proposta di regolamento relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, infatti, conferma la soglia del 25% aggiungendo, però, che essa vada riferita “a ogni livello di proprietà”.

⁵¹³ La norma prevede, quindi, che il controllo societario quale criterio di attribuzione della titolarità effettiva sia applicato solo nel caso in cui non possa farsi riferimento alla partecipazione al capitale sociale. L'art. 42 della proposta di regolamento della Commissione, invece, prevede che il soggetto obbligato debba verificare se il controllo sia esercitato con mezzi diversi dalla titolarità di una partecipazione, da sola non sufficiente a identificare il titolare effettivo. La verifica del controllo esercitato “mediante altri mezzi” non dovrebbe essere eventuale e successiva all'accertamento della detenzione di una partecipazione rilevante, bensì concomitante.

⁵¹⁴ Decreto del Presidente della Repubblica 10 febbraio 2000, n. 361.

⁵¹⁵ Comma così sostituito dall'art. 2, comma 1, lett. d), n. 1), del D.lgs. 4 ottobre 2019, n. 125.

⁵¹⁶ Per tali intendendosi, ai sensi dell'art. 22 comma 5-bis, gli enti e gli istituti che, per assetto e funzioni, determinano effetti giuridici equivalenti a quelli dei *trust* espressi, anche avuto riguardo alla destinazione dei beni a uno scopo ed al controllo da parte di un soggetto diverso dal proprietario, nell'interesse di uno o più beneficiari o per il perseguimento di uno specifico fine.

del reddito o beneficiari del fondo o beneficiari di entrambi) e nelle altre persone fisiche che esercitano il controllo sul *trust* o sull'istituto giuridico affine attraverso la proprietà diretta, indiretta o altri mezzi⁵¹⁷.

Si rileva, infine, che il D.lgs. 125/2019 ha aggiunto un ultimo criterio residuale⁵¹⁸ nell'art. 20, comma 5, del D.lgs. 231/2007, da applicare qualora tutti quelli elencati in precedenza non siano sufficienti: in assenza di altri elementi, infatti, è indice di titolarità effettiva la detenzione dei poteri "di rappresentanza legale, amministrazione o direzione della società o del cliente comunque diverso dalla persona fisica", coerentemente con gli assetti organizzativi o statutari adottati.

Un'ulteriore aggiunta introdotta dal correttivo del 2019 è la previsione per cui i soggetti destinatari dell'obbligo di adeguata verifica devono conservare traccia dell'*iter* percorso per la ricostruzione della titolarità effettiva, così come, eventualmente, delle motivazioni per cui la stessa non è stata possibile⁵¹⁹.

Sempre il D.lgs. 125/2019 ha previsto sia richiesto direttamente al titolare effettivo di fornire i propri dati identificativi. Nella nuova formulazione, infatti, le informazioni relative al titolare effettivo "sono acquisite, a cura degli amministratori, richiedendole al titolare effettivo, individuato ai sensi dell'art. 20, anche sulla base di quanto risultante dalle scritture contabili e dai bilanci, dal libro dei soci, dalle comunicazioni relative all'assetto proprietario o al controllo dell'ente, cui l'impresa è tenuta secondo le disposizioni vigenti".

Alla luce delle previsioni e delle finalità descritte, la trasparenza e la conoscibilità delle informazioni relative al titolare effettivo risultano fondamentali per evitare che eventuali anomalie o reati non possano essere ricondotti ai loro autori⁵²⁰.

In quest'ottica la normativa europea⁵²¹ prevede che gli Stati membri si dotino di strumenti adeguati per consentire l'acquisizione, la conservazione e l'accessibilità delle informazioni relative alla titolarità effettiva degli enti costituiti sui propri territori. In Italia, in attuazione di questa previsione, gli enti interessati sono tenuti a individuare il proprio titolare effettivo e mantenere in merito informazioni accurate e aggiornate.

Sempre a livello europeo è stata prevista l'istituzione di un registro centrale, esterno alla società, nel quale confluiscono tutte le informazioni sopra menzionate, con il fine di realizzare una maggiore condivisione di

⁵¹⁷ Cfr. anche art. 3, par. 6, lett. b, della direttiva UE/2015/849.

⁵¹⁸ Gli Orientamenti EBA ribadiscono che il ricorso a questo criterio deve avvenire in via del tutto eccezionale, dopo aver esaurito ogni tentativo volto a individuare i titolari del possesso o controllo dell'ente e sempreché l'esito negativo della ricerca non debba considerarsi sospetto. Ove le motivazioni addotte dai clienti appaiano plausibili, andrà identificato come titolare effettivo chi, avendo la responsabilità ultima e generale del cliente, prende decisioni vincolanti per suo conto. L'applicazione del criterio residuale dovrà essere inoltre motivata con un'esauriente relazione scritta (cfr. i punti da 4.19 a 4.22). Nei casi in cui il cliente sia un'amministrazione pubblica o un'impresa statale, tuttavia, il titolare effettivo non può che essere un dirigente di alto livello. Per tale ragione, lo stesso andrà individuato seguendo come principali i criteri che per gli enti privati sono previsti come residuali (cfr. punto 4.23).

⁵¹⁹ Comma così modificato dall'art. 2, comma 1, lett. e), del D.lgs. 4 ottobre 2019, n. 125.

⁵²⁰ Cfr. considerando n. 14 direttiva UE/2015/849 e considerando n. 25 della direttiva UE/2018/843 nonché le Raccomandazioni del GAFI, in particolare nn. 24 e 25. Si tenga presente che a marzo 2022 è stata modificata la Raccomandazione n. 24 e la relativa Nota Interpretativa, al fine di garantire maggiore trasparenza e mitigare i rischi di uso improprio delle stesse. Inoltre, il 2 novembre 2022 il GAFI ha posto in pubblica consultazione l'aggiornamento delle proprie linee guida in materia, per sostenere l'attuazione dei nuovi requisiti adottati nella plenaria del marzo 2022 (la predetta consultazione è terminata il 6 dicembre 2022 e il GAFI analizzerà le osservazioni ricevute durante le riunioni di febbraio 2023). In particolare, le modifiche prevedono l'utilizzo di una combinazione di meccanismi diversi per la raccolta accentrata delle informazioni sulla titolarità effettiva. Gli Stati devono richiedere alle società di ottenere e conservare informazioni adeguate, accurate e aggiornate sul titolare effettivo e di mettere tali informazioni a disposizione delle autorità competenti in modo tempestivo. Inoltre, la nota interpretativa della Raccomandazione n. 24 fa espresso riferimento alla necessità, per gli Stati, di assicurare la disponibilità di informazioni sul titolare effettivo anche nell'ambito degli appalti pubblici (per le P.A. la conoscibilità della titolarità effettiva delle controparti, ad es. in materia di appalti, riveste un'importanza centrale e dovrebbe quindi essere garantita nella generalità dei procedimenti che contemplano valutazioni a fini antiriciclaggio, sia consentendo alle stesse l'accesso alle fonti informative sia prevedendo l'obbligo di comunicazione della titolarità effettiva da parte dei soggetti con cui esse vengono in contatto, in particolare dei partecipanti alle gare pubbliche. Per completezza, si sottolinea che un obbligo analogo è già previsto dalla disciplina europea che istituisce il dispositivo per la ripresa e resilienza (art. 22 del regolamento UE/2021/241), con riferimento ai destinatari di fondi e agli appaltatori interessati dall'attuazione di riforme e progetti nell'ambito dei piani nazionali. Ulteriormente, il 23 giugno 2022 era stata avviata la consultazione per la revisione della Raccomandazione n. 25, in tema di trasparenza e titolarità effettiva di negozi giuridici di natura fiduciaria, in modo da garantire standard sulla titolarità effettiva coerenti ed efficaci. Attualmente, il lavoro del GAFI sul punto è in corso: non sono stati approvati progetti di emendamento al testo della raccomandazione, ma le osservazioni ricevute e le proposte di revisione saranno valutate nelle riunioni di febbraio 2023.

⁵²¹ Cfr. art. 30 della direttiva UE/2015/849.

dati e trasparenza⁵²², garantendone – a determinate condizioni – l’accessibilità ai soggetti interessati⁵²³. Su quest’ultimo aspetto è poi intervenuta la direttiva UE/2018/843, che, modificando la disciplina dell’accesso alla sezione del Registro, ha disposto la possibilità per chiunque di prendere visione dei dati in esso contenuti.

Su queste basi è nato il Sistema di interconnessione dei registri centrali dei titolari effettivi (c.d. “BORIS” – Beneficial Ownership Registers Interconnection System), divenuto pienamente operativo il 22 marzo 2021, a seguito della pubblicazione nella Gazzetta ufficiale dell’Unione europea del regolamento di esecuzione 2021/369 della Commissione, recante, in allegato, le specifiche tecniche e le procedure necessarie al suo funzionamento.

L’Italia ha istituito un registro nazionale dei titolari effettivi di società e *trust* nella forma di una Sezione Speciale nel Registro delle Imprese, subordinandone peraltro l’effettiva implementazione all’emanazione da parte del Ministro dell’Economia e delle finanze, di concerto con il Ministro dello Sviluppo economico⁵²⁴ e sentito il Garante per la protezione dei dati personali⁵²⁵ di apposito decreto attuativo⁵²⁶. Quest’ultimo è stato pubblicato il 25 maggio 2022 – DM 55/2022 – e dovrebbe consentire all’Italia di partecipare al sistema di interconnessione dei registri dei titolari effettivi sopra menzionato. Si tratta di un elemento fondamentale “nella costruzione di un efficace presidio di prevenzione del riciclaggio, da tempo atteso anche per allineare il nostro Paese agli standard internazionali”⁵²⁷. L’efficace applicazione delle norme sul registro, inoltre, risulta essenziale per garantire un’adeguata irrogazione di sanzioni finanziarie mirate, tema centrale nell’attuale quadro internazionale compromesso dal conflitto russo-ucraino⁵²⁸.

Il provvedimento disciplina comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di *trust* produttivi di effetti giuridici rilevanti ai fini fiscali e di istituti giuridici affini al *trust* e si prefigge di “prevenire e contrastare l’uso del sistema economico e finanziario a scopo di riciclaggio e di finanziamento del terrorismo”⁵²⁹.

Più in particolare, poi, l’art. 5 – relativo all’accesso al Registro delle Autorità che vi sono elencate⁵³⁰ – prevede che le modalità tecniche e operative dell’accesso siano regolate con apposita convenzione sottoscritta da ciascuna Autorità interessata con Unioncamere e InfoCamere S.C.p.A (il “gestore”); l’art. 6, invece, disciplina l’accesso alla sezione autonoma e alla sezione speciale del registro delle imprese, previo accreditamento, dei soggetti obbligati ex art. 3, del D.lgs. 231/2007, per la consultazione dei dati e delle informazioni sulla titolarità effettiva a supporto degli adempimenti concernenti l’adeguata verifica della clientela. La norma stabilisce, inoltre, che i soggetti obbligati possano segnalare eventuali difformità tra le informazioni sulla titolarità effettiva ottenute per effetto della consultazione del registro e quelle acquisite in sede di adeguata verifica. Le segnalazioni così acquisite sono consultabili da parte delle Autorità abilitate all’accesso di cui al menzionato art. 5, secondo le modalità indicate nelle convenzioni, garantendo, in ogni caso, l’anonimato dei soggetti obbligati segnalanti.

⁵²² Cfr. ancora considerando 14 e art. 30, par. 3, della direttiva UE 2015/849.

⁵²³ Per il novero dei soggetti legittimati all’accesso si veda art. 30, par. 5 direttiva UE 2015/849. Per la possibilità di prevedere deroghe all’accesso cfr. par. 9 del medesimo articolo. Al riguardo, si sottolinea che il 22 novembre 2022, con la sentenza emessa nelle cause riunite C-37/20 e C-601/20, la Corte di Giustizia dell’Unione europea ha posto un limite all’accessibilità al registro da parte del “pubblico”, stabilendo che la predetta disposizione di cui all’art. 30, par. 5, nella sua attuale formulazione, violi i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali dei cittadini sanciti dagli artt. 7 e 8 della Carta europea. Secondo la Corte, infatti, consentire l’accesso ai dati sulla situazione materiale e finanziaria del titolare effettivo a un numero potenzialmente indefinito di soggetti potrebbe creare conseguenze negative. Il rischio aumenta se si pensa che, una volta pubblicate, le informazioni potrebbero essere consultate, conservate e diffuse senza una possibilità concreta di individuare l’autore di eventuali abusi. La sentenza potrebbe incidere sulla normativa degli Stati dell’Unione europea che hanno correttamente recepito la disposizione della direttiva dichiarata invalida dalla Corte: i giudici nazionali, infatti, se investiti della questione dovrebbero disapplicare le norme interne che confliggono con tale pronuncia. Inoltre, la sentenza potrebbe avere impatti anche sul negoziato in corso relativo al c.d. “AML package” che – in linea di continuità con la quinta direttiva AML – avrebbe previsto la possibilità per il pubblico – tranne specifiche eccezioni – di accedere al registro del titolare effettivo.

⁵²⁴ Art. 21 del D.lgs. 231/2007.

⁵²⁵ La partecipazione del Garante è stata prevista con il D.lgs. 125/2019.

⁵²⁶ Il decreto ha subito varie battute d’arresto: dopo essere stato posto in pubblica consultazione e aver ottenuto il parere favorevole del Garante per la protezione dei dati personali, è stato bloccato a seguito del parere interlocutorio (negativo) reso dal Consiglio di Stato il 19 marzo 2021. Lo stesso Consiglio, poi, il 6 dicembre 2021 ha dato il proprio parere positivo (parere n. 1835).

⁵²⁷ Cfr. Direttore della UIF, [Presentazione del Rapporto sull’attività svolta nel 2021](#) (in particolare, p. 12).

⁵²⁸ In questo senso si è espressa anche la Commissione europea nella relazione sulla valutazione dei rischi del 2022 (COM(2022) 554 final, p. 5).

⁵²⁹ Cfr. art. 2, del DM n. 55/2022.

⁵³⁰ Ministero dell’Economia e delle finanze, Autorità di vigilanza di settore, UIF, Direzione Investigativa Antimafia, Nucleo Speciale Polizia Valutaria della Guardia di Finanza, Direzione Nazionale Antimafia e Antiterrorismo; Autorità giudiziaria, autorità preposte al contrasto dell’evasione fiscale.

Dalla lettura complessiva delle norme si deduce che gli oneri gestionali del Registro saranno significativi, ma potranno essere compensati dai vantaggi realizzabili in termini di complessiva trasparenza delle attività e di omogeneità dei comportamenti. Non si possono ignorare, tuttavia, le esigenze di corretto bilanciamento tra costi e opportunità per gli utilizzatori, chiamati a sostenere oneri economici per l'acquisizione dei dati, a valutare la correttezza delle informazioni censite e a comunicare al Registro eventuali difformità rilevate.

Lo stesso decreto aveva previsto, poi, che a far data dalla sua entrata in vigore – il 9 giugno 2022 – il Ministero dello Sviluppo economico avrebbe dovuto emanare, entro sessanta giorni, quattro ulteriori provvedimenti attuativi per approvare il modello digitale necessario all'effettuazione della comunicazione agli uffici del registro delle imprese; accertare l'operatività del sistema di comunicazione; fissare i diritti di segreteria; adottare i modelli per il rilascio di certificati e copie anche digitali⁵³¹. In particolare, la pubblicazione del decreto del Ministero dello Sviluppo economico che attesta l'operatività del sistema di comunicazione dei dati e delle informazioni sulla titolarità effettiva è fissata come punto di riferimento temporale per le comunicazioni dei dati e delle informazioni relative ai titolari effettivi delle imprese dotate di personalità giuridica, delle persone giuridiche private e dei *trust*. Queste, infatti, dovranno essere effettuate entro sessanta giorni successivi alla pubblicazione in Gazzetta del citato provvedimento del MISE⁵³². Il termine per l'emanazione dei provvedimenti elencati è ormai trascorso e si resta quindi in attesa della loro pubblicazione.

In chiusura, si sottolinea che, nonostante l'innegabile utilità informativa⁵³³ degli strumenti nazionali e sovranazionali sopra descritti, l'utilizzo dei dati contenuti nei registri dei titolari effettivi non esaurisce, di per sé, l'obbligo delle imprese di assumere misure adeguate al rischio per identificare il titolare effettivo e verificarne l'identità. Esse, infatti, potrebbero dover adottare mezzi ulteriori, soprattutto “qualora il rischio associato al rapporto continuativo risulti elevato o l'impresa nutra dubbi che la persona iscritta nel registro sia il titolare effettivo”⁵³⁴. In altri termini, “appare necessario assicurare una applicazione non meccanicistica del sistema” evitando che i destinatari degli obblighi di adeguata verifica “si appiattiscano” sulle indicazioni contenute nel Registro; è opportuno, invece, sollecitare “la sana curiosità degli intermediari e degli altri destinatari” oltre che un aperto confronto “sulle eventuali difformità rilevate, specie nel caso di catene partecipative complesse e con forte proiezione estera”, casi in cui può essere difficoltoso “giungere a conclusioni univoche”. È essenziale che in tali valutazioni sia incluso anche il contributo delle Autorità a vario titolo coinvolte nella prevenzione del riciclaggio⁵³⁵.

5. Misure di adeguata verifica della clientela (*M. Colonnello*)

5.1. Misure semplificate

Alla luce del principio dell'approccio basato sul rischio, che permea tutta la disciplina antiriciclaggio e che trova fondamento nella quarta direttiva comunitaria, il legislatore ha ritenuto opportuno graduare le condotte dei soggetti obbligati in funzione del rischio che si trovano a gestire.

In questa ottica, sono state introdotte misure diverse, semplificate o rafforzate, con le quali i destinatari possono calibrare, nella loro piena autonomia valutativa, l'intensità e la profondità degli obblighi di adeguata verifica della clientela.

⁵³¹ Cfr. art. 3, commi 5 e 6 e art. 8, commi 1 e 3, del DM n. 55/2022.

⁵³² Art. 3, comma 6, ultima parte, del DM n. 55/2022.

⁵³³ Sull'importanza dei registri dei titolari effettivi ha richiamato l'attenzione anche la Commissione europea che, nella relazione sulla valutazione dei rischi del 2022, ha reiterato le raccomandazioni “a *provvedere a mantenere adeguate, accurate e aggiornate le informazioni sulla titolarità effettiva delle persone giuridiche e degli istituti giuridici*” e “*attuare completamente le disposizioni della direttiva antiriciclaggio concernenti i i registri dei titolari effettivi*” (COM(2022) 554 final, p. 21).

⁵³⁴ Cfr. punto 4.13, degli Orientamenti dell'EBA. Lo stesso principio è espresso nell'art. 21, comma 7, del D.lgs. 231/2007 (“*La consultazione dei registri [...] non esonera i soggetti obbligati dal valutare il rischio di riciclaggio e finanziamento del terrorismo cui sono esposti nell'esercizio della loro attività e dall'adottare misure adeguate al rischio medesimo*”).

⁵³⁵ Si veda, ancora, [Presentazione del Rapporto sull'attività svolta nel 2021](#), p. 12.

Da un lato, infatti, la previsione di misure semplificate di adeguata verifica per situazioni di basso rischio garantisce un sistema preventivo più efficiente, riducendo gli sforzi dei soggetti obbligati, anche in termini di costi di *compliance*; dall'altro, aver definito misure rafforzate per i casi di clientela ad alto rischio significa aver fornito idonei strumenti ai destinatari per gestire in modo più efficace tutte quelle situazioni che richiedono monitoraggi e analisi più approfondite, evitando, in tal modo, che si arrivi ad escludere ingiustificatamente dal circuito economico e finanziario intere categorie ritenute più "pericolose" in termini di rischio di riciclaggio⁵³⁶.

Il quadro complessivo delle indicazioni utili a calibrare l'intensità delle misure si è progressivamente arricchito: a livello nazionale, la riforma del 2017 ha ampliato, rispetto al passato, sia le ipotesi per le quali i destinatari possono svolgere l'adeguata verifica in modalità non ordinaria sia le modalità tecniche per darvi attuazione; a livello comunitario, oltre alle novità introdotte dalla quinta direttiva antiriciclaggio, si segnala che, in ambito creditizio e finanziario, l'EBA ha pubblicato, nel 2021, le *"Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (The ML/TF Risk Factors Guidelines)" under Articles 17 and 18(4) of Directive (EU) 2015/849*, per garantire indicazioni accurate e rilevanti sulle modalità per gestire i rischi relativi alla clientela, attraverso la corretta applicazione degli obblighi di adeguata verifica⁵³⁷.

Le misure semplificate e rafforzate di adeguata verifica sono disciplinate dagli artt. 15-24 della direttiva 2015/849/UE, che detta alcuni principi fondamentali: innanzitutto, non è mai possibile prescindere né da una valutazione del rischio nella situazione concreta né da controlli che consentano in ogni caso di individuare operazioni anomale o sospette; in secondo luogo, la direttiva indirizza gli Stati membri nello stabilire le casistiche di basso e ad alto rischio, attraverso l'indicazione di fattori di rischio nell'allegato II del medesimo testo normativo e rimandando agli orientamenti dell'EBA.

Il legislatore nazionale ha trasposto tali principi nella normativa di attuazione, indicando, per entrambe le tipologie di misure, una serie di fattori che possono connotare, anche se non in via esaustiva, i contesti in cui sia rinvenibile un livello di rischio minore o maggiore. Ulteriori fattori di rischio, ad integrazione o modifica rispetto a quelli posti dal legislatore, sono stati indicati dalle Autorità di vigilanza di settore e dagli Organismi di autoregolamentazione⁵³⁸.

L'art. 23 del D.lgs. 231/2007 disciplina i casi in cui, in presenza di un basso rischio, sia possibile adottare misure semplificate di adeguata verifica, riducendo l'estensione e la frequenza degli adempimenti.

Risulta importante sottolineare che la "semplificazione" riguarda esclusivamente la modalità, meno approfondita, con cui sono posti in essere gli adempimenti previsti dalle verifiche ordinarie, che devono comunque essere completamente attuati. Non vi è quindi alcuna possibilità che l'adeguata verifica semplificata si traduca in un esonero dall'acquisizione del documento di identità o dal controllo costante del rapporto; può semmai significare, ad esempio, una diminuzione della frequenza con cui i dati raccolti per l'adeguata verifica sono aggiornati, una riduzione della profondità nel monitoraggio delle operazioni che coinvolgano il rapporto, una dilazione dei tempi per l'identificazione del cliente o una semplificazione nelle informazioni da raccogliere.

Come anticipato poc'anzi, nell'art. 23 si dettagliano, in modo esemplificativo e non esaustivo, anche indici di basso rischio (coerentemente con quanto previsto dall'allegato II della direttiva) di cui i soggetti

⁵³⁶ L'applicazione corretta e graduata, in funzione del rischio concreto, delle misure di adeguata verifica è in effetti il principale strumento proprio per affrontare il fenomeno del c.d. de-risking, che si riferisce al comportamento degli intermediari che decidono di evitare, in radice, ogni relazione con categorie di soggetti potenzialmente esposte a rischio elevato, al fine di eliminare, invece di gestire, i relativi rischi di riciclaggio/finanziamento del terrorismo.

⁵³⁷ L'EBA è stata incaricata di emanare gli orientamenti sui fattori di rischio AML e TF ai sensi degli artt. 17 e 18, par. 4, della direttiva (UE) 2015/849, modificata dalla direttiva (UE) 2019/2177. In particolare, nel 2019, il legislatore europeo ha consolidato i mandati AML/CFT di tutte e tre le ESA all'interno dell'EBA. Le Guidelines sostituiscono le linee guida originali (JC/2017/37), effettuandone un riesame per garantire accuratezza e rilevanza in aree che richiedevano una valutazione anche alla luce dell'entrata in vigore della quinta direttiva antiriciclaggio e aggiornando le indicazioni con riferimento a ulteriori settori: ad esempio si dedicano approfondimenti all'utilizzo di piattaforme di crowdfunding, alla finanza aziendale, ai fornitori di servizi di informazione sui conti (AISP), ai fornitori di servizi di avvio dei pagamenti (PISP) e le imprese che forniscono attività di cambio valuta; si forniscono anche maggiori dettagli sui fattori di rischio di finanziamento del terrorismo.

⁵³⁸ Si richiamano al riguardo i diversi atti di normazione secondaria che arricchiscono il quadro fornito dal legislatore, e in particolare, il Provvedimento di Banca d'Italia del 30 luglio 2019, il regolamento Consob n. 20570/2018, il regolamento IVASS n. 44 del 12 febbraio 2019 nonché le Regole Tecniche elaborate dal CNN, dal CNF, dal CNDEC.

obbligati devono tener conto, suddivisi in tre principali categorie: una prima, relativa alla tipologia dei clienti; una seconda riferita alla tipologia di prodotti, servizi operazioni o canali di distribuzione; una terza riguardante il rischio geografico. Saranno ovviamente i destinatari a definire, nel proprio documento di *policy* antiriciclaggio, le misure da assumere in relazione alle diverse tipologie di clienti e di prodotti, motivando adeguatamente la scelta.

A chiusura dell'art. 23, il legislatore specifica che è comunque esclusa l'applicazione di obblighi semplificati di adeguata verifica quando vi sia sospetto di riciclaggio o finanziamento del terrorismo.

Importante sottolineare, infine, che anche in situazioni di basso rischio rimangono immutati gli ordinari obblighi di segnalazione di operazioni sospette e di conservazione.

5.2. Misure rafforzate

Gli artt. 24 e 25 del D.lgs. 231/2007 disciplinano le misure rafforzate di adeguata verifica della clientela, che, specularmente a quanto avviene per quelle semplificate, sono attuate in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo che debba essere gestito e mitigato nel modo più efficiente possibile.

Analogamente a quanto previsto per le misure semplificate, anche in questo caso i soggetti obbligati tengono conto, nelle proprie valutazioni, di fattori di rischio relativi al cliente, a prodotti, servizi, operazioni o canali di distribuzione o fattori di rischio geografici dettagliati, seppur non in via esaustiva, nel testo dell'art. 24 del decreto.

Come indicato nella relazione illustrativa alla riforma del 2017, il legislatore ha ritenuto opportuno anche elencare alcune ipotesi di presunzione *iuris et de iure* di elevata rischio per le quali è sempre richiesto, ai soggetti obbligati, di applicare misure di adeguata verifica rafforzata. Si tratta in particolare, dei casi di: i) rapporti continuativi, prestazioni professionali ed operazioni che coinvolgono Paesi terzi ad alto rischio; ii) rapporti di corrispondenza transfrontalieri che comportano l'esecuzione di pagamenti con un ente creditizio o istituto finanziario corrispondente di un pPaese terzo; iii) rapporti continuativi, prestazioni professionali o operazioni con clienti e relativi titolari effettivi che siano persone politicamente esposte (PEPs), salve le ipotesi in cui queste agiscano come organi della Pubblica amministrazione.

Inoltre, anche nel caso di operazioni caratterizzate da importi insolitamente elevati oppure rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate, i soggetti obbligati rafforzano il grado e la natura delle verifiche atte a determinare se le operazioni siano sospette. In quest'ultimo caso, rispetto alle altre ipotesi che si basano su criteri oggettivi, si richiede quindi una vera e propria attività valutativa sulla rischio di elevata. Si tratta, pertanto, di determinare in modo critico, ad esempio, se l'importo dell'operazione sia eccessivo rispetto al profilo del cliente o allo scopo del rapporto.

Non rientra invece nei casi di presunzione *ex lege*, ma di ipotesi rimessa all'esclusiva valutazione dei destinatari, quella introdotta nel comma 6-*bis* dell'art. 25 che, come si legge dalla relazione illustrativa della riforma del 2017, è stata introdotta per rispondere a un rilievo della Commissione per incompleto recepimento della quarta direttiva (procedura di infrazione 2019/2042). Si tratta, in particolare, del caso delle succursali o filiazioni, aventi sede in Paesi terzi ad alto rischio, controllate da soggetti obbligati aventi sede in Italia o in altro Stato membro, quando tali succursali o filiazioni si conformino alle politiche e alle procedure di gruppo.

L'art. 25 del decreto dettaglia le modalità con cui devono essere attuate le misure di adeguata verifica rafforzata. In modo diametralmente opposto a quanto avviene per la modalità semplificata di attuazione dell'obbligo, si richiede ai soggetti obbligati di eseguire l'adeguata verifica con maggiore attenzione, profondità, estensione e frequenza. Ciò significa, concretamente, l'acquisizione di informazioni ulteriori, un controllo con scadenze temporali più ravvicinate o, ad esempio, il coinvolgimento dell'alta dirigenza per decidere se instaurare o meno un rapporto.

È opportuno precisare che, dinanzi a una situazione di rischio elevato, la previsione di un rafforzamento delle misure ordinarie è atto proprio a consentire al soggetto obbligato di gestire in modo più efficace il rischio che si presenta. Ciò può avvenire, da un lato, prevenendo che il rischio sia evitato *tout court*, come già detto nelle ipotesi di *de-risking*; dall'altro, impedendo che il tutto si risolva nella automatica trasmissione di segnalazioni di operazioni sospette senza che avvenga una valutazione preventiva e accurata che accerti se vi sia o meno sospetto di riciclaggio o finanziamento del terrorismo.

L'art. 25, inoltre, elenca anche le particolari modalità di adeguata verifica rafforzata che devono essere poste in essere per le situazioni di rischio elevato ritenute tali dallo stesso legislatore, dettagliate dall'art. 24 (rapporti di corrispondenza transfrontalieri, Paesi terzi ad alto rischio e PEPs).

Anche in queste ipotesi, un contributo rilevante è fornito dalla normativa secondaria: per i rapporti con i PEPs, in particolare, la Banca d'Italia ha pubblicato una serie di "buone prassi" per migliorare i controlli di questo fattore di rischio, considerato cruciale in ragione del legame che può sussistere tra questa tipologia di clientela e un più elevato pericolo di condotte corruttive, fenomeno che può provocare danni particolarmente rilevanti nell'intero circuito economico e che può esporre il settore finanziario anche a rischi reputazionali e legali.

6. Esecuzione degli obblighi di adeguata verifica da parte di terzi (M. Foppiani)

Gli obblighi di adeguata verifica della clientela di cui agli artt. 17 ss. del D.lgs. 231/2007 ("Decreto") possono essere eseguiti, oltre che dai soggetti obbligati parte del rapporto in via di instaurazione, anche da terzi rientranti nelle categorie indicate dal D.lgs. 231/2007 (artt. 26-30) e dalle disposizioni di attuazione emanate dalle Autorità di vigilanza di settore. Il soggetto obbligato può avvalersi del terzo al fine di identificare e verificare l'identità del cliente, dell'esecutore e/o del titolare effettivo (art. 18, comma 1, lett. a) e b)) e, in alcuni casi, anche per acquisire e valutare le informazioni sullo scopo e sulla natura del rapporto continuativo o dell'operazione (art. 18, comma 1, lett. c)). Rimane invece escluso dal perimetro della disciplina dell'esecuzione degli obblighi di adeguata verifica da parte di terzi il controllo costante del rapporto con il cliente (art. 18, comma 1, lett. d)) che, avendo luogo nel concreto dipanarsi del rapporto, non può essere eseguito che da parte dello stesso soggetto obbligato. Ferma restando la responsabilità di quest'ultimo, gli obblighi di adeguata verifica della clientela si considerano assolti previo rilascio da parte del terzo di idonea attestazione (art. 27).

La possibilità di esternalizzare l'esecuzione degli obblighi di adeguata verifica si iscrive in un'ottica di razionalizzazione e semplificazione degli adempimenti, *"sul presupposto dell'economicità e del reimpiego dei dati e delle informazioni acquisite da un soggetto comunque rientrante nel novero dei soggetti obbligati ai sensi della vigente normativa"*⁵³⁹. Invero, laddove i dati di cui all'art. 18, comma 1, lett. a), b) e c), del Decreto siano già stati acquisiti in altre sedi dai soggetti a ciò legittimati, la reiterazione dei medesimi adempimenti si porrebbe in contrasto con il divieto di *"gold plating"* di derivazione europea⁵⁴⁰.

La disciplina dell'esternalizzazione degli obblighi di adeguata verifica, già presente nella versione originale del Decreto, è stata integrata e riorganizzata in occasione dell'emanazione delle direttive UE 2015/849 (c.d. quarta direttiva) e 2018/843 (c.d. quinta direttiva) attuate, rispettivamente, dal D.lgs. 90/2017 e dal D.lgs. 125/2019. Un ruolo fondamentale è poi svolto dalla normativa secondaria emanata dalle Autorità di vigilanza di settore, cui il Decreto in più punti rinvia per la disciplina di dettaglio. Si fa riferimento, in particolare, alle Disposizioni della Banca d'Italia del 30 luglio 2019⁵⁴¹ (Parte Quinta), al regolamento dell'IVASS n. 44 del 12 febbraio 2019 (Sezione V – artt. 51-54) e alla Delibera Consob n. 20570 del 4 settembre 2018 (c.d. regolamento Consob, art. 32).

⁵³⁹ Cfr. Relazione illustrativa allo schema di decreto legislativo recante attuazione della Dir. UE 2015/849, p. 11.

⁵⁴⁰ In tal senso, si veda il considerando n. 35 della Dir. UE 2015/849 per cui *"per evitare il ripetersi delle procedure d'identificazione dei clienti, che sarebbe fonte di ritardi e di inefficienze nelle attività economiche, è opportuno consentire, fatti salvi adeguati presidi, che i clienti la cui identificazione sia già stata effettuata altrove vengano accettati dai soggetti obbligati."*

⁵⁴¹ Cfr. S. Galmarini (a cura di), *Antiriciclaggio*, Wolters Kluwer, 2019, p. 345, dove si afferma che *"il Provvedimento rappresenta un'evoluzione delle disposizioni stabilite dal Provvedimento della Banca d'Italia del 3 aprile 2013 e, rispetto al precedente, rafforza le procedure per gli adempimenti degli obblighi di adeguata verifica della clientela"*. Inoltre, le Disposizioni della Banca d'Italia attuano gli Orientamenti emanati del 4 gennaio 2018 congiuntamente dalle Autorità di Vigilanza europee (EBA, ESMA e EIOPA - ESAs) sulle misure semplificate e rafforzate di adeguata verifica e sui fattori di rischio (cc.dd. *"Orientamenti congiunti"*).

L'esecuzione degli obblighi di adeguata verifica della clientela non possono essere esternalizzati nei confronti di qualsiasi soggetto terzo; invero, solo coloro che rientrano nelle categorie previste dal Decreto possono eseguirli in luogo del soggetto obbligato. Da una lettura sistematica delle disposizioni vigenti, emergono due macro-categorie di "terzi"⁵⁴²: quelli che possono solamente identificare e verificare l'identità dei clienti e quelli che, invece, possono altresì acquisire e valutare le informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale. A quest'ultima categoria appartengono i soggetti di cui all'art. 26, comma 2, ossia: (i) gli intermediari bancari e finanziari di cui all'art. 3, comma 2; (ii) gli intermediari bancari e finanziari aventi sede in altri Stati membri; (iii) gli intermediari bancari e finanziari aventi sede in un Paese terzo che soddisfano determinati requisiti⁵⁴³ e (iv) i professionisti nei confronti di altri professionisti. Tale elencazione, da considerarsi tassativa in quanto derogatoria della regola generale, che postula la coincidenza tra il soggetto obbligato e l'esecutore degli obblighi di adeguata verifica della clientela, in passato annoverava anche gli agenti in attività finanziaria italiani, limitatamente all'effettuazione di operazioni occasionali di pagamento di importo inferiore a 15.000 euro (ad es. la rimessa di denaro) o di distribuzione di moneta elettronica. L'inclusione di tali soggetti – seppur oggettivamente circoscritta – apparve però poco giustificabile, poiché ampliava eccessivamente la libertà dell'agente in relazione a operazioni ad alto rischio di riciclaggio e disciplinava in maniera irragionevolmente difforme l'attività degli agenti prestatori di servizi di pagamento per conto di intermediari comunitari che, invece, potevano soltanto eseguire gli obblighi di identificazione⁵⁴⁴. Per tali ragioni, il D.lgs. 125/2019 è intervenuto, tra l'altro, sopprimendo l'art. 26, comma 2, lett. b), del Decreto. Una precisazione appare necessaria con riguardo alla categoria dei professionisti: l'art. 26, comma 2, lett. e), del Decreto considera "terzo" solo il professionista nei confronti di un altro professionista⁵⁴⁵. Alla radice di tale disciplina c'è, a parere di alcuni, una precisa scelta di politica legislativa dovuta alla *"diversità di dati ed informazioni che sono acquisiti dagli uni e dagli altri destinatari in ragione della diversità sostanziale delle operazioni svolte dagli intermediari finanziari rispetto alle prestazioni eseguite dai professionisti"*⁵⁴⁶. Pertanto, un intermediario bancario o finanziario, ad esempio, non potrà avvalersi del professionista per l'esecuzione degli obblighi di adeguata verifica della clientela; controverso è, invece, se il professionista possa o meno avvalersi dell'adeguata verifica eseguita da un intermediario bancario o finanziario⁵⁴⁷ per il quale la lettera della legge non prevede espressamente un'analogia restrizione.

L'art. 27, commi 4 e 5, invece, individua i soggetti terzi legittimati a eseguire i soli obblighi di identificazione e di verifica dell'identità della clientela (art. 18, comma 1, lett. a) e b) del Decreto). In entrambi i casi, ci si trova dinanzi a un'esternalizzazione soltanto parziale, poiché il completamento degli obblighi di adeguata verifica spetta necessariamente al destinatario⁵⁴⁸. Nello specifico, l'art. 27, comma 4, prevede che i soggetti obbligati possono acquisire le informazioni relative all'identificazione del cliente dai soggetti di cui all'art. 3, comma 3, lett. b) e c), del Decreto, ossia dai mediatori creditizi e dagli agenti in attività finanziaria, che le abbiano precedentemente reperite in occasione del contatto con il cliente avvenuto per il loro tramite. Al comma 5, poi, è previsto che, in relazione ai soli rapporti continuativi relativi all'erogazione di credito al consumo, di *leasing* o di altre tipologie operative indicate dalla Banca

⁵⁴² Tale dicotomia è confermata anche dall'impostazione seguita dalle Disposizioni della Banca d'Italia che, nella Parte Quinta-Sezione I, dividono i terzi in sub a) (*"soggetti terzi che possono effettuare tutte le fasi dell'adeguata verifica, a eccezione del controllo costante dell'operatività"*) e sub b) (*"Soggetti terzi che possono effettuare solo l'identificazione del cliente, dell'esecutore e del titolare effettivo, inclusa l'acquisizione di copia dei documenti di identità"*).

⁵⁴³ In particolare, essi devono essere tenuti ad applicare misure di adeguata verifica della clientela e di conservazione dei documenti di livello analogo a quelle previste dalla direttiva e devono essere sottoposti a controlli di vigilanza in linea con quelli previsti dal diritto dell'Unione europea.

⁵⁴⁴ In tal senso, M. Carbone, P. Bianchi e V. Vallefucio, *Le nuove regole antiriciclaggio*, cit., p. 629.

⁵⁴⁵ Ad es. l'avvocato difensore potrà essere considerato terzo nei confronti del collega domiciliatario.

⁵⁴⁶ M. Krogh, *Identificazione a distanza ai fini antiriciclaggio nella prestazione notarile: aspetti pratici e criticità (commento alla normativa)*, in *Notariato*, n. 1, 1 gennaio 2021, p. 55.

⁵⁴⁷ In senso positivo, v. S. Galmarini (a cura di), *Antiriciclaggio*, cit., p. 550. Maggiormente controversa è l'opinione di M. Krogh, *Identificazione a distanza ai fini antiriciclaggio nella prestazione notarile*, cit., p. 55.

⁵⁴⁸ A ben vedere, l'esternalizzazione degli obblighi di adeguata verifica è sempre parziale, in quanto il controllo costante di cui all'art. 18, comma 1, lett. c), in ogni caso, deve essere eseguito in proprio dal soggetto obbligato.

d'Italia⁵⁴⁹, i “*collaboratori esterni legati all'intermediario da apposita convenzione, nella quale siano specificati gli obblighi [...] e ne siano conformemente regolate le modalità di adempimento*”, possano effettuare l'identificazione del cliente. La necessità di un'apposita convenzione risiede nel fatto che la norma non richiede che i collaboratori siano anch'essi soggetti obbligati ai sensi dell'art. 3 del Decreto. Ai fini di una corretta esecuzione degli obblighi di adeguata verifica, pertanto, è opportuno – se non necessario – che il trasferimento dei poteri dal soggetto obbligato al proprio collaboratore esterno sia accompagnato da indicazioni relative all'*ubi consistam* di tali obblighi e alle modalità di esecuzione. Per tale motivo, la convenzione non è richiesta nel caso di esecuzione degli obblighi da parte di mediatori creditizi o agenti in attività finanziaria *ex* art. 27, comma 4, essendo entrambe le figure già ricomprese nel novero dei soggetti destinatari degli obblighi antiriciclaggio (cfr. comma 3, lett. b) e c)). Sempre con riguardo alla categoria di terzi di cui all'art. 27, comma 5, le Disposizioni della Banca d'Italia del 2019 esigono altresì che i collaboratori esterni operino “*in nome e per conto dei destinatari nel proporre alla clientela la sottoscrizione dei contratti*” relativi alle predette tipologie operative.

Inoltre, le Disposizioni della Banca d'Italia del 2019 prevedono che anche i “*soggetti convenzionati e agenti*” (cfr. art. 1, comma 2, lett. nn), del D.lgs. 231/2007) rientrino nella categoria dei terzi che possono effettuare l'identificazione della clientela, purché operino “*con le modalità previste dall'articolo 44 del decreto antiriciclaggio*”. Coerentemente con quanto richiesto dall'art. 27, comma 5 per i collaboratori esterni – e attesa l'estraneità dei soggetti convenzionati e degli agenti alla categoria dei soggetti obbligati – anche l'art. 44, comma 2, prevede la necessità di un “*atto di convenzionamento o di un mandato per la regolamentazione dei rapporti tra le parti*”, che indichi “*espressamente*” gli adempimenti relativi all'identificazione della clientela e le modalità di adempimento dei medesimi.

La gamma dei terzi che possono effettuare solo l'identificazione della clientela è stata ulteriormente ampliata dal D.lgs. 125/2019, che ha introdotto il comma 1-*bis* all'art. 30 del Decreto, demandando alle Autorità di vigilanza di settore l'individuazione di “*specifici presidi organizzativi in presenza dei quali l'assolvimento degli obblighi di adeguata verifica di cui all'articolo 18, comma 1, lettere a) e b) può essere esternalizzato a terzi diversi da quelli di cui all'articolo 26, comma 2*”⁵⁵⁰. Trattasi di una cauta apertura del sistema antiriciclaggio italiano, dettata dall'esigenza di avvicinare la disciplina nazionale a quella di molti paesi europei che già consentono una piena esternalizzazione degli obblighi di adeguata verifica a imprese specializzate, in particolare a quelle che offrono soluzioni tecnologicamente innovative⁵⁵¹.

Ancora, l'art. 27, comma 5-*bis*, prevede che le Autorità di vigilanza di settore possano adottare disposizioni al fine di ritenere assolti gli obblighi di adeguata verifica da parte di terzi appartenenti al gruppo dell'intermediario bancario o finanziario obbligato, purché nel rispetto dei requisiti previsti dal medesimo articolo.

Non possono essere considerati terzi, invece, il fornitore del servizio esternalizzato o l'agente che siano “*equiparabili ai dipendenti*”⁵⁵² o [...] a soggetti stabilmente incardinati nell'organizzazione dei soggetti obbligati per i quali svolgono la propria attività” (art. 30, comma 1)⁵⁵³. La legge abbraccia pertanto un approccio sostanzialistico in forza del quale non può essere considerato “terzo” – con conseguente inapplicabilità della relativa disciplina – il soggetto che, sebbene formalmente distinto dal soggetto obbligato parte del rapporto, sia riconducibile a quest'ultimo in forza dei rapporti di dipendenza o di stabile inquadramento nella struttura

⁵⁴⁹ A tal proposito, le Disposizioni della Banca d'Italia prevedono, oltre al credito al consumo e al leasing, anche il factoring, il microcredito e il credito agrario e peschereccio.

⁵⁵⁰ Non solo, ma anche diversi da quelli previsti dall'art. 27, comma 4 e 5, del Decreto.

⁵⁵¹ Cfr. M. Carbone, P. Bianchi e V. Vallefucio, *Le nuove regole antiriciclaggio*, cit., p. 631 e s.

⁵⁵² Pertanto, l'identificazione compiuta dalla segreteria del notaio (v. Cass. sent. n. 28823 del 30 novembre 2017) non ricade nell'ambito della disciplina dell'esecuzione degli obblighi di adeguata verifica da parte di terzi. Inoltre, a completamento dell'art. 30 del D.lgs. 231/2007, la l. n. 89/1913, l'art. 49, nel testo novellato con l. n. 333/1976, non prevede più la necessità che la certezza circa l'identità personale della parte stipulante costituisca “un risultato da ottenersi personalmente ed esclusivamente dal notaio”. Per maggiori approfondimenti della questione, si veda A. Parrotta, *Notai: obblighi di adeguata verifica e identificazione del cliente (commento alla normativa)*, in *Notariato*, n. 6, 2019, p. 600.

⁵⁵³ Le Disposizioni della Banca d'Italia del 2019 prevedono che nei gruppi bancari o finanziari disciplinati dagli artt. 60 e 109 del TUB e all'art. 11 del TUF, si assumono come stabilmente incardinate nell'organizzazione del destinatario le società del gruppo con sede in Italia alle quali viene esternalizzato l'adempimento degli obblighi di adeguata verifica.

organizzativa *lato sensu* intesi⁵⁵⁴. A tal proposito, il GAFI, nelle Raccomandazioni di febbraio 2012, ha chiarito che, affinché il soggetto possa essere considerato “terzo”, è necessario che egli applichi proprie procedure di adeguata verifica della clientela, non potendo eseguire tali adempimenti né “in nome e per conto” del soggetto obbligato e secondo le procedure da quest’ultimo elaborate, né sotto il suo controllo⁵⁵⁵. L’approccio sostanzialistico è confermato dalla nozione di “personale” data dall’art. 1, comma 2, lett. cc), del Decreto, che prescinde dalla sussistenza di un formale rapporto di lavoro subordinato per ritenere esistente l’inserimento del soggetto nell’organizzazione del destinatario⁵⁵⁶.

Inoltre è fatto espresso divieto ai soggetti obbligati di avvalersi di terzi aventi sede in Paesi terzi ad alto rischio (art. 29).

Ai sensi dell’art. 27, commi 1 e 2, affinché gli obblighi di adeguata verifica della clientela possano essere considerati validamente eseguiti dal terzo, è necessario che questi trasmetta al soggetto obbligato “*idonea attestazione*” di avervi personalmente e correttamente adempiuto. Non è pertanto consentito al terzo di avvalersi a sua volta di ulteriori soggetti per l’esecuzione degli obblighi, né tantomeno per la trasmissione della predetta attestazione⁵⁵⁷. Quest’ultima, inoltre, deve essere univocamente riconducibile al terzo e deve contenere la conferma della coincidenza tra il cliente verificato e il soggetto a cui l’attestazione si riferisce. Ciò riguarda solamente il contenuto minimo dell’attestazione⁵⁵⁸ il cui oggetto varia a seconda dello specifico obbligo di adeguata verifica cui essa è diretta, potendo così contenere i dati identificativi, l’indicazione delle tipologie delle fonti utilizzate per l’accertamento e la verifica dell’identità e, a seconda dei casi, anche le informazioni sulla natura e sullo scopo del rapporto da instaurare o dell’operazione occasionale da eseguire⁵⁵⁹. L’art. 27, comma 3, demanda alle Autorità di vigilanza di settore l’individuazione di idonee forme e modalità di attestazione. A questo proposito, le Disposizioni della Banca d’Italia del 2019 prevedono che il destinatario possa predisporre una specifica modulistica per il rilascio delle attestazioni, che può avvenire tanto in forma cartacea quanto tramite sistemi informatici⁵⁶⁰. Oltre alla trasmissione dell’attestazione, il terzo deve anche mettere a disposizione del destinatario “*le informazioni richieste in occasione dell’adempimento degli obblighi*” e, su richiesta del soggetto obbligato, deve trasmettere senza ritardo le copie dei documenti acquisiti (art. 27, comma 3).

Nonostante gli illustrati compiti incombenti sul terzo, la responsabilità per la corretta esecuzione degli obblighi di adeguata verifica permane in capo al soggetto obbligato parte del rapporto, unico destinatario della normativa antiriciclaggio⁵⁶¹. Il principio di responsabilità è previsto, anzitutto, dalla quarta direttiva che, al considerando n. 36, prevede che “*la responsabilità in merito alla conformità alla presente direttiva spetti in primo luogo al soggetto obbligato*”⁵⁶² e, all’art. 25, che “*il soggetto obbligato che ricorre a terzi mantiene la responsabilità finale dell’assolvimento di tali obblighi*”. Il D.lgs. 231/2007 conferma tale impostazione. Invero, oltre all’incipit dell’art. 26 (“*ferma restando la responsabilità dei soggetti obbligati*”), l’art. 28 statuisce la responsabilità dei soggetti obbligati, precisandone i confini. Lungi dal costituire

⁵⁵⁴ Cfr. S. Galmarini (a cura di), *Antiriciclaggio*, cit., p. 341.

⁵⁵⁵ Cfr. FATF Recommendation February 2012, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, p. 79: “*the third party will usually have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This can be contrasted with an outsourcing/ agency scenario, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution’s control of the effective implementation of those procedures by the outsourced entity*”.

⁵⁵⁶ Cfr. M. Catenacci, *L’esternalizzazione degli obblighi di adeguata verifica della clientela da parte di intermediari bancari e finanziari*, 2018, in dirittobancario.it, p. 11.

⁵⁵⁷ Le Disposizioni della Banca d’Italia del 2019 espressamente escludono che l’attestazione possa essere trasmessa dal cliente.

⁵⁵⁸ S. Galmarini (a cura di), *Antiriciclaggio*, cit., p. 340.

⁵⁵⁹ M. Carbone, P. Bianchi e V. Vallefucio, *Le nuove regole antiriciclaggio*, cit., p. 629, nota 117.

⁵⁶⁰ A tal proposito, “il soggetto obbligato e il terzo devono disciplinare all’interno dell’accordo di esternalizzazione le modalità di attestazione delle informazioni raccolte da quest’ultimo [...] al fine di assicurarne la coerenza” con quelle attinenti agli obblighi di adeguata verifica non esternalizzati e, pertanto, raccolte dal soggetto obbligato. Così, M. Catenacci, *L’esternalizzazione degli obblighi di adeguata verifica della clientela*, cit., p. 8.

⁵⁶¹ Ciò in coerenza con quanto disposto dall’art. 1228 c.c., in base al quale “*salva diversa volontà delle parti, il debitore che nell’adempimento dell’obbligazione si vale dell’opera di terzi, risponde anche dei fatti dolosi o colposi di costoro*”. In tal caso, però, il D.lgs. 231/2007 non sembra lasciare spazio alla “volontà delle parti” a fini derogativi.

⁵⁶² Quale naturale conseguenza del fatto che “gli obblighi AML/CFT applicabili a tali agenti o prestatori dei servizi esternalizzati in quanto spettanti ai soggetti obbligati, potrebbero derivare unicamente dal contratto tra le parti, e non dalla presente direttiva”.

una responsabilità di tipo oggettivo⁵⁶³, è richiesto al soggetto obbligato di valutare l'idoneità e la sufficienza degli elementi raccolti e delle verifiche effettuate dai terzi e di verificare, nei limiti della diligenza professionale, la veridicità dei documenti ricevuti. Benché il richiamo alla diligenza professionale sia riferito alla sola verifica della veridicità dei documenti, si può ritenere che anche in punto sufficienza e idoneità degli elementi raccolti e delle verifiche effettuate dal terzo si sia in presenza di una responsabilità di tipo soggettivo. Tale conclusione sembra essere suffragata dalle Disposizioni della Banca d'Italia del 2019, che orientano i soggetti obbligati verso un comportamento quanto più possibile prudente e diligente. Invero, mentre l'art. 28 prevede unicamente che, in caso di dubbio sull'identità del cliente, dell'esecutore o del titolare effettivo, il soggetto obbligato debba provvedere in proprio all'esecuzione degli obblighi di adeguata verifica, le Disposizioni della Banca d'Italia delineano una serie graduale di adempimenti da esperire, non solo in caso di dubbio, ma anche laddove il soggetto obbligato ritenga inidonea e insufficiente l'esecuzione degli obblighi da parte del terzo⁵⁶⁴. Oltre ad adempiere in via diretta agli obblighi oggetto di esternalizzazione, il soggetto, "*a seconda dei casi e delle circostanze*", dovrà informare il terzo, apportare rettifiche e integrazioni, astenersi dall'instaurare il rapporto o dall'eseguire l'operazione e valutare se trasmettere una segnalazione sospetta all'UIF.

Non si può fare a meno di notare che la quarta direttiva, da un lato, prevede che la responsabilità spetti "*in primo luogo*" al soggetto obbligato (cfr. considerando n. 36) e, dall'altro, qualifica la stessa come "*finale*" (cfr. art. 25)⁵⁶⁵. Tali precisazioni lasciano supporre che il terzo non vada comunque esente da qualsiasi tipo di responsabilità. Infatti, il trasferimento degli obblighi di adeguata verifica dal soggetto obbligato al terzo trova la sua fonte nell'accordo tra le parti (c.d. accordo di esternalizzazione), non discendendo dalla legge alcun obbligo del terzo di prestare la propria collaborazione. La violazione dell'accordo determina pertanto l'insorgenza di forme di responsabilità per mancato o inesatto adempimento (cfr. art. 1218 c.c.) con conseguente obbligo al risarcimento del danno (cfr. art. 1223 ss. c.c.)⁵⁶⁶. Pertanto, si ritiene che il soggetto obbligato responsabile della corretta esecuzione degli obblighi di adeguata verifica ai sensi dell'art. 56 del D.lgs. 231/2007, potrà agire in regresso verso il terzo laddove – e nella misura in cui – questi abbia agito con dolo o colpa.

7. L'astensione (R. Tiberi)

All'obbligo di astensione è dedicato l'art. 42, col quale comincia e si esaurisce l'intero Capo IV, Titolo II⁵⁶⁷, del D.lgs. 231 del 2007. Detta norma impone ai soggetti obbligati di astenersi dall'instaurazione o prosecuzione del rapporto, ovvero dall'esecuzione di un'operazione o prestazione professionale, qualora non possano espletare l'adeguata verifica della clientela ai sensi dell'art. 19, comma 1, lett. a), b) e c), e cioè: identificare o verificare le generalità del cliente, dell'esecutore e del titolare effettivo, ovvero conseguire le dovute informazioni sullo scopo o natura del rapporto continuativo o della prestazione professionale. Giova al riguardo sottolineare come tale impossibilità prescinda del tutto dalle capacità organizzative del soggetto obbligato, essendo concepita come oggettiva⁵⁶⁸.

⁵⁶³ In tal senso, v. Cass. sent. n. 28823 del 30 novembre 2017.

⁵⁶⁴ Cfr. Disposizioni della Banca d'Italia del 2019, p. 27: "*Il destinatario [...] valuta se gli elementi raccolti e le verifiche effettuate dai soggetti terzi siano aggiornati, idonei e sufficienti per l'assolvimento degli obblighi previsti dalla legge*".

⁵⁶⁵ Le locuzioni riportate sono presenti anche nelle versioni originali in inglese ("*ultimate responsibility*"; "*the responsibility [...] should remain primarily with the obliged entity*") e francese ("*responsabilité finale*"; "*La responsabilité [...] devrait donc continuer d'incomber principalement à l'entité assujettie*").

⁵⁶⁶ V. M. Catenacci, *L'esternalizzazione degli obblighi di adeguata verifica della clientela*, cit., p. 9.

⁵⁶⁷ A seguito delle modifiche introdotte dal D.lgs. 25 maggio 2017, n. 90. L'impianto previgente disciplinava l'obbligo di astensione all'art. 23.

⁵⁶⁸ In tal senso, può essere utile anche un raffronto testuale col previgente art. 23, comma 1: "*Quando gli enti o le persone soggetti al presente decreto non sono in grado di rispettare gli obblighi di adeguata verifica della clientela*". Analoga formulazione risulta tuttora presente nei Regolamenti di attuazione Consob (Delibera n. 20570 del 4 settembre 2018, art. 29) e IVASS (n. 44 del 12 febbraio 2019, art. 42), rispettivamente per i revisori legali e le imprese di assicurazione.

A seguito dell'astensione il soggetto obbligato, valutata la presenza delle condizioni necessarie, procede con l'inoltro di una segnalazione di operazioni sospette a norma dell'art. 35, D.lgs. 231/2007.

Non esiste una corrispondenza automatica fra astensione e trasmissione di una S.O.S., giacché mentre la prima consiste in un atto dovuto (pur conseguente all'impossibilità di espletare l'adeguata verifica), la seconda è frutto dei processi valutativi posti in essere dai soggetti obbligati e della discrezionalità loro concessa, sulla base del c.d. *risk based approach*. Solo attraverso un'adeguata conoscenza del cliente, del suo profilo soggettivo, è possibile comprendere se l'operatività richiesta o concretamente posta in essere sia incoerente, inusuale o illogica e come tale suscettibile di essere segnalata.

La disposizione in esame, di derivazione comunitaria⁵⁶⁹, corrisponde alla Raccomandazione GAFI n. 10 e attribuisce agli operatori qualificati il compito di presidiare l'accesso al sistema finanziario⁵⁷⁰, per impedire che soggetti non adeguatamente noti vi introducano disponibilità di incerta provenienza⁵⁷¹. Ciò vale anche per il comma seguente, il quale introduce un obbligo ancor più stringente: tale disposizione impone infatti ai soggetti obbligati di astenersi dall'operare, ovvero di porre fine al rapporto o prestazione già in essere, ove risultino esserne parte (direttamente o indirettamente) società fiduciarie, *trust*, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio⁵⁷². Al fine di evitare la persistenza di coni d'ombra, il legislatore ha voluto specificare che dette misure si applicano anche nei confronti delle ulteriori entità giuridiche altrimenti denominate, aventi sede nei paesi in questione, di cui non sia possibile identificare il titolare effettivo e verificarne l'identità (art. 42, comma 2, ultimo periodo)⁵⁷³. A differenza dell'obbligo enucleato al comma 1, condizionato all'oggettiva impossibilità di condurre in concreto l'adeguata verifica, l'astensione imposta dall'art. 42, comma 2, si riferisce a specifiche categorie di clienti e incide sull'autonomia negoziale dei soggetti obbligati, i quali non possono intrattenere qualsiasi tipo di relazione di natura economica o professionale nelle situazioni ivi descritte. Questa considerazione, pur restando valida per entrambe le fattispecie esaminate dalla norma, deve assumere tuttavia sfumature diverse per ciascun caso.

E difatti, per società fiduciarie, *trust*, società anonime o controllate attraverso azioni al portatore, trattandosi di entità strutturalmente caratterizzate da opacità degli assetti proprietari, il legislatore ha presunto l'impossibilità di individuarne il titolare effettivo e verificarne l'identità, se collocate in giurisdizioni non cooperative. Detta presunzione, assoluta e incondizionata, impone l'astensione quand'anche la partecipazione di tali soggetti sia solamente indiretta. Diversamente sembra potersi dire per la categoria residuale enucleata nell'ultimo periodo dell'art. 42, comma 2: con riferimento alle "ulteriori entità giuridiche altrimenti denominate", infatti, l'obbligo di astensione è esplicitamente subordinato all'impossibilità concreta di individuarne il titolare effettivo e verificarne l'identità, attraverso procedure di adeguata verifica rafforzata⁵⁷⁴.

L'astensione non consiste in un obbligo inderogabile, anzi: specifiche eccezioni sono enucleate nei successivi e ultimi due commi dell'art. 42. Innanzi tutto, i professionisti citati nel comma terzo ne sono esonerati limitatamente ai casi in cui esaminano la posizione giuridica del loro cliente o espletano compiti di difesa o di rappresentanza dello stesso in un procedimento innanzi a un'Autorità giudiziaria o in

⁵⁶⁹ Art. 24 della quarta direttiva antiriciclaggio.

⁵⁷⁰ Un'applicazione distorta dell'obbligo di astensione può accentuare la tendenza al c.d. *de-risking*, definito già dal GAFI (Plenaria del 23 ottobre 2014) come il fenomeno in base al quale i destinatari degli obblighi di collaborazione, anziché gestire il rischio di riciclaggio e finanziamento del terrorismo, ritengono preferibile evitarlo del tutto, ponendo termine ai rapporti con intere fasce di clientela. È evidente che un abuso di questo strumento possa incidere su diritti costituzionalmente garantiti, in particolare sulla libertà di iniziativa economica privata (art. 41 Cost.). Per garantire il migliore equilibrio possibile fra simili istanze e la prevenzione dei fenomeni di riciclaggio, l'EBA ha emanato nuovi Orientamenti (EBA/GL/2021/02, del 1 marzo 2021), relativi ai fattori di rischio per l'adeguata verifica. L'applicazione delle linee guida è stata quindi disposta dalla Banca d'Italia con nota n. 15 del 4 ottobre 2021.

⁵⁷¹ È appena il caso di osservare come il GAFI, nella nota interpretativa alla citata Raccomandazione n. 10 (par. 3 - 4), faccia espressamente prevalere le esigenze investigative sopra quelle di adeguata verifica del cliente (CDD), sollecitando di considerare l'astensione dal compimento dell'adeguata verifica ove questa possa, allertando il cliente, pregiudicare gli approfondimenti di intelligence. L'art. 17, comma 2, del D.lgs. 231/2007 impone invece "*in ogni caso*" ai soggetti obbligati il completamento dell'adeguata verifica, anche in presenza di sospetto di riciclaggio o finanziamento del terrorismo, "*indipendentemente da qualsiasi deroga, esenzione o soglia applicabile*".

⁵⁷² Cfr. art. 1, comma 2, lett. bb), del D.lgs. 231/2007.

⁵⁷³ La disposizione ha riprodotto e abrogato l'art. 28, comma 7-ter, del previgente D.lgs. 231/2007, in base al quale il Ministro dell'Economia e delle finanze doveva individuare, con decreto, sentito il Comitato di sicurezza finanziaria, una black list di Paesi in ragione del rischio di riciclaggio o di finanziamento del terrorismo ovvero della mancanza di adeguati scambi di informazioni anche in materia fiscale. Decreto peraltro mai emanato, con la conseguenza che la disciplina in questione non aveva mai trovato effettiva applicazione.

⁵⁷⁴ Procedure imposte, stante la ricorrenza dei requisiti di cui all'art. 24, comma 1, D.lgs. 231/2007. Cfr. M. Carbone, P. Bianchi e V. Vallefucio, *Le nuove regole antiriciclaggio*, cit., p. 601 s.

relazione a tale procedimento, ivi compresa la consulenza sull'eventualità di intentarlo o evitarlo⁵⁷⁵. Pare evidente che, in questo caso, il legislatore abbia voluto salvaguardare le esigenze defensionali garantite, ad ogni livello, dall'ordinamento nazionale e sovranazionale⁵⁷⁶.

Inoltre in base all'art. 42, comma 4, è fatta salva l'applicazione dell'art. 35, comma 2, nei casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto: in tal caso i soggetti obbligati, ricevuto l'atto o eseguita l'operazione, ne informano immediatamente la UIF⁵⁷⁷. L'obbligo di ricevere l'atto, essendo previsto da specifica disposizione di legge, prevale sull'astensione imposta ai sensi del Decreto Antiriciclaggio, senza naturalmente incidere sul successivo inoltro di una segnalazione di operazioni sospette. Infine, non è stata riproposta la norma sulla restituzione dei fondi nei casi di impossibilità di completare l'adeguata verifica della clientela, che introdotta nel vecchio art. 23, comma 1-*bis* aveva creato non poche criticità di applicazione.

Occorre a questo punto soffermarsi brevemente su alcuni risvolti applicativi della disciplina, compiutamente esaminata, dell'art. 42 D.lgs. 231/2007. L'obbligo di astensione ivi delineato, conseguente all'impossibilità di eseguire l'adeguata verifica, non rileva soltanto ai fini delle esigenze di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo, ma può altresì incidere su rapporti in corso di esecuzione fra soggetti obbligati e clienti. Detti rapporti sono disciplinati dal diritto privato: la decisione del destinatario degli obblighi antiriciclaggio di astenersi e interrompere un rapporto in corso va correttamente qualificata dal punto di vista civilistico, al fine di valutarne le conseguenze anche sotto il profilo del risarcimento dell'eventuale danno patito dal cliente. In giurisprudenza l'adempimento dell'obbligo di porre fine al rapporto continuativo o alla prestazione professionale è stato quindi inquadrato negli schemi del recesso privatistico.

Pronunciatosi al riguardo, il Tribunale di Trieste⁵⁷⁸ ha ritenuto che, in presenza delle circostanze indicate dalla legge, il recesso dell'intermediario dai rapporti in corso è insindacabile, in quanto atto dovuto⁵⁷⁹. Nel caso di specie, una società di gestione del risparmio (SGR) aveva rappresentato al cliente la propria volontà di recedere dal contratto di gestione di portafogli, adducendo di non essere in grado di rispettare gli obblighi di adeguata verifica⁵⁸⁰.

Sotto il profilo del risarcimento del danno, riteneva il giudice di primo grado che, col recesso dal contratto di gestione di portafoglio, l'intermediario non è più legittimato a compiere atti di gestione sul patrimonio del cliente e, in caso di successiva liquidazione dei titoli, si realizza una prosecuzione della gestione in eccesso di potere rappresentativo (art. 1398 c.c.) o gestorio (art. 1711 c.c.), che dà luogo a responsabilità del gerente e al conseguente risarcimento del danno. In tale ammontare, tuttavia, non va incluso ciò che il creditore (cliente) avrebbe potuto evitare usando l'ordinaria diligenza ai sensi dell'art. 1227 c.c.

Pur confermando il dispositivo di primo grado, la Corte d'Appello constatava in diritto che, venuto meno il rapporto contrattuale per effetto del recesso dell'intermediario, quest'ultimo si era limitato alla liquidazione del controvalore economico degli strumenti finanziari. D'altra parte, ha precisato la Suprema Corte⁵⁸¹ che il recesso dal contratto consegue, in tali casi, all'osservanza di un obbligo di legge: qualora le disponibilità, anziché essere liquidate, fossero state trasferite ad un altro intermediario (come richiesto dal cliente), il rapporto anziché essere cessato sarebbe illegittimamente proseguito. Le specifiche previsioni di legge debbono quindi prevalere sia sulle norme regolamentari che su quelle contrattuali, dipendano quest'ultime da appositi accordi oppure dalla disciplina generale del contratto di mandato. Dunque non è la violazione contrattuale ad essere in questione, bensì la correttezza della condotta dell'intermediario a cui i predetti obblighi di legge sono imposti.

⁵⁷⁵ Cfr. S. Galmarini (a cura di), *Antiriciclaggio*, cit., p. 542 ss.

⁵⁷⁶ L'art. 24 della Carta fondamentale sancisce l'inviolabilità del diritto alla difesa. Esso è inoltre tutelato dalla Carta di Nizza (divenuta diritto primario comunitario), nonché dall'art. 6 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU).

⁵⁷⁷ Cfr. anche M. Carbone, P. Bianchi e V. Vallefucio, *Le nuove regole antiriciclaggio*, cit., p. 602.

⁵⁷⁸ Sentenza del 2 gennaio 2012, confermata dalla Corte d'Appello triestina in data 15 maggio 2013. Al riguardo, cfr. la nota di A. Barbazza, *L'obbligo di customer due diligence ed il recesso dal contratto ai sensi dell'art. 23 D.lgs. 231/2007*, in Banca e Borsa 2013, 2, II, pp. 413-432.

⁵⁷⁹ I giudici attribuiscono agli intermediari il ruolo di "gatekeepers dell'integrità del sistema finanziario". Questa funzione di sorveglianza, postulato fondamentale dell'approccio basato sul rischio, poggia proprio sullo strumento dell'astensione. Nell'azione preventiva di contrasto al riciclaggio, l'adeguata verifica è ritenuta un aspetto primario dal legislatore e, ove l'intermediario reputi di non riuscire a svolgere adeguatamente la *due diligence*, ha l'obbligo di non instaurare il rapporto, ovvero di porvi fine ove esso sia già in corso, operando il recesso.

⁵⁸⁰ Ai sensi del (vigente *ratione temporis*) art. 23 del D.lgs. 231/2007.

⁵⁸¹ Cass. civ., Sez. I, sent. 25/08/2017, n. 20393.

8. Gli obblighi di conservazione (P. Bianchi)

Gli obblighi di conservazione rappresentano uno dei tre pilastri su cui si poggia la normativa in materia di prevenzione e contrasto al riciclaggio e finanziamento del terrorismo. Essi perseguono diverse finalità: innanzitutto i dati e le informazioni conservati a fini AML/CFT devono facilitare l'attività di indagine, agevolando l'individuazione e l'acquisizione di prove documentali per rafforzare ipotesi investigative nel corso di procedimenti penali. Riferimenti normativi in tale senso si trovano nelle raccomandazioni emanate dal FATF/GAFI⁵⁸² nonché nelle direttive comunitarie in materia⁵⁸³. In particolare, l'obbligo di conservare dati e informazioni a fini di indagine è stato previsto già nella direttiva 91/308/CEE all'art. 4, la cui locuzione è stata sostanzialmente riproposta nelle Direttive emanate negli anni successivi⁵⁸⁴. Nell'ordinamento nazionale le stesse finalità erano riportate all'art. 36, comma 1, del D.lgs. 231/2007 di recepimento della direttiva 2005/60/UE (c.d. terza direttiva), segnatamente, previgente al recepimento della quarta e quinta direttiva 2005/60/UE⁵⁸⁵. Le attuali previsioni in materia di conservazione dopo il recepimento della quarta e quinta direttiva (Titolo II, Capo II, artt. da 31 a 34), non contengono più tale riferimento; cionondimeno si ritiene che tale finalità sia implicitamente riconosciuta in considerazione dalla stretta interrelazione esistente tra la normativa antiriciclaggio e l'attività di contrasto svolta dalle Autorità investigative.

Oltre alle finalità di indagine, i dati e le informazioni conservati in conformità alla normativa AML/CFT devono consentire all'Unità di Informazione Finanziaria per l'Italia (UIF) e alle altre Autorità competenti di svolgere analisi a supporto delle rispettive funzioni. Gli obblighi di conservazione sono pertanto strumentali alle attività di controllo, sia di natura cartolare sia ispettiva, svolte dalle Autorità di vigilanza di settore, dalla FIU nonché dalla Guardia di Finanza ovvero da altre Autorità dotate di poteri di controllo ai sensi del D.lgs. 231/2007.

Oltre alle finalità espressamente previste dalla legge, i dati e le informazioni conservati a fini AML/CFT sono utilizzati anche dagli stessi soggetti destinatari in considerazione del legame strettamente funzionale all'adempimento degli obblighi di conservazione e di quelli di adeguata verifica e di segnalazione di operazioni sospette. Come è noto, l'articolazione del processo di adeguata verifica prevede l'obbligo di effettuare il controllo costante del rapporto con il cliente, per tutta la sua durata, attraverso il monitoraggio continuo – spesso attraverso strumenti informatici – della complessiva operatività posta in essere dal cliente medesimo. Tale controllo si estende, in funzione del rischio associato al cliente e all'operatività, anche alla verifica della provenienza dei fondi e delle risorse nella disponibilità del cliente sulla base di informazioni conservate dal soggetto destinatario in ragione dell'esercizio dell'attività istituzionale svolta. Ne consegue che, qualora dovessero emergere nel corso del controllo costante anomalie suscettibili di valutazione ai fini della collaborazione attiva sulla base dei dati e delle informazioni conservati ai sensi del decreto antiriciclaggio, gli obblighi in trattazione sono requisito fondamentale per un'efficace collaborazione.

8.1. Destinatari e contenuti degli obblighi di conservazione

Il D.lgs. 231/2007 estende gli obblighi di conservazione a tutti i soggetti indicati all'art. 3 del decreto medesimo⁵⁸⁶. L'unica eccezione riguarda gli intermediari indicati al comma 8 del citato articolo, ai quali si

⁵⁸² Raccomandazione n. 11.

⁵⁸³ Si fa riferimento all'art. 4 della direttiva 91/308/CEE, al considerando 15 della direttiva 2001/97/UE e all'art. 30 della direttiva 2005/60/UE. Le ultime due direttive, (UE) 2015/846 e (UE) 2018/843, hanno apportato limitate modifiche alle disposizioni in tema di conservazione o registrazione di dati e informazioni a fini AML/CFT.

⁵⁸⁴ Cfr. art. 4, direttiva 91/308/CEE.

⁵⁸⁵ L'art. 36, comma 1, del D.lgs. 231/2007, prima del recepimento delle Direttive (UE) 2015/846 e (UE) 2018/843, prevedeva che “i soggetti indicati negli articoli ... conservano i documenti e registrano le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo”. Nell'ordinamento nazionale, prima del recepimento della direttiva 2005/60/UE, si trovava un riferimento in tal senso all'art. 2 della legge n. 197/91.

⁵⁸⁶ Intermediari bancari e finanziari, altri operatori finanziari, professionisti, altri operatori non finanziari e prestatori di servizi di gioco. Gli obblighi di conservazione si applicano anche alle succursali insediate sul territorio nazionale dei medesimi soggetti aventi sede legale e amministrazione centrale in uno stato estero.

applicano esclusivamente gli obblighi di segnalazione di operazioni sospette e di trasmissione delle comunicazioni oggettive previsti agli artt. 35 e 47 del D.lgs. 231/2007. Tale categoria di soggetti include importanti operatori del sistema finanziario quali, ad esempio, Borsa Italiana Spa, Cassa compensazione e Garanzia Spa e Monte Titoli Spa.

Le modifiche introdotte con il D.lgs. 90/2017, di recepimento della direttiva (UE) 2015/846, hanno inciso profondamente sulla disciplina che regola gli obblighi di conservazione. Al fine di semplificare e razionalizzare il precedente quadro normativo in materia, sono previsti un set minimo di dati e informazioni ritenuti essenziali per adempiere agli obblighi di conservazione⁵⁸⁷ nonché alcuni requisiti di carattere generale che le modalità di conservazione utilizzate dai soggetti destinatari devono garantire per essere conformi alla normativa⁵⁸⁸.

Rispetto al precedente regime, non sono più previste disposizioni specifiche per tipologia di soggetti destinatari, fatta eccezione per la categoria dei notai, per la quale la legge indica espressamente i documenti ritenuti idonei per adempiere agli obblighi di conservazione⁵⁸⁹.

Con l'entrata in vigore del D.lgs. 90/2017 (4 luglio 2017), non sono più previsti obblighi di registrazione che imponevano dettagliate regole di archiviazione e di rappresentazione dei dati e delle informazioni in forma standardizzata nonché modalità specifiche di utilizzo dei medesimi. L'abolizione dei predetti obblighi di registrazione ha comportato l'eliminazione dell'obbligo di istituire e gestire anche l'Archivio Unico Informatico (in seguito AUI), modalità attraverso la quale gran parte dei soggetti destinatari assolvevano agli obblighi precedentemente in vigore⁵⁹⁰.

Con riferimento ai contenuti degli obblighi di conservazione, il D.lgs. 231/2007 stabilisce, come detto, un set minimo di dati e informazioni: deve essere conservata copia dei documenti acquisiti in fase di identificazione nonché, per quanto riguarda le operazioni, l'originale ovvero copia aventi efficacia probatoria ai sensi della normativa vigente delle relative scritture e registrazioni. Al riguardo, si sottolinea che l'abolizione dell'obbligo di registrazione nell'AUI ha fatto venir meno l'importo soglia di 15.000 euro oltre il quale scattava il predetto obbligo per operazioni di importo pari o superiore a tale soglia, indipendentemente dal fatto che si tratti di un'operazione unica o di più operazioni collegate o frazionate.

L'art. 31, comma 2, D.lgs. 231/2007 indica i dati e le informazioni ritenuti rilevanti ai fini degli obblighi di conservazione. Alle lett. da a) a d) viene stabilito che la documentazione conservata deve consentire, quanto meno, di ricostruire in modo univoco: la data di instaurazione del rapporto continuativo o del conferimento dell'incarico⁵⁹¹; i dati identificativi del cliente, *“ivi compresi, ove disponibili, i dati ottenuti mediante i mezzi di identificazione elettronica e i pertinenti servizi fiduciari di cui al Regolamento UE n. 910/2014 o mediante procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale”*, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione⁵⁹²; la data, l'importo e la causale dell'operazione⁵⁹³; i mezzi di pagamento utilizzati⁵⁹⁴.

⁵⁸⁷ Art. 31, comma 2, del D.lgs. 231/2007.

⁵⁸⁸ Art. 32, comma 2, del D.lgs. 231/2007.

⁵⁸⁹ Ai sensi dell'art. 34, comma 2, del D.lgs. 231/2007, costituiscono idonee modalità di conservazione il fascicolo del cliente, con la custodia dei relativi documenti, attestazioni e atti, nonché la tenuta dei repertori notarili; completano le modalità di conservazione per i notai la descrizione dei mezzi di pagamento negli atti per garantire la tracciabilità dei flussi finanziari connessi con la stipula di atti notarili.

⁵⁹⁰ L'AUI è utilizzato dai principali intermediari bancari e finanziari, dalle società di revisione ex art. 161 del TUF, da operatori di gioco online nonché dalla Cassa Depositi e Prestiti Spa; per alcune categorie erano previste modalità semplificate di registrazione.

⁵⁹¹ Per la definizione di “rapporto continuativo” e di “conferimento di un incarico” si rinvia all'art. 1, comma 2 del D.lgs. 231/2007 rispettivamente alle lett. ll) e h).

⁵⁹² Per la definizione di “dati identificativi” si rinvia all'art. 1, comma 2, lett. n), del D.lgs. 231/2007, per la definizione di “cliente” alla lett. f), per la definizione “titolare effettivo” alla lett. pp) e per la definizione di “esecutore” alla lett. p). La parte in corsivo è stata introdotta con il decreto legislativo n. 125/2019, che ha introdotto all'art. 31, comma 2, del D.lgs. 231/2007 la lett. b-bis) relativa all'obbligo di conservare anche *“la consultazione ove effettuata dei registri di cui all'articolo 21, con le modalità ivi previste”* per verificare l'identità dei titolari effettivi. La comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, di persone giuridiche private, di trust produttivi di effetti giuridici rilevanti a fini fiscali e di istituti giuridici affini al trust sono stati regolamentati con il Decreto del Ministero dell'Economia e delle finanze dell'11 marzo 2022, n. 55.

⁵⁹³ Per la definizione di “operazione” si rinvia all'art. 1, comma 2, lett. t), del D.lgs. 231/2007.

⁵⁹⁴ Per la definizione di “mezzi di pagamento” si rinvia all'art. 1, comma 2, alla lett. s), del D.lgs. 231/2007.

8.2. Le modalità di conservazione e le disposizioni specifiche emanate dalle Autorità

Accanto al set minimo di dati e informazioni ritenuti essenziali per l'adempimento degli obblighi di conservazione, il D.lgs. 231/2007 detta numerose caratteristiche che le modalità e i sistemi di conservazione devono garantire⁵⁹⁵.

Per la finalità di consentire alle Autorità di svolgere le proprie attività di analisi e di controllo, i sistemi di conservazione devono innanzitutto garantire l'accessibilità completa e tempestiva ai dati e alle informazioni da parte del Ministero dell'Economia e delle finanze, della UIF, della Autorità di vigilanza di settore, della Direzione Investigativa Antimafia e della Guardia di finanza attraverso il Nucleo speciale di polizia valutaria.

Sotto il profilo tecnico, i sistemi adottati dai soggetti destinatari devono prevenire qualsiasi perdita dei dati e garantire la tracciabilità delle operazioni. Sotto il profilo organizzativo si chiede ai soggetti destinatari di individuare le persone fisiche legittimate ad alimentare il sistema di conservazione e accedere ai dati e alle informazioni ivi conservati.

I soggetti destinatari hanno 30 giorni di tempo dall'instaurazione, variazione o chiusura del rapporto continuativo o del conferimento dell'incarico per lo svolgimento della prestazione professionale ovvero dall'esecuzione dell'operazione per acquisire gli elementi nei sistemi di conservazione utilizzati.

Inoltre, i sistemi di conservazione devono garantire l'integrità e la non alterabilità dei dati e delle informazioni nonché la trasparenza, la completezza e la chiarezza dei medesimi; infine, i sistemi devono garantire il mantenimento della storicità per dieci anni dei dati e delle informazioni per consentire la ricostruibilità di una determinata posizione finanziaria.

Con riferimento alla normativa sulla *privacy*, i soggetti destinatari devono adottare sistemi di conservazione idonei a garantire il rispetto delle disposizioni dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità perseguite dalla normativa AML/CFT. Con il parere n. 150/2019 il Garante per la protezione dei dati personali ha ritenuto opportuno evidenziare alcuni aspetti rilevanti al fine di rendere il trattamento conforme a quanto stabilito con il regolamento (UE) 2016/679: le persone fisiche incaricate del trattamento dei dati personali devono essere individuate sulla base di elevati requisiti di affidabilità e competenza, preferibilmente tra persone con un rapporto stabile con il soggetto destinatario; tali incaricati devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del citato regolamento e garantisca la tutela dei diritti dell'interessato⁵⁹⁶; tenuto conto anche delle dimensioni del soggetto destinatario, devono essere adottati meccanismi di cifratura e di sicurezza finalizzati rispettivamente a proteggere le informazioni, ad assicurare l'integrità del contenuto e a prevenirne alterazioni⁵⁹⁷; l'accesso alle informazioni in tutte le fasi del trattamento, anche dopo la cifratura, deve essere circoscritto, per impostazione predefinita, ad un numero il più possibile limitato di persone sottoposte all'autorità del soggetto destinatario⁵⁹⁸; qualora i soggetti obbligati decidano di affidare la comunicazione a soggetti esterni, designati responsabili del trattamento o persone sottoposte all'autorità del titolare, i dati devono essere forniti loro già in modalità cifrata⁵⁹⁹.

Oltre alle norme di carattere generale previste dal D.lgs. 231/2007, le Autorità di vigilanza di settore, avvalendosi della facoltà prevista dall'art. 34, comma 3, del medesimo decreto, hanno adottato disposizioni specifiche per la conservazione e messa a disposizione dei documenti, dei dati e delle informazioni a fini AML/CFT.

La Consob, con Delibera n. 20570 del 4 settembre 2018, ha adottato il regolamento recante disposizioni di attuazione per i revisori legali. Per gli operatori del settore assicurativo, l'IVASS ha emanato il regolamento n. 44 del 12 febbraio 2019. Per gli intermediari bancari e finanziari sottoposti alla vigilanza della Banca d'Italia è stato adottato il provvedimento il 24 marzo 2020⁶⁰⁰. Quest'ultime disposizioni, in particolare, mirano a coniugare obiettivi di flessibilità e di riduzione dei costi per gli intermediari con l'obiettivo di garantire la disponibilità di dati e informazioni utili per consentire alla

⁵⁹⁵ Art. 32 del D.lgs. 231/2007.

⁵⁹⁶ Art. 28, par. 1, regolamento 2016/679 (GDPR).

⁵⁹⁷ Art. 32, regolamento 2016/679 (GDPR).

⁵⁹⁸ Art. 25, par. 2, regolamento 2016/679 (GDPR).

⁵⁹⁹ Artt. 28 e 29 del regolamento (UE) 2016/679 (GDPR) e art. 2-*quaterdecies* del D.lgs. 193/2006.

⁶⁰⁰ Il Provvedimento è stato pubblicato nella Gazzetta Ufficiale n. 89 il 3 aprile 2020.

Banca d'Italia e alla UIF di svolgere efficacemente le proprie funzioni. Il provvedimento prevede l'obbligo di rendere disponibili alcuni dati e informazioni ulteriori rispetto a quelli stabiliti dalla legge al fine di agevolare l'attività di controllo e di analisi senza comportare significativi costi aggiuntivi per gli intermediari. I soggetti vigilati già dispongono di questi dati e informazioni nei loro sistemi contabili, anagrafici e gestionali.

Le Disposizioni della Banca d'Italia mantengono fermi criteri uniformi e standardizzati in base ai quali gli intermediari devono rendere disponibili i dati e le informazioni per facilitare la ricostruibilità dell'operatività della clientela e per agevolare la tracciabilità dei flussi nel sistema finanziario. In tale contesto, i soggetti vigilati potranno scegliere tra due opzioni: 1) avvalersi di archivi standardizzati, tra cui anche l'AUI, che sarà alimentato secondo codici e *standard* consolidati in sostanziale continuità con le precedenti regole di registrazione. Questa opzione tiene conto della circostanza che gran parte del settore bancario e finanziario ha ammortizzato la spesa per la costituzione e la tenuta dell'AUI (in vigore dal 1993) e ritiene conveniente continuare a utilizzarlo per le finalità previste dalla legge. Tale scelta è conforme alla previsione legislativa che consente di dettare specifiche disposizioni per la conservazione in *"archivi informatizzati, ivi compresi quelli già istituiti presso i soggetti rispettivamente vigilati"*; 2) estrarre i dati dal sistema di conservazione di cui dispongono, inclusi i sistemi contabili-gestionali in uso, necessariamente informatizzati, senza l'obbligatorietà di istituire e gestire un archivio *ad hoc*, come l'AUI. Le estrazioni, tuttavia, devono essere fornite nel rispetto di specifiche tecniche e degli *standard* stabiliti dalle Disposizioni al fine di garantire schemi standardizzati e uniformi per non pregiudicare, come detto in precedenza, l'efficacia dell'azione di prevenzione e di contrasto da parte delle Autorità di controllo.

Tra le semplificazioni introdotte, fermo restando l'obbligo di conservazione previsto dalla legge, le Disposizioni della Banca d'Italia stabiliscono una soglia di importo unitario pari o superiore a euro 5.000 per la messa a disposizione di dati relativi alle operazioni; contestualmente sono state abolite le operazioni frazionate, risolvendo a monte le problematiche applicative sovente riscontrate per l'aggregazione delle transazioni rilevanti a fini del *"cumulo"*⁶⁰¹. Le Disposizioni sono corredate da quattro allegati che dettano gli *standard* tecnici e le compatibilità informatiche per l'estrazione di dati e informazioni dai sistemi gestionali ovvero per la registrazione nell'AUI nonché le codifiche per le causali analitiche delle operazioni e per le tipologie degli intermediari vigilati.

Per quanto concerne i professionisti – ad eccezione dei notai, per i quali, come detto, la legge ha stabilito quali sono le idonee modalità di conservazione – l'art. 11 del D.lgs. 231/2007 assegna agli organismi di autoregolamentazione delle singole categorie professionali la responsabilità di emanare specifiche regole in materia. Il Consiglio Nazionale Forense nonché il Consiglio Nazionale dei Dottori Commercialisti e degli esperti contabili hanno adottato rispettivamente il 20 settembre 2019 e 22 maggio 2019 apposite regole tecniche antiriciclaggio e linee guida. Completano il quadro le Regole Tecniche adottate dal Consiglio Nazionale dei Consulenti del Lavoro il 7 giugno 2022. A fini degli obblighi di conservazione è rimasta sostanzialmente invariata l'alternativa di mantenere un archivio formato e gestito a mezzo di strumenti informatici o predisporre un registro della clientela a fini antiriciclaggio in cui inserire i dati richiesti dalla legge che può essere gestito su base cartacea, informatica o mista.

Ai fini dell'obbligo di conservazione, assume particolare rilievo anche il fascicolo di studio, in particolare per gli avvocati e commercialisti, che documenta l'intervento del professionista nella sua interezza. Detto fascicolo tende a racchiudere sia l'attività professionale eseguita a fronte dell'incarico, e di conseguenza i dati riferibili all'operazione richiesta dalle parti, sia quella di adeguata verifica del cliente stesso inclusi i dati del titolare effettivo, e in particolare quella di approfondimento circa le effettive volontà manifestate del cliente.

Per gli altri operatori non finanziari, categoria composta da soggetti con operatività altamente diversificata, in assenza di rinvii a regolamentazioni attuative da parte di organismi di autoregolamentazione o di controllo, tra l'altro spesso assenti o difficilmente individuabili, si applicano le regole generali previste dal D.lgs. 231/2007.

La difficoltà per l'assolvimento degli obblighi di conservazione da parte di tale tipologia di operatori si cela sovente nella difficoltà di individuare e gestire in modo integrato ed efficace i dati e le informazioni rilevanti per le finalità perseguite dalla normativa AML/CFT. Per i soli operatori non finanziari che

⁶⁰¹ Anche nel previgente regime, le operazioni sotto i 5.000 euro non erano normalmente oggetto di registrazione, in quanto per prassi solo le operazioni al di sopra di questa soglia venivano rilevate ai fini della determinazione delle operazioni frazionate.

esercitano le attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'art. 134 TULPS, limitatamente all'attività di trattamento di banconote in euro, in presenza dell'iscrizione nell'elenco di cui all'art. 8 del DL 25 settembre 2001, n. 350, convertito, con modificazioni, dalla Legge 23 novembre 2001, n. 409, la Banca d'Italia ha adottato il Provvedimento del 23 aprile 2019, che tuttavia non contiene disposizioni specifiche per la conservazione dei dati e delle informazioni a fini AML/CFT.

8.3. *Gli utilizzi*

I dati e le informazioni conservati a fini AML/CFT, come detto, svolgono un importante ruolo per le analisi effettuate dalle Autorità sia in fase di controllo cartolare, segnatamente per lo sviluppo di metodi di analisi e di modelli per la valutazione del rischio, sia nel corso di accertamenti ispettivi. Sui medesimi dati e informazioni si basa l'invio alla UIF delle Segnalazioni Anti-Riciclaggio Aggregate (c.d. SARA)⁶⁰² nonché delle comunicazioni oggettive⁶⁰³.

Le norme relative agli obblighi di conservazione presentano, inoltre, collegamenti con la disciplina del c.d. monitoraggio fiscale prevista dal decreto-legge 28 giugno 1990, n. 167, convertito, con modificazioni, dalla legge 4 agosto 1990, n. 227. Secondo le disposizioni attuative dell'art. 1 del citato decreto-legge diffuse nel 2014, riguardanti le modalità e i termini di comunicazione all'Agenzia delle Entrate dei trasferimenti, anche attraverso movimentazione di conti, da o verso l'estero, di mezzi di pagamento, i soggetti destinatari potevano utilizzare le registrazioni nell'AUI, selezionando le pertinenti operazioni con l'estero. Con le modifiche introdotte dal D.lgs. 90/2017 che, come detto, ha abolito l'AUI, si è reso necessario un adeguamento delle norme in tema di monitoraggio fiscale. Tale adeguamento è avvenuto a opera dell'art. 16 del decreto-legge del 21 giugno 2022 n. 73⁶⁰⁴, che ha ridotto da 15.000 a 5.000 euro la soglia prevista per la trasmissione da parte degli intermediari all'Agenzia delle Entrate di specifici dati sulle operazioni di trasferimento da o verso l'estero e ha eliminato, allo stesso tempo, la necessità di ricostruire le operazioni frazionate.

I dati e le informazioni richiesti per adempiere agli obblighi di conservazione, infine, sono utilizzati anche dai soggetti destinatari per il monitoraggio dell'operatività della clientela nel continuo, strettamente funzionale al controllo costante richiesto nell'adempimento degli obblighi di adeguata verifica e particolarmente rilevante per un'efficace collaborazione attiva. In questo ambito si presentano le sfide maggiori per gli intermediari caratterizzati da un'operatività e da un'organizzazione complessa dove è particolarmente impegnativo individuare e gestire i dati e le informazioni necessari per l'osservanza degli obblighi AML/CFT.

Anche sotto la spinta della "liberalizzazione" delle regole di registrazione, introdotta con l'abolizione dell'AUI, gli obblighi di conservazione si presentano sempre di più ora come un tassello fondamentale per progettare e gestire gli strumenti informatici per la rilevazione di operazioni potenzialmente sospette e per i sistemi di controllo interno, in particolare per i controlli di linea, che spesso in passato si basavano sui dati registrati nell'archivio medesimo.

⁶⁰² Art. 33 D.lgs. 231/2007.

⁶⁰³ Art. 47 D.lgs. 231/2007.

⁶⁰⁴ Misure urgenti in materia di semplificazioni fiscali.

CAPITOLO 4

Segnalazione di operazioni sospette

(a cura di D. Muratti)

Premessa (D. Muratti e A. Tidu)

Nel sancire l'obbligo segnaletico, l'art. 35 del decreto antiriciclaggio ne indica anche i parametri di riferimento: da un lato, si pongono i destinatari della norma, intermediari finanziari, professionisti e altri operatori qualificati, ai quali è richiesto di enucleare in tempo reale – già prima di dare esecuzione all'operazione richiesta – il sospetto di riciclaggio o di finanziamento del terrorismo; dall'altro, si trova la UIF, alla quale il flusso segnaletico deve essere trasmesso tempestivamente per la successiva disseminazione alle altre autorità antiriciclaggio.

Nell'affermare la finalità di pubblico interesse della normativa antiriciclaggio, il legislatore ha dunque affidato il perseguimento di questo obiettivo all'interazione virtuosa tra settore privato – una platea di segnalanti vasta ed eterogenea – e pubbliche istituzioni; tramite questo innovativo sinallagma, si realizza lo scopo della norma, ovvero preservare il sistema finanziario dai possibili abusi, garantendone la sua primaria funzione di canale di scambio delle risorse economiche per finalità lecite, e, in ultima analisi, quella di fattore propulsivo dello sviluppo socio-economico del paese.

L'impianto della normativa di contrasto del riciclaggio e del terrorismo scaturisce dalle fonti internazionali ed è incentrato sul concetto di segnalazione di operazione sospetta, la cui rilevazione è affidata alla capacità dei segnalanti di individuare gli eventuali comportamenti criminogeni dei clienti/utenti e alla loro propensione alla collaborazione attiva. Si tratta di un'attività il cui valore aggiunto risiede nella valutazione e ponderazione degli elementi di rischio della clientela da parte dei *gate keeper* del sistema, ovvero un'ampia e diversificata platea di segnalanti, cui appartengono banche, intermediari finanziari e di pagamento, professionisti, aziende e imprese fornitrici di servizi, pubbliche amministrazioni.

Sul lato di chi riceve le SOS, si trovano le Financial Intelligence Units, ovvero gli *entry point* del flusso segnaletico; esse ne garantiscono la ricezione, la conservazione e la disseminazione con criteri di sicurezza e rapidità. Ciascuna FIU raccoglie, a livello nazionale, le informazioni antiriciclaggio dai diversi segnalanti e le concentra al fine di favorirne una valutazione omogenea e integrata, in grado di cogliere collegamenti soggettivi e oggettivi e dinamiche di rete, tracciare flussi finanziari anche oltre i confini nazionali, e di curarne la tempestiva e adeguata disseminazione alle altre autorità che condividono lo stesso obiettivo di salvaguardare gli scambi da utilizzi illeciti. Esse costituiscono una rete che, attraverso il reciproco scambio di informazioni, diffonde la conoscenza di tecniche innovative di riciclaggio, alcune con dimensioni transnazionali, e consente ai segnalanti di individuare prontamente le fattispecie connotate da maggior rischio.

La disponibilità di un ampio patrimonio informativo consente alla UIF di avere una visione integrata e di osservare alcune fenomenologie criminogene. Su questa base, vengono elaborati indicatori e schemi di anomalia, poi messi a disposizione dei segnalanti per orientarne e affinarne la capacità di enucleare le minacce e individuare le operatività sospette; oltre a garantire a tutti gli operatori lo stesso *level playing field*, la UIF contribuisce così anche ad innalzare la capacità dei destinatari della norma di cogliere fenomenologie che possono essere scarsamente visibili, soprattutto a un livello iniziale, consentendone la pronta individuazione.

Per l'invio delle SOS la UIF ha messo a disposizione dei segnalanti un apposito canale informatico, riservato e protetto, cui fanno ricorso non solo al momento della trasmissione delle SOS, ma anche in occasione dei successivi contatti per le analisi e gli approfondimenti, come previsto dal comma 6 dell'art. 38 del decreto antiriciclaggio. Anche l'interlocuzione con la rete estera delle FIU e con l'autorità

giudiziaria, nonché la disseminazione verso gli Organi investigativi, avviene con modalità analoghe. L'imputazione diretta dei dati, tra l'altro, determina l'aggiornamento in tempo reale degli archivi della UIF e gli alert di rischio, elevando la capacità di individuazione dei contesti maggiormente pericolosi e l'efficienza complessiva del sistema.

L'andamento del flusso segnaletico nel tempo risulta in forte crescita; si è passati dalle 14.602 SOS del 2008, primo anno di attività della UIF, alle 139.524 del 2021. Le segnalazioni ricevute dalla UIF scaturiscono in massima parte dal sospetto di riciclaggio, mentre quelle connesse al finanziamento del terrorismo e dei programmi di proliferazione di armi di distruzione di massa rimangono tuttora contenute. Le SOS che ora pervengono alla UIF contengono molti dati e informazioni; questo fattore, unito alla complessità dei contesti rappresentati, indica che il sistema dei segnalanti è in grado di individuare le fattispecie a maggior rischio. Significativo, in tal senso, il salto quali-quantitativo nella serie storica delle SOS avvenuto alla fine della prima decade del 2000. Esso coincide con due eventi rilevanti; da un lato, l'entrata in funzione dell'applicativo RADAR (Raccolta e Analisi Dati AntiRiciclaggio) su piattaforma Infostat-UIF, rilasciato dalla UIF nel maggio del 2011 per la ricezione delle SOS e la loro disseminazione agli OO.II., dall'altro la definitiva adozione di un approccio *risk based* da parte dei segnalanti.

Ne è risultato un flusso segnaletico più elevato e tempestivo, con un numero di operazioni e una quantità di informazioni nettamente superiori. La disponibilità di informazioni strutturate, rese in un formato che ne consente l'elaborazione con applicativi di calcolo avanzati, ha conferito al patrimonio informativo un'ulteriore valenza; da un lato, esso ha consentito di evidenziare collegamenti che sarebbero altrimenti rimasti solo impliciti, dall'altro, esso fornisce alla UIF una base più ampia di valutazione in occasione dell'esame dei casi di sospensione delle segnalazioni di operazioni sospette, aumentando, così, la capacità di intercettare i casi a maggior rischio e di potenziare la funzione di prevenzione.

La gestione di un flusso segnaletico in continua crescita ed evoluzione rappresenta una vera sfida per la struttura e richiede il costante adeguamento della capacità di selezione, prioritizzazione e analisi delle informazioni; la diffusione del fin-tech, il crescente ricorso a strumenti alternativi come le valute virtuali, richiedono studio e strumenti di analisi adeguati per l'individuazione del rischio e il rafforzamento delle misure di prevenzione. Nuove prospettive e plessi informativi più articolati, talvolta frammentati ma riconducibili a medesimi perimetri di attività, richiedono una più spiccata flessibilità nell'approccio analitico e un più ampio impiego di strumenti di analisi che siano nel contempo alternativi e integrativi dei precedenti; è in questo contesto che si colloca il ricorso alle tecniche di analisi aggregata, che viene utilizzata per riconciliare un elevato numero di informazioni spesso parcellizzate in un numero elevato di segnalazioni, al fine di far emergere un centro di imputazione centrale.

La UIF, infine, è innervata in un apparato di prevenzione costituito da una pluralità di attori, che hanno ruoli, competenze e professionalità distinte ma convergenti verso gli stessi interessi generali, al quale essa apporta, oltre al patrimonio che scaturisce dall'analisi delle SOS, anche il valore aggiunto che deriva dall'appartenenza a una rete internazionale di istituzioni consimili; lo sviluppo di adeguati meccanismi di cooperazione con tutte le autorità del sistema, e in particolare con quelle attive nel contrasto alla criminalità organizzata rappresenta un fondamentale fattore di successo dell'intera filiera.

1. La segnalazione di operazioni sospette (D. Muratti)

Oltre agli obblighi di adeguata verifica e di conservazione della documentazione, i soggetti individuati nell'art. 3 hanno anche l'obbligo di individuare e segnalare le operazioni sospette di riciclaggio e di terrorismo; infatti l'art. 35 del D.lgs. 231 del 2007 prevede la comunicazione alla UIF delle operazioni della specie, quando essi "sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa".

La norma, che riproduce una struttura lessicale già adottata dalla normativa europea, introduce, quindi, una graduazione della consapevolezza alla base della segnalazione, dal momento che accanto ai due diversi gradi di giudizio ordinari - il "sapere" e il "sospettare" - che fanno riferimento alla maggiore o minore consapevolezza del segnalante circa la probabilità che si sia stata compiuta o tentata un'operazione di riciclaggio o di finanziamento del terrorismo, viene richiamata anche la sussistenza di "motivi ragionevoli per sospettare". Ci si soffermerà di seguito su quest'ultimo concetto per elaborare un ragionamento sul grado di consapevolezza richiesto per l'effettuazione di una segnalazione alla UIF,

rimandando, per il concetto di sapere e sospettare ai numerosi commenti presenti in letteratura⁶⁰⁵.

La formulazione che indica i “motivi ragionevoli per sospettare” quale presupposto per l’attività segnaletica può giustificare un’interpretazione estensiva degli obblighi segnaletici e porsi quale ulteriore grado di giudizio, un *tertium genus* distinto e aggiuntivo al sapere o al sospettare, al quale il destinatario degli obblighi di collaborazione attiva può far ricorso nel caso di un’operazione sulla quale ha valutato la mera possibilità di connessione a riciclaggio, e effettui comunque la segnalazione pur avendone un livello di consapevolezza minimale, che confina quasi con il “non poter escludere”⁶⁰⁶.

L’applicazione del principio dei motivi ragionevoli di sospetto potrebbe ampliare la portata dell’obbligo previsto dall’art. 35, poiché renderebbe possibile inviare una segnalazione all’UIF anche solo in presenza di una mera anomalia e in difetto di una sia pur minimale consapevolezza di un sospetto di riciclaggio, e potrebbe fare emergere nuove fenomenologie che potrebbero formare oggetto di segnalazione alla UIF, fermo restando che il flusso segnaletico basato esclusivamente sui “motivi ragionevoli per sospettare” risulterebbe incentrato su *alert* basilari, e produrrebbe segnalazioni tendenzialmente oggettive, ovvero fondate su elementi di mera anomalia e non già sulla rilevazione di un sospetto in base alla valutazione dell’insieme di elementi oggettivi e soggettivi, e nemmeno sulla coerenza tra il profilo soggettivo, le transazioni poste in essere dal cliente, la natura delle controparti. Si verificherebbe, quindi, l’ipotesi in cui il destinatario degli obblighi segnaletici non sa né sospetta l’esistenza concreta del riciclaggio in base alla valutazione fattuale di una serie di indicatori, ma effettua la segnalazione solamente in base a uno o due elementi che potrebbero indicare lo svolgimento potenziale di attività di riciclaggio.

In applicazione di questo principio, quindi, le segnalazioni verrebbero inoltrate alla filiera dei controlli antiriciclaggio solo sulla base di una mera anomalia, senza alcun riferimento alla valutazione di coerenza con il profilo soggettivo e con le prassi operative seguite dal cliente fino a quel momento; il rischio è che il contenuto informativo di simili segnalazioni sia tendenzialmente oggettivo e privo di elementi discriminanti del rischio, in assenza dei quali i sistemi di selezione, classificazione e valutazione delle autorità antiriciclaggio potrebbero non essere sufficienti a definire la complessiva rischiosità del contesto segnalato.

È ciò che potrebbe accadere se sistemi automatizzati di screening antiriciclaggio venissero adottati dai segnalanti senza gli opportuni accorgimenti valutativi volti a filtrare gli alert, valorizzando quelli più rilevanti e scartando quelli che non restituiscono esiti di rischiosità sufficienti a tradursi in una segnalazione di operazione sospetta; in mancanza di una valutazione di merito, quindi, il flusso segnaletico può aumentare in misura esponenziale senza poter essere opportunamente classificato in base al rischio effettivo. In una simile prospettiva, risulta evidente quanto il rischio di perdita di efficacia del sistema possa diventare concreto, trasformando gli iniziali risparmi dovuti al ricorso a sistemi automatizzati di selezione delle SOS in un costo effettivo dell’intera filiera.

Sulla necessità che il segnalante agisca in base a una gradazione di consapevolezza si è espressa anche la giurisprudenza, secondo la quale la segnalazione delle operazioni sospette non è subordinata alla creazione di un quadro indiziario di riciclaggio da parte del segnalante, né all’affermazione – del tutto personale – di estraneità dell’operazione a un’attività delittuosa. La segnalazione dovrebbe essere subordinata, invece, soltanto a un giudizio puramente tecnico di valutazione degli elementi oggettivi e soggettivi che caratterizzano le operazioni individuate⁶⁰⁷.

L’indicazione giurisprudenziale è stata recepita anche nelle istruzioni che la UIF ha emanato sul contenuto delle segnalazioni di operazioni sospette, laddove è precisato che i segnalanti sono chiamati a fornire un’accurata e completa rappresentazione delle operazioni e dei soggetti, fornendo una valutazione compiuta ed esplicita dei motivi del sospetto⁶⁰⁸.

Coerentemente con questa impostazione che valorizza un approccio valutativo sostanziale, il comma 1 dell’art. 35 fornisce un’indicazione di massima del percorso analitico da compiere per desumere il sospetto, che deve essere collegato a motivi sia oggettivi sia soggettivi. Interessante notare come il richiamo della norma ad alcune caratteristiche del soggetto che dispone le operazioni osservate richieda una conoscenza del medesimo che presuppone lo svolgimento di un iter di adeguata verifica dinamico e

⁶⁰⁵ Sul sospetto di riciclaggio e sull’obbligo di segnalazione cfr. L. Criscuolo, *La normativa antiriciclaggio in Italia a seguito del recepimento della III direttiva comunitaria*, in E. Cappa e U. Morera (a cura di), *Normativa antiriciclaggio e segnalazione di operazioni sospette*, Bologna 2008. p. 13 ss. Numerosi sono poi i commenti espressi dalla dottrina, specie nell’ambito di convegni e incontri formativi.

⁶⁰⁶ Sull’ammissibilità della prova basata sul grado di consapevolezza minimo o su evidenze scientifiche e induttive si veda l’interessante intervento di G. Canzio *Prova scientifica, ricerca della “verità” e decisione giudiziaria nel processo penale*, reperibile in <http://www.progettoinnocenti.it/>, che rinvia alla più significativa letteratura sul tema.

⁶⁰⁷ Cfr. Cass., sez. II, 18 aprile 2007, n. 9312.

⁶⁰⁸ Cfr. *Rapporto annuale della UIF per il 2011*, pp. 27-28.

costantemente aggiornato, al fine di rendere possibile una compiuta valutazione di coerenza sull'operatività del segnalato, sulle sue controparti, sugli importi e sugli strumenti utilizzati per il suo sviluppo.

Un secondo aspetto da sottolineare è legato alla tempestività della segnalazione: l'attuale formulazione della norma contiene espliciti riferimenti al riguardo, poiché indica che la segnalazione debba essere inviata alla UIF "prima di compiere l'operazione" e "senza ritardo". La perentorietà di questa formulazione trova completamente nel secondo comma dello stesso art. 35, laddove i segnalanti sono invitati a non compiere l'operazione finché non hanno effettuato la segnalazione e nell'obbligo di astensione previsto dall'art. 42 nel caso in cui non sia possibile completare l'adeguata verifica della clientela o in presenza di elementi di opacità che non rendono chiaro il contesto operativo di riferimento⁶⁰⁹.

Solo nel caso in cui l'operazione debba necessariamente essere eseguita, la segnalazione può essere fatta alla sua conclusione⁶¹⁰. Questa previsione mitiga il taglio iniziale della norma e lo rende più concretamente applicabile, nella misura in cui contempla casi quali la sussistenza di un obbligo di legge a ricevere un atto ovvero i casi in cui il differimento dell'operazione possa ostacolare le indagini ovvero in alcuni casi – ormai invero frequenti – in cui le transazioni si concludono in tempo reale (ad esempio gli *Instant Payments*). Ovviamente, una volta eseguita la transazione, l'obbligo segnaletico rimane del tutto valido e deve avvenire in tempi estremamente contenuti.

La norma, quindi, rafforza la funzione preventiva della segnalazione antiriciclaggio e antiterrorismo e cerca di anticiparne la genesi disancorandola dalla mera fase esecutiva e di realizzazione del reato presupposto per riferirne la valenza all'intero *iter criminis*, che comprende anche le fasi di ideazione e di preparazione del disegno criminale. Ciò trova conferma nella locuzione utilizzata nel primo comma dell'art. 35 e riferita alle operazioni anche solo tentate – e quindi non perfezionate – che devono ugualmente essere segnalate alla UIF laddove sollevino sospetti di riciclaggio o di terrorismo. Per agevolare il processo segnaletico, il comma 4 dello stesso art. 35 afferma che *le comunicazioni delle informazioni, effettuate in buona fede dai soggetti obbligati, dai loro dipendenti o amministratori ai fini della segnalazione di operazioni sospette [...] non comportano responsabilità di alcun tipo anche nelle ipotesi in cui colui che le effettua non sia a conoscenza dell'attività criminosa sottostante e a prescindere dal fatto che l'attività illegale sia stata realizzata*.

Più in generale, il comma 4 dell'art. 35 stabilisce che le informazioni fornite con le segnalazioni di operazioni sospette non costituiscono violazione di obblighi di riservatezza, sia pur imposti *in sede contrattuale o da disposizioni legislative, regolamentari o amministrative*, purché, ovviamente, persista il presupposto della buona fede. L'obbligo segnaletico diventa, in tal modo, cogente per tutte le categorie di segnalanti, con l'unica eccezione per i professionisti, per i quali vige un principio di esenzione a comunicare le informazioni acquisite nell'ambito dell'esercizio del diritto di difesa. Il comma 5 dell'art. in commento, prevede infatti che l'obbligo di segnalazione delle operazioni sospette non si applica ai professionisti per le informazioni che essi ricevono *da un loro cliente o ottengono riguardo allo stesso nel corso dell'esame della posizione giuridica o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso*. La norma precisa meticolosamente il perimetro dell'esenzione, ma resta tuttavia difficile, nella pratica quotidiana, riuscire a distinguere la tipologia e la destinazione delle informazioni raccolte.

Come già documentato nel presente volume, ai fini dell'adempimento dell'obbligo di segnalazione delle operazioni sospette, costituiscono riciclaggio non le condotte penalmente rilevanti descritte dall'art. 648-*bis* del c.p., ma un novero di azioni previste dall'art. 2 del D.lgs. 231/2007. Esse rappresentano la c.d. nozione amministrativa del riciclaggio, che rispetto a quella avente rilevanza penale di cui all'art. 648-*bis*

⁶⁰⁹ In sede di modifica del D.lgs. 231/2007 era stato previsto che anche il termine di 30 giorni dalla transazione sospetta per l'assolvimento dell'obbligo segnaletico. La proposta, rimossa a seguito di un acceso dibattito, si sarebbe posta in aperta contraddizione con la possibilità, frequente nei fatti, che il sospetto può emergere anche a distanza temporale superiore ai trenta giorni dallo svolgimento della transazione; ciò avrebbe indotto i segnalanti a una posizione difensiva e all'invio di segnalazioni destituite di una completa valutazione di sospetto e soltanto ancorate alla mera ricorrenza di deboli alert di anomalia, peraltro nemmeno sempre verificabili.

⁶¹⁰ È questo il caso, tra l'altro, dei notai, che non possono rifiutare di compiere l'atto che viene loro richiesto di formalizzare.

c.p., si caratterizza per la maggiore ampiezza nella definizione delle condotte e nell'individuazione dei presupposti oggettivi e soggettivi in presenza dei quali dovrebbe scattare l'obbligo di segnalazione delle operazioni sospette⁶¹¹. Inoltre, la conoscenza, l'intenzione o la finalità, che debbono costituire un elemento di tali atti, possono essere dedotte da circostanze di fatto obiettive.

L'art. 35 non fornisce indicazioni sulle fenomenologie a maggior rischio di riciclaggio, lasciando a ciascun segnalante il compito di organizzare metodi e procedure per l'emersione del sospetto, tranne che per il contante, considerato indicatore di rischio elevato di riciclaggio, a prescindere dal segno delle operazioni poste in essere e dagli importi movimentati. Si legge, infatti nella parte finale dell'art. 35 che *il ricorso frequente o ingiustificato ad operazioni in contante, anche se non eccedenti la soglia di cui all'articolo 49 e, in particolare, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente, costituisce elemento di sospetto*. Secondo il legislatore, quindi, anche nel caso del contante, per il quale viene comunque prevista una soglia di utilizzo dall'art. 49, non esistono automatismi segnaletici, essendo, invece, necessario valutare la coerenza delle transazioni in contante in relazione al profilo di rischio del cliente.

Gli obblighi segnaletici si estendono anche alle fattispecie relative al finanziamento del terrorismo o alla produzione e commercio di armi di distruzione di massa. Per finanziamento del terrorismo si intende qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali, indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette. Molto più delicata la definizione del sospetto nelle transazioni finalizzate alla produzione o al commercio di armi di distruzione di massa; quello che viene intercettato dagli intermediari riguarda la compravendita di componentistica che potrebbe essere anche utilizzata a scopi industriali non collegati alla produzione di armi (*dual use*); rilevante, in questi contesti, la conoscenza del cliente (solitamente persona non fisica) e delle sue controparti commerciali usuali, come pure un costante aggiornamento in merito alle misure internazionali volte a sanzionare tali attività.

In conclusione, l'art. 35 impone ai segnalanti l'obbligo di segnalazione di operazioni sospette che, come già argomentato altrove, non costituisce una denuncia di reato, ma una forma di cooperazione doverosa richiesta a soggetti dotati di conoscenze in grado di agevolare l'accertamento di eventuali illeciti penali, con l'unica eccezione dei professionisti che non sono tenuti alla segnalazione di operazioni sospette la cui notizia sia stata acquisita nell'esercizio del diritto di difesa dell'imputato.

Lo stesso articolo prevede che la segnalazione sia fatta tempestivamente, quando si ha il fondato sospetto della sussistenza di operazioni di riciclaggio o di finanziamento del terrorismo ovvero della provenienza dei fondi da attività criminose, indipendentemente dalla loro entità.

Il riferimento alla provenienza da attività criminose, che di per sé comporta un allargamento delle ipotesi di illecito da sottoporre a valutazione, viene in qualche modo ridimensionato dalla necessità di verificare anche la sussistenza di una specifica finalità dissimulativa di tale origine dei beni o l'intento di aiutare chiunque sia coinvolto nell'attività criminosa, affinché si sottragga alle conseguenze giuridiche delle proprie azioni, rilevabile anche in base a circostanze di fatto obiettive (cfr. art. 2, comma 4, del D.lgs. 231/2007).

2. L'emersione del sospetto e le procedure di segnalazione (A. Monaco)

L'art. 36, comma 1, prevede che i destinatari degli obblighi antiriciclaggio pongano in essere un'organizzazione – calibrata in modo coerente con le scelte organizzative aziendali – e processi atti alla rilevazione del sospetto, e che si possano anche avvalere di strumenti informatici e telematici. In particolare, la norma prescrive che strumenti e procedure siano atte non solo a consentire la rapida enucleazione del sospetto, ma che siano anche in grado di mantenere evidenza del tracciato di analisi e di soddisfare gli obblighi di conservazione dei dati e delle informazioni raccolti e analizzati nell'ambito dell'istruttoria segnaletica, sia che la segnalazione venga inviata, sia che venga scartata e mantenuta agli atti. Tale passaggio risulta essenziale non soltanto in un'ottica di *accountability* del processo segnaletico, ma anche per consentire alla UIF di svolgere ogni approfondimento, senza contare che i contesti scartati in

⁶¹¹ In tal senso anche U. Morera, *Sul sospetto di riciclaggio e sull'obbligo di segnalazione*, in E. Cappa e U. Morera (a cura di), *Normativa antiriciclaggio*, cit., p. 118.

quanto privi di elementi sufficienti di sospetto potrebbero essere rivalutati a seguito di successive transazioni ed evidenze⁶¹².

È interessante sottolineare che i commi 2 e 3 dello stesso articolo forniscono, altresì, indicazioni – invero piuttosto dettagliate – volte a instaurare una dialettica interna all’intermediario; in particolare, infatti, il comma 2 prevede che le segnalazioni che siano scaturite in un qualunque *“punto operativo, unità organizzativa, o struttura”*, accentrato o decentrato che sia, *“cui compete l’amministrazione e la gestione concreta dei rapporti con la clientela”*, devono essere comunicate *“senza ritardo al titolare della competente funzione [ndr antiriciclaggio] o al legale rappresentante o ad altro soggetto all’uopo delegato”*.

Da questa disposizione si evincono altre due indicazioni: da un lato, la comunicazione interna deve essere tempestiva (*“senza ritardo”*); dall’altro è necessario che gli strumenti di emersione dei sospetti siano disponibili alle articolazioni operative dell’intermediario che gestiscono *“concretamente”* i rapporti con la clientela. Gli elementi tipici della dialettica amministrativa interna sono, quindi, ben richiamati da questa sorta di *four eyes principle* che prende avvio nel punto più prossimo al cliente (ovvero grava su chi meglio è in grado di conoscere le scelte e i comportamenti del cliente stesso), al fine di garantire l’affinamento dei motivi del sospetto e, in ultima analisi, al completamento dell’istruttoria della segnalazione di operazione sospetta.

Non v’è dubbio che anche il ricorso a strumenti informatici e telematici, richiamati nel primo comma, può contribuire a rendere più cogente la previsione, nella misura in cui essi consentono la trasmissione dei rilievi all’interno del segnalante in modo rapido, ma soprattutto sicuro e protetto.

Le previsioni mirano a stimolare una risposta omogenea, sia pure nel rispetto dell’autonomia aziendale di ciascun intermediario, e trovano completamento in quanto sancito dall’art. 38, comma 6, che impone ai segnalanti di utilizzare canali telematici per trasmettere alla UIF le segnalazioni di operazioni sospette e ogni altra documentazione prodotta a integrazione delle medesime, *“con modalità idonee a garantire la tutela della riservatezza, la riferibilità della trasmissione dei dati ai soli soggetti interessati, nonché l’integrità delle informazioni trasmesse”*. In ossequio a questa previsione, nel 2011 la UIF ha messo a disposizione dei segnalanti il portale internet Infostat-UIF⁶¹³, al quale essi possono accedere previa registrazione e abilitazione⁶¹⁴.

L’introduzione del nuovo schema segnaletico ha accelerato il processo di informatizzazione delle procedure antiriciclaggio presso i segnalanti; si è quindi osservato un notevole incremento del numero di segnalazioni pervenute alla UIF che, nel 2021 si sono attestate a quasi 140.000 (a fronte delle circa 50.000 del 2011). A tale tendenza, nell’ultimo triennio si è affiancato anche un evidente aumento della complessità dei contenuti, che si è tradotto in una maggiore ricchezza informativa in termini di soggetti, operazioni e rapporti contenuti in media in ciascuna segnalazione⁶¹⁵.

La tendenza descritta sembra derivare dall’utilizzo, specie presso i primari intermediari bancari, di nuovi e più sofisticati meccanismi di individuazione delle anomalie che, sostituendosi ovvero affiancandosi ai tradizionali sistemi di monitoraggio, consentono di individuare (e quindi trasporre all’interno delle SOS) contesti complessi di operatività sospetta, caratterizzati dal coinvolgimento di molteplici entità (soggetti, rapporti e operazioni). Tali nuovi meccanismi sono probabilmente basati anche sull’applicazione di tecniche informatiche avanzate che permettono di trattare l’enorme mole di informazioni a disposizione.

L’introduzione di sistemi avanzati di rilevamento delle anomalie presso i soggetti obbligati presenta indubbi aspetti positivi derivanti, in particolare, dalla capacità di intercettare fenomeni e schemi operativi difficilmente individuabili con gli strumenti tradizionali, ampliando la possibilità di comprendere il ruolo svolto dai diversi soggetti coinvolti nell’operatività,

⁶¹² La norma si riferisce agli intermediari bancari e finanziari, agli altri operatori finanziari e alle società di gestione degli strumenti finanziari già citati all’art. 3, comma 8.

⁶¹³ A partire da gennaio 2020 lo stesso portale viene utilizzato per inviare le richieste di informazioni e recepire le relative risposte nell’ambito degli approfondimenti svolti dalla UIF sulle SOS pervenute. Tali modalità di scambio informativo assicurano la tutela della riservatezza e l’integrità delle informazioni.

⁶¹⁴ L’iscrizione prevede una prima fase di registrazione al portale e una seconda fase di richiesta di autorizzazione alla trasmissione delle segnalazioni mediante la compilazione e l’invio a mezzo posta elettronica certificata di un modulo di adesione. Le abilitazioni per l’accesso al portale sono rilasciate, di regola, entro alcuni giorni lavorativi a partire dalla ricezione del modulo. Le informazioni di dettaglio sulle procedure di registrazione e la relativa documentazione di supporto sono disponibili in un’apposita sezione del sito della UIF (<https://uif.bancaditalia.it/portale-infostat-uif/modalita-accesso/index.html>).

⁶¹⁵ Nel 2019, a fronte di 106 mila segnalazioni, erano stati segnalati alla UIF circa 500 mila soggetti (in media 4,7 per ogni SOS), mentre nel 2021, in relazione a 140 mila segnalazioni, i soggetti segnalati si sono attestati a oltre 1 milione e 300 mila (9,6 per segnalazione) facendo segnare un aumento di oltre il 170%. Il trend è confermato anche guardando al numero di operazioni segnalate (+215%) e, di conseguenza, di rapporti finanziari coinvolti nell’operatività sospetta (+135%).

soprattutto in contesti specifici che ben si prestano a metodologie di analisi aggregata dei flussi. A fronte di ciò non va, tuttavia, sottaciuto che l'utilizzo di una più spinta automazione nella delicata fase di individuazione delle anomalie espone gli intermediari bancari a rischi che vanno adeguatamente gestiti e presidiati.

Da un lato, infatti, è necessario un costante aggiornamento della base di calcolo dei sistemi automatizzati; non sempre, infatti, i dati utilizzati per il training degli algoritmi sono di qualità adeguata e talvolta essi potrebbero essere superati dall'acquisizione di nuove informazioni o di nuove fenomenologie. È altresì necessario che i menzionati algoritmi non presentino difetti di trasparenza rispetto alle motivazioni e alle modalità con cui sono selezionate le fattispecie sospette. I citati rischi potrebbero tradursi in una non piena comprensione dei meccanismi di funzionamento degli algoritmi da parte degli stessi addetti all'area antiriciclaggio dei soggetti obbligati e, di conseguenza, riflettersi sulla qualità del flusso segnaletico inviato alla UIF.

Anche assicurando il più attento presidio degli algoritmi, inoltre, occorre evitare il rischio che la loro applicazione possa soppiantare in gran parte l'elemento valutativo umano; questi sistemi avanzati, in altri termini, non possono portare a produrre flussi segnaletici "oggettivi", ovvero segnalazioni prodotte quasi automaticamente e senza alcuna forma di "validazione" del sospetto da parte della funzione antiriciclaggio. Il maggior apporto di tale sistema dovrebbe piuttosto contribuire all'emersione di fenomenologie innovative, o di fattori di anomalia legati a controparti o operazioni, alla graduazione del rischio di riciclaggio, ovvero a fornire alla funzione antiriciclaggio elementi di valutazione atti a produrre segnalazioni più mirate, con valutazioni di rischio più commisurate e più idonee a orientare le successive analisi.

La descritta evoluzione del contesto di riferimento in termini di mole e complessità delle informazioni a disposizione rende sempre più urgente il ricorso, da parte delle autorità competenti per l'analisi delle segnalazioni, a strumenti avanzati di approfondimento. Un approccio più avanzato richiede il ricorso a metodi e applicativi di *social network analysis*, per far emergere le connessioni e le logiche di rete tra soggetti, operazioni e rapporti; altrettanto necessari sono i sistemi automatici di valutazione del rischio e di classificazione mediante la combinazione di tecniche rule-based e di machine learning.

L'introduzione di tali meccanismi di analisi non può prescindere da interventi sulle modalità di acquisizione del flusso segnaletico; potrebbe, quindi, essere necessario apportare modifiche all'attuale schema segnaletico al fine di renderlo quanto più possibile aderente alle peculiarità delle diverse categorie di soggetti obbligati (sulla falsariga di quanto già fatto per gli operatori dei comparti dei money transfer, delle carte di pagamento, dei giochi o delle valute virtuali) nonché per adeguarlo ai vistosi cambiamenti registrati nell'operatività negli ultimi anni (si pensi, ad esempio, alla crescita dell'operatività bancaria/finanziaria a distanza, anche mediante l'utilizzo di smartphone e app). L'eventuale revisione dello schema segnaletico, inoltre, dovrebbe tener conto anche delle specifiche esigenze di organizzazione dei dati sottese all'utilizzo dei sopra menzionati strumenti avanzati di analisi (anche in termini di aumento dei dettagli informativi contenuti nelle SOS).

Una ulteriore linea di intervento potrebbe riguardare la qualità delle segnalazioni che deve essere innalzata per consentire la progettazione di efficaci strumenti automatici di ausilio all'analisi, alla classificazione e alla prioritizzazione delle SOS. L'attuale andamento delle SOS, incrementate nel numero e nella complessità, infatti, rende ancor più importante lo scrupoloso rispetto da parte dei soggetti obbligati delle istruzioni di compilazione emanate dalla UIF per consentire una efficace attività di approfondimento del contenuto delle segnalazioni da parte delle autorità preposte. Miglioramenti in questo campo potrebbero essere ottenuti ottimizzando i controlli che presiedono alla validazione delle SOS prima della loro acquisizione nel sistema nonché avviando iniziative volte alla riduzione degli oneri segnaletici in capo ai soggetti obbligati ovvero finalizzate a supportarli nella corretta compilazione delle segnalazioni⁶¹⁶.

3. Il modello segnaletico (R. Marzano)

Il contenuto e le modalità di trasmissione delle segnalazioni sono disciplinati dalle *Istruzioni sui dati e le informazioni da inserire nelle segnalazioni di operazioni sospette*⁶¹⁷, emanate dalla UIF il 4 maggio 2011, anno in cui l'intero processo di segnalazione ha subito un profondo mutamento grazie all'adozione di uno schema segnaletico uniforme per tutti i segnalanti, provvisto di un maggior numero di informazioni in forma strutturata, e all'introduzione, per l'acquisizione delle segnalazioni, di un canale telematico basato sulla rete Internet, in grado di sfruttarne la diffusione capillare e i più recenti protocolli di sicurezza; esso, quindi, si compone di entità obbligatorie che confluiscono in elementi testuali e descrittivi e in campi strutturati, e di altre opzionali, ovvero di informazioni aggiuntive che il segnalante può decidere di fornire a sua discrezione sotto forma di allegati.

⁶¹⁶ In questa direzione va la pubblicazione, a febbraio 2022, da parte della UIF dei "casi d'uso", un documento contenente indicazioni pratiche di carattere generale per la corretta compilazione delle SOS nonché esempi concreti relativi a specifiche casistiche ricorrenti (il documento è stato pubblicato sul sito internet della UIF al link https://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/casi_d_uso.pdf).

⁶¹⁷ Cfr. <https://uif.bancaditalia.it/normativa/norm-antiricic/provv-2011-05-04/index.html>.

Nel corso degli anni le modalità di compilazione della SOS si sono evolute per tenere conto delle caratteristiche dell'operatività di alcuni soggetti obbligati (operatori dei comparti dei money transfer, delle carte di pagamento, dei giochi o delle valute virtuali). Per tali categorie di utenti, le cui segnalazioni sono tipicamente caratterizzate da un elevato numero di elementi, sono stati introdotti strumenti di ausilio alla compilazione per caricare automaticamente sul Portale dati presenti in file in un formato .csv estratti direttamente dai propri sistemi gestionali, riducendo così l'onere di digitazione e inserendo in un modello segnaletico piuttosto rigido un grado di flessibilità che rende possibile accogliere le segnalazioni che dovessero provenire da segnalanti attivi in settori innovativi.

Come detto, una segnalazione si compone di diverse sezioni informative: una sezione c.d. strutturata, in cui ciascuna informazione è riportata nel corrispondente campo dello schema segnaletico secondo le codifiche previste; una sezione liberamente editabile, in cui il segnalante descrive in forma testuale l'operatività osservata e i motivi del sospetto; una sezione dedicata all'inserimento di documentazione di supporto, nei formati previsti.

La sezione strutturata assume un ruolo di particolare importanza per le successive attività di analisi finanziaria: le segnalazioni in ingresso sono sottoposte a diversi processi di pre-elaborazione automatica, basati prevalentemente su dati strutturati, volti a integrare le nuove informazioni con gli elementi già presenti nelle basi dati a disposizione dell'Unità, in modo da poter ridefinire e ampliare il contesto segnalato, identificare soggetti e relazioni, ricostruire i flussi finanziari sottostanti all'operatività descritta.

La componente strutturata comprende, oltre a informazioni di carattere generale utili alla classificazione della segnalazione⁶¹⁸, una scheda specifica per ogni entità coinvolta nell'operatività: operazioni, soggetti, rapporti, nonché i legami che intercorrono tra le stesse. Ai fini della trasmissione della segnalazione è richiesto che siano indicati almeno un'operazione classificata come sospetta e almeno un soggetto collegato all'operazione con il relativo legame; in base alle caratteristiche di tali entità sono poi richiesti obbligatoriamente ulteriori elementi⁶¹⁹.

Nella scheda relativa all'operazione è possibile inserire sia transazioni di natura finanziaria, sia prestazioni professionali o di natura non finanziaria, nell'ambito delle quali il segnalante ha riscontrato l'operatività sospetta oggetto di segnalazione. Quando un'operazione si accompagna a una movimentazione di risorse economiche è richiesto di specificare lo strumento finanziario attraverso il quale è stata effettuata la transazione, in modo da agevolare la UIF nel tracciamento dei fondi movimentati. Per ciascuna operazione segnalata è necessario indicare tutti i soggetti a vario titolo coinvolti, compilando, per ciascuno di essi, un'apposita scheda in cui, oltre ai dati necessari all'identificazione, occorre anche fornire una valutazione in merito al livello di rischio soggettivo. Se presenti, dovranno altresì essere indicati i dati identificativi dei rapporti coinvolti nell'operazione. A seconda della tipologia di operazione è richiesto di specificare i dati dei rapporti finanziari su cui transitano le movimentazioni di denaro, le prestazioni professionali erogate ai soggetti segnalati oppure informazioni relative a rapporti accessi in ambiti non finanziari⁶²⁰. Infine, per consentire un'accurata ricostruzione delle transazioni, occorre descrivere tutte le relazioni che intercorrono tra le diverse entità in gioco, inserendo il legame esistente; in particolare è richiesto che ciascun soggetto e ciascun rapporto sia collegato con almeno un'operazione attraverso un legame diretto oppure indiretto. Il corretto inserimento dei legami è essenziale per l'utilizzo di moderne tecniche di analisi basate su *social network analysis* (SNA), che consentono l'individuazione e l'approfondimento di reti finanziarie di elevata complessità, anche trasversali alle singole segnalazioni di operazioni sospette, e il riconoscimento, attraverso una visuale più ampia, di contesti rilevanti da sottoporre a ulteriori approfondimenti, quali ad esempio quelli riferiti a network criminali.

Per quanto riguarda le informazioni da fornire per ciascuna entità, nell'Allegato 2 delle *Istruzioni* è riportato l'elenco dei campi del tracciato segnaletico con la relativa descrizione e livello di obbligatorietà⁶²¹. In tale documento è altresì chiarito che i campi obbligatori rappresentano l'insieme *minimo* di dati da fornire per procedere tecnicamente alla trasmissione della segnalazione: resta fermo l'obbligo, in capo a ciascun segnalante, di fornire sempre *tutte* le informazioni in proprio possesso in merito alla casistica segnalata⁶²².

⁶¹⁸ A titolo esemplificativo: identificativi univoci, categoria (riciclaggio, terrorismo, ecc.), livello di rischio dell'operatività complessiva, elenco di eventuali fenomeni a cui è possibile ricondurre la casistica (selezionati tra gli indicatori di anomalia e i modelli e schemi rappresentativi di comportamenti anomali diffusi dalla UIF).

⁶¹⁹ A titolo esemplificativo, per le operazioni a valere su rapporti finanziari intestati a propri clienti, il segnalante è tenuto a inserire anche una scheda per indicare i dati del rapporto interessato.

⁶²⁰ A mero titolo esemplificativo: consulenze, amministrazioni fiduciarie di beni, polizze assicurative, conti di gioco, commercio di oro e oggetti preziosi, portafogli di valute virtuali.

⁶²¹ Obbligatorio, facoltativo oppure condizionato. I campi condizionati sono campi normalmente facoltativi, ma che diventano obbligatori al ricorrere di alcune circostanze, specificate sempre nell'Allegato 2.

⁶²² Per adattare lo schema segnaletico alle caratteristiche specifiche di ciascuna categoria di soggetti obbligati, solo un numero ristretto di campi è stato classificato come obbligatorio ai fini della trasmissione della segnalazione: tuttavia, ove noti, il segnalante deve obbligatoriamente valorizzare anche i campi definiti facoltativi o condizionati all'interno dello schema segnaletico.

L'individuazione delle casistiche da portare all'attenzione della UIF è un processo delicato che richiede al segnalante l'acquisizione di tutte le informazioni necessarie alla valutazione del livello di rischio insito nell'operatività della clientela. Il ricorso a strumenti di rilevazione automatica può costituire un ausilio per il segnalante che, tuttavia, non può limitarsi alla mera attivazione di algoritmi automatici: per contribuire in maniera efficace all'impianto antiriciclaggio è necessaria un'attenta fase di valutazione, volta a discernere consapevolmente gli elementi di anomalia, valutandone la rilevanza ai fini della segnalazione.

3.1. Le segnalazioni dei professionisti (ruolo degli ordini professionali)

L'art. 11 del D.lgs. 231/2007 sottolinea il ruolo svolto, nel sistema antiriciclaggio, dagli Ordini professionali che *“promuovono e controllano l'osservanza degli obblighi previsti dal presente decreto da parte dei professionisti iscritti nei propri albi ed elenchi”* anche attraverso iniziative formative e l'emanazione di regole tecniche in materia di procedure e metodologie di analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo cui i professionisti sono esposti nell'esercizio della propria attività. L'art. 11 prevede anche che gli organismi di autoregolamentazione possano fungere da tramite tra la UIF e i propri associati per quanto riguarda la segnalazione di operazioni sospette: ciascun professionista può scegliere se aderire al sistema della UIF e trasmettere la segnalazione direttamente all'Unità oppure avvalersi del supporto dell'Ordine per trasmettere la segnalazione in forma anonima.

In questo secondo caso il professionista non si registra al sistema anagrafico della UIF, ma inoltra la segnalazione al proprio Ordine professionale attraverso modalità di scambio stabilite dall'ordine stesso. Quest'ultimo poi trasmette la segnalazione, priva del nominativo del professionista, utilizzando il Portale UIF. Anche eventuali scambi di informazioni successivi, che dovessero rendersi necessari durante la fase di approfondimento della segnalazione, sono sempre intermediati dall'Ordine in modo che la UIF non abbia alcun contatto diretto con il professionista.

Gli organismi di autoregolamentazione che possono ricevere le segnalazioni per il successivo inoltro alla UIF sono individuati con un apposito decreto del Ministro dell'Economia e delle Finanze. Successivamente tali organismi stipulano un protocollo d'intesa con la UIF per concordare le modalità di canalizzazione dei flussi e i presidi a tutela della riservatezza dei professionisti. A oggi gli Ordini abilitati a interporre tra i rispettivi iscritti e la UIF sono il Consiglio Nazionale del Notariato, il Consiglio Nazionale dei Consulenti del Lavoro e il Consiglio Nazionale dell'ordine dei Dottori Commercialisti e degli Esperti Contabili.

4. Indicatori e schemi di anomalia (L. La Rocca)

Le operazioni sospette che i destinatari degli obblighi antiriciclaggio sono tenuti a segnalare alla UIF sono individuate sulla base dei criteri – invero generali – elencati nell'art. 35, comma 1, del D.lgs. 231/2007, inerenti ai connotati oggettivi delle operazioni (caratteristiche, entità e natura), al profilo del soggetto coinvolto (capacità economica e attività svolta) e a ogni altra circostanza conosciuta dai medesimi destinatari, in ragione delle funzioni esercitate⁶²³.

Rispetto a tale ampio precetto, gli indicatori di anomalia rappresentano una fonte secondaria integrativa prevista dal decreto antiriciclaggio, al fine di agevolare l'individuazione delle operazioni sospette e, conseguentemente, ridurre i margini di incertezza connessi alle valutazioni soggettive e ai comportamenti discrezionali dei destinatari, assicurando il contenimento degli oneri e il corretto e omogeneo adempimento dell'obbligo di segnalazione⁶²⁴.

⁶²³ L'art. 35, comma 1, del D.lgs. 231/2007 fornisce un'indicazione specifica di ciò che costituisce elemento di sospetto solo in relazione a taluni utilizzi di contante e, in particolare, con riguardo al ricorso frequente o ingiustificato a operazioni in contante, anche se non eccedenti la soglia di cui all'art. 49 del D.lgs. 231/2007 e al prelievo o al versamento in contante di importi non coerenti con il profilo di rischio del cliente. Si veda anche L. Criscuolo e L. La Rocca, *La nuova nozione di operazione sospetta*, in G. Castaldi e C. Conforti (a cura di), *Manuale antiriciclaggio*, cit., p. 228 e ss.

⁶²⁴ Cfr. il citato art. 35, comma 1, del D.lgs. 231/2007. Si veda anche l'art. 3, comma 2, dei provvedimenti recanti indicatori di anomalia citati. L'emanazione e l'aggiornamento degli indicatori è stabilita dall'art. 6, comma 4, lett. e), del D.lgs. 231/2007, il quale dispone anche che gli indicatori di anomalia sono pubblicati dalla UIF nella Gazzetta Ufficiale della Repubblica italiana e in apposita sezione del proprio sito istituzionale.

Ai predetti indicatori si affiancano ulteriori strumenti complementari messi a disposizione dalla UIF su profili di anomalia intercettati nello svolgimento delle proprie attività di analisi e studio: modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario nonché le comunicazioni e le altre pubblicazioni⁶²⁵ rivolte dall'Unità ai segnalanti concorrono, infatti, a delineare l'insieme esemplificativo delle circostanze, in presenza delle quali il sistema di prevenzione AML/CFT richiede al destinatario di valutare se, a suo giudizio, ricorre un sospetto meritevole di segnalazione. Da questo punto di vista, le anomalie delineate negli indicatori e nelle altre pubblicazioni dell'Unità rappresentano esempi di situazioni che possono venire all'attenzione del destinatario degli obblighi antiriciclaggio, ma che in quanto tali non rappresentano "sospetti" suscettibili di segnalazione fino a quando il medesimo destinatario non avrà svolto gli approfondimenti e le valutazioni del caso in relazione agli elementi conoscitivi di cui dispone⁶²⁶.

Di seguito si fornirà una trattazione sintetica degli indicatori, degli schemi e delle comunicazioni della UIF⁶²⁷, delineandone le caratteristiche generali e avendo comunque presente che l'Unità sta svolgendo un lavoro di revisione integrale volto a far confluire in un atto normativo organico le casistiche rappresentate nel corso del tempo in provvedimenti indirizzati alle diverse categorie di destinatari, in alcuni schemi o modelli di comportamento anomalo e in varie comunicazioni; in coerenza con quanto sopra riportato sulla differenza tra "anomalia" e "sospetto", si coglie l'intento di chiedere ai segnalanti la rappresentazione di sospetti qualificati in modo chiaro e appropriato, correlando sempre i profili oggettivi e soggettivi cui fa cenno l'art. 35 del D.lgs. 231/2007 e descrivendo sempre le valutazioni compiute, anche quando esse muovono da procedure automatiche di selezione delle operatività individuate⁶²⁸.

È d'altra parte in via di definizione il negoziato sul c.d. *AML Package*, proposto dalla Commissione europea nel luglio del 2021, che accentuerà la convergenza delle discipline dei singoli Stati membri attraverso regolamenti di diretta applicazione e il consolidamento di un *rulebook* europeo completato da disposizioni secondarie⁶²⁹. In tale contesto verrà istituita un'agenzia europea con personalità giuridica, l'*Anti-Money Laundering Authority*, che agirà con compiti sovranazionali quale supervisore antiriciclaggio europeo e Meccanismo di supporto e coordinamento delle FIU e che avrà tra l'altro il compito di emanare e aggiornare indicatori di anomalia per i segnalanti, pur non essendo titolare di competenze dirette di analisi finanziaria e senza disporre di informazioni sulle segnalazioni di operazioni sospette⁶³⁰.

La UIF ha acquisito il potere di emanare direttamente gli indicatori di anomalia a seguito dell'entrata in vigore del D.lgs. 90/2017, che ha modificato il D.lgs. 231/2007. Prima del 2017, l'Unità aveva solo un potere di proposta degli indicatori⁶³¹, la cui emanazione era affidata – ai sensi del previgente art. 41, comma 2, del D.lgs. 231/2007 – a distinte Autorità (Banca d'Italia, Ministro della Giustizia, Ministro dell'Interno), in ragione delle competenze a esse attribuite sulle diverse categorie di destinatari degli obblighi antiriciclaggio. Tali provvedimenti sono stati adottati tra il 2010 e il 2015⁶³² e, all'indomani

⁶²⁵ Cfr. art. 6, comma 7, lett. b), del D.lgs. 231/2007. Più in generale le forme di supporto all'attività dei segnalanti sono integrate dalla pubblicazione di quaderni di casistiche, newsletter, manuali, statistiche e studi, nonché dallo sviluppo di modalità segnaletiche indirizzate a specifiche categorie, sul presupposto che il dialogo tra autorità e destinatari degli obblighi innesca un circolo virtuoso che accresce la capacità di individuare specifiche aree di esposizione ai rischi di riciclaggio e promuove un efficace e completo sfruttamento del patrimonio informativo di cui gli operatori sono in possesso. In argomento si veda il [Rapporto annuale della UIF per il 2021](#), p. 6.

⁶²⁶ Cass. civ., sez. II, 8 agosto 2018, n. 20647, fa riferimento allo svolgimento da parte del destinatario di "specifiche indagini per valutare, in base alle altre notizie di cui dispone in virtù della propria attività, la loro effettiva natura sostanziale".

⁶²⁷ Esula dal presente paragrafo la trattazione degli indicatori emanati dalla UIF nel 2018 per agevolare la rilevazione delle operazioni sospette da parte delle Pubbliche amministrazioni, ai sensi dell'art. 10 del D.lgs. 231/2007.

⁶²⁸ Cfr. [Presentazione del Rapporto sull'attività svolta nel 2021](#).

⁶²⁹ La proposta di *AML Package* è consultabile alla pagina https://ec.europa.eu/info/publications/210720-anti-money-laundering-counteracting-financing-terrorism_en. Per la descrizione più dettagliata dei relativi contenuti si rinvia al [Rapporto annuale della UIF per il 2021](#), p. 103 e ss.

⁶³⁰ Cfr. il citato [Rapporto annuale della UIF per il 2021](#), p. 107.

⁶³¹ Tale potere di proposta è stato comunque valorizzato nel previgente quadro normativo osservando che la UIF ricopre il ruolo di "osservatorio privilegiato per la rilevazione di tecniche di riciclaggio e finanziamento del terrorismo. La centralità del patrimonio informativo dell'Unità discende, non solo dall'analisi finanziaria delle segnalazioni di operazioni sospette, ma anche dal fecondo scambio di informazioni che, in materia di tipologie e prassi criminali, la stessa ha sviluppato con autorità nazionali e controparti estere" (K. Bucaioni e L. La Rocca, *Indicatori di anomalia, schemi e modelli di anomalia, comunicazioni della UIF*, in G. Castaldi e C. Conforti (a cura di), *Manuale antiriciclaggio*, cit., p. 236).

⁶³² Si considerino anche le [Indicazioni operative per l'esercizio di controlli rafforzati contro il finanziamento dei programmi di proliferazione di armi di distruzione di massa](#) emanate dalla Banca d'Italia il 27 maggio 2009.

dell'entrata in vigore del citato D.lgs. 90/2017, ne è stata affermata l'ultrattività al fine di evitare vuoti normativi⁶³³.

Gli indicatori, prima della loro emanazione, sono sottoposti al Comitato di sicurezza finanziaria (CSF) per assicurarne il coordinamento⁶³⁴, così realizzando un momento di condivisione tra tutte le autorità coinvolte nella prevenzione e nel contrasto del riciclaggio e del finanziamento del terrorismo; anche prima dell'invio formale della proposta al CSF si svolgono consultazioni con le medesime autorità e confronti preliminari con le associazioni e gli ordini rappresentativi delle diverse categorie di segnalanti⁶³⁵.

Per quanto attiene ai contenuti dei provvedimenti recanti gli indicatori di anomalia, a oggi distinti in base alla tipologia di soggetto tenuto alla collaborazione attiva (rispettivamente, intermediari bancari e finanziari e altri operatori finanziari⁶³⁶, professionisti e revisori contabili⁶³⁷, operatori non finanziari⁶³⁸ nonché società di revisione e revisori legali con incarichi di revisione su enti di interesse pubblico⁶³⁹), sono richiamati gli aspetti definitori e le regole e i principi generali da applicare, unitamente agli indicatori in concreto rappresentativi delle anomalie che potrebbero essere intercettate dai destinatari nello svolgimento della propria attività professionale.

Dal punto di vista generale viene chiarito che gli indicatori non hanno carattere esaustivo e che la mera ricorrenza di indicatori non è motivo di per sé sufficiente per la segnalazione di una operazione sospetta, dovendo piuttosto attivarsi una valutazione complessiva dell'operatività rilevata sulla base di tutte le informazioni disponibili al destinatario; d'altra parte, l'assenza di indicatori può non essere sufficiente a escludere che l'operazione sia sospetta, dovendosi valutare con la massima attenzione ulteriori comportamenti che, sebbene non descritti nei provvedimenti, configurino in concreto profili di sospetto.

Per talune categorie di segnalanti (intermediari, altri operatori finanziari e società di revisione e revisori legali con incarichi di revisione su enti di interesse pubblico) è previsto l'impiego di procedure di selezione automatica delle operazioni anomale basate su parametri quantitativi, quali l'importo o la frequenza delle operazioni, e qualitativi, quali la tipologia delle stesse, senza tuttavia legittimare la segnalazione di tutto quanto evidenziato dalle predette procedure, che dovrà invece essere attentamente vagliato e approfondito al fine di stabilire se ricorrono sospetti da segnalare ai sensi dell'art. 35 del decreto antiriciclaggio.

Gli indicatori sono articolati di norma in sub-indici per favorirne l'intelleggibilità; i sub-indici costituiscono un'esemplificazione dell'indicatore di riferimento e devono essere valutati congiuntamente al contenuto dello stesso; circostanze oggettive (quali, ad esempio, la ripetitività dei comportamenti o la rilevanza economica dell'operazione) ovvero soggettive (quali, ad esempio, l'eventuale giustificazione adottata o la coerenza con il profilo economico del cliente), seppure non specificamente richiamate, valgono anche con riferimento ai relativi sub-indici.

Data l'eterogeneità dei soggetti tenuti alle segnalazioni, è inoltre esplicitato che gli indicatori rappresentano uno strumento operativo per la valutazione della sussistenza di un'operazione sospetta, da utilizzare selezionando quelli rilevanti alla luce della concreta attività prestata dal destinatario⁶⁴⁰.

Ulteriori previsioni riguardano profili attuativi dell'obbligo di segnalazione delle operazioni sospette e sono più analitiche nel caso dei professionisti e degli operatori non finanziari, stante la necessità di accrescerne quantità e qualità della collaborazione nel raffronto con gli intermediari bancari e finanziari.

⁶³³ Cfr. comunicato della UIF del 4 luglio 2017 sul [Decreto di attuazione della direttiva \(UE\) 2015/849](#). L'Unità ha altresì precisato di non avere richiamato tra i provvedimenti ultrattivi gli indicatori di anomalia emanati con decreto del Ministro dell'Interno del 25 settembre 2015 relativi agli uffici della pubblica amministrazione, tenuto conto di quanto disposto dall'art. 10 del D.lgs. 231/2007. I nuovi indicatori per le Pubbliche amministrazioni sono stati emanati in data 23 aprile 2018.

⁶³⁴ Cfr. previgente art. 41, comma 3, del D.lgs. 231/2007. Anche il vigente art. 6, comma 4, lett. e), del D.lgs. 231/2007 stabilisce che la UIF emani e aggiorni periodicamente gli indicatori "previa presentazione al Comitato di sicurezza finanziaria".

⁶³⁵ Il vigente art. 11, comma 2, del D.lgs. 231/2007 stabilisce che gli ordini professionali "sono sentiti dalla UIF ai fini dell'adozione e dell'aggiornamento degli indicatori di anomalia di cui all'art. 6, comma 4, lett. e) che li riguardano".

⁶³⁶ [Provvedimento recante indicatori di anomalia emanato dalla Banca d'Italia il 24 agosto 2010](#).

⁶³⁷ [Decreto del Ministro della Giustizia del 16 aprile 2010](#).

⁶³⁸ [Decreto del Ministro dell'Interno del 17 febbraio 2011](#) (come modificato in [data 27 febbraio 2012](#)).

⁶³⁹ [Provvedimento della Banca d'Italia del 30 gennaio 2013](#).

⁶⁴⁰ Cfr. art. 3, comma 8, del [Decreto del Ministro della Giustizia del 16 aprile 2010](#) nonché art. 3, comma 7, del [Decreto del Ministro dell'Interno del 17 febbraio 2011](#) (come modificato in [data 27 febbraio 2012](#)).

Quanto agli indicatori rappresentativi delle anomalie che potrebbero essere intercettate dai destinatari nello svolgimento della propria attività professionale, ne sono stati finora complessivamente individuati centonove, esemplificati in duecentododici sub-indici: ventuno (con complessivi centoventi sub-indici) riguardano gli intermediari e gli altri operatori finanziari (quattro connessi al cliente, quattro alle operazioni o ai rapporti, quattro ai mezzi e alle modalità di pagamento, sette relativi alle operazioni in strumenti finanziari e ai contratti assicurativi e due inerenti al finanziamento del terrorismo); ventotto (esemplificati con ventitré sub-indici) per i professionisti e i revisori (sette connessi al cliente, tre alle modalità di esecuzione delle prestazioni professionali, quattro relativi alle modalità di pagamento dell'operazione, due inerenti alla costituzione e alla amministrazione di imprese, società, trust ed enti analoghi, sei concernenti operazioni aventi a oggetto beni immobili o mobili registrati e sei inerenti a relativi a operazioni contabili e finanziarie); trentasette (con trentacinque sub-indici) riguardano invece gli operatori non finanziari (sette connessi all'identità o all'atteggiamento del cliente, tre alle modalità di esecuzione delle operazioni, quattro relativi ai mezzi di pagamento utilizzati, ventitré relativi a specifiche attività rilevanti a fini antiriciclaggio); infine, ventitré (con trentaquattro sub-indici) riguardano le società di revisione e revisori legali con incarichi di revisione su enti di interesse pubblico (cinque per il profilo soggettivo, quattro per il profilo oggettivo, tre relativi alle modalità di pagamento e undici inerenti a operazioni contabili e finanziarie).

A titolo esemplificativo, dal punto di vista soggettivo, rilevano elementi quali la riluttanza nel fornire informazioni al destinatario, l'eventuale inesattezza, incompletezza o falsità dei dati forniti, nonché la non usualità di taluni comportamenti, la notizia di circostanze pregiudizievoli, quale il coinvolgimento in procedimenti giudiziari, e la ricorrenza di profili di rischio geografici. Dal punto di vista oggettivo, seppur con le peculiarità proprie di ciascun indicatore in relazione all'attività svolta dal destinatario, si fa riferimento a operazioni o prestazioni professionali incoerenti o illogiche, non corrispondenti alle comuni prassi, non compatibili con il profilo economico-patrimoniale o l'attività del soggetto o ancora caratterizzate dall'intervento immotivato di terzi.

Gli indicatori di anomalia sono stati affiancati nel tempo da schemi e comunicazioni elaborati dalla UIF ad ausilio della collaborazione attiva. Il frequente ricorso a tali strumenti è stato probabilmente agevolato dal processo di elaborazione complesso degli indicatori, i quali richiedono, da un lato, il censimento onnicomprensivo degli elementi sui quali richiamare l'attenzione dei destinatari degli obblighi antiriciclaggio e, dall'altro, il coinvolgimento di un ampio novero di autorità e soggetti privati, aggravato, prima della riforma del 2017, dalla scissione del potere di proposta ed emanazione del provvedimento.

Nell'elaborazione delle predette pubblicazioni, la UIF tiene conto dell'evoluzione delle tecniche e dei metodi di riciclaggio e di finanziamento del terrorismo, descrivendo possibili schemi di operatività illecite, usi distorti di istituti e modelli contrattuali ammessi nell'ordinamento nonché di nuovi strumenti e canali sempre più sofisticati, spesso digitali e a distanza. *Alert* in tal senso sono stati tratti dalle stesse segnalazioni di operazioni sospette e sono stati poi sviluppati alla luce dell'analisi finanziaria, degli studi e delle collaborazioni svolte dall'Unità nell'ambito dei propri rapporti istituzionali, al fine di restituire al sistema di prevenzione aggiornamenti utili alla collaborazione.

Gli schemi si compongono di due parti: una premessa esplicativa delle esigenze che hanno indotto la UIF alla pubblicazione e una parte descrittiva delle anomalie, articolate per punti e distinte sotto il profilo soggettivo e oggettivo, in modo da risultare concatenate dal punto di vista logico e temporale; esse differiscono da quelle poste alla base degli indicatori, poiché sono riferite a un particolare fenomeno o attività criminale e non sono articolate in sub-indici. Inoltre, ai fini del corretto adempimento dell'obbligo di segnalazione di operazioni sospette, da un lato, non è necessario che ricorrano contemporaneamente tutti gli elementi descritti nello schema; dall'altro, la mera ricorrenza di un singolo elemento non è di per sé motivo sufficiente per procedere alla segnalazione: le circostanze soggettive e oggettive riportate negli schemi rilevano ai fini dell'individuazione di ipotesi di operazioni sospette se, in base alle informazioni disponibili valutate nel loro complesso, risultano concatenate dal punto di vista logico e temporale in modo da risultare funzionali all'ipotesi descritta negli schemi stessi.

Il primo schema è stato diffuso dall'UIF il 24 settembre 2009, riprendendo le indicazioni fornite nel 2003 dall'Ufficio Italiano dei Cambi, allo scopo di richiamare l'attenzione sull'evoluzione dei rapporti intrattenuti con soggetti in difficoltà economica o finanziaria, maggiormente esposti a influenze criminali e al rischio di ricevere illegali erogazioni di finanziamento. Il monitoraggio del rischio di riciclaggio che può derivare dalla diffusione di fenomeni usurari è stato poi costantemente monitorato dall'UIF, che ha pubblicato un nuovo schema in tema di usura in data 9 agosto 2011. Ulteriori schemi hanno riguardato i c.d. conti dedicati (13 ottobre 2009)⁶⁴¹, le frodi informatiche (5 febbraio 2010), l'abuso di finanziamenti pubblici (8 luglio 2010), le frodi nell'attività di leasing (17 gennaio 2011), il rischio di frodi nell'attività di factoring (16 marzo 2012), il settore dei giochi e delle scommesse (11 aprile 2013), l'anomalo utilizzo di trust (2 dicembre 2013), l'operatività con carte di

⁶⁴¹ Lo schema sui c.d. conti dedicati è stato richiamato dalla UIF anche in occasione delle "Linee-guida" emanate il 12 agosto 2010 e il 31 dicembre 2010 dal Comitato di coordinamento per l'alta sorveglianza delle grandi opere in materia di ricostruzione di edifici pubblici e privati post-terremoto in Abruzzo.

pagamento (18 febbraio 2014)⁶⁴², l'operatività over the counter con società estere di intermediazione mobiliare (1° agosto 2016) e, da ultimo, gli illeciti fiscali (10 novembre 2020), realizzando in questo caso un focus specifico sulla cessione di crediti fiscali fittizi e altri indebiti utilizzi e un intervento di aggiornamento delle precedenti comunicazioni della UIF del 15 febbraio 2010 e del 23 aprile 2012, rispettivamente, in tema di frodi sull'IVA intracomunitaria e in materia di frodi fiscali internazionali e frodi nelle fatturazioni⁶⁴³.

Quanto allo strumento della comunicazione, oltre che per diffondere gli schemi ai sensi dell'art. 6, comma 7, lett. b), del D.lgs. 231/2007, è utilizzato dalla UIF anche per richiamare l'attenzione su taluni fenomeni che espongono i segnalanti a un elevato rischio di coinvolgimento in fatti di riciclaggio o di finanziamento del terrorismo. Anche per tali *alert* l'Unità richiama la natura esemplificativa degli elementi individuati e la circostanza che l'impossibilità di ricondurre operazioni o comportamenti a uno o più di essi non è sufficiente a escludere l'obbligo di segnalazione ai sensi dell'art. 35 del D.lgs. 231/2007, dovendosi piuttosto verificare se ricorrano ulteriori comportamenti e caratteristiche sospette delle operatività portate all'attenzione.

La prima comunicazione è stata pubblicata il 9 novembre 2009 sulla presentazione di banconote in lire per la conversione in euro; le successive hanno riguardato le operazioni di c.d. "scudo fiscale" (24 febbraio 2010), l'utilizzo anomalo di valute virtuali (30 gennaio 2015 e 28 maggio 2019), la prevenzione del finanziamento del terrorismo internazionale (18 aprile 2016 e 13 ottobre 2017), la prevenzione di fenomeni di criminalità finanziaria connessi con l'emergenza da COVID-19 e, da ultimo, anche l'utilizzo dei fondi connessi con l'attuazione del Piano Nazionale di Ripresa e Resilienza (c.d. PNRR), inserito all'interno del programma Next Generation EU (NGEU) come iniziativa di solidarietà finanziaria in risposta alla crisi pandemica e volto al rilancio economico dell'Italia (16 aprile 2020, 11 febbraio 2021 e 11 aprile 2022)⁶⁴⁴.

Tanto con riguardo agli schemi quanto alle altre comunicazioni la UIF invita i soggetti obbligati a provvedere affinché, nell'ambito della propria autonomia organizzativa e con le modalità ritenute più idonee, le indicazioni fornite siano tenute presenti dal personale e dai collaboratori incaricati di rilevare eventuali sospetti. La segnalazione è richiesta con la massima tempestività e, ove possibile, prima di dar corso all'esecuzione delle operazioni sospette.

5. Selezione automatica delle operazioni sospette (*F. Berghella*)

L'utilizzo di procedure di selezione automatica delle operazioni da valutare ai fini del sospetto deriva dalla constatazione che qualunque operazione economica, che non comporti lo scambio diretto di denaro contante tra persone, si traduce in una registrazione informatica che costituisce una traccia, il cui esame può ricondurre alla scoperta dei fenomeni illeciti. La verifica della compatibilità tra le singole operazioni e il profilo economico-finanziario del cliente, rilevando eventuali incongruenze rispetto alla sua normale operatività e ad altre caratteristiche soggettive e oggettive, può evidenziare comportamenti anomali da sottoporre alla valutazione umana per attivare la segnalazione in assenza di giustificazioni.

Il ruolo e le caratteristiche delle procedure di selezione automatica e le modalità di utilizzo sono contenuti principalmente nel decreto antiriciclaggio e nei provvedimenti recanti gli indicatori e gli schemi di anomalia⁶⁴⁵. L'insieme delle prescrizioni forniscono le indicazioni che ne autorizzano l'uso conforme alla normativa sintetizzabile nei seguenti principi:

- gli strumenti informatici e telematici, ai fini della segnalazione di operazioni sospette, svolgono un ruolo di ausilio e, insieme ad altre procedure di esame delle operazioni, tengono conto, tra le altre,

⁶⁴² Lo schema in argomento era stato preceduto dalla comunicazione sull'utilizzo anomalo di carte di pagamento per prelevamenti di contante del 27 febbraio 2012.

⁶⁴³ Gli schemi tuttora applicabili sono consultabili sul sito internet della UIF, sezione [Indicatori, schemi e comunicazioni inerenti a profili di anomalia - Modelli e schemi di comportamenti anomali](#); quelli non più applicabili sono comunque disponibili sul medesimo sito, sezione [Antiriciclaggio – Normativa nazionale e disposizioni attuative previgenti](#).

⁶⁴⁴ Le comunicazioni sono consultabili sul sito internet della UIF, sezione [Indicatori, schemi e comunicazioni inerenti a profili di anomalia - Altre comunicazioni](#).

⁶⁴⁵ In particolare agli artt. 6, 11, 35 e 36 del D.lgs. 231/2007, nella versione aggiornata dal D.lgs.90/2017, e alla delibera della Banca d'Italia n. 616 del 24 agosto 2010.

delle evidenze desunte dall'analisi dei dati e dalle informazioni contenute nei sistemi di conservazione (archivio unico informatico)⁶⁴⁶;

- per le elaborazioni utili alla valutazione, le procedure di selezione considerano tutti gli altri dati pertinenti ricavabili dalle informazioni disponibili sul cliente, compresi quelli acquisiti nel corso degli adempimenti degli obblighi di adeguata verifica, di valutazione e di profilazione del rischio del cliente;
- le procedure di selezione automatica delle operazioni anomale sono basate su parametri quantitativi, quali l'importo o la frequenza delle operazioni, e qualitativi, come la tipologia e le modalità di utilizzazione dei servizi;
- l'individuazione delle operazioni sospette è agevolata dagli indicatori di anomalia e dai modelli e schemi rappresentativi di comportamenti anomali riferibili a possibili attività di riciclaggio e di finanziamento del terrorismo;
- la ricorrenza di comportamenti descritti in uno o più indicatori o schemi di anomalia, la rilevazione di una difformità tra le informazioni acquisite in sede di adeguata verifica e quelle tratte da altre fonti, la ripetitività dei comportamenti (frequenza evidenziata), la rilevanza economica dell'operazione (ammontare dell'importo), l'incoerenza con il profilo economico, il carattere non usuale o la illogicità dell'operatività emerse dalla procedura automatica non costituiscono motivo sufficiente per inviare una segnalazione, dovendosi sempre valutare l'operatività nel suo complesso;
- le circostanze descritte negli indicatori, quando evidenziate dalle procedure automatiche, non costituiscono anomalie se risultano giustificate da ragioni plausibili sulla base degli elementi conoscitivi forniti dal soggetto cui è riferita l'operatività o altrimenti acquisite;
- il trattamento dei dati eseguito dai sistemi per la selezione è svolto in conformità alle disposizioni del Codice in materia di protezione dei dati personali e del regolamento (UE) 2016/679.

Questi principi, che costituiscono la base giuridica del trattamento automatizzato, seguono la normativa preventiva sin dalle sue origini. Già le prime "Indicazioni operative per la segnalazione di operazioni sospette", predisposte dalla Banca d'Italia nel gennaio 1993 e novembre 1994⁶⁴⁷ (*c.d. decalogo*), invitavano gli intermediari a verificare la compatibilità tra le singole operazioni e il profilo economico-finanziario del cliente, rilevando eventuali incongruenze rispetto alla sua fascia di operatività normale ed attivare la segnalazione ove lo scostamento fosse privo di giustificazione, consentendo agli intermediari di utilizzare programmi per una selezione automatica delle operazioni in base ai profili di anomalia idonei ad essere trattati con mezzi informatici. La normativa successiva ha confermato l'impostazione⁶⁴⁸ ampliandola e perfezionandola.

Il ruolo di ausilio degli strumenti informatici è riaffermato dalla giurisprudenza in sentenze relative a vicende processuali connesse ai reati di riciclaggio e che citano la funzione del sistema GIANOS. La Corte Suprema di Cassazione⁶⁴⁹ ha precisato che lo strumento: «funge da ausilio nell'attività di vigilanza rimessa all'intermediario finanziario, il quale è comunque chiamato a compiere una propria autonoma valutazione, proprio alla luce delle caratteristiche soggettive e oggettive delle operazioni effettuate»; analogamente il Tribunale di Palermo⁶⁵⁰ afferma che lo strumento: «è indubbiamente di ausilio e di supporto all'operatore bancario, consentendo di eseguire una prima scrematura delle posizioni, ma non si sostituisce all'operatore stesso né lo sottrae alle sue responsabilità, in quanto spetta sempre a lui la

⁶⁴⁶ Le procedure informatiche per l'individuazione automatica di operazioni anomale assumono carattere obbligatorio nei casi l'operatività sia effettuata attraverso canali telefonici o telematici, sia eseguita nei servizi di tramitazione, o che transiti sui conti correnti di corrispondenza o assimilabili (cfr. art. 6 della delibera Banca d'Italia n. 616 del 24 agosto 2010).

⁶⁴⁷ Nel 1993 un gruppo di studio di esperti bancari e delle associazioni bancarie, coordinati dall'ABI, e in presenza di osservatori della Banca d'Italia e dell'UIC, delinearono le specifiche per la realizzazione del primo programma informatico per la Generazione di Indici di Anomalia per Operazioni Sospette (GIANOS), attribuendo alla procedura un ruolo di ausilio all'operatore, evitando valutazioni svolte con modalità esclusivamente automatiche. La Banca d'Italia, nelle Indicazioni operative per la segnalazione di operazioni sospette del novembre 1994, affermò che *"rientra nell'autonomia decisionale degli intermediari utilizzare anche programmi per una selezione automatica delle operazioni in base a quei profili di anomalia che siano suscettibili di trattamento informatico"*. L'ABI, con lettera circolare del 3 gennaio 1995, informò che: *"viene in sostanza riconosciuta l'importanza e le legittimità dell'utilizzazione del sistema informatico denominato GIANOS ... consistente in un insieme di strumenti automatici di analisi delle operazioni allo scopo di evidenziare quelle, ... da sottoporre alle ulteriori valutazioni richieste dalla legge"*. L'esperienza e la procedura vennero positivamente illustrate ai commissari del GAFI nelle visite ispettive fatte all'Italia nel 1997 (memorandum ABI-Pos.201) e nel 2005 *"la maggior parte delle segnalazioni all'UIC trae origine proprio dalla procedura GIANOS"*.

⁶⁴⁸ Banca d'Italia, Istruzioni operative per l'individuazione delle operazioni sospette del 12 gennaio 2001; Banca d'Italia, Provvedimento recante gli indicatori di anomalia per gli intermediari, delibera n. 616 del 24 agosto 2010.

⁶⁴⁹ II sezione civile, sentenza 20212/2017.

⁶⁵⁰ Sentenza del 19/12/2006 n.53 R.G.A.C. 2002.

verifica finale dell'operazione sospetta»; così anche la Corte di Appello di Roma⁶⁵¹ che asserisce: «non esime gli appellanti da responsabilità, poiché il funzionario dell'intermediario se ne può avvalere solo come ausilio, ma è tenuto ad effettuare autonome valutazioni».

Il principio è riportato anche negli orientamenti settoriali EBA del 1 marzo 2021, rivolti alle attività di *retail banking*, che alla misura 9.12 prescrivono che gli intermediari, qualora si avvalgano di sistemi automatizzati per l'individuazione del rischio di ML/TF associato ai singoli rapporti continuativi o alle operazioni occasionali e per l'individuazione delle operazioni sospette, dovrebbero assicurarsi che tali sistemi siano adatti allo scopo in linea con i criteri generali degli orientamenti e che, l'impiego di sistemi informatici automatizzati non dovrebbe mai essere considerato un'alternativa all'effettuazione di controlli da parte del personale.

La selezione automatica delle operazioni anomale e dei comportamenti economico-finanziari inattesi richiede l'ideazione di regole idonee a rappresentare i fenomeni inusuali da cercare e la successiva codifica delle condizioni ipotizzate, in una sequenza di istruzioni logiche e algebriche comprensibili all'elaboratore. L'algoritmo è realizzabile a condizione che gli eventi anomali da automatizzare siano traducibili in termini numerici e statistici, in coerenza con i principi di liceità che ne autorizzano l'uso.

La traduzione informatica degli eventi da selezionare è preceduta dalla preventiva individuazione e definizione di un comportamento o di un'operazione a rischio da valutare ai fini della sospettabilità, seguita dalla ricerca, nei propri sistemi, di dati e informazioni trattabili riferiti allo schema anomalo in esame. Molti eventi richiedono anche la definizione dell'operazione o del comportamento atteso, espresso in termini di normalità operativa del cliente. Il profilo economico-finanziario normale è valutato sulla base di una significativa serie storica di dati, la cui estensione temporale è proporzionata alla tipologia dell'operazione ed è sufficiente a rilevare gli scostamenti tra l'operazione realizzata e i comportamenti pregressi. Altre transazioni potenzialmente sospette sono estraibili direttamente, senza condizioni di confronto con le operazioni pregresse.

L'intero processo dovrebbe essere sottoposto a preventiva sperimentazione per verificarne il funzionamento, la validità e l'efficacia della regola ideata. La mutabilità dell'operatività illegale, unitamente alla variabilità dei prodotti e servizi offerti dagli intermediari, richiedono la verifica costante degli algoritmi adottati e frequenti revisioni, sostituzioni o l'annullamento delle regole obsolete.

Il metodo usato, per ragioni di liceità ed opposizione in sede giudiziaria o ispettiva, dovrebbe consentire la ricostruibilità della sequenza che ha generato l'estrazione, in modo che a una determinata causa segua solo un effetto certo e identificabile che sostenga l'eventuale segnalazione o il rifiuto dell'evidenza generata dal sistema informatico.

Le operazioni estratte automaticamente non sempre corrispondono a motivi di sospetto e vengono percepite come falsi positivi derivanti da molte cause, tra cui la mancata corrispondenza della regola all'indicatore di anomalia, l'adattamento non adeguato dell'algoritmo alla realtà operativa in esame, la parziale o errata alimentazione del sistema informatico. Se si escludono le circostanze di errore che inficiano il risultato della selettività automatica, il concetto di falso positivo, essendo basato sulla condizione binaria di vero o falso, non è appropriato alle valutazioni di sospetto che deve compiersi ponderando tutti gli elementi informativi a disposizione. Uno schema di anomalia, per quanto ragionato, non sempre può consentire di individuare con immediatezza le finalità sottostanti, perché la configurazione oggettiva dell'operazione è di per sé neutra⁶⁵², e la mera ricorrenza di comportamenti descritti in uno o più indicatori di anomalia non è motivo sufficiente per la segnalazione di operazioni sospette. Sarebbero più adatte, pertanto, le definizioni di vero positivo o vero negativo. Il grado di precisione della selettività di un algoritmo può essere aumentato utilizzando criteri di specificità della regola, con valori basati su parametri riferiti a ciascun soggetto fisico o giuridico.

Il costante aumento della numerosità e complessità dei dati e delle informazioni da esaminare in relazione ai rischi e alla sospettabilità, unitamente allo sviluppo delle tecnologie, propongono prospettive di sviluppo innovativo verso l'applicazione di metodi basati sull'intelligenza artificiale, che permetterebbero d'interconnettere e analizzare rapidamente una grande quantità di informazioni e di formulare un maggior numero di ipotesi decisionali. Il processo di *machine learning* richiede l'istruzione preventiva dell'algoritmo al fine di organizzarne l'apprendimento progressivo del fenomeno da ricercare. Con l'evolvere dei dati analizzati, l'algoritmo potrà auto-modificarsi migliorandosi, ma con il rischio che la logica utilizzata per la selezione dei casi non sia più identificabile e perda il fondamento giuridico che ne consente l'uso.

Il Consiglio di Stato ha precisato che la conoscibilità dell'algoritmo deve essere garantita in tutti gli aspetti: «dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella

⁶⁵¹ Sentenza n. 2412 del n.53 R.G.A.C. 2002, 01/04/2021.

⁶⁵² Caratteristica evidenziata nelle Istruzioni operative per l'individuazione di operazioni sospette emanate dalla Banca d'Italia il 12 gennaio 2001.

procedura valutativa e decisionale e dei dati selezionati come rilevanti”⁶⁵³. La Commissione europea, nel “Libro bianco sull’intelligenza artificiale”,⁶⁵⁴ propone la tenuta di registri su cui annotare le fasi di programmazione e addestramento dell’algoritmo nei sistemi di IA ad alto rischio, a garanzia dei requisiti di riproducibilità, verificabilità e trasparenza. Il Garante per la protezione dei dati personali, nel parere reso alla Banca d’Italia il 24 febbraio 2022 sull’uso di algoritmi d’intelligenza artificiale in procedure interne di gestione degli esposti, esprime parere favorevole sulla metodologia organizzata dalla vigilanza, riscontrando che le tecniche di *machine learning* proposte prevedono il continuo riaddestramento mediante il coinvolgimento di esperti in grado di guidare il processo di definizione, aggiornamento e validazione dei modelli di apprendimento, con una sorveglianza umana qualificata. Inoltre, la metodologia è in grado di fornire una rappresentazione del funzionamento interno dell’algoritmo, finalizzata alla spiegazione dei risultati prodotti, ed è prevista la conservazione della documentazione che dà conto del continuo perfezionamento dell’algoritmo al solo fine di controllo versione del modello e di monitoraggio dello sviluppo nel corso del tempo, nel rispetto dei principi di trasparenza e di responsabilità⁶⁵⁵.

In merito alla conoscibilità degli algoritmi da parte delle persone che svolgono la prima valutazione dei comportamenti anomali della clientela, è utile distinguere tra l’obbligo di formare tali risorse al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo⁶⁵⁶ e l’opportunità o meno, che esse conoscano anche i particolari dell’algoritmo utilizzato. Il principio di prudenza fondato sulla necessità di tutelare gli operatori da possibili ritorsioni e condizionamenti ambientali, dall’esigenza di ottenere una compiuta e ragionata autonoma valutazione, di evitare che la diffusione incontrollata dei criteri di valutazione possa favorire le operazioni di riciclaggio eludendo i controlli, suggeriscono la scelta di limitare a pochi soggetti l’intera conoscenza degli algoritmi⁶⁵⁷, e di inserire nelle parti visibili dell’applicativo informatico solo un generico riferimento all’indicatore di anomalia o alla regola attivati⁶⁵⁸.

Le procedure informatiche di selezione delle operazioni potenzialmente sospette garantiscono, mediamente, buoni risultati, dando origine ad una discreta quantità di segnalazioni sospette e hanno contribuito a migliorarne la qualità, come riscontrato dal Servizio Studi del Senato della Repubblica e della Camera dei deputati in occasione dell’aggiornamento del D.lgs. 231/2007 per il recepimento della quarta direttiva antiriciclaggio.

6. Approfondimento delle segnalazioni (F. Fiorini, E. Prizio, G. Paoni e D. Colombo)

L’analisi finanziaria della UIF è volta a individuare operazioni e situazioni riconducibili a finalità di riciclaggio o di finanziamento del terrorismo. Le informazioni contenute nella segnalazione vengono integrate con gli elementi presenti nelle varie basi dati a disposizione dell’Unità al fine di ridefinire e ampliare il contesto segnalato, identificare soggetti e relazioni, ricostruire i flussi finanziari sottostanti all’operatività descritta.

L’analisi, preceduta da una fase di arricchimento automatico dei dati forniti dai segnalanti, viene effettuata sfruttando il patrimonio informativo della UIF e consente di classificare le segnalazioni in base al rischio e al fenomeno correlato. I contesti più rilevanti vengono così selezionati, trattati nel modo più efficace e disseminati per i successivi sviluppi investigativi. Il processo segue l’approccio *risk-based* definito dagli standard internazionali e consente di adattare l’azione dell’Unità tenendo conto delle minacce e delle vulnerabilità identificate nell’ambito degli esercizi di *risk assessment* e dei risultati dell’analisi strategica.

6.1. Il primo passo dell’analisi: la classificazione delle SOS

Raccolta e gestione delle segnalazioni sono supportate dall’applicativo RADAR, attivo sulla piattaforma Infostat-UIF che ne garantisce la tempestività e la sicurezza. RADAR riceve le segnalazioni secondo il modello segnaletico sopra descritto ed è strutturato in modo da definire i legami tra i campi soggetto-rapporto-operazioni; l’efficacia del suo funzionamento, quindi, è funzione diretta della capacità dei segnalanti di fornire le informazioni strutturate in modo esaustivo e preciso.

⁶⁵³ Consiglio di Stato, Sentenza n. 2270, 8 aprile 2019.

⁶⁵⁴ “White Paper. On Artificial Intelligence - A European approach to excellence and trust”, 19 febbraio 2020.

⁶⁵⁵ Art. 5, commi 1, lett. a), e 2, e art. 24 del regolamento generale sulla protezione dei dati personali.

⁶⁵⁶ Art. 16, comma 3, D.lgs. 231/2007.

⁶⁵⁷ Sulla segretezza degli algoritmi della procedura GIANOS si vedano: Senato della Repubblica, *Indagine conoscitiva sui possibili fenomeni di riciclaggio connessi all'imminente circolazione dell'euro nel nostro paese*, Audizione dell’Associazione Bancaria Italiana del 18/10/2001, p. 6; CNEL, Osservatorio socioeconomico sulla criminalità, *Indagine sul riciclaggio del denaro proveniente da attività illecite*, audizione del 25/11/2002 dal Direttore centrale dell’ABI; The World Bank, *A Practical Guide for Bank Supervisors- Preventing Money Laundering and Terrorist Financing*.

⁶⁵⁸ Cfr. F. Berghella, *La conformità della tecnologia nel contrasto al riciclaggio. Fondamenti normativi delle procedure di ausilio e degli algoritmi, contributo del Sistema GLANOS*, Bancaria Editrice, 2021.

Nel tempo l'applicativo RADAR è stato integrato con ulteriori funzionalità fino a diventare un ecosistema complesso e articolato, al cui interno si svolge anche lo scambio di documentazione integrativa per l'analisi delle SOS e la disseminazione agli Organi investigativi. Esso ospita un datawarehouse che consente di incrociare le informazioni di archivio con quelle tratte da database esterni.

Una delle funzioni di base di RADAR è l'arricchimento del flusso segnaletico; al momento del loro ingresso nel sistema, infatti, le informazioni strutturate della SOS vengono sottoposte a una prima classificazione automaticamente dal sistema che ricerca, al suo interno, eventuali corrispondenze negli archivi in datawarehouse; al termine di questo processo, alla segnalazione viene assegnato un livello di rating di sistema che, insieme al rischio attribuito dal segnalante, costituisce uno strumento iniziale di selezione dei flussi e di graduazione delle priorità⁶⁵⁹.

Tutte le segnalazioni di operazioni sospette che pervengono alla UIF sono assoggettate a un'analisi di primo livello volta a valutare l'effettivo grado di rischio e a definire il trattamento più appropriato. Sulla base delle informazioni acquisite sia in sede di arricchimento automatico sia da altre fonti, viene valutata la fondatezza del sospetto di riciclaggio o di finanziamento del terrorismo e la necessità di effettuare ulteriori approfondimenti.

L'appropriata valutazione del rischio delle segnalazioni di operazioni sospette è funzionale sia all'attività di analisi finanziaria sia alle successive fasi investigative. La UIF ha affinato sistemi di selezione e di classificazione delle informative al fine, da un lato, di individuare i contesti di maggior rischio e, dall'altro, di definire le tipologie di analisi da adottare.

Dal 2020 è stato avviato, a tal riguardo, un progetto finalizzato a sviluppare un sistema di classificazione automatica delle segnalazioni da integrare nel processo di analisi (in particolare in sede di prima valutazione della segnalazione), con l'obiettivo di mantenerne elevata l'efficienza (in termini di risorse umane in esso impiegate) e l'efficacia (in termini di capacità degli analisti di individuare i contesti più meritevoli di ulteriori attività di approfondimento finanziario).

Tale progetto, giunto in una fase avanzata di sperimentazione, muove dalla premessa dell'esistenza nel complessivo flusso segnaletico di una consistente percentuale di segnalazioni il cui contenuto si caratterizza per la ricorrenza di taluni elementi, riflessi nei dati strutturati o nelle note descrittive, riconducibili a specifiche fattispecie operative molto frequenti. A fianco di ciò, considerato il sempre crescente numero di segnalazioni, sussiste la pressante esigenza di individuare prontamente quelle segnalazioni riguardanti contesti connotati da maggiore rischio, quali quelli che vedono il possibile coinvolgimento della criminalità organizzata, potenziali casi di corruzione o di evasione/frode fiscale.

Per facilitare l'individuazione delle diverse tipologie di segnalazioni sono stati definiti alcuni algoritmi di classificazione automatica, mettendo a fattor comune l'esperienza di valutazione consolidata nel tempo dagli analisti. Gli algoritmi, che intendono gestire in via automatica processi operativi relativamente semplici ma molto ricorrenti (e quindi complessivamente onerosi in termini di risorse impiegate), sono stati successivamente tradotti in procedure informatiche secondo un approccio *rule based*: al verificarsi di determinate successioni di condizioni nei dati strutturati o nei risultati dell'analisi testuale delle note descrittive della segnalazione, il sistema propone automaticamente all'analista la classificazione della segnalazione secondo un dato fenomeno.

La classificazione è corredata da indicatori che evidenziano la presenza di elementi informativi cui sono associate prassi operative codificate (è il caso, per esempio, della presenza di soggetti su cui pendono richieste della Autorità Giudiziaria, per i quali, di norma, viene attivato un approfondimento finanziario) e/o l'eventuale presenza di elementi di rischio (come la presenza di PEP o di individui emersi dall'incrocio dei dati della segnalazione con il flusso informativo scambiato con la DNA). Un'ulteriore componente del sistema mira a individuare i contesti segnalati a maggior rischio di coinvolgimento della criminalità organizzata. In tale modo l'analista, cui compete la decisione circa l'estensione dell'approfondimento da operare sulla segnalazione, esprime la propria valutazione sulla base di una prima classificazione effettuata dal sistema, potendo così operare con maggiori rapidità ed efficacia.

I risultati della sperimentazione del sistema di classificazione si sono dimostrati incoraggianti rispetto alla sua capacità di replicare gli esiti della valutazione umana, proponendo classificazioni sovrapponibili o comunque coerenti con essa. Su tale base sono state individuate ulteriori fattispecie ricorrenti cui applicare il sistema, che promette di consentire importanti guadagni di efficienza nel processo di analisi, consentendo di incrementare la capacità selettiva dei contesti connotati da maggior rischio al fine di veicolarvi le risorse disponibili all'Unità.

⁶⁵⁹ Il rating automatico è articolato su cinque livelli sulla base di un algoritmo strutturato su variabili prevalentemente quantitative. Esso tiene conto di dell'ampio spettro informativo disponibile negli archivi della UIF. Più che dalle valutazioni di rischio espresse dal segnalante, che vengono comunque prese in considerazione, la sua accuratezza dipende principalmente dalla corretta e completa compilazione dello schema segnaletico da parte dei soggetti obbligati, ovvero dal grado di affidabilità delle informazioni di base. Per recepire adeguatamente tutti gli elementi di rischio di natura tipicamente qualitativa rilevabili in sede di analisi finanziaria è previsto un intervento correttivo degli analisti al termine della fase di valutazione della SOS; il rating finale viene infine associato alla segnalazione e trasmesso agli Organi investigativi.

Essendo il sistema basato sull'elaborazione automatica delle informazioni presenti nelle segnalazioni, va da sé che assumono un ruolo cruciale la completezza e la qualità dei dati strutturati nella segnalazione e l'accuratezza delle note descrittive redatte dal segnalante.

6.2. L'analisi finanziaria

L'analisi di secondo livello è destinata di norma alle segnalazioni che, all'esito dell'analisi di primo livello, non risultino immediatamente associabili a fenomeni e casistiche già noti all'Unità o che, anche qualora tale associazione sia possibile, contengano elementi di attenzione che si ritiene opportuno esplorare, comprendere e valutare mediante un approfondimento finanziario mirato. Nell'ambito della valutazione della rilevanza della segnalazione ai fini della scelta del trattamento in parola assumono rilevanza l'entità e le caratteristiche dell'operatività finanziaria segnalata nonché le informazioni disponibili sul profilo soggettivo delle persone fisiche e giuridiche coinvolte, acquisite anche tramite lo scambio informativo sistematico con la DNA e le collaborazioni con gli Organi inquirenti e con la Magistratura.

L'analisi di secondo livello è ispirata a principi di coerenza e proporzionalità. Il percorso di approfondimento è infatti sviluppato in maniera coerente rispetto a: 1) l'origine della segnalazione, con riferimento in particolare alla categoria del sospetto (riciclaggio, finanziamento del terrorismo o di proliferazione di armi di distruzione di massa); 2) le caratteristiche soggettive e oggettive dell'operatività segnalata, tenendo principalmente conto del tipo di operazioni e della loro ricorrenza nonché delle eventuali fenomenologie finanziarie o modelli di comportamento emergenti dal contesto segnalato; c) i canali utilizzati per il trasferimento dei fondi.

Profondità, spessore ed intensità dell'approfondimento sono inoltre modulati secondo l'approccio *risk-based*, in base al quale all'aumentare del rischio emergente dalla segnalazione aumentano la numerosità e la natura delle fonti da cui sono ricercate e acquisite le informazioni, l'estensione e il livello di dettaglio dei contenuti informativi sottoposti all'analisi, l'orizzonte temporale di riferimento nonché la ampiezza dei possibili nodi attraverso i quali sviluppare le indagini.

Sotto il profilo operativo, l'approfondimento è articolato in tre momenti fondamentali: la comprensione del contesto segnalato, la ricostruzione dei flussi finanziari e la valutazione delle ipotesi di sospetto. Idealmente distinti secondo un ordine logico-sequenziale, queste tre fasi presentano nella pratica continue sovrapposizioni, frutto dello sviluppo e dell'interazione dei processi materiali (ricerca, acquisizione e raccolta delle informazioni) e cognitivi (interpretazione e valutazione delle informazioni raccolte) che li costituiscono.

Nella fase della comprensione del contesto segnalato, propedeutica all'impostazione dell'attività di analisi, risulta fondamentale disporre di un quadro informativo iniziale il più possibile completo ed esteso. In tal senso alcune casistiche approfondite dall'Unità nel corso degli anni hanno rappresentato la testimonianza dell'insostituibile contributo che gli operatori finanziari e i professionisti sono in grado di dare a un'efficace attività di prevenzione e contrasto delle attività criminali, quando la segnalazione, lungi dall'essere percepita come un mero e cautelativo adempimento di un dovere, è supportata da elevate competenze professionali e dal reale intento di dare un contributo alla tutela della legalità.

Dopo la ricostruzione dei flussi dei movimenti finanziari sospetti, l'analisi di secondo livello è completata da un accurato processo di valutazione attraverso cui l'analista, nell'ambito della più chiara ed ampia visuale resa disponibile dagli approfondimenti, riesamina i fattori critici che hanno indotto il segnalante alla segnalazione e valuta tutti gli elementi di anomalia oggettivi e soggettivi raccolti nel corso delle indagini finanziarie, cercando di fornire una possibile chiave di lettura del contesto esaminato.

Le valutazioni condotte dall'analista trovano espressione sinteticamente nell'attribuzione alla segnalazione del definitivo livello di rischio e, in maniera più analitica, nella redazione di un documento destinato ad accompagnare la segnalazione agli Organi investigativi.

Durante l'analisi di secondo livello gli analisti dispongono di una pluralità di opzioni e strumenti di approfondimento: oltre allo sfruttamento del patrimonio informativo disponibile nel database dell'Unità, è possibile contattare il segnalante e l'intera platea di soggetti obbligati nonché interloquire con la rete estera delle FIU.

Sotto il primo profilo, l'Unità ha profuso negli ultimi anni un costante impegno nell'ampliamento delle fonti informative accessibili, anche attraverso la stipula di specifici protocolli di intesa. Tra le iniziative avviate negli anni più recenti si annoverano i lavori per l'accesso ai dati dell'Agenzia delle Entrate, all'archivio contenente i dati sui finanziamenti e le relative garanzie, erogati da banche autorizzate in Italia, e alle basi dati statistiche su strumenti finanziari. Significativo contributo

all'irrobustimento e alla velocizzazione del processo di analisi è stato fornito anche dalla progressiva integrazione delle fonti informative all'interno del *datavarehouse* dell'Unità, che ha consentito di automatizzare il *matching* tra le informazioni presenti nelle basi dati a disposizione e quelle contenute nelle segnalazioni o successivamente acquisite nel corso dell'analisi.

Parimenti, anche la fase di interlocuzione con i soggetti obbligati è stata recentemente oggetto di intervento tramite l'avvio nel 2020 di un progetto che ha innalzato significativamente i presidi di sicurezza degli scambi informativi e ha consentito una gestione più veloce ed efficiente dell'intero processo di acquisizione ed elaborazione delle informazioni raccolte. In tale contesto, ruolo centrale rivestono la tempestività e l'accuratezza con cui i soggetti obbligati soddisfano le richieste di informazioni formulate dall'Unità nell'ambito degli approfondimenti finanziari condotti.

Anche la collaborazione con le FIU estere, infine, si è progressivamente intensificata anche grazie ad un meccanismo di scambio di informazioni, il cui utilizzo è stato consolidato e sistematizzato dall'Unità in modo da consentire l'emersione di collegamenti dell'operatività segnalata con altri paesi non evidenti dal contesto analizzato.

L'analisi di secondo livello non solo risponde all'esigenza di approfondire uno specifico contesto segnaletico a vantaggio delle successive attività di competenza degli Organi investigativi, ma rappresenta anche un'occasione fondamentale per l'Unità per l'acquisizione e il consolidamento di conoscenze rispetto ad aree di rischio di interesse.

Tramite gli approfondimenti infatti, nella moltitudine di comportamenti segnalati come sospetti, è possibile individuare, anche grazie all'interlocuzione con altri attori istituzionali, tipologie caratterizzate da elementi ricorrenti e rilevanti per la valutazione dei rischi di riciclaggio o di finanziamento del terrorismo. Le conoscenze acquisite, trasfuse in indicatori di anomalia e schemi di comportamento anomalo, sono condivise con la platea dei soggetti obbligati e costituiscono per questi ultimi un elemento di orientamento nella individuazione e valutazione delle operazioni sospette.

Tale attività è particolarmente rilevante in un contesto in cui le tecniche di riciclaggio sono in continua evoluzione rendendo così difficile o eccessivamente costoso per i singoli operatori stare al passo con esse. In tal senso, mettere a fattor comune tutto ciò che i singoli componenti del sistema riescono a individuare come caratteristica sospetta rappresenta pertanto un modo per aumentare l'efficienza complessiva dell'apparato di prevenzione, ridurre i costi e fornire un incentivo positivo all'implementazione dei presidi antiriciclaggio.

6.3. L'analisi aggregata

Con il continuo e sostenuto incremento dei flussi segnaletici e il conseguente arricchimento del patrimonio informativo disponibile è venuta sempre più affermandosi l'esigenza di affiancare ai tradizionali metodi di analisi finanziaria, incentrata su segnalazioni singole, o comunque su un numero limitato di segnalazioni collegate, nuovi approcci di analisi di più ampio respiro. Si tratta di metodologie incentrate sul trattamento in forma massiva delle informazioni contenute in insiemi di segnalazioni "aggregate" sulla base di caratteristiche comuni che garantiscano l'omogeneità dell'analisi, ad esempio la riconducibilità a specifiche fattispecie di operatività.

Complementare a quella tradizionale, l'analisi aggregata delle segnalazioni aiuta ad intercettare possibili contesti rilevanti di riciclaggio o finanziamento del terrorismo, la cui individuazione può rendersi difficoltosa utilizzando i metodi di analisi tradizionali.

L'approccio risulta particolarmente promettente in quei settori (es: servizi di money transfer, carte di pagamento, giochi e scommesse, valute virtuali) in cui l'operatività segnalata è connotata da caratteristiche di "frammentazione" e parcellizzazione determinate da fattori comuni, quali la presenza di numerosi soggetti e di operazioni, generalmente di importo contenuto, segnalate a seguito di anomalie di natura "oggettiva", e di una rete "distributiva" capillare, ma può rivelarsi particolarmente utile ogni volta che sia necessario ricostruire una rete relazionale tra i segnalati e le controparti, come avviene nelle segnalazioni relative a contesti di criminalità organizzata.

Le informazioni in questi casi possono assumere rilievo diverso aggregando i dati di più segnalazioni, in base al presupposto che gli elementi comuni (ricorrenza degli stessi soggetti, rapporti, punti operativi, controparti) possano aiutare a identificare e a ricostruire contesti più ampi "frammentati" su più segnalazioni, circostanza che spesso ricorre nel caso di operatività che sottende trasferimenti di fondi (servizi di *money transfer* e carte di pagamento).

Si tratta, peraltro, di settori che negli ultimi anni hanno avuto una crescita significativa, anche grazie allo sviluppo dei canali virtuali, all'ingresso di nuovi operatori nei servizi di pagamento, anche del c.d. *fintech*, che hanno reso sempre più facili e rapide le transazioni tra soggetti operanti e/o residenti anche in paesi diversi e molto distanti tra loro. La velocità e la semplicità delle modalità transattive permette di trasferire elevati importi in tempi molto ravvicinati, superando anche i limiti imposti dalle soglie normative introdotte per alcune tipologie di operazioni finanziarie.

In questo scenario, caratterizzato da una crescita significativa di segnalazioni provenienti dagli operatori di questi settori, aumenta in modo esponenziale il numero sia delle transazioni che dei soggetti coinvolti, e di conseguenza si infittisce anche la “rete” transazionale, spazialmente e temporalmente, rendendo sfidante per le autorità AML/CFT la predisposizione di analisi esaustive dei rischi che sono chiamate a presidiare. L’approccio basato sull’approfondimento della singola transazione e/o delle operazioni riconducibili ad un solo soggetto o ad un gruppo ristretto di persone non riesce sempre a cogliere, da solo, tutta la complessità di questo nuovo vasto insieme operativo, sempre più interconnesso.

Il punto di partenza dell’analisi aggregata è costituito dalla selezione di un insieme sufficientemente esteso di segnalazioni riferite a un intervallo temporale determinato, riguardanti una specifica categoria di operatori ovvero afferenti a una determinata fattispecie di operatività. Le informazioni estratte dalle segnalazioni (soggetti, operazioni, punti vendita) vengono messe assieme in forma aggregata e rielaborate, anche attraverso la creazione di indicatori di rischio specifici per ciascun comparto esaminato, finalizzati a cogliere fenomeni potenzialmente rilevanti attraverso diverse prospettive di analisi.

Sotto il profilo soggettivo, l’analisi è finalizzata alla individuazione dei soggetti più rilevanti e alla ricostruzione delle “reti” di entità collegate tramite transazioni (es: trasferimenti di rimesse, ricariche di carte prepagate); l’analisi dei punti operativi consente di intercettare eventuali situazioni di “concentrazione” di anomalie che possano rivelare l’esistenza di azioni “coordinate” da parte di organizzazioni criminali, con eventuale possibile coinvolgimento degli stessi punti operativi; l’analisi georeferenziata permette di cogliere alcuni fenomeni di natura territoriale, che possono essere espressione di attività di organizzazioni criminali locali, italiane o straniere.

Nell’ambito del settore dei *money transfer*, l’analisi aggregata può essere fondata su indicatori incentrati ad esempio sugli esecutori delle rimesse (*sender* o *receiver* in Italia), gli agenti, e sui “corridoi” che caratterizzano i trasferimenti. Per esecutori, rileva ad esempio la dimensione dell’operatività anomala (numero e importi delle transazioni effettuate nel periodo), la ricorrenza di segnalazioni, le circostanze di anomalia segnalate (es: incoerenze territoriali, numerosità paesi di scambio, numerosità delle controparti, utilizzo di più agenzie o di circuiti diversi, etc.). Per gli agenti, rileva soprattutto la ricorrenza di alcune fattispecie di anomalie segnalate (es: “frazionamenti”, incoerenze tra luoghi di origine dei mittenti e destinazione delle rimesse), che, anche se apparentemente riferibili ai clienti, possano rivelare – specie nel caso di agenzie di piccole dimensioni o insediate in zone poco densamente popolate – un possibile coinvolgimento in irregolarità volte a eludere obblighi normativi, se non in vere e proprie attività illecite. Per i “corridoi” viene eseguita una mappatura della localizzazione delle agenzie, dei paesi di origine degli esecutori e di origine/destinazione delle rimesse, volta a identificare ricorrenze anomale che possano essere rappresentative di organizzazioni criminali locali, italiane o straniere, ovvero di alcuni fenomeni caratterizzati da specifiche connotazioni geografiche (es: commerci illeciti, pedopornografia, traffico di esseri umani, truffe e frodi informatiche).

Anche nel settore dei giochi e delle scommesse, l’analisi aggregata può caratterizzarsi tramite l’elaborazione di indicatori di rischio riferiti ai soggetti, ad esempio, sulla base dell’ammontare delle operazioni, del profilo soggettivo, della ricorrenza di segnalazioni e di fattispecie di anomalia segnalate, e alle eventuali “reti” di giocatori che possano emergere ad esempio nell’ambito di operazioni di gioco “collusive” (gioco online). Analogamente al settore dei *money transfer*, è possibile identificare, nel caso di gioco fisico, le sale da gioco più rischiose, sulla base della frequenza delle anomalie ovvero di altre circostanze che possano essere espressione di irregolarità, come ad esempio legami familiari o finanziari tra i gestori delle sale e i giocatori.

Nel comparto delle carte, la prospettiva dell’analisi aggregata è tipicamente quella di ricostruire le “reti” transazionali di soggetti, espresse tipicamente nella forma di ricariche di carte prepagate, in contanti o a mezzo trasferimenti da carta a carta, tra una moltitudine di soggetti. L’operatività sottostante viene spesso segnalata in maniera estremamente frammentata, non solo per ragioni temporali connesse con la rilevazione periodica delle anomalie, ma anche per il diffuso ricorso a prestanome, indotto anche dalla necessità di eludere i limiti operativi imposti dagli emittenti. L’analisi aggregata consente di ricomporre i tasselli della rete e di ricostruire, attraverso l’analisi ricorsiva delle transazioni, le reti transazionali; una volta identificate le reti, è possibile anche in questo caso elaborare indicatori di rischio specifici finalizzati a individuare le più rilevanti. In alcune circostanze, inoltre anche nel settore delle carte è possibile identificare attività anomale presso specifici punti operativi, sulla base della localizzazione delle operazioni ovvero del coinvolgimento diretto nelle reti di soggetti titolari o di persone a loro collegate.

L’analisi aggregata consente in definitiva di identificare e recuperare contesti segnaletici rilevanti, non emersi con l’analisi tradizionale, da destinare a ulteriori approfondimenti mirati; si tratta spesso di contesti di particolare complessità, essendo distribuiti su una moltitudine di segnalazioni, ovvero situazioni di anomalia che possano riguardare i soggetti che gestiscono la rete distributiva, che in alcune circostanze potrebbero essere coinvolti in comportamenti illeciti. L’analisi aggregata, essendo incentrata su grandi masse di informazioni, si avvale anche di strumenti informatici e metodi dedicati per lo sfruttamento dei c.d. *big data* e per l’analisi delle reti transazionali (*data mining* e *Social Network Analysis*). La SNA si presta ad essere tipicamente applicata all’analisi delle reti, specie in quelle delle carte prepagate connotate da particolare complessità. L’utilizzo di numerose metriche messe a disposizione dall’analisi sociale delle reti permette non solo di evidenziare quali siano i soggetti più rilevanti all’interno di un preciso insieme di segnalazioni/operazioni, come avviene anche nell’approccio per indicatori, ma anche di

identificarne precisamente il loro ruolo (ad es., i *gatekeeper* ossia i principali intermediari, i soggetti più operativi sia in dare che in avere, le entità più importanti, quali le “authority” o gli “hub”, a seconda che siano rispettivamente ricevitori o datori di fondi, ecc.). È possibile anche identificare sottogruppi di rilievo (*cluster* o *clique*), a loro volta caratterizzati da specifiche modalità operative e/o di collocamento territoriale. Come già sopra accennato per l’analisi aggregata tramite indicatori, anche nelle elaborazioni tramite SNA, è possibile associare all’analisi della rete transazionale anche quella degli eventuali legami soggettivi (es. residenza, numero di cellulare, rapporti economico-finanziari in ambiti societari, eventuali indagini degli OO.II., informazioni da fonti aperte, anche da *social network*...), arrivando quindi ad avere una visione complessiva dei profili oggettivi e soggettivi, caratteristici dell’analisi AML/CFT. La SNA permette inoltre di evidenziare in dettaglio le interrelazioni tra i soggetti in esame, sia dal punto di vista statico, come appena visto, che dinamico. Si riesce in questo caso a vedere come, al passare del tempo, i ruoli e la rilevanza delle entità della rete, con le relative interdipendenze, mutano.

Utili possono essere anche le elaborazioni aggregate riferite a settori diversi da quelli precedentemente indicati; sviluppi interessanti stanno rivenendo dall’implementazione di analisi dei *big data* / *machine learning*, principalmente finalizzate a evidenziare, all’interno di un qualunque perimetro di analisi, i più noti *pattern* ad alto rischio, eventualmente anche in termini previsionali. Si fa riferimento all’identificazione automatica, per esempio, di fenomeni di false fatturazioni (identificando automaticamente la presenza di “cartiere”), oppure di frodi informatiche, oppure ancora nel riscontro di potenziali fenomeni di distrazione/monetizzazione di fondi aziendali, solo per citarne alcuni.

7. Sospensione delle operazioni sospette (B. Bastioni)

Tra le attribuzioni caratteristiche di una Financial Intelligence Unit rientra un potere particolare e incisivo che consente di bloccare temporaneamente l’esecuzione di operazioni sospette di riciclaggio o di finanziamento del terrorismo. Si tratta di un potere che in passato è stato disciplinato solo in minima parte dalla normativa internazionale e comunitaria, sino ad arrivare alla più recente e approfondita trattazione che ne viene fatta nell’ambito del pacchetto di proposte legislative della Commissione europea del luglio 2021.

Nella disciplina nazionale questo potere, già previsto nel regime antecedente pur se per una durata inferiore⁶⁶⁰, trova fondamento nell’art. 6, comma 4, lett. c), del D.lgs. 231/2007, come modificato dal D.lgs. 90/2017, secondo il quale la UIF può sospendere operazioni sospette, per un massimo di cinque giorni lavorativi, anche su richiesta di autorità qualificate – Nucleo Speciale di Polizia Valutaria della Guardia di finanza, Direzione Investigativa Antimafia, Autorità giudiziaria, FIU estera – ad una precisa condizione, ovvero che non ne derivi pregiudizio per il corso delle indagini.

Tale istituto, ben distinto dal congelamento dei fondi di cui al D.lgs. 109/2007 in materia di contrasto al finanziamento del terrorismo, è espressione del potere amministrativo conferito alla UIF di ritardare, in via provvisoria, l’esecuzione di operazioni sospette allo scopo di completare le proprie attività di analisi finanziaria e di fornire all’Autorità giudiziaria il tempo necessario per intervenire sul caso con misure cautelari. Questa finalità sostanziale di supporto alle funzioni dell’Autorità giudiziaria caratterizza in modo peculiare l’istituto ed è al contempo il riflesso, come si vedrà, dei principi di collaborazione e coordinamento tra la UIF e gli organi delle indagini.

7.1. La cornice normativa internazionale

I riferimenti della normativa internazionale all’istituto della sospensione sono molto limitati. Da un’analisi in materia condotta dalla Banca Mondiale in uno studio congiunto con il Gruppo Egmont del 2013⁶⁶¹ non esistono standard internazionali universali che regolino il potere delle FIU di sospendere operazioni sospette, né esiste una definizione normativa di detto potere che sia riconosciuta in sede internazionale.

In ambito regionale la prima fonte internazionale che tratta la materia è la Convenzione del Consiglio d’Europa del 2005 sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo: essa all’art. 14 prevede espressamente che ciascuno Stato adotti le misure legislative necessarie a consentire che, in caso di sospetto riciclaggio, la FIU sia in grado di adottare azioni urgenti per sospendere o non autorizzare l’esecuzione di operazioni allo scopo di

⁶⁶⁰ L’art. 3 comma 6 del DL 143/1991, convertito con modificazioni dalla legge 197/1991 e come sostituito dall’art. 1 del D.lgs. 153/1997, attribuiva all’Ufficio italiano dei cambi il potere di sospendere l’operazione, anche su richiesta degli Organi investigativi, per un massimo di quarantotto ore “sempre che ciò non possa determinare pregiudizio per il corso delle indagini e per l’operatività corrente degli intermediari, dandone immediata notizia agli Organi investigativi medesimi.”

⁶⁶¹ K. Stroligo, H. Intscher e S. Davis-Crockwell, *Suspending Suspicious Transactions*, World Bank Study, 2013.

analizzare le transazioni e confermare il sospetto; è previsto inoltre che la durata massima della sospensione sia fissata dalla legge nazionale. L'art. 47 della stessa Convenzione poi prevede che il potere di sospensione possa essere attivato anche su richiesta di una FIU estera, per la durata e nel rispetto delle regole previste dall'ordinamento della FIU che riceve la richiesta, a condizione che la transazione sia relativa a riciclaggio e che la stessa sarebbe stata sospesa qualora fosse stata oggetto di una segnalazione di operazione sospetta domestica.

Il potere di sospensione non è espressamente regolato da raccomandazioni del GAFI o da altri standard globali internazionali. Secondo il citato studio della Banca Mondiale⁶⁶² esso può tuttavia considerarsi collegato all'attuazione di due raccomandazioni del GAFI: la numero 20 sull'obbligo di segnalazione di operazioni sospette, da cui può ricavarsi che la FIU debba avere il tempo sufficiente per condurre le proprie analisi, e la numero 4 sulla confisca e le misure cautelari, in base alla quale le autorità competenti devono essere in grado di congelare, sequestrare e confiscare, anche per equivalente, beni riciclati, proventi o utilità collegati a riciclaggio o a reati presupposto o a finanziamento del terrorismo potendo attivare, tra l'altro, misure finalizzate a prevenire o evitare che sia pregiudicata la capacità dello Stato di sequestrare e recuperare valori soggetti a confisca.

Nel diritto comunitario, il tema è stato disciplinato con la terza direttiva antiriciclaggio 2005/60/CE solo in via indiretta e incidentale: all'art. 24, comma 1, si prevedeva che i soggetti obbligati dovessero astenersi dall'eseguire operazioni sospette di riciclaggio o di finanziamento del terrorismo prima di aver informato la FIU e che, in conformità della legislazione nazionale, potevano essere impartite istruzioni di non eseguire l'operazione. Non era tuttavia precisato che questo compito dovesse rientrare nelle competenze specifiche della FIU, restando rimessa la decisione al legislatore nazionale.

Solo con la successiva direttiva antiriciclaggio 2015/849/UE è stata delineata una più ampia disciplina dell'istituto della sospensione, compendiando di fatto le diverse disposizioni sopra citate di fonte internazionale e comunitaria. Viene infatti previsto all'art. 32, par. 7, che *“Gli Stati membri provvedono affinché, in presenza del sospetto che un'operazione sia collegata ad attività di riciclaggio o di finanziamento del terrorismo, sia conferita alla FIU la facoltà di intraprendere, direttamente o indirettamente, azioni urgenti per sospendere o rifiutare il consenso all'esecuzione dell'operazione allo scopo di analizzare l'operazione, confermare il sospetto e disseminare i risultati dell'analisi alle autorità competenti. È conferita alla FIU la facoltà di intraprendere, direttamente o indirettamente, tali azioni su richiesta di una FIU di un altro Stato membro per il periodo e alle condizioni specificati nella normativa nazionale della FIU che riceve la richiesta”*⁶⁶³.

Il pacchetto di proposte legislative della Commissione europea del luglio 2021 contiene, in particolare nella proposta di direttiva AML, una disciplina organica del potere di sospensione delle FIU. In particolare con l'art. 20 della proposta di direttiva AML, interamente dedicato al potere di sospensione delle FIU, la Commissione riordina e consolida la regolamentazione vigente già prevista dalla quarta direttiva 2015/849/UE, introducendo tuttavia anche alcune rilevanti novità.

In primo luogo (par. 1) si prevede che la misura della sospensione debba essere applicata nei confronti del soggetto obbligato entro un termine massimo di 48 ore dal ricevimento della segnalazione e che la durata complessiva della sua efficacia non possa essere superiore ad un massimo di 15 giorni di calendario a decorrere dal giorno dell'imposizione al soggetto obbligato. Viene poi ampliato l'ambito oggettivo di applicazione del potere (par. 2) che non è più limitato all'operazione sospetta ma viene esplicitamente esteso ai rapporti bancari o conti di pagamento, in presenza del sospetto che tali rapporti siano interessati da varie operazioni collegate ad attività di riciclaggio o di finanziamento del terrorismo. In tal caso, la sospensione, che deve essere imposta sempre entro 48 ore al soggetto obbligato, può avere una durata massima di 5 giorni a decorrere dal giorno dell'imposizione. Infine (par. 3) è previsto che debba essere garantita dagli Stati l'effettiva possibilità di contestare la sospensione in sede giurisdizionale da parte delle persone i cui conti bancari e di pagamento ne sono l'oggetto, in conformità delle procedure del diritto nazionale.

⁶⁶² K. Stroligo, H. Intscher e S. Davis-Crockwell, *Suspending Suspicious Transactions*, cit., p. 8.

⁶⁶³ La locuzione “direttamente o indirettamente” utilizzata dalla quarta direttiva sembra potersi intendere nel senso che la FIU debba essere in grado di esercitare il potere anche su richiesta di una competente autorità domestica; parrebbe infatti meno plausibile un'interpretazione tale per cui la FIU possa sospendere operazioni avvalendosi dell'azione di una autorità terza. Viene confermato invece che la sospensione va intesa quale strumento che la FIU utilizza per completare le proprie analisi, confermando se del caso il sospetto e – in aggiunta rispetto alle disposizioni sopra citate – disseminando i risultati delle analisi alle autorità competenti, analogamente a quanto avviene per le ordinarie funzioni di analisi finanziaria di segnalazioni di operazioni sospette: l'esercizio del potere di sospensione viene in tal modo pienamente ricondotto nell'alveo delle tipiche funzioni delle *Financial Intelligence Unit*. È confermata, infine, l'attivazione dell'istituto anche nell'ambito della collaborazione internazionale, nel rispetto delle condizioni previste dall'ordinamento della FIU che riceve la richiesta.

Alcune di queste misure, senz'altro ambiziose e orientate al tentativo di armonizzare la configurazione di un potere così importante per le FIU, sono al centro di riflessioni e proposte di modifica nell'ambito dei negoziati in corso tra i Paesi membri, in ragione della profonda diversità tra le giurisdizioni e della tendenza a voler preservare le specifiche prerogative nazionali; è molto probabile quindi che molti punti potranno essere oggetto di revisione rispetto alla proposta originaria della Commissione⁶⁶⁴.

7.2. La disciplina nazionale

La disciplina nazionale di cui al D.lgs. 231/2007 attribuisce alla UIF il potere di sospendere operazioni sospette di riciclaggio o finanziamento del terrorismo per un massimo di cinque giorni lavorativi, anche su richiesta degli Organi investigativi e dell'autorità giudiziaria e di una FIU estera, a condizione che non si rechi pregiudizio ad indagini in corso. Si tratta di un potere amministrativo di durata temporanea e di natura sostanzialmente cautelare, che mira a preservare lo stato di fatto o di diritto esistente – ovvero la mancata esecuzione, pur in via temporanea, di un'operazione sospetta di riciclaggio o finanziamento del terrorismo – in attesa del sopraggiungere, preferibilmente, di misure di sequestro da parte dell'Autorità giudiziaria.

In proposito, il già citato studio della Banca Mondiale fornisce una definizione della sospensione, quale misura tipicamente provvisoria finalizzata a fornire alla FIU il tempo di completare la sua valutazione circa la fondatezza del sospetto di riciclaggio o di finanziamento del terrorismo e ad agevolare le competenti autorità nell'adozione delle opportune misure cautelari⁶⁶⁵.

Nella disciplina nazionale antiriciclaggio, la sospensione può considerarsi il più rilevante provvedimento amministrativo di competenza della UIF. Ai fini della sua adozione l'Unità compie una serie di atti interni di analisi finanziaria e di carattere istruttorio che sono finalizzati, per un verso, a valutare la fondatezza del sospetto e la ricorrenza dei presupposti di legge, per l'altro, a verificare il rispetto della condizione di non recare intralcio ad indagini in corso.

Presupposto essenziale per l'esercizio del potere è la presenza di operazioni sospette, non ancora eseguite, di riciclaggio o di finanziamento del terrorismo, di cui la UIF può avere conoscenza per effetto dell'iniziativa in via d'urgenza da parte dei soggetti obbligati, della richiesta da parte di autorità qualificate ovvero in via autonoma nell'esercizio delle proprie funzioni di analisi finanziaria.

Affinché sia integrato tale requisito non è sufficiente la rappresentazione di una mera o generica anomalia operativa o comportamentale, ma deve sussistere un fondato e motivato sospetto che i valori relativi all'operazione di cui è imminente l'esecuzione siano riconducibili a riciclaggio o a un reato presupposto o a finanziamento del terrorismo⁶⁶⁶.

Affinché l'operazione possa essere valutata a fini di sospensione è poi necessario che essa sia stata formalmente richiesta da parte del cliente e non meramente annunciata come oggetto di generica intenzione ovvero che essa sia chiaramente determinata o almeno determinabile nei suoi elementi essenziali. In altre parole, il soggetto obbligato deve effettivamente trovarsi in punto di esecuzione dell'operazione stessa: non può valutarsi a fini di sospensione una transazione il cui perfezionamento dipenda dal completamento di requisiti formali ancora mancanti o dal verificarsi di una condizione sospensiva, magari meramente potestativa (caso in cui l'operazione potrebbe anche non essere mai eseguita).

⁶⁶⁴ Per una rassegna dei diversi approcci nazionali nella configurazione del potere di sospensione si veda anche il Research Report del Moneyval (Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures), *The postponement of financial transactions and the monitoring of bank accounts*, April, 2013.

⁶⁶⁵ K. Stroligo, H. Intscher e S. Davis-Crockwell, *Suspending Suspicious Transactions*, cit., p. 15, ove si legge: "Postponement of transactions is typically a short-term, interim measure intended to provide time for the FIU to complete its assessment as to whether there are grounds to suspect that the funds or assets involved are proceeds from criminal activity or related to terrorist financing, and for the competent authorities to initiate freezing and restraint measures, when appropriate."

⁶⁶⁶ Deve trattarsi pertanto di operazioni sospette ad alto rischio - ad esempio tipicamente bonifici esteri, prelevamenti di contante - la cui immediata esecuzione avrebbe l'effetto di sottrarre fondi ad eventuali provvedimenti cautelari dell'Autorità giudiziaria. La valutazione istruttoria svolta dalla UIF sulla fondatezza del sospetto rappresentato dal segnalante, unitamente agli altri elementi conoscitivi acquisiti come si dirà anche dagli Organi investigativi, costituisce il cuore della motivazione del provvedimento di sospensione.

Come evidente, il potere di sospensione è strettamente collegato all'obbligo di segnalare operazioni sospette possibilmente prima della loro esecuzione⁶⁶⁷: la tempestività della rappresentazione del sospetto alla UIF, prerogativa fondamentale del sistema di collaborazione attiva, diventa una imprescindibile condizione di procedibilità del procedimento amministrativo ai fini sospensione.

Nel definire l'oggetto del potere di sospensione la norma nazionale parla chiaramente di "operazioni" sospette di riciclaggio o di finanziamento del terrorismo: è quindi da considerarsi pacifico che il provvedimento di sospensione possa riguardare non solo una singola operazione ma anche molteplici transazioni ovvero, nei casi a maggior livello di rischio, tutte le operazioni in addebito a valere di rapporti la cui alimentazione possa essere fondatamente ricondotta ad attività di natura illecita. Tale interpretazione è d'altro canto funzionale a garantire la migliore efficacia ed utilità all'esercizio del potere di sospensione che potrebbe agevolmente essere vanificato in caso di richiesta da parte del cliente di un'operazione alternativa rispetto a quella specifica indicata nel provvedimento.

Sotto il profilo della durata, il D.lgs. 231/2007 prevede che la sospensione possa essere disposta per un massimo di cinque giorni lavorativi; la decorrenza del termine ha inizio dal momento in cui il provvedimento viene notificato dalla UIF al destinatario soggetto obbligato.

In considerazione della limitata durata temporanea del provvedimento di sospensione, l'ordinamento nazionale non prevede un apposito diritto di appello o di un diverso rimedio attivabile da parte del privato titolare dei rapporti incisi dal provvedimento amministrativo. Come riconosciuto dalla giurisprudenza della Corte europea dei diritti dell'uomo, i diritti fondamentali come quello di proprietà possono legittimamente subire restrizioni in base alla legge, nel rispetto del principio di proporzionalità, quando sia necessario tutelare obiettivi di interesse generale quali quelli di prevenzione del riciclaggio e del finanziamento del terrorismo.

Nell'ordinamento nazionale il provvedimento di sospensione, motivato sulla base di fondati elementi di sospetto rilevati nell'esercizio dei compiti di analisi finanziaria, è destinato ad essere notificato in via esclusiva e riservata solo al soggetto obbligato: non è prevista dalla legge la notifica dello stesso al cliente né appare configurabile la sua ostensione a quest'ultimo da parte del soggetto obbligato, eventualità che, oltre a compromettere la riservatezza dello stesso segnalante, potrebbe creare rischi di *tipping off* ponendosi in contrasto con il divieto di comunicazione di cui all'art. 39 del D.lgs. 231/2007 assistito da apposita sanzione penale⁶⁶⁸.

Più in generale al procedimento amministrativo di sospensione, atteso il carattere di riservatezza e urgenza a supporto dei poteri di carattere giudiziario, non si applicano le disposizioni della L. 241/90 relative alla comunicazione di avvio e alla individuazione dei termini di conclusione del procedimento.

Come già accennato, l'art. 6, comma 4, lett. c), del D.lgs. 231/2007 definisce una precisa condizione al legittimo esercizio del potere di sospensione: non deve arrecarsi pregiudizio ad indagini in corso⁶⁶⁹. Il rispetto di tale condizione implica un necessario e immediato coordinamento tra la UIF e gli organi delle indagini allo scopo di consentire una tempestiva condivisione delle informazioni disponibili sul caso e verificare che, confermata la fondatezza del sospetto e la ricorrenza dei presupposti di legge, il provvedimento di sospensione non crei intralcio alle indagini in corso, ma anzi possa eventualmente agevolare l'intervento di misure cautelari da parte dell'Autorità giudiziaria.

La naturale funzione della sospensione, infatti, data la sua durata temporanea, è quella, come detto, di preservare lo stato di fatto e di diritto ritardando l'esecuzione dell'operazione sospetta al fine di verificare la fondatezza del sospetto, se possibile fino al sopraggiungere di un provvedimento di sequestro da parte del magistrato competente. La condizione è quindi senz'altro verificata positivamente quando si raggiunge un'intesa affinché la sospensione dell'operazione sospetta da parte della UIF consenta agli organi delle indagini di avere il tempo necessario per l'adozione di apposite misure cautelari. Nel contempo, va precisato che il successivo intervento del sequestro non è di per sé un elemento essenziale dell'istituto

⁶⁶⁷ Il riferimento è all'art. 35, commi 1 e 2 del D.lgs. 231/2007.

⁶⁶⁸ Cfr. art. 55, comma 4 del D.lgs. 231/2007.

⁶⁶⁹ È interessante notare che nel regime previgente al D.lgs. 231/2007 la condizione di legge era più ampia in quanto si richiedeva l'assenza di pregiudizio non solo per il corso delle indagini ma anche "per l'operatività corrente degli intermediari" (cfr. art. 3, comma 6 del DL 143/1991, convertito con modificazioni dalla legge 197/1991, come sostituito dall'art. 1 del D.lgs. 153/1997).

della sospensione e non ne condiziona la legittimità, che dipende esclusivamente dalla inidoneità dell'atto ad arrecare intralcio alle indagini.

È infatti ben possibile, sebbene accada raramente, che al provvedimento di sospensione della UIF non segua il successivo sequestro da parte dell'Autorità giudiziaria la quale, proprio attraverso le attività d'indagine svolte nel periodo di sospensione, può maturare un convincimento diverso rispetto a quello originariamente espresso. In tal caso, e sempre che non si rechi intralcio alle indagini, il provvedimento di sospensione resta comunque legittimo nella sua funzione primaria di consentire alla UIF il completamento dei propri compiti di analisi finanziaria. Tuttavia, le nuove informazioni acquisite in questi casi possono mettere in dubbio la fondatezza del sospetto ovvero possono far emergere il rischio di una compressione sproporzionata dei diritti del privato essendovi la ragionevole certezza che l'atto non verrebbe seguito da misure cautelari: in queste ipotesi, pertanto, la UIF può rivalutare la situazione e, se del caso, procedere alla revoca del provvedimento di sospensione, pur legittimo, divenuto successivamente inopportuno per circostanze sopravvenute⁶⁷⁰.

Sul punto lo studio della Banca Mondiale raccomanda agli Stati di prevedere che la FIU sia in grado di ritirare la sospensione non appena emerga che il sospetto iniziale non è confermato o quando determinate condizioni non sono verificate⁶⁷¹.

Il potere di sospensione può essere esercitato dalla UIF anche su richiesta di omologhe FIU estere: in queste ipotesi l'informativa che proviene dall'autorità estera assume la valenza di una segnalazione di operazione sospetta domestica e, in relazione ad essa, viene comunque verificata la sussistenza delle condizioni previste dall'ordinamento nazionale per l'istituto.

La mancata osservanza del provvedimento di sospensione da parte dei soggetti obbligati comporta l'applicazione di una sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro (art. 58, comma 6, D.lgs. 231/2007, come modificato dal D.lgs. 90/2017).

Nell'esperienza applicativa dell'istituto, ancorché sia previsto dall'ordinamento nazionale, non si danno frequentemente casi di sospensione di operazioni sospette di terrorismo. Ciò probabilmente in ragione della particolare natura delle segnalazioni della specie, le quali originano, per lo più, da coincidenze anagrafiche, anche parziali, con nominativi censiti in liste internazionali e da cui derivano, peraltro, obblighi diretti di congelamento a carico degli intermediari. Nei diversi casi di segnalazioni di terrorismo in cui il sospetto non deriva da evidenze anagrafiche, ma da anomalie legate all'operatività, può rivelarsi probabilmente difficoltoso intercettare, in corso di esecuzione, operazioni di importo in genere molto contenuto e di origine spesso lecita, ma destinate ad essere utilizzate per finalità illecite. Si tratta, in altre parole, di elementi di sospetto che generalmente vengono decifrati e segnalati dagli intermediari solo in una fase successiva a quella di esecuzione dell'operazione.

⁶⁷⁰ Il riferimento è all'art. 21-*quinquies* della legge 241/1990 secondo il quale i provvedimenti amministrativi ad efficacia durevole possono essere revocati dagli organi che li hanno adottati per sopravvenuti motivi di pubblico interesse, sulla base di nuovi presupposti di fatto o di una nuova valutazione delle originarie circostanze di fatto. La revoca quindi implica la presenza di vizi di merito e non di legittimità e riguarda un atto divenuto inopportuno per circostanze sopravvenute o per una nuova valutazione di quelle originarie; di conseguenza ha efficacia *ex nunc*. L'annullamento d'ufficio invece, di cui all'art. 21 *nonies* della legge 241/1990, riguarda atti amministrativi *ab origine* illegittimi ed ha pertanto efficacia retroattiva.

⁶⁷¹ Da K. Stroligo, H. Intscher e S. Davis-Crockwell, *Suspending Suspicious Transactions*, cit., p. 26: "It is therefore recommended that FIUs be legally authorized to lift a postponement order as soon as it is determined that the initial suspicion has not been confirmed or that certain other conditions are met. Such conditions may include the following: There is no longer a risk that the funds, the client, or the suspect will flee the jurisdiction. The FIU can no longer effectively mitigate the risk of a client or suspect being alerted about the postponement order. A formal restraining order or freezing order has been issued by competent authorities. The legal origin of funds in question has been proven. Investigation into the person or transaction has ceased."

7.3. Indipendenza della UIF e coordinamento con gli Organi investigativi

Come si è detto, la norma stabilisce che la UIF sospende operazioni sospette di riciclaggio o di finanziamento del terrorismo anche su richiesta degli Organi investigativi, dell'autorità giudiziaria o di una FIU estera.

Come osservato nel citato studio della Banca Mondiale, questa configurazione del potere, attivabile anche su richiesta di un'autorità esterna, caratterizza un significativo numero di giurisdizioni⁶⁷². Ci si potrebbe chiedere in proposito se tale previsione non rischi di determinare un possibile condizionamento dell'indipendenza e dell'autonomia decisionale di cui la FIU deve avvalersi nell'esercizio delle sue funzioni.

In merito va rammentato infatti che la raccomandazione n. 29 del GAFI e la relativa nota interpretativa richiedono che la FIU sia dotata di indipendenza ed autonomia operativa ovvero che essa abbia l'autorità e la capacità di esercitare le sue funzioni in maniera libera. In coerenza con tale previsione è da ritenere che la norma nazionale lasci del tutto impregiudicata la piena e autonoma capacità decisionale della UIF che, anche nel caso – invero assai raro – di richiesta di sospensione da parte di una autorità esterna qualificata, dovrà comunque valutare la ricorrenza dei presupposti di legge e la fondatezza del sospetto di riciclaggio o di finanziamento del terrorismo.

Nella prassi applicativa in genere è proprio la UIF che si attiva grazie, a sua volta, alla tempestiva comunicazione da parte di un soggetto obbligato, per condividere con gli Organi investigativi la notizia di un'operazione sospetta in fase di esecuzione suscettibile di valutazione a fini di sospensione.

Negli ultimi anni, inoltre, la UIF ha sviluppato una autonoma strategia di monitoraggio quotidiano sulle segnalazioni di operazioni sospette non eseguite a elevato rischio, incrementando la capacità di avviare d'iniziativa l'iter del procedimento di sospensione, con un tasso di esito positivo superiore a quello riscontrato su impulso dei segnalanti⁶⁷³.

Pertanto si può ritenere che il coordinamento informativo e operativo, che avviene con gli Organi investigativi nel caso della sospensione, non vada inteso quale limitazione dell'autonomia decisionale della UIF ma anzi quale momento di massima espressione del principio di collaborazione tra le autorità preposte alla prevenzione del riciclaggio e del finanziamento del terrorismo, ciascuna nel pieno esercizio delle proprie funzioni. La UIF, infatti, attraverso il sistema della collaborazione attiva acquisisce in "anteprima" l'informazione sull'operazione sospetta in corso di esecuzione e la trasmette tempestivamente agli Organi investigativi al fine di completare il processo di analisi finanziaria e conoscere l'eventuale interesse dell'Autorità giudiziaria al blocco dei relativi fondi. Questo processo di condivisione delle rispettive informazioni ha lo scopo di permettere la convergenza verso una strategia operativa concertata che si articola in due tempi: l'immediata sospensione dell'operazione sospetta da parte della UIF per cinque giorni lavorativi, nel corso dei quali possa intervenire, se del caso, il sequestro dei relativi fondi da parte dell'Autorità inquirente.

La particolare efficacia di questa strategia concertata emerge in particolare nei casi in cui la sospensione si dimostra in grado di ritardare, fino all'intervento di misure di sequestro, un prelevamento di contante o un deflusso verso l'estero di fondi di origine illecita, la cui immediata esecuzione avrebbe vanificato l'azione cautelare della magistratura; attraverso la sospensione, inoltre, la UIF riesce ad allertare l'autorità inquirente circa l'imminente esecuzione di transazioni distrattive, dissipative o dissimulatorie, di cui molto spesso non vi era alcuna precedente conoscenza, dando all'autorità stessa il tempo di porvi rimedio con le opportune misure e notevole contributo allo sviluppo delle indagini.

Infine è da tener presente che, malgrado il numero apparentemente esiguo dei provvedimenti di sospensione adottati per anno dalla UIF (30 nel 2021) in rapporto al numero delle istruttorie avviate (227 nello stesso anno), l'iniziativa di condivisione informativa molto spesso è in grado di intercettare situazioni di concreto interesse per gli organi inquirenti, sebbene non venga poi emanato un provvedimento amministrativo. In altre parole, l'esito negativo del procedimento di sospensione dato dalla mancata adozione del provvedimento da parte della UIF è da intendersi spesso come indicazione di inopportunità della sospensione da parte dell'Autorità giudiziaria, che ha manifestato un preciso interesse investigativo sul caso e ha preferito non interrompere l'operatività per esigenze legate alle indagini in corso. In questo senso, sul totale delle istruttorie avviate nel 2021 che non si sono concluse con un provvedimento, in oltre il 76% dei casi la fattispecie è stata ritenuta dagli Organi inquirenti meritevole di essere portata all'attenzione dell'Autorità giudiziaria ed ha quindi intercettato situazioni di potenziale interesse investigativo.

⁶⁷² K. Stroligo, H. Intscher e S. Davis-Crockwell, *Suspending Suspicious Transactions*, World Bank Study, cit., p. 20.

⁶⁷³ Cfr. Rapporto annuale UIF per il 2021, p. 39.

Il potere di sospensione è uno strumento particolarmente efficace nel sistema di prevenzione del riciclaggio e di finanziamento del terrorismo: esso consente alla FIU, autorità incaricata di ricevere le segnalazioni di operazioni sospette dalla variegata platea di soggetti obbligati, di intervenire a ritardare l'esecuzione di operazioni ad elevato rischio, il cui immediato perfezionamento avrebbe l'effetto di far perdere irrimediabilmente le tracce di fondi di natura illecita ovvero di sottrarre quei fondi all'applicazione di misure cautelari da parte della magistratura.

Come si è visto, data la disciplina prevista dal D.lgs. 231/2007 e la sua limitata durata nel tempo, la sospensione si configura come un atto amministrativo cautelare sostanzialmente propedeutico a una successiva misura giudiziaria di sequestro. Questa naturale sequenza di atti si perfeziona all'esito di un processo stringente di condivisione informativa e coordinamento operativo tra la UIF e gli organi incaricati delle indagini, che mira a definire una strategia concertata di intervento sul caso sospetto. Tale processo di condivisione informativa e operativa se, per un verso, colma la lacuna derivante dal mancato accesso diretto per la UIF ai dati di natura criminale, per l'altro, può ritenersi uno dei momenti di massima espressione della collaborazione e del coordinamento tra la UIF e gli organi delle indagini a fini di prevenzione del riciclaggio e finanziamento del terrorismo.

Al tempo stesso va rammentato che il fattore che innesca l'intero processo è molto spesso rappresentato dalla collaborazione attiva da parte dei soggetti obbligati. Le comunicazioni realmente rilevanti riguardano non generiche anomalie operative ma motivi di sospetto fondati, ponderati e soprattutto tempestivi, in grado di portare all'attenzione della UIF operazioni, in procinto di essere eseguite, ad alto livello di rischio di riciclaggio o di finanziamento del terrorismo. In tal senso, si può dire che le segnalazioni provenienti dai soggetti obbligati che, all'esito del processo di collaborazione e coordinamento tra la UIF e gli organi delle indagini, conducono all'adozione del provvedimento di sospensione – in specie se seguito poi da un decreto di sequestro da parte dell'autorità giudiziaria – possono considerarsi l'esempio della migliore e più efficace collaborazione attiva nella prevenzione del riciclaggio e del finanziamento del terrorismo.

8. Tutela della riservatezza e divieto di comunicazione (D. Muratti)

La riservatezza delle segnalazioni di operazioni sospette rappresenta un valore da tutelare in maniera rigorosa per il corretto funzionamento del sistema antiriciclaggio nel suo complesso, poiché su di esso si fonda il rapporto di fiducia tra segnalanti e UIF che consente lo sviluppo della collaborazione in modo oggettivo e libero da condizionamenti; inoltre, il segreto sulle informazioni rilevanti ai fini del D.lgs. 231/2007 è assoluto e può essere derogato unicamente nei casi indicati dall'art. 12 del medesimo decreto. Ne consegue che, al di fuori delle doverose comunicazioni tra segnalante e autorità di controllo antiriciclaggio nell'esercizio dei poteri analitici, ispettivi o investigativi, l'approccio debba essere restrittivo e improntato alla massima riservatezza. A queste finalità rispondono gli ingenti investimenti volti a informatizzare il settore adottando sistemi che garantiscano anche la sicurezza degli scambi e della conservazione dei dati.

Approcci meno orientati a garantire la tutela dei dati esporrebbero i segnalanti al rischio di subire condizionamenti e comportamenti ritorsivi in grado di pregiudicare la collaborazione in materia antiriciclaggio; ne potrebbero derivare carenze nell'attività segnaletica e, quindi, effetti negativi sul buon funzionamento e sull'efficacia dell'intero sistema di prevenzione nonché sulla connessa azione pubblica di contrasto dei reati.

Il sistema antiriciclaggio si basa sulla comprensione ed elaborazione di dati e informazioni, essenziali per valutare adeguatamente il dittico dati personali/profilo operativo della clientela che deriva dall'adeguata verifica della clientela; quest'ultimo si è evoluto passando, nel tempo, dalla mera identificazione fino a giungere a comprendere anche l'insieme di attività e procedure volte alla valutazione delle operazioni poste in essere, occasionalmente o in via continuativa. Si tratta di un processo dinamico e progressivo, ricco di sfumature, che impone un costante aggiornamento delle informazioni e una conseguente valutazione di coerenza tra gli elementi conoscitivi acquisiti nel momento dell'*on boarding* del cliente/utente.

Il tema della sicurezza nella gestione dei dati va assumendo un peso preponderante e una peculiare connotazione in una realtà sempre più permeata dall'utilizzo della rete e delle nuove tecnologie informatiche.

Tralasciando il ruolo chiave delle aziende del web, per le quali il dato grezzo assume un valore strategico strettamente funzionale al proprio posizionamento sul mercato, giova qui ricordare che, sia la Convenzione europea dei Diritti dell'Uomo (CEDU), sia il Trattato sul Funzionamento dell'Unione europea (TFUE) riconoscono il diritto alla protezione dei dati come un diritto fondamentale dell'individuo, del tutto autonomo e distinto dal più generale diritto alla riservatezza, usualmente indicato come *privacy*⁶⁷⁴.

Contestualmente a tali principi, però, si è gradualmente affermata la necessità che l'esercizio del diritto di tutela della protezione dei dati debba poter coesistere con l'esercizio degli altri diritti, compresa la libertà di stampa e ogni forma di libera manifestazione del pensiero, ma soprattutto con le esigenze connesse alla sicurezza e alla protezione di altri diritti fondamentali. Il già citato art. 8 della CEDU, infatti, al comma 2 stabilisce che *“non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui”*⁶⁷⁵.

È quindi ben possibile che l'istanza di protezione del dato coesista con le esigenze di suo sfruttamento per finalità quali la garanzia della sicurezza nazionale, del benessere economico nazionale, la prevenzione dei reati o la protezione dei diritti e delle libertà; in un sistema come quello dell'antiriciclaggio, basato sulle segnalazioni di operazioni sospette, che si colloca nel comparto della prevenzione e non della repressione, la tutela della riservatezza si estende fino a tutelare anche l'identità del segnalante, per evitare ogni condizionamento – diretto o indiretto – all'esercizio della collaborazione attiva. Si impone, quindi, una delicata ricerca di bilanciamento tra i diritti, al quale il sistema antiriciclaggio non può sottrarsi.

8.1. Genesi delle segnalazioni antiriciclaggio e tutela della riservatezza

La fonte principale delle informazioni antiriciclaggio sono le segnalazioni di operazioni sospette, che scaturiscono dall'analisi di dati e informazioni che possono afferire alla sfera soggettiva o transazionale della clientela. Si tratta di un'attività il cui valore aggiunto risiede nella valutazione e ponderazione degli elementi di rischio insito nella clientela da parte di un'ampia e diversificata platea di segnalanti, cui appartengono banche, intermediari finanziari e di pagamento, professionisti, aziende fornitrici di servizi, pubbliche amministrazioni.

Il semplice possesso di informazioni, per quanto ampie, complete e tempestive, appare quindi di per sé insufficiente a generare un flusso segnaletico, come anche la rilevazione di una semplice anomalia; sono condizioni necessarie ma non sufficienti. Motore di tutto il sistema antiriciclaggio è la collaborazione attiva degli operatori; il legislatore europeo ne ha incentivato lo sviluppo facendola rientrare nella sfera

⁶⁷⁴ Cfr. art. 8 della Convenzione europea sui Diritti dell'Uomo, e art. 16 del Trattato sul funzionamento dell'Unione europea. La versione più recente della CEDU, firmata a Roma il 4 novembre 1950, si trova al link https://www.echr.coe.int/Documents/-Convention_ITA.pdf; per quanto riguarda il TFUE, invece, si rimanda al link <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12012E%2FTXT>. Il diritto alla privacy è strettamente connesso a uno dei valori fondanti di tutte le carte dei diritti, ovvero la tutela della dignità umana; più che connotare un diritto autonomo, la *privacy* è volta ad affermare uno *ius excludendi alios* dalla propria vita privata senza un consenso esplicito, a meno che non si tratti di informazioni già note e di pubblico dominio e interesse. A differenza della privacy, che rappresenta un diritto della persona a veder tutelata la propria sfera personale dalle interferenze pubbliche, la riservatezza scaturisce da accordo fiduciario tra le parti che si obbligano a non divulgare specifiche informazioni a persone e con modalità non autorizzate. Ne deriva che, mentre il regime della privacy impedisce a chiunque di interferire nelle questioni personali di una persona, nella riservatezza, al contrario, le informazioni possono essere comunicate solo ed esclusivamente ad alcune persone che abbiano determinati requisiti e possano garantire l'uso corretto delle medesime.

⁶⁷⁵ Il diritto alla protezione dei dati personali è stato affermato per la prima volta nell'art. 12 della Dichiarazione universale dei diritti dell'uomo (UDHR) delle Nazioni Unite (ONU) del 1948, che ha di fatto ispirato i successivi strumenti legislativi. Nell'ambito dell'Unione europea, esso è stato sancito nella Carta dei diritti dell'Unione europea (Carta di Nizza) proclamata nel 2000; originariamente un documento politico, la Carta di Nizza diventa giuridicamente vincolante nel 2007 con la firma del Trattato di Lisbona entrato in vigore nel 2009. L'art. 7 della Carta prevede il rispetto della vita privata e familiare (quindi la privacy), mentre l'art. 8 sancisce la tutela dei dati di carattere personale (*data protection*). Con il trattato di Lisbona tale diritto entra nel novero dei diritti fondamentali; dovendo essere garantito allo stesso modo in tutti gli Stati dell'Unione e coesistere con gli altri diritti, compresa la libertà di stampa e di manifestazione del pensiero esso ha richiesto un apposito regolamento, e precisamente il regolamento (UE) 2016/679 del 27 aprile 2016, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

coperta dall'interesse pubblico, come si legge all'art. 43 della direttiva (UE) 2015/849, che recepisce l'art. 8 della CEDU⁶⁷⁶.

La tutela della riservatezza – che, come vedremo, ha subito una sua evoluzione nel tempo – configura il presupposto e la garanzia affinché i soggetti cui viene demandato il compito di esercitare la collaborazione attiva operino in totale libertà, senza condizionamenti e ingerenze di qualsivoglia natura. La normativa europea ha affermato tale principio introducendo nella direttiva citata uno speciale regime di riservatezza, che si applica alla persona fisica incaricata di effettuare la segnalazione di operazione sospetta: l'art. 37 della citata direttiva (UE) 2015/849 si pone come garanzia di libertà e di indipendenza del soggetto segnalante nelle valutazioni relative al profilo di rischio della clientela stessa. A rafforzare il principio, il successivo art. 38 sancisce la protezione personale di tutti i soggetti che sono a vari titoli coinvolti nella definizione del flusso segnaletico, affermando l'obbligo per gli Stati membri di tutelarli *“da qualsiasi minaccia o atto ostile, in particolare da atti avversi o discriminatori in ambito lavorativo”*⁶⁷⁷.

Questi principi sono stati integralmente – e letteralmente – recepiti nell'art. 38 del D.lgs. 231/2007, secondo cui il principio di tutela della riservatezza si applica alle persone fisiche incaricate di effettuare le segnalazioni di operazioni sospette, le quali devono poter svolgere le attività di ricognizione e di valutazione delle transazioni disposte dalla clientela senza subire costrizioni o condizionamenti ambientali, aziendali o derivanti dal rapporto con la stessa clientela osservata. La previsione si completa con l'obbligo di conservazione della documentazione e con la disposizione dell'art. 39 dello stesso decreto, che stabilisce un divieto assoluto di divulgazione dei contenuti segnaletici, esteso anche alla semplice divulgazione dell'esistenza stessa della segnalazione e che può essere derogato, come si vedrà, solo nei casi previsti dall'art. 12 del decreto e nell'ambito dei rapporti tra segnalante e Autorità di controllo antiriciclaggio nell'esercizio, da parte di queste ultime, dei poteri ispettivi o investigativi⁶⁷⁸.

Le norme richiamate sono applicabili a vari contesti; per quanto concerne la sfera di interesse e attività dei segnalanti, esse mirano ad assicurare, alle persone fisiche cui viene demandato l'intero processo segnaletico, di poter operare in totale libertà e senza condizionamenti.

La protezione della funzione antiriciclaggio risulta rinforzata da due ulteriori disposizioni: da un lato, dal comma 2 dell'art. 38, che prevede l'obbligo di custodia della documentazione assicurandone la riservatezza, dall'altro, dalla sanzione prevista dall'art. 55, comma 4, che punisce chi, essendo a conoscenza di una segnalazione di operazione sospetta, violi il divieto di darne comunicazione a terzi stabilito dall'art. 39.

Ne deriva che né la segnalazione, né i dati utilizzati per l'analisi delle transazioni individuate come sospette – finiti o semilavorati – possano circolare all'interno dell'azienda di appartenenza, se non nella normale dialettica con la funzione antiriciclaggio, che gode di un particolare regime di autonomia decisionale rispetto ad altre funzioni aziendali.

Se la segnalazione proviene da un professionista, l'applicazione di questo principio si profila piuttosto lineare; per le segnalazioni antiriciclaggio effettuate da banche e altri intermediari finanziari, invece, si possono intravedere alcune criticità nella misura in cui le tutele di riservatezza appaiono rivolte essenzialmente alla persona fisica e sembrano non comprendere anche l'azienda per conto della quale questa opera.

Come detto, la norma italiana è la letterale trasposizione delle disposizioni stabilite a livello europeo, che sembrano piuttosto incentrate sul tema della protezione della persona fisica del segnalante contro eventuali ritorsioni aziendali.

La tutela della persona fisica che viene così affermata sembrerebbe più coerente con la normativa del *whistleblowing*, in quel contesto, infatti, denunciato e denunciante lavorano insieme e le denunce rimangono endogene alla stessa realtà lavorativa, andando a creare una specie di meccanismo di protezione interno all'amministrazione stessa da cui promanano. Al contrario, l'output della funzione antiriciclaggio non ha una rilevanza esterna (né è anzi preclusa la conoscenza, tranne nei casi di sospensione seguita da sequestro) ed è destinato a essere condiviso con una filiera di *stakeholders* esterni, al cui centro si trova la UIF e alla quale partecipano Organi investigativi, Autorità giudiziarie e organi di coordinamento centrali come la Direzione Nazionale Antimafia e Antiterrorismo.⁶⁷⁹ In secondo luogo, nel *whistleblowing* la tutela della persona fisica è finalizzata a

⁶⁷⁶ Cfr. art. 43 della direttiva (UE) 2015/849. L'art. 8 della CEDU - Convenzione europea sui Diritti dell'Uomo considera l'attività segnaletica antiriciclaggio *“necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui”*.

⁶⁷⁷ Cfr. artt. 37 e 38 della direttiva (UE) 2015/849.

⁶⁷⁸ Cfr. artt. 38, comma 1, e 39, comma 1, del D.lgs. 231/2007.

⁶⁷⁹ La normativa sul *whistleblowing* è un'acquisizione recente nell'ordinamento italiano, in cui solo di recente sono state introdotte specifiche misure per tutelare i soggetti che scelgono di denunciare illeciti, all'interno delle organizzazioni pubbliche in cui prestano servizio. Per una rassegna più completa sul tema, vedasi il sito dell'Agenzia Nazionale Anti Corruzione <https://www.anticorruzione.it/-/whistleblowing>.

prevenire ritorsioni e a favorire la formazione di una sorta di sistema immunitario organico; il *whistleblower* aiuta la sua amministrazione a individuare al suo interno gli elementi i cui comportamenti divergenti potrebbe creare danni reputazionali, patrimoniali o economici. Nell'antiriciclaggio, invece, la segnalazione di operazione sospetta rimane strettamente limitata alla struttura da cui promana e può essere comunicata solo ai destinatari previsti dalla legge (UIF e Organi investigativi e/o Autorità giudiziaria ove previsto).

Di fatto, l'assetto normativo primario vigente, che si fonda sui principi di tutela della persona fisica-protezione dei dati-divieto di loro divulgazione, è un indiretto riconoscimento del fatto che il reale valore aggiunto della collaborazione attiva consiste proprio nella possibilità di esprimere valutazioni rigorose e oggettive degli elementi di sospetto da parte del responsabile delle segnalazioni di operazioni sospette.

L'esperienza, tuttavia, indica che l'efficacia della funzione antiriciclaggio in ambito bancario dipende anche dalle scelte fatte dall'azienda in merito al grado di autonomia che le viene conferito, dall'efficacia e tempestività delle procedure di adeguata verifica, dalle dotazioni tecnologiche che l'azienda mette a disposizione per rendere fluido e sicuro lo scambio tra il primo e il secondo livello di rilevazione antiriciclaggio. Essa è, inoltre, direttamente proporzionale alla possibilità di accesso alle informazioni aziendali e a data base esterni; quanto più questa è ampia, tanto migliore sarà la qualità delle informazioni veicolate alla UIF – e per il tramite di questa, all'intera filiera antiriciclaggio – attraverso i flussi segnaletici.

Il livello di efficienza della funzione antiriciclaggio dipende, quindi, in buona misura da una serie di decisioni aziendali che devono essere improntate alla più alta condivisione degli obiettivi di prevenzione del riciclaggio. Appare evidente che l'attuale formulazione della norma crea un'asimmetria tra l'azienda e la funzione antiriciclaggio; l'azienda è tenuta a creare le condizioni ottimali affinché la funzione antiriciclaggio operi al meglio, ma risulta totalmente priva di qualsivoglia protezione in termini di riservatezza, che appare appannaggio silo della persona fisica del segnalante.

L'*impasse* si potrebbe superare adottando un'interpretazione estensiva della norma, nata con l'intento di rendere la funzione antiriciclaggio forte all'interno dell'azienda; se, infatti, la tutela della riservatezza del responsabile delle SOS può garantirne il corretto esercizio dell'attività segnaletica, la sua estensione all'intera azienda potrebbe essere un forte incentivo a favore della definizione di una cornice organizzativa e di competenze che elevino il livello della collaborazione attiva. Viceversa, un'interpretazione restrittiva e letterale, che limita il regime di protezione della riservatezza alla persona fisica, potrebbe rappresentare una criticità e frenare molti investimenti. Si pensi, ad esempio, agli interventi volti ad agevolare e rendere più sicura e tempestiva la comunicazione tra il primo e il secondo livello di rilevazione aziendale, oppure alla necessità di investire nella formazione, o, infine, alle dotazioni di strumenti di analisi ed elaborazione necessari per sfruttare tutto il potenziale informativo dei database interni o esterni.

La mancata garanzia di tutela della riservatezza aziendale, inoltre, potrebbe indurre i segnalanti ad affidare la rilevazione del sospetto a sistemi informatici tarati su semplici anomalie, limitando al massimo l'apporto valutativo del responsabile della funzione antiriciclaggio e producendo flussi segnaletici sempre più oggettivi. Il minor apporto valutativo della funzione antiriciclaggio – che in questo modo andrebbe attenuando la sua rilevanza – influirebbe negativamente sulla completezza e significatività delle informazioni, che risulterebbero piuttosto scaturite da elementi di rischio generici, poco utili ad analisi mirate, complete e tempestive su singole posizioni e, in ultima analisi, non conformi allo spirito della normativa antiriciclaggio.

Questa prospettiva ha già iniziato a diventare realtà, favorita in gran misura dai cambiamenti indotti dall'era web 2.0. in cui la tradizionale relazione con la clientela non è più personale, ma cede il passo alla tecnologia informatica; è esperienza condivisa il fatto che ormai tutte le fasi della relazione bancaria, dall'*on boarding* fino al processo di KYC, siano affidate a sistemi informatizzati, che ne permettono lo svolgimento a distanza. Se, da un lato, questa evoluzione apporta efficienza, abbate i costi e velocizza le diverse operazioni, dall'altro, potrebbe portare a una minor profondità della conoscenza del cliente, con conseguenze evidenti per attività, come quella dell'antiriciclaggio, basate sulla valutazione del richiamato dittico profilo soggettivo-tipologia delle transazioni.

D'altro canto, anche i sistemi di rilevazione antiriciclaggio hanno subito la spinta innovativa della tecnologia e, in particolare, dell'evoluzione legata all'intelligenza artificiale che, tuttavia appare ancora insufficiente a sostituire la capacità di valutazione degli esseri umani, all'attuale grado di sviluppo; occorre, quindi, presidiare costantemente i processi affidati ai sistemi automatici di rilevazione per evitare che essi attenuino sostanzialmente l'efficacia dell'intero sistema antiriciclaggio, creando il paradosso di un numero elevatissimo di segnalazioni di basso contenuto informativo.

8.2. I presidi normativi a tutela della riservatezza

Come già detto, il principio di riservatezza previsto dal D.lgs. 231/2007 è assoluto e può essere derogato solo nelle ipotesi previste dall'art. 12 e in occasione dei rapporti tra segnalante e Autorità di controllo antiriciclaggio nell'esercizio da parte di queste ultime dei poteri ispettivi o investigativi.

Poiché, come già detto in premessa, il rispetto del principio di riservatezza costituisce il presupposto per un rapporto fiduciario con i segnalanti, all'interno di un sinallagma nel quale la collaborazione attiva risulta incoraggiata e favorita dall'impegno a non divulgare né i dati comunicati né l'identità del segnalante al di fuori dei casi e secondo le modalità previste dalla legge, la UIF ha dato un'interpretazione estensiva agli obblighi che il decreto antiriciclaggio prevede per la tutela del segnalante, estendendone l'applicazione a tutte le informazioni raccolte, conservate e gestite dall'Unità.

A tal fine è stata data piena attuazione a quanto prescritto dal comma 6 dell'art. 38 del decreto antiriciclaggio, adottando canali riservati e sicuri per l'acquisizione, la conservazione e la gestione dei flussi segnaletici⁶⁸⁰. L'Unità di informazione finanziaria utilizza da oltre un decennio un sistema informatico dotato di adeguati presidi di sicurezza, che garantisce ai segnalanti un apposito canale – riservato e protetto – per lo scambio delle informazioni, utilizzato non solo al momento dell'imputazione e della conservazione dei dati nel sistema, ma anche in occasione dei successivi contatti per le analisi e gli approfondimenti, in piena coerenza con quanto previsto dal richiamato comma 6 dell'art. 38 del decreto antiriciclaggio. Analogo sistema è stato approntato per l'interlocuzione con la rete estera delle FIU e con l'autorità giudiziaria; l'utilizzo di questi sistemi non solo rende più sicuri gli scambi di informative a livello istituzionale, ma consente anche di effettuare l'immediato aggiornamento degli archivi che registrano in tempo reale le richieste pervenute dalla Magistratura e producono immediati alert di sistema, elevando la capacità di individuazione dei contesti a maggior rischio e l'efficienza del sistema.

Anche la disseminazione verso gli Organi investigativi avviene attraverso canali dedicati, caratterizzati da misure di sicurezza che garantiscono comunicazioni protette e tempestive. Come con i segnalanti, anche con gli Organi investigativi le comunicazioni funzionano in entrambe le direzioni, e quindi, attraverso gli stessi canali e con gli stessi presidi di sicurezza gli archivi UIF sono alimentati da feedback ed esiti investigativi, per un aggiornamento in tempo reale delle valutazioni di rischio che vengono effettuate in sede di analisi delle SOS.

Particolare attenzione viene posta alla consultazione dei dati da parte del personale dell'Unità. La consultazione degli archivi UIF è sottoposta a un sistema di audit interno basato su log attraverso cui sono censiti gli accessi dei singoli analisti alle segnalazioni di operazioni sospette, sulla falsariga di quanto disposto dal Garante della protezione dei dati per l'accesso ai dati bancari, nelle diverse fasi di gestione del flusso segnaletico. L'insieme dei log consente il tracciamento della diffusione dell'informativa all'interno dell'Unità in connessione con le esigenze di approfondimento e di analisi dei flussi principali e di quelli collegati, e persegue l'obiettivo di rafforzare e rendere cogente il principio di riservatezza⁶⁸¹.

Ovviamente si tratta di un processo che, una volta avviato, deve essere opportunamente presidiato per assicurare che la rapida obsolescenza dell'infrastruttura informatica non diminuisca il livello di sicurezza del sistema. Una struttura efficiente deve, infatti, garantire non solo il livello di qualità del proprio output, ma anche l'aggiornamento dei presidi di sicurezza che devono rimanere elevati e in grado di fronteggiare le minacce lungo tutte le fasi di elaborazione dei flussi. A questo fine, tutte le componenti del sistema informatico sono periodicamente sottoposte ad apposite verifiche atte a individuare tempestivamente la presenza di potenziali vulnerabilità di sicurezza e ad applicare i necessari aggiornamenti con l'obiettivo di evitare accessi indebiti ai dati riservati.

Il comma 3 dell'art. 38 del decreto antiriciclaggio estende l'obbligo di tutela del segnalante anche alle informazioni che la UIF fornisce in riscontro di specifiche richieste dell'autorità giudiziaria procedente. Secondo quanto attualmente previsto dalla norma appena richiamata, la UIF invia alla Magistratura i flussi segnaletici richiesti senza l'indicazione dell'identità del segnalante, a meno che questa non sia esplicitamente richiesta con decreto motivato.

⁶⁸⁰ Cfr. art. 38, comma 6 del D.lgs. 231/2007.

⁶⁸¹ Pur trovando applicazione in un ambito completamente diverso, questo approccio risulta coerente con quanto indicato alle banche dal Garante della protezione dei dati che con il provvedimento 192/2011 ha introdotto l'obbligo per banche e imprese finanziarie, di utilizzare specifiche tecnologie per conservare traccia dell'attività dei dipendenti nell'ambito delle rispettive mansioni sul luogo di lavoro. Finalità di tale obbligo è tutelare i clienti da accessi non autorizzati e intrusioni indebite. In sostanza il Garante indica alle banche la necessità di realizzare un sistema di audit log di tutta l'attività degli incaricati del trattamento che operano sui dati patrimoniali e personali della clientela a vario titolo, e di creare un sistema di alert volti a segnalare intrusioni o accessi anomali e abusivi ai sistemi informativi.

Recentemente, la norma richiamata è stata innovata dalle disposizioni del DL 228/2021, convertito con modificazioni dalla legge 25 febbraio 2022, n. 15; a seguito di tale intervento normativo l'oggetto di tutela appare più ampio e copre non soltanto l'identità del segnalante ma anche la stessa segnalazione di operazioni sospette e tutte le altre informazioni trasmesse alla UIF⁶⁸².

Nulla è cambiato per i "dati identificativi dei segnalanti", per i quali continua a vigere il divieto di inserimento nei fascicoli processuali e dibattimentali a meno che ciò risulti indispensabile ai fini dell'accertamento dei reati per i quali si procede; come prima, essi possono essere acquisiti solo tramite decreto motivato e con l'adozione delle cautele necessarie ad assicurare la tutela del segnalante e dei contenuti informativi della SOS. A rafforzare gli obblighi di tutela della riservatezza, viene infine introdotta una sanzione penale per chi riveli indebitamente l'identità del segnalante ovvero ne consenta l'identificazione divulgando il contenuto delle segnalazioni⁶⁸³.

La nuova disciplina della tutela della riservatezza risulta, in tal modo, ampliata dal punto di vista oggettivo, poiché non si limita a fare riferimento all'identità del segnalante, ma anche al contenuto informativo delle segnalazioni e dei dati acquisiti nel corso delle analisi finanziarie condotte in sede UIF o acquisite nell'ambito dei contatti con la rete estera delle FIU; risulta, inoltre, rafforzata, nella misura in cui si prevede che il decreto di acquisizione delle SOS debba presentare un nesso esplicito con l'accertamento penale in corso.

Quest'ultima previsione, peraltro, richiedendo che nelle richieste alla UIF debbano essere incluse anche argomentazioni utili a rendere chiaro perché la conoscenza dell'identità del segnalante sia indispensabile ai fini dell'accertamento dei reati per cui si procede, potrebbe essere di difficile applicazione nei casi in cui la riservatezza delle indagini non consenta all'AG di motivare adeguatamente la *disclosure* sul segnalante.

Un'ulteriore criticità potrebbe essere rappresentata dall'adozione, da parte dell'AG, di cautele necessarie ad assicurare la tutela del segnalante e, ove possibile, la riservatezza della segnalazione e delle informazioni trasmesse dalle FIU; dovrà essere deciso in sede interpretativa quali siano le cautele ritenute idonee allo scopo e coerenti con l'impianto delle normative processuali attualmente vigente.

Andrebbe, inoltre, valutato se il divieto previsto dalla nuova formulazione del comma 3, secondo cui i dati "*non [...] possono essere in altro modo rivelati*" sia da riferirsi soltanto all'Autorità giudiziaria, come il resto delle previsioni dello stesso comma. Se si optasse per questa linea interpretativa, il divieto potrebbe non applicarsi alla UIF in sede di riscontro delle richieste da parte dell'Autorità giudiziaria; ne risulterebbe una pericolosa attenuazione della tutela della riservatezza, poiché la UIF sarebbe legittimata a rivelare i dati identificativi dei segnalanti (ove noti, anche quelli delle persone fisiche) anche in assenza di decreto motivato, rimanendo poi in capo all'Autorità giudiziaria l'onere di assicurare la riservatezza o di disporre con decreto motivato la *disclosure* se indispensabile ai fini dell'accertamento dei reati. Questa interpretazione, tuttavia, appare in controtendenza con lo spirito stesso della modifica normativa, con il rischio che eventuali rivelazioni possano essere ritenute indebite e contestate anche in sede penale.

9. Il flusso di ritorno (I. Longhi)

Il ruolo svolto dai soggetti obbligati nel sistema di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo è di rilevanza cruciale. La UIF è quindi da sempre attenta a mantenere un sinergico dialogo con i segnalanti, quale strumento importante per aumentare l'efficacia della collaborazione attiva in termini di incisività delle informazioni fornite.

Le occasioni di confronto con gli operatori sono molteplici, comprendono sia una serie di attività divulgative, che si sostanziano in convegni e seminari in cui relatori della UIF presentano tematiche di interesse generale nonché nella diffusione di diverse tipologie di pubblicazioni per presentare il risultato di analisi, studi e casistiche di particolare interesse, sia mirati flussi di ritorno sulla collaborazione attiva del segnalante, costituiti da incontri e invii di comunicazioni periodiche con dati e informazioni relativi al flusso segnaletico di ciascun segnalante.

Gli incontri con i segnalanti sono una costante nell'attività dell'Unità e sono articolati in varie iniziative, che includono riunioni o anche solo note formali e informali, focalizzandosi su specifici aspetti tematici, spesso indotti da importanti novità legislative o tecnologiche, o promossi sulla base dei continui monitoraggi che l'Unità svolge sui segnalanti. Altre iniziative

⁶⁸² Cfr. art. 38, comma 3 del D.lgs. 231/2007.

⁶⁸³ Cfr. art. 38, comma 3-*bis* del D.lgs. 231/2007.

possono essere dirette a quegli intermediari i cui apporti segnaletici appaiono sottodimensionati rispetto ai volumi di operatività gestiti, con l'invito di fornire dettagli sul processo interno di compliance e sui parametri impiegati nell'individuazione delle operazioni sospette.

Al contrario degli incontri che, seppur continuativi vengono organizzati secondo le necessità riscontrate, le comunicazioni periodiche sono trasmesse dalla UIF ai segnalanti interessati in maniera strutturata e sono distinte in due tipologie: gli esiti delle segnalazioni e le schede di feedback.

In linea con quanto previsto dall'art. 41, comma 2, del D.lgs. 231/2007 la UIF trasmette periodicamente ai segnalanti comunicazioni relative agli esiti delle segnalazioni di operazioni sospette. In particolare la UIF trasmette, con cadenza semestrale, l'elenco delle SOS che, alla luce degli approfondimenti effettuati dall'Unità e dei riscontri ricevuti dagli Organi investigativi, sono ritenute "non rilevanti" in quanto le analisi non hanno evidenziato significativi elementi a supporto del sospetto di riciclaggio e di finanziamento del terrorismo.

Con cadenza annuale, inoltre, la UIF trasmette, ai maggiori segnalanti dei comparti banche e Poste e money transfer, la c.d. scheda di feedback contenente indicatori sintetici sull'attività segnaletica confrontati con quelli della rispettiva categoria di appartenenza. Tale iniziativa ha lo scopo di migliorare la qualità e l'efficacia complessiva del sistema, favorendo meccanismi di autovalutazione dei segnalanti, che potranno confrontare il rispettivo posizionamento con quello dei soggetti appartenenti alla medesima categoria e adottare misure mirate di perfezionamento dell'attività segnaletica.

9.1. Le segnalazioni non rilevanti

Uno degli esiti dell'analisi finanziaria svolta dalla UIF è costituito dalle segnalazioni che, nell'iter del processo valutativo, sono ritenute non rilevanti in termini di rischio di riciclaggio o di finanziamento del terrorismo. Il vigente dettato normativo è focalizzato su criteri di selezione delle segnalazioni di operazioni sospette in base alla valutazione del rischio e non più sul concetto di manifesta infondatezza, di conseguenza la valutazione della UIF per le segnalazioni c.d. "non rilevanti" è basata sull'evidenza di un quadro in cui le informazioni di natura finanziaria, supportate anche da quelle investigative, non consentono di confermare il sospetto che ha indotto il segnalante all'invio della SOS.

Il D.lgs. 90/2017 ha, infatti, modificato in parte la disposizione previgente su questa materia, eliminando il riferimento esplicito all'archiviazione delle segnalazioni ritenute infondate⁶⁸⁴ e introducendo l'obbligo per la UIF di mantenere evidenza per 10 anni delle segnalazioni non trasmesse agli Organi investigativi in quanto ritenute prive di significativi elementi di rischio di riciclaggio o finanziamento del terrorismo, assicurando al contempo la possibilità di consultazione da parte degli Organi investigativi mediante opportune procedure di accesso⁶⁸⁵. Tuttavia, al fine di assicurare il costante allineamento delle basi dati della UIF e degli Organi investigativi, si è concordemente ritenuto preferibile continuare a trasmettere le segnalazioni della specie. In questa maniera l'Unità – nel rispetto della citata cornice normativa – contempera l'esigenza di garantire la piena condivisione con gli Organi delle indagini delle informazioni in suo possesso con l'esercizio di un'efficace azione di selezione.

L'individuazione di segnalazioni che evidenziano contesti considerati a basso rischio di riciclaggio e di finanziamento del terrorismo riveste particolare importanza nel confronto con i segnalanti, consentendo di migliorare la qualità della collaborazione attiva. In una ottica di massima condivisione delle informazioni tale flusso informativo costituisce un orientamento per i soggetti obbligati sugli elementi utili da considerare nel ciclo valutativo a supporto del sospetto dei contesti potenzialmente anomali, oltre ad attestare l'assenza, in capo ai soggetti segnalati, di precedenti di polizia. Unitamente all'interesse da parte degli Organi investigativi, infatti, la valutazione della UIF è determinata da numerosi elementi atti a fornire indicazioni sulla gradazione del rischio, quali gli eventuali raccordi dei soggetti presenti nelle segnalazioni, il loro comparto di attività, l'operatività espressa e le caratteristiche delle operazioni effettuate, al fine di scongiurare la presenza di fattispecie indicative di contesti a rischio.

⁶⁸⁴ Cfr. art. 47 comma 1, lett. c), del D.lgs. 231/2007, testo ante riforma.

⁶⁸⁵ Cfr. art. 40 comma 1, lett. f), del D.lgs. 231/2007.

La comunicazione delle segnalazioni a basso rischio è attualmente veicolata attraverso la piattaforma Infostat-UIF, grazie a una funzionalità appositamente sviluppata, che favorisce i destinatari nell'acquisizione dell'informazione all'interno dei propri sistemi informativi in vista di successive elaborazioni.

9.2. Le schede di feedback

Le indicazioni fornite attraverso le schede di feedback non hanno carattere valutativo dell'attività di segnalazione. Esse, tuttavia, correlate alle specificità di ciascun operatore, possono fornire indicazioni utili al possibile miglioramento della collaborazione attiva. La finalità di tale flusso di ritorno è quella di migliorare l'interazione tra l'Unità e i soggetti obbligati, rendendo questi ultimi maggiormente consapevoli dell'efficacia informativa delle segnalazioni inviate e agevolandoli nella selezione di fenomeni e operazioni meritevoli di approfondimento.

Le schede di feedback sono state inviate per la prima volta e in via sperimentale nel 2015 (sui dati dell'anno precedente) ai maggiori segnalanti delle categorie banche e Poste e successivamente, nel 2018, anche agli operatori nel settore dei money transfer. Per ottenere risultati statisticamente affidabili gli indicatori sono calcolati su un numero sufficientemente elevato di segnalazioni: le schede vengono quindi prodotte per i segnalanti della categoria banche e Poste che abbiano inviato nell'anno precedente almeno 200 SOS e per i segnalanti della categoria money transfer che abbiano inviato nell'anno precedente almeno 100 SOS.

Gli indicatori rilevano diversi aspetti e posizionano il profilo di ciascun operatore rispetto alla media della categoria di appartenenza⁶⁸⁶. Gli aspetti considerati negli indicatori sono i seguenti: *l'ampiezza della collaborazione*, misurata in base alla quantità di segnalazioni inviate dal segnalante nel periodo considerato in rapporto al totale di quelle inviate dal gruppo di riferimento. È un parametro che permette di valutare la dimensione quantitativa dell'attività segnaletica dell'operatore; *la tempestività*, rappresentata dalla distribuzione percentuale delle segnalazioni per classi temporali e dal valore mediano dei tempi di inoltro delle segnalazioni. Permette di valutare la velocità di reazione del singolo segnalante al verificarsi degli elementi costitutivi del sospetto; *la qualità*, misurata da indicatori che colgono la rilevanza delle segnalazioni (livello di rischio, esito dell'analisi finanziaria e presenza di interesse da parte degli Organi investigativi). Sintetizza la capacità del segnalante di intercettare operazioni a effettivo rischio di riciclaggio rispetto a elementi di rischio oggettivo; *la complessità*, misurata per i segnalanti appartenenti alla categoria "banche e Poste", rileva la capacità di rappresentare i sospetti in modo adeguato, completo ed efficace. L'indicatore si basa sulla numerosità dei soggetti e delle operazioni rilevanti contenuti nelle segnalazioni e sul livello di strutturazione degli elementi forniti; *l'emersione di anomalie*, indicatore rilevato per i money transfer, evidenzia la capacità di individuare le anomalie con riferimento a una pluralità di ambiti (operatività, profili soggettivi della clientela, comportamenti della rete territoriale di vendita).

Un'attenzione particolare è stata dedicata agli operatori di money transfer, per i quali l'attività di monitoraggio ha considerato, oltre ai consueti indicatori, *l'adeguatezza del numero di segnalazioni* inoltrate dai segnalanti in relazione alla loro dimensione operativa ricavata dai dati delle rimesse rilevate dalla Banca d'Italia per la bilancia dei pagamenti. Il confronto tra la quota di mercato dei singoli operatori e la percentuale di segnalazioni inoltrate sul totale del comparto ha permesso di individuare operatori con apporti segnaletici elevati rispetto ai volumi transati e altri per i quali, al contrario, il contributo potrebbe essere deficitario.

Gli indicatori elaborati per i segnalanti hanno consentito inoltre – se considerati complessivamente – di descrivere in modo sintetico lo stato della collaborazione attiva in termini di "qualità" e "complessità" delle segnalazioni inviate. Il livello di "qualità" è il risultato di un indice sintetico della rilevanza (o rischiosità) della segnalazione, calcolato sulla base dei giudizi espressi dagli analisti della UIF (rating finale) e dagli Organi investigativi. Il grado di "complessità" è direttamente legato al livello di strutturazione della segnalazione, dove un indicatore più alto corrisponde, in genere, a operatività ricostruite in modo più dettagliato e con maggior potenziale di utilità ai fini delle analisi e delle indagini. Tale capacità è di fondamentale importanza perché vi è il rischio che la trascuratezza nella descrizione dei comportamenti non consenta di individuare elementi d'interesse ai fini dell'analisi.

Nel corso degli anni i risultati evidenziati dagli indicatori delle schede di feedback, soprattutto per i maggiori contribuenti della categoria banche e Poste rivelano, in media, l'impegno profuso nel consolidare i risultati in linea con i profili di qualità e adeguatezza del contenuto segnaletico proposti dagli indicatori.

⁶⁸⁶ Questa è costituita per i money transfer dall'insieme degli operatori che hanno mandato nell'anno di riferimento almeno 1 segnalazione di operazione sospetta. Per i segnalanti bancari invece, al fine di rendere più omogenei i confronti tra segnalanti aventi caratteristiche simili, sono state individuate tre categorie di riferimento: banche di dimensioni rilevanti (grandi), banche di dimensioni contenute (piccole), e banche specializzate.

A seguito degli esiti positivi della sperimentazione condotta, l'Unità ha in programma di inviare le schede a un più ampio numero di destinatari e di aumentare gli aspetti esaminati. Estendere la platea dei destinatari delle schede è doveroso per render merito a tutte le categorie di segnalanti che hanno mostrato, soprattutto nell'ultimo biennio, una partecipazione attiva elevata e sono entrati in posizioni apicali nella segnalazione di contesti sospetti; la disponibilità di nuovi dati e informazioni, che nel corso del tempo hanno progressivamente ampliato il patrimonio informativo della UIF, permette di predisporre ulteriori indicatori per esplorare aspetti aggiuntivi del profilo segnaletico dei soggetti obbligati, quali la capacità diagnostica nel saper cogliere anomalie con riferimento a una pluralità di ambiti e la prontezza della collaborazione attiva, intesa come celerità e completezza di risposta alle richieste di informative da parte della UIF.

CAPITOLO 5

I presìdi organizzativi

(a cura di R. Cercone)

Premessa (A. Marrone e F. Lelli)

La prevenzione del rischio di coinvolgimento, anche inconsapevole, in fatti di riciclaggio, presuppone che l'azienda destinataria degli obblighi in materia sia dotata di assetti organizzativi e procedure atti ad azzerare o quantomeno a mitigare efficacemente il rischio in questione.

A tale scopo, l'art. 7, comma 1, lett. a), del D.lgs. 231/2007 attribuisce espressamente alle Autorità di Vigilanza di settore il potere di adottare nei confronti dei soggetti vigilati disposizioni attuative in materia di organizzazione, procedure e controlli interni. La Banca d'Italia ha emanato le Disposizioni del 26 marzo 2019 che – nel sostituire le previgenti disposizioni sullo stesso argomento del 10 marzo 2011 – recepiscono le novità normative introdotte dal D.lgs. 90/2017 ⁽⁶⁸⁷⁾.

Le cennate disposizioni introducono nell'ordinamento italiano una disciplina organica dei profili organizzativi e dei controlli interni in materia di antiriciclaggio. Dal punto di vista soggettivo, le disposizioni della Banca d'Italia si rivolgono a un'ampia platea di destinatari, che include gli intermediari sottoposti a vigilanza prudenziale come le banche, gli istituti di moneta elettronica, gli istituti di pagamento, le SIM, le SGR, le SICAV, gli intermediari iscritti nell'elenco di cui all'art. 106 del TUB, Poste Italiane, Cassa Depositi e Prestiti e i soggetti eroganti micro-credito, ai sensi dell'art. 111 TUB. Le disposizioni trovano inoltre applicazione nei confronti delle succursali di banche e società finanziarie extracomunitarie e comunitarie che operano sul territorio della Repubblica nonché nei confronti dei prestatori di servizi di pagamento con sede in altri paesi UE tenuti all'istituzione del punto di contatto centrale in Italia.

L'eterogeneità dei soggetti destinatari ha indotto a predisporre una normativa che, nel fissare le linee guida e gli orientamenti di massima cui i destinatari devono uniformarsi nel disegno dei controlli antiriciclaggio, rimettesse agli stessi, secondo logiche di modularità, la determinazione delle soluzioni organizzative più adatte alle proprie specificità operative e dimensionali.

Più in dettaglio, le nuove disposizioni si pongono in linea di sostanziale continuità con la disciplina del 2011, confermando alcuni elementi cardine dell'impianto previgente, tra cui: la neutralità delle norme rispetto alle scelte di governo societario; la proporzionalità rispetto alle caratteristiche operative e dimensionali dei destinatari (le norme prevedono che le prescrizioni vengano applicate in coerenza con la forma giuridica, le dimensioni, l'articolazione organizzativa, le caratteristiche e la complessità dell'attività svolta); la responsabilizzazione di tutta la struttura aziendale e dei collaboratori esterni; la specializzazione dei controlli tra responsabile antiriciclaggio e responsabile delle segnalazioni di operazioni sospette.

Coerentemente con le innovazioni introdotte dal D.lgs. 90/2017, le disposizioni valorizzano il più sistematico ricorso all'approccio basato sul rischio al fine di orientare le modalità e la profondità delle analisi che gli intermediari sono tenuti a condurre per adempiere agli obblighi in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

In applicazione di tale principio, a fronte della possibilità di graduare la loro attività in base al rischio, si richiede agli intermediari di: i) condurre un esercizio di autovalutazione dei rischi, funzionale alla definizione ed attuazione, da parte degli organi e delle funzioni aziendali, di strategie nonché di misure organizzative e procedurali idonee a evitare o ridurre il rischio di coinvolgimento in fenomeni di riciclaggio e di finanziamento del terrorismo; ii) definire una *policy* che indichi in modo analitico e motivato le scelte che essi in concreto intendono compiere sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni.

⁶⁸⁷ Le disposizioni in materia di controlli interni applicabili alle imprese assicurative sono contenute nel regolamento IVASS n. 44 del 12 febbraio 2019.

Di particolare rilievo l'introduzione di una disciplina sui presidi organizzativi minimi. Le nuove disposizioni precisano che – ferma restando la possibilità di calibrare gli assetti organizzativi antiriciclaggio in forza del principio di proporzionalità – i soggetti destinatari devono in ogni caso garantire alcuni presidi minimi tra cui rileva, in particolare, l'attribuzione della responsabilità di assicurare l'adeguatezza, la funzionalità e l'affidabilità dei presidi antiriciclaggio a una funzione aziendale di controllo.

Nei paragrafi che seguono, in coerenza con la struttura delle disposizioni, si approfondiscono le novità introdotte in tema di: funzioni di governo societario (par. 1); funzione antiriciclaggio, responsabile della segnalazione di operazioni sospette e funzione di revisione interna (par. 2); assetti organizzativi a livello di gruppo (par. 3); punto di contatto centrale (par. 4); esercizio di autovalutazione dei rischi (par. 5). Si prospettano, infine, le principali innovazioni derivanti dagli Orientamenti di recente adottati dall'Autorità bancaria europea in materia di ruolo e compiti del responsabile antiriciclaggio (par. 6).

1. Organi societari: compiti e responsabilità (A. Marrone e F. Lelli)

Le Disposizioni rimarcano l'esigenza di un pieno coinvolgimento degli organi di vertice nella gestione e mitigazione dei rischi di riciclaggio. A tale scopo, i destinatari sono chiamati a dotarsi di un sistema organizzativo e di controllo nonché di strategie, regole, risorse, procedure e funzioni chiaramente individuate e adeguatamente specializzate idonee ad assicurare l'efficace prevenzione dei rischi di riciclaggio.

In particolare, gli organi aziendali – ciascuno secondo le proprie competenze e responsabilità – sono tenuti a: definire politiche aziendali coerenti con i principi e le regole antiriciclaggio; adottare linee di *policy* idonee a preservare l'integrità aziendale; porre in atto misure organizzative e operative idonee a evitare il rischio di riciclaggio; svolgere controlli sul rispetto della normativa e sull'adeguato presidio dei rischi.

L'organo con funzione di supervisione strategica è responsabile degli indirizzi strategici e delle politiche di governo dei rischi di riciclaggio che, in aderenza all'approccio basato sul rischio, devono essere commisurate all'entità e alla tipologia di rischi cui è concretamente esposta l'attività del destinatario.

Tra le funzioni assegnate all'organo con funzione di supervisione strategica, si richiamano: l'approvazione della c.d. *policy* antiriciclaggio, funzionale a illustrare e motivare le scelte che l'intermediario compie sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati; l'approvazione dell'istituzione della funzione antiriciclaggio, individuandone compiti e responsabilità nonché le modalità di coordinamento e di collaborazione con le altre funzioni aziendali di controllo; la nomina e la revoca del responsabile antiriciclaggio e del responsabile delle segnalazioni di operazioni sospette; l'esame, con cadenza almeno annuale, delle relazioni relative all'attività svolta dal responsabile antiriciclaggio e ai controlli eseguiti dalle funzioni competenti, nonché del documento di autovalutazione dei rischi di riciclaggio.

L'organo con funzione di gestione cura l'attuazione degli indirizzi strategici e delle politiche di governo del rischio di riciclaggio approvati dall'organo con funzione di supervisione strategica ed è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio.

A tale scopo, definisce e cura l'attuazione di un sistema di controlli interni funzionale alla pronta rilevazione e gestione del rischio di riciclaggio; assicura che le procedure operative e i sistemi informativi consentano il corretto assolvimento degli obblighi di adeguata verifica della clientela, conservazione dei documenti e delle informazioni nonché di segnalazione delle operazioni sospette; definisce la *policy* antiriciclaggio, sottoposta all'approvazione dell'organo con funzione di supervisione strategica, e ne cura l'attuazione; stabilisce i programmi di addestramento e formazione del personale sugli obblighi previsti dalla disciplina antiriciclaggio; stabilisce gli strumenti idonei a consentire la verifica dell'attività svolta dal personale in modo da rilevare eventuali anomalie.

L'organo con funzione di controllo vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei sistemi di controllo antiriciclaggio, avvalendosi delle strutture interne per lo svolgimento delle verifiche e degli accertamenti necessari.

Laddove a fronte dei controlli eseguiti emergano carenze, anomalie o irregolarità, l'organo promuove l'adozione di idonee misure correttive. L'organo con funzione di controllo è sentito nelle procedure di nomina del responsabile della funzione antiriciclaggio e del responsabile delle segnalazioni di operazioni sospette e nella definizione degli elementi dell'architettura complessiva del sistema di gestione e controllo del rischio di riciclaggio.

Ai sensi dell'art. 46 del decreto antiriciclaggio, i componenti dell'organo con funzione di controllo comunicano senza ritardo alla Banca d'Italia tutti i fatti di cui vengano a conoscenza che possano integrare violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge applicabili e delle relative disposizioni attuative.

2. La funzione antiriciclaggio, il responsabile delle segnalazioni di operazioni sospette e la funzione di revisione interna (A. Marrone e F. Lelli)

La struttura dei controlli antiriciclaggio disegnati dalle Disposizioni si impernia su una specifica funzione di controllo di secondo livello chiamata a valutare e mitigare in maniera specifica il rischio di coinvolgimento dell'intermediario in fatti di riciclaggio. La funzione è stata costruita sulla falsariga della funzione di *compliance* bancaria: il rischio di coinvolgimento in fatti di riciclaggio, infatti, costituisce sostanzialmente una specificazione di quei più ampi rischi reputazionali che la *compliance* è chiamata a presidiare.

Alla funzione antiriciclaggio sono quindi assegnati compiti che in larga parte ricalcano quelli propri della funzione di conformità: i) identificazione delle norme applicabili e valutazione del loro impatto su processi e procedure aziendali; ii) collaborazione all'individuazione del sistema dei controlli interni; iii) verifica dell'efficacia degli adeguamenti organizzativi proposti e elaborazione di proposte di modifiche organizzative per assicurare il presidio del rischio di riciclaggio; iv) consulenza e assistenza agli organi aziendali e all'alta direzione e rilascio di pareri in caso di offerta di prodotti e servizi nuovi; v) predisposizione, in raccordo con le altre funzioni aziendali competenti, di un adeguato piano di formazione dei dipendenti e dei collaboratori dell'azienda; vi) predisposizione di flussi informativi diretti agli organi aziendali e all'alta direzione.

Inoltre, spetta al responsabile antiriciclaggio verificare l'affidabilità del sistema informativo di alimentazione dell'archivio unico informatico (o dello strumento avente analoghe funzioni) nonché trasmettere alla UIF i dati aggregati concernenti le registrazioni presenti in archivio.

Peculiare è invece la previsione in base alla quale al responsabile può essere affidato il compito di svolgere le attività di rafforzata verifica della clientela nei casi in cui il rischio di riciclaggio sia particolarmente elevato: si tratta, infatti, di un'attività di natura più operativa, che si ammette possa essere attribuita ad una figura di controllo (quale il responsabile antiriciclaggio) in considerazione dell'importanza di assicurare, nei casi più problematici, un rigoroso presidio della fase genetica dei rapporti continuativi.

Tale funzione deve essere indipendente, dotata di adeguate risorse qualitative e quantitative e deve avere accesso a tutte le attività/informazioni del soggetto destinatario della disciplina. I destinatari sono tenuti, inoltre, a formalizzare in modo chiaro il mandato della funzione antiriciclaggio, a definire i rapporti di quest'ultima con le altre funzioni aziendali, a garantire adeguati flussi informativi rivolti direttamente al vertice aziendale, a nominare un responsabile indipendente. Questi può essere un amministratore non esecutivo o un dirigente che non abbia responsabilità diretta di aree operative.

Tenuto conto dei molteplici profili professionali richiesti per l'espletamento dei controlli antiriciclaggio, le relative attività possono essere svolte da personale di altre strutture organizzative del soggetto destinatario (legale, organizzazione, rischio operativo, ecc.), purché sia assicurato il coordinamento e la supervisione da parte del responsabile della funzione antiriciclaggio. Il personale incaricato di compiti antiriciclaggio, anche se inserito in aree operative, riferisce direttamente al responsabile antiriciclaggio per le questioni attinenti a detti compiti. La regolamentazione rimette agli intermediari le scelte relative alla collocazione organizzativa della funzione AML e ai rapporti di questa con le altre unità aziendali. Essa richiama il principio della collaborazione al fine di sviluppare idonee metodologie di gestione del rischio e processi aziendali conformi alla normativa.

Il personale addetto ad altre aree operative riporta solo funzionalmente al responsabile antiriciclaggio, senza vincolo gerarchico. I requisiti minimi di stabilità e indipendenza richiesti al responsabile antiriciclaggio sono disciplinati dalle Disposizioni.

La nomina e la revoca del responsabile antiriciclaggio passano attraverso una procedura rafforzata che, nel coinvolgere tutti gli organi di vertice dell'azienda, mira ad assicurare l'indipendenza e

l'inalterabilità – se non per giusta causa – di tale figura. Sul punto, le nuove Disposizioni introducono un elemento di novità, prevedendo che il responsabile antiriciclaggio (così come il responsabile per la segnalazione delle operazioni sospette) sia nominato dall'organo di supervisione strategica, sentito l'organo con funzioni di controllo; tale innovazione è volta ad allineare la disciplina antiriciclaggio a quella prevista più in generale per il sistema dei controlli interni. Le Disposizioni precisano che gli intermediari possono introdurre, in coerenza con le proprie caratteristiche operative e dimensionali, ulteriori presidi di stabilità e indipendenza del responsabile.

Le Disposizioni confermano la possibilità di accorpate la funzione antiriciclaggio con la funzione *compliance* e/o *risk management*⁶⁸⁸ ma richiedono che questa scelta sia preceduta da una valutazione di idoneità in coerenza, con i principi di proporzionalità e di approccio basato sul rischio.

Come chiarito nel documento di resoconto della consultazione pubblica, la valutazione riguarda l'idoneità della soluzione organizzativa ad assicurare la corretta gestione del rischio di riciclaggio cui il destinatario è esposto nonché il regolare adempimento degli obblighi antiriciclaggio, alla luce delle caratteristiche operativo/dimensionali del destinatario. Inoltre, quando le funzioni siano già state accorpate in base alla previgente disciplina non è necessario procedere alla valutazione esplicita di idoneità prevista dalle nuove disposizioni. La valutazione di idoneità sarà necessaria solo per le decisioni di accorpamento delle funzioni assunte dopo l'entrata in vigore delle Disposizioni.

In caso di accorpamento, le Disposizioni prevedono che il ruolo di responsabile antiriciclaggio può essere assegnato solo al responsabile della funzione di *compliance* ovvero al *risk manager* e non a personale di livello gerarchico inferiore.

È infine prevista la possibilità di esternalizzare la funzione a soggetti terzi sulla base di uno specifico contratto, ferma la necessità di individuare un “responsabile interno” alla funzione antiriciclaggio, con il compito di monitorare le modalità di svolgimento del servizio da parte dell'*outsourcer*. Il referente interno deve essere comunque in possesso degli specifici requisiti di indipendenza, autorevolezza e professionalità fissati in generale per il responsabile antiriciclaggio; la normativa esclude espressamente la possibilità del ricorso all'esternalizzazione in caso di imprese che presentano significative dimensioni e complessità operative. Al riguardo, le nuove Disposizioni chiariscono che la disciplina dell'esternalizzazione della funzione antiriciclaggio deve essere applicata congiuntamente a quella della Banca d'Italia in materia di esternalizzazione o delega delle altre funzioni aziendali di controllo.

La figura del responsabile per la segnalazione delle operazioni sospette (SOS) rappresenta uno degli snodi più delicati dell'architettura antiriciclaggio disegnata dall'ordinamento. Si tratta infatti del soggetto – che l'art. 36 del decreto antiriciclaggio individua nel “titolare dell'attività, nel rappresentante legale ovvero un suo delegato” – chiamato a valutare le segnalazioni di operazioni anomale e a decidere in ordine alla fondatezza dei motivi di sospetto ai fini del successivo inoltro delle stesse all'Unità di Informazione Finanziaria, per le analisi di competenza. Nel caso di succursale, il responsabile delle segnalazioni di operazioni sospette è il legale rappresentante della stessa, salva la possibilità di delega ad un membro del personale della succursale. Se i destinatari sono tenuti all'istituzione di un punto di contatto centrale, il responsabile delle SOS coincide in ogni caso con il responsabile del punto di contatto centrale.

In senso stretto, il responsabile delle segnalazioni di operazioni sospette non rientra nel novero delle figure di controllo, tant'è che il decreto attribuisce tale ruolo in prima battuta “al titolare dell'attività ovvero al legale rappresentante dell'azienda”. L'attività di segnalazione, di per sé, costituisce un'attività di tipo operativo, come tale soggetta essa stessa alle verifiche e ai controlli di secondo e terzo livello. Ciò posto, è innegabile che, ai fini di un sereno esercizio di tale delicato compito, la valutazione del “responsabile” deve, per quanto possibile, non essere inquinata dall'esigenza di perseguire obiettivi anche commerciali o di *budget*.

In tale luce vanno inquadrare le Disposizioni che, in maniera speculare a quanto richiesto per il responsabile antiriciclaggio, fissano una serie di regole e principi che i destinatari devono rispettare per assicurare l'indipendenza e lo spessore professionale del responsabile delle SOS, applicabili anche nel caso in cui la funzione non sia oggetto di delega.

⁶⁸⁸ La responsabilità della funzione antiriciclaggio non può essere attribuita alla revisione interna.

In particolare, al fine di presidiare l'efficacia delle valutazioni effettuate dal responsabile delle SOS, le Disposizioni hanno rafforzato i requisiti di indipendenza, autorevolezza, professionalità del medesimo e di riservatezza (interna) della sua attività. Egli non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree. Il conferimento della delega è deliberato dall'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo⁶⁸⁹.

La delega può essere attribuita al responsabile antiriciclaggio che, in tal caso, acquisisce un ruolo a tutto tondo nella materia accentrando in sé compiti organizzativi, di controllo e operativi. In ogni caso, anche laddove il responsabile antiriciclaggio non riceva la delega per le segnalazioni, è importante che il delegato e il responsabile antiriciclaggio collaborino intensamente tra loro. Con riferimento alla delega alle segnalazioni presso gli intermediari di rilevanti dimensioni, si dà la possibilità di attribuire la delega per le SOS a più soggetti. Non può essere nominato delegato l'*Internal Auditor*, al fine di assicurare l'assoluta terzietà di tale figura.

Per quanto attiene ai rapporti tra “delegato” alle operazioni sospette e responsabili di “primo livello”, le Disposizioni prevedono che il primo comunichi l'esito della valutazione effettuata sulla segnalazione al responsabile della dipendenza che ha dato origine alla stessa affinché questi individui le misure di monitoraggio della posizione più opportune in funzione dell'esito (archiviazione ovvero inoltro alla UIF) della procedura di segnalazione. Si precisa che rientra nei compiti del responsabile SOS anche valutare le operazioni sospette delle quali abbia avuto conoscenza anche in altro modo (quindi anche a prescindere da un *input* di primo livello) e mantenere evidenza delle valutazioni compiute pure in caso di operazioni ritenute non meritevoli di segnalazione alla UIF.

Come chiarito dalla Banca d'Italia nel documento di resoconto della consultazione pubblica, ai sensi dell'art. 36 del decreto antiriciclaggio, il responsabile SOS esamina tutte le segnalazioni che gli siano pervenute, mentre i responsabili delle strutture di primo livello (ossia quelle preposte all'amministrazione e alla gestione concreta dei rapporti con la clientela) hanno l'obbligo di segnalare al responsabile SOS le operazioni sospette.

Le disposizioni specificano anche che il responsabile delle SOS effettua verifiche, anche a campione, sulla congruità delle valutazioni dell'operatività della clientela da parte del primo livello.

Infine, ferma la tutela della riservatezza dell'identità del “segnalante” di primo livello, i delegati possono autorizzare la costituzione, all'interno dell'azienda, di una base dati contenente i nominativi (accessibili dai responsabili delle diverse strutture operative) di tutti i clienti oggetto di segnalazione. In ogni caso, tale archivio va impostato con modalità tali da assicurare un corretto bilanciamento tra le esigenze di massima circolarità – all'interno della struttura – delle informazioni relative a singoli clienti e operazioni eventualmente oggetto di segnalazione (stante la pregnanza che esse possono rivestire in sede di adeguata verifica) e l'esigenza – parimenti rilevante – di garantire la riservatezza dei soggetti che effettuano la segnalazione, a tutela della relativa incolumità.

Al di fuori del caso dei gruppi, il processo di segnalazione non può essere esternalizzato. Ciò discende da norme di legge volte ad assicurare un diretto coinvolgimento delle strutture aziendali (es. dei responsabili delle dipendenze, che rappresentano il c.d. “primo livello” del processo segnalatico) nel processo di segnalazione.

La funzione di revisione interna, nel settore dell'intermediazione bancaria e finanziaria, ha assunto negli ultimi anni un ruolo centrale nell'ambito del sistema dei controlli interni aziendali.

Le Disposizioni, nel riconoscere la rilevanza di tale funzione anche ai fini dei controlli antiriciclaggio, puntualizza i compiti che la stessa è chiamata a svolgere nel settore in esame, anche ai fini di una più proficua collaborazione con la funzione antiriciclaggio. Più in dettaglio, in base alle disposizioni, la funzione di revisione interna verifica il costante rispetto dell'obbligo di adeguata verifica, l'effettiva acquisizione e l'ordinata conservazione dei dati e dei documenti prescritti dalla normativa, il corretto funzionamento dei sistemi di registrazione e conservazione nonché il rispetto degli obblighi di collaborazione attiva.

Nello svolgimento dei propri controlli la funzione di revisione può effettuare accessi ispettivi al fine di esaminare la conformità alle norme delle condotte tenute dai dipendenti che attendono a compiti rilevanti ai sensi della disciplina

⁶⁸⁹ Si tratta di un'innovazione delle Disposizioni del 2019 che uniformano, anche per quanto attiene alle procedure di nomina e revoca, il regime del responsabile antiriciclaggio e quello del delegato alle operazioni sospette. Come chiarito dal documento di resoconto della consultazione pubblica, la nuova procedura di nomina/revoca si applica solo alle deleghe conferite dopo l'entrata in vigore delle disposizioni.

antiriciclaggio. L'utilizzo in via ordinaria dello strumento ispettivo rappresenta una prerogativa tipica dell'*internal audit* che contribuisce a distinguere la relativa operatività da quella della funzione antiriciclaggio che, ai sensi delle Disposizioni, può effettuare controlli in loco solo "su base campionaria".

Le norme contengono anche alcune indicazioni in merito alle metodologie che la funzione deve utilizzare nello svolgimento dei propri controlli, richiedendo che gli interventi ispettivi siano pianificati in modo tale da consentire che tutte le strutture centrali e periferiche siano sottoposte a verifica in un congruo arco di tempo e che – secondo un approccio *risk based* – le iniziative ispettive e di *follow-up* siano più frequenti nei confronti delle strutture maggiormente esposte ai rischi di riciclaggio e di finanziamento del terrorismo.

La funzione deve periodicamente riferire direttamente agli organi aziendali in ordine alle iniziative intraprese e ai relativi esiti. Va infine evidenziato che, ove la costituzione di una specifica funzione di revisione interna non sia imposta al destinatario da altre disposizioni settoriali allo stesso applicabili, il Provvedimento, in applicazione del principio di proporzionalità, si limita a richiedere che i relativi compiti siano assegnati a un amministratore che, salvo il caso dell'amministratore unico, deve essere privo di deleghe operative.

3. Gli assetti organizzativi antiriciclaggio nei gruppi bancari e finanziari (A. Marrone e F. Lelli)

Le Disposizioni richiedono ai gruppi bancari e finanziari di adottare un approccio consolidato nella gestione del rischio di riciclaggio; pertanto, la capogruppo deve definire le linee strategiche che andranno implementate dalle controllate. Si tratta di un'indicazione coerente con le più generali linee della vigilanza prudenziale sugli intermediari finanziari che, negli ultimi anni, ha focalizzato la propria azione sulla necessità di un'analisi consolidata dei rischi che vanno valutati, gestiti e mitigati unitariamente dalla società capogruppo con riferimento all'intero gruppo.

Gli organi aziendali delle società del gruppo devono comunque essere consapevoli delle scelte assunte in materia di *policy* antiriciclaggio dalla capogruppo e sono responsabili, ciascuno secondo le proprie competenze, dell'attuazione delle direttive di quest'ultima. In base alle Disposizioni, quindi, la capogruppo stabilisce e approva: *i*) una metodologia di gruppo per la valutazione dei rischi di riciclaggio; *ii*) procedure formalizzate di coordinamento e di condivisione delle informazioni rilevanti fra le società appartenenti al gruppo; *iii*) *standard* generali in materia di adeguata verifica della clientela, conservazione dei dati e individuazione e segnalazione delle operazioni sospette.

Le Disposizioni del 2019 prevedono anche che la capogruppo sia tenuta ad istituire una base informativa comune che consenta a tutte le società appartenenti al gruppo di valutare in modo omogeneo la clientela. L'obbligo di istituire una base informativa comune persegue l'obiettivo di accrescere l'omogeneità delle valutazioni effettuate sulla clientela comune alle entità del gruppo e di accrescere la capacità del gruppo di prevenire e gestire i rischi di riciclaggio. L'obbligo si applica a tutti i gruppi, non solo a quelli che abbiano scelto di dotarsi, a fini di controllo, di un responsabile antiriciclaggio unico (c.d. modello accentrato). Come chiarito dalla Banca d'Italia nel documento di resoconto della consultazione pubblica, le Disposizioni non individuano in maniera analitica la tipologia di informazioni da condividere: esse consentono alla capogruppo di modellare le caratteristiche e la tipologia di informazioni da mettere a fattore comune in base alle effettive esigenze del gruppo e delle varie entità che lo compongono⁶⁹⁰.

Nei gruppi con operatività transfrontaliera, la capogruppo assicura che le procedure in essere presso le succursali e le società del gruppo con sede in Paesi terzi siano allineate agli *standard* di gruppo e consentano la condivisione delle informazioni nel gruppo, inclusa la notizia dell'avvenuta segnalazione di operazioni sospette, salvo il rispetto dei limiti imposti o degli specifici adempimenti prescritti dall'ordinamento del paese ospitante. Più in dettaglio, fermo il rispetto degli specifici adempimenti prescritti dall'ordinamento del paese ospitante, le procedure in essere presso le succursali e le filiazioni estere (anche extracomunitarie) devono essere in linea con le regole generali del gruppo e tali da assicurare

⁶⁹⁰ A titolo esemplificativo, potrebbe essere utile la condivisione almeno delle informazioni anagrafiche e del profilo di rischio attribuito al cliente da ciascuna entità del gruppo. Nel documento di resoconto della consultazione pubblica, si chiarisce che non è obbligatorio inserire tra i soggetti tenuti ad accedere alla base informativa comune le società controllate non rientranti nel perimetro della definizione di gruppo contenuta nelle Disposizioni (ad es. le imprese assicurative). In un'ottica di gestione integrata del rischio di riciclaggio, la società capogruppo può valutare di estendere, su base volontaria, la base informativa anche a queste società, a condizione che siano esse stesse destinatarie, in base alla legge, degli obblighi antiriciclaggio (come nel caso delle imprese assicurative).

la condivisione delle informazioni a livello consolidato. La norma riveste particolare pregnanza nei confronti dei gruppi bancari operanti in paesi extracomunitari. Infatti, in tali ipotesi, il formale rispetto da parte della succursale o della filiazione estera della normativa in vigore nel Paese ospitante – se meno rigorosa di quella applicabile alla capogruppo – potrebbe non essere sufficiente a evitare il coinvolgimento del gruppo nel suo insieme in fatti di riciclaggio, con conseguenti, negative refluenze sul profilo reputazionale (e quindi anche patrimoniale) del medesimo gruppo. Qualora l'ordinamento del paese ospitante non consenta alle succursali e alle società del gruppo ivi stabilite di adeguarsi agli *standard* generali o di condividere le informazioni rilevanti con le altre società del gruppo, la capogruppo ne dà comunicazione alla Banca d'Italia nei termini e con le modalità previsti dal regolamento (UE) 758/2019, adottato dalla Commissione ai sensi dell'art. 45, par. 7, della quarta direttiva⁶⁹¹.

Proprio allo scopo di rafforzare la gestione consolidata del rischio di riciclaggio, la funzione antiriciclaggio può essere esternalizzata presso una delle società del gruppo (generalmente la capogruppo), con la costituzione di un responsabile antiriciclaggio unico ("modello accentrato") che ha accesso a tutte le banche dati contenenti informazioni utili all'espletamento dei propri compiti. Presso la società esternalizzante va comunque individuato un referente ovvero una specifica unità antiriciclaggio che, coordinandosi con il responsabile antiriciclaggio di gruppo, presidi i processi collegati alla normativa antiriciclaggio nella società di riferimento. Va rilevato che l'attribuzione della funzione antiriciclaggio a un'altra società del gruppo rappresenta una forma di esternalizzazione; le Disposizioni chiariscono sul punto che vi si applicano le previsioni dettate in materia di esternalizzazione delle funzioni aziendali di controllo all'interno del gruppo dalla disciplina prudenziale.

In mancanza di una disciplina settoriale, la funzione antiriciclaggio può essere esternalizzata alla capogruppo ovvero ad altra società del gruppo indipendentemente dalle dimensioni e dalla complessità operativa del soggetto che esternalizza, nel rispetto delle (altre) previsioni dettate dalle medesime Disposizioni. Nel caso in cui i gruppi non ricorrano al modello accentrato nonché laddove la funzione antiriciclaggio sia esternalizzata solo da alcune società del gruppo, le società del gruppo che non hanno esternalizzato la funzione alla capogruppo o ad altra società del gruppo: i) informano in maniera compiuta e tempestiva il responsabile antiriciclaggio della capogruppo o di gruppo degli esiti delle attività di controllo effettuate presso la società dal responsabile antiriciclaggio, ove rilevanti per l'attività del responsabile della capogruppo o di gruppo; ii) assicurano al responsabile antiriciclaggio della capogruppo o di gruppo l'accesso a tutte le banche dati contenenti informazioni utili all'espletamento dei relativi compiti.

Al pari della funzione antiriciclaggio, anche la responsabilità per la segnalazione delle operazioni sospette può essere gestita in maniera accentrata nei gruppi. Pertanto, i legali rappresentanti delle società appartenenti al gruppo con sede in Italia possono conferire la delega di cui all'art. 42, comma 4, del D.lgs. 231/2007 al delegato di una delle società del gruppo (in genere la capogruppo). Ciascuna delega è adeguatamente formalizzata e resa nota all'interno del gruppo, nonché tempestivamente comunicata alla UIF. Al riguardo, si sottolinea che la possibilità di delegare all'esterno, a terzi, la responsabilità per la

⁶⁹¹ In particolare, il regolamento: 1) richiede alle società capogruppo di gruppi finanziari insediati in Paesi extra-UE con una filiazione o una succursale di valutare - in relazione a ciascuno di questi Paesi terzi (art. 2) - il rischio di riciclaggio cui è esposto il gruppo di appartenenza e tenerne conto nelle proprie politiche e procedure; 2) individua le possibili fattispecie in cui, a causa di previsioni normative in vigore in un paese extra-UE, la capogruppo non è in grado di acquisire informazioni sulla clientela della succursale o della filiazione insediata in quel paese extra-UE (in quanto, ad esempio, le leggi ivi in vigore vietano lo scambio di informazioni infragruppo sulla clientela o la comunicazione alla capogruppo delle segnalazioni di operazioni sospette inoltrate da un'entità del gruppo ovvero in quanto in quel Paese non è permessa la conservazione dei dati secondo standard equivalenti a quelli europei); 3) prevede che, nei casi sub 2, la capogruppo deve comunicare alla propria Autorità di Vigilanza i problemi riscontrati e verificare se questi ostacoli non possano essere superati grazie alla collaborazione della clientela della locale filiale o filiazione (se l'ostacolo alla trasmissione dei dati nasce da disposizioni in materia di privacy, ad esempio, potrebbe essere sufficiente ottenere il consenso dei clienti per acquisire le informazioni); 4) elenca le contromisure da adottare per sopperire all'accresciuto rischio di coinvolgimento del gruppo in fatti di riciclaggio che le situazioni sub 1 comportano (laddove il consenso del cliente non sia idoneo a superare gli ostacoli); 5) stabilisce infine che, quando le contromisure adottate non sono comunque idonee a mitigare il rischio di riciclaggio, la Capogruppo dovrà, nei casi più gravi, chiudere i rapporti d'affari con clienti residenti nel Paese terzo ovvero cessare in tutto o in parte l'intera attività della succursale o filiazione. Alla Banca d'Italia spetta il compito di: i) assicurare che i gruppi italiani rispettino le previsioni, anche in punto di obblighi di comunicazione, del regolamento (UE) 758/2019; l'art. 62, comma 7, del Decreto Legislativo 231/2007, infatti, estende la competenza sanzionatoria della Banca d'Italia anche alle violazioni di questo regolamento; ii) valutare l'adeguatezza delle misure supplementari adottate dai gruppi; qualora queste non siano sufficienti, in base alla AMLD4, l'Autorità di vigilanza deve rafforzare la propria supervisione, anche prescrivendo che il gruppo non instauri rapporti d'affari o vi ponga termine e non effettui operazioni e, se necessario, chiedendo al gruppo di cessare l'operatività nel Paese terzo.

segnalazione delle operazioni sospette rappresenta una peculiarità della disciplina dei gruppi; infatti, in generale, tale responsabilità (a differenza di quanto accade per la funzione antiriciclaggio) non può mai essere attribuita a terzi estranei all'impresa.

In caso di adozione del modello accentrato, le Disposizioni prevedono che le operazioni da valutare siano trasmesse al delegato di gruppo in esito a una procedura caratterizzata da un limitato numero di livelli. Il delegato di gruppo può acquisire, direttamente o per il tramite delle strutture designate all'interno di ciascuna società delegante, tutte le informazioni utili per la valutazione delle operazioni sottoposte al suo esame. Inoltre, le società che, nell'esercizio della propria autonomia imprenditoriale, abbiano ritenuto di non conferire la delega, debbono comunque trasmettere al delegato di gruppo copia delle segnalazioni inviate alla UIF o archiviate, complete della motivazione di tale decisione. È da ritenersi che non sussista analogo obbligo di trasmettere le segnalazioni effettuate al delegato della capogruppo laddove nessuna delle società del gruppo abbia esternalizzato la responsabilità in questione.

Infine, in caso di gruppi o intermediari di rilevanti dimensioni, possono essere designati più delegati (in numero comunque contenuto), ciascuno competente ad esempio, in relazione a una determinata area geografica ovvero tipologia di prodotto o servizio offerto. Il responsabile delle SOS di gruppo, ai fini dell'approfondimento delle operazioni e dei rapporti anomali in un'ottica di gruppo, può acquisire informazioni dalle società del gruppo, anche di quelle che non hanno conferito la delega. Il medesimo responsabile delle SOS di gruppo fornisce ai responsabili delle SOS delle società del gruppo le informazioni rilevanti sulla clientela comune. La capogruppo assicura che le società del gruppo con sede in Italia o in un altro Stato comunitario consentano in ogni caso al responsabile delle SOS della capogruppo o di gruppo l'accesso alle informazioni attinenti alle segnalazioni trasmesse e a quelle ritenute infondate, corredate della motivazione della decisione.

4. Il punto di contatto centrale (*D. Muschella*)

La direttiva, con riferimento alla prestazione transfrontaliera di servizi di pagamento e di emissione di moneta elettronica, ha ampliato il concetto di “stabilimento” – utile ai fini dell'applicazione della disciplina in base al principio di territorialità – riconoscendo l'esistenza di forme di insediamento diverse dalla succursale. L'art. 45, comma 9, della direttiva prevede infatti che ciascuno Stato membro possa richiedere agli emittenti di moneta elettronica e ai prestatori di servizi di pagamento⁶⁹², che siano “*stabiliti nel suo territorio in forma diversa da una succursale*”, la nomina di un “punto di contatto centrale”, con la finalità di assicurare il rispetto delle norme AML/CFT e facilitare la vigilanza da parte delle Autorità competenti.

La modifica è in linea con la novità introdotta dalla direttiva PSD2, emanata qualche mese dopo rispetto alla quarta direttiva, che ha esplicitamente contemplato la possibilità che un istituto di pagamento possa operare in regime di stabilimento in un altro Stato membro non solo quando vi insedi una succursale, ma anche quando notifichi l'operatività attraverso agenti. Anche la PSD2 ha introdotto, per questa fattispecie di insediamento, un'analogia organizzativa (insediamento di un punto di contatto) per il presidio delle materie della PSD2 pure applicabili in base al principio di territorialità (trasparenza e diritti e obblighi delle parti, di cui ai Titoli III e IV della direttiva).

Nel precedente quadro disegnato dalla PSD1 (direttiva 2007/64) – che ha introdotto la figura degli istituti di pagamento, specializzati nella prestazione di servizi di pagamento, pure codificati dalla direttiva – il regime che governava l'attività transfrontaliera era basato sulla tradizionale dicotomia, tutt'oggi valida per le banche, della libera prestazione di servizi ovvero della libertà di stabilimento per il tramite di una succursale. La direttiva prevedeva tuttavia anche la possibilità di offrire servizi all'estero notificando, tramite “passaporto”, l'utilizzo di distributori esterni, qualificati dalla PSD1 come “agenti”, dislocati sul territorio dello Stato membro ospitante. Il controllo del corretto operato di tali reti era demandato, nel quadro disegnato dalla PSD1, all'Autorità del Paese di origine, che avrebbe potuto avvalersi, eventualmente, dell'ausilio dell'Autorità del paese ospitante. Sin dalle prime notifiche fu tuttavia evidente che i modelli di business tipici degli istituti di pagamento, caratterizzati dall'ampio ricorso a reti di agenti, a volte piuttosto ampie e articolate, mal si prestavano ad essere inquadrati, ai fini della notifica dell'attività in un paese *host*, quale libera prestazione di servizi. Si tratta in particolare, di reti che, per taluni servizi, quali ad esempio le rimesse di denaro, possono raggiungere numeri nell'ordine di diverse centinaia e per gli operatori di maggiori dimensioni, anche qualche migliaio. L'assetto dei controlli sulle reti, conseguenza dell'inquadramento delle stesse quale libera prestazione di servizi, si rivelò ben presto inadatto al presidio dei rischi posti dalle stesse, soprattutto in considerazione della circostanza che tali reti, per il principio di territorialità erano comunque incluse tra i destinatari degli obblighi imposti dalle norme antiriciclaggio italiane⁶⁹³.

⁶⁹² La categoria dei prestatori di servizi di pagamento include le banche, gli IMEL e gli istituti di pagamento. Gli emittenti di moneta elettronica sono le banche e gli IMEL.

⁶⁹³ Cfr. art. 11, comma 3, lett. d), del D.lgs. 231/2007, come modificato dal D.lgs. 141/2010.

La soluzione del punto di contatto recepisce e codifica soluzioni nate, all'indomani della PSD1, per mitigare il problema posto dai controlli su vaste reti distributive, allorché diversi paesi comunitari, tra quelli maggiormente interessati dal fenomeno delle notifiche di vaste reti distributive (Italia e Spagna) da parte di IP autorizzati in altri paesi comunitari (in prevalenza Regno Unito e Irlanda) introdussero prime forme di punto di contatto, ancorché con compiti e ambiti limitati.

Per l'Italia, l'obbligo di insediare un punto di contatto in presenza di due o più agenti, venne introdotto con il D.lgs. 19 settembre 2012, n. 169⁶⁹⁴. La misura riguardava solo gli IP e non anche altri PSP, quali le banche e gli IMEL e non si applicava alla distribuzione di moneta elettronica, svolta tramite analoghe reti di soggetti convenzionati (c.d. "distributori") nello Stato membro ospitante.

Il punto di contatto introdotto dalla quarta direttiva e meglio definito dal regolamento delegato (UE) 2018/1108 ha, innanzitutto, un ambito di applicazione più ampio rispetto a quello precedente definito dall'ordinamento nazionale in quanto, come detto, deve essere istituito non solo per la prestazione di servizi di pagamento, ma anche per la distribuzione di moneta elettronica. Anche i soggetti tenuti all'obbligo sono aumentati rispetto al passato regime, in quanto la misura si applica a tutti i PSP e a tutti gli emittenti di moneta elettronica e quindi include ora anche le banche⁶⁹⁵ e gli IMEL.

Anche i compiti assegnati al punto di contatto assumono un maggior rilievo rispetto a quelli di mera raccolta e trasmissione di informazioni previsti dal precedente assetto e presuppongono anche un maggior livello di competenze. Per svolgere la funzione di assicurare il rispetto delle norme AML/CFT da parte dell'ente che lo istituisce e facilitare la vigilanza da parte delle Autorità competenti, infatti, "il punto di contatto centrale dovrebbe conoscere in modo approfondito gli obblighi applicabili in materia di AML/CFT e facilitare l'elaborazione e l'attuazione di politiche e procedure AML/CFT" (considerando 5 del regolamento) e "dovrebbe, tra l'altro, avere un ruolo centrale di coordinamento tra l'emittente di moneta elettronica o il prestatore di servizi di pagamento che ha effettuato la nomina e le sue sedi e tra l'emittente di moneta elettronica o il prestatore di servizi di pagamento e le Autorità competenti dello Stato membro in cui operano le sedi, al fine di facilitare la vigilanza" (considerando 6).

In concreto, in base al regolamento, il punto di contatto ha il compito di facilitare l'elaborazione e l'attuazione di politiche e procedure AML/CFT; vigilare sull'effettivo rispetto da parte di agenti e distributori sia degli obblighi in materia di AML/CFT applicabili nello Stato membro ospitante che della conformità delle reti a politiche, controlli e procedure stabilite dal PSP o dall'emittente di moneta elettronica, informandolo di eventuali violazioni e assicurando l'adozione di misure correttive; assicurare lo svolgimento e la partecipazione delle reti ai programmi di formazione; rappresentare l'emittente di moneta elettronica o il prestatore di servizi di pagamento nelle comunicazioni con le Autorità competenti e con la FIU dello Stato membro ospitante. Il regolamento prevede inoltre la possibilità di assegnare al punto di contatto funzioni supplementari in materia di collaborazione attiva e rapporti con la FIU. Tale possibilità è stata prevista nell'ordinamento italiano.

Il regolamento stabilisce altresì i criteri per la nomina di un punto di contatto, la cui istituzione può essere prevista dallo Stato membro ospitante al ricorrere di uno dei criteri dettati dallo stesso regolamento, ovvero "qualora tale obbligo sia proporzionato al livello di rischio di riciclaggio o di finanziamento del terrorismo connesso all'attività di tali sedi", basando "la propria valutazione del livello di rischio di riciclaggio o di finanziamento del terrorismo connesso all'attività di dette sedi sui risultati delle valutazioni del rischio" effettuate dalla Commissione e sulla valutazione del rischio nazionale condotta dallo Stato membro, nonché su altre fonti credibili e affidabili di cui dispongono⁶⁹⁶.

⁶⁹⁴ Il D.lgs. 169/2012 ha modificato l'art. 42, comma 3 del s.lgs. 231/2007, rendendo obbligatoria "la costituzione del punto di contatto (...) in caso di pluralità di agenti" e individuando tale unità organizzativa quale tramite per l'inoltro alla UIF delle SOS prodotte dagli agenti. La modifica dell'art. 128-*quater* del TUB, introdotta dal medesimo decreto del 2012, ha assegnato al punto di contatto il compito di trasmettere in modo unificato all'OAM i dati relativi agli agenti operanti sul territorio per conto di IP comunitari.

⁶⁹⁵ Per le banche, a differenza di IP e IMEL, il regime dei passaporti previsto dalle norme comunitarie (CRD), non prevede la fattispecie dell'operatività tramite agenti e la conseguente notifica, nel passaporto, dell'utilizzo di reti distributive nel paese di destinazione. Nel caso di prestazione di servizi, peraltro sempre più frequente, mediante utilizzo di soggetti convenzionati da parte di banche comunitarie, manca a livello di normativa comunitaria una previsione che consenta di inquadrare con certezza questo tipo di operatività nella libera prestazione di servizi ovvero in una forma di stabilimento. Conseguentemente, può darsi il caso di una banca che convenzioni in un Paese terzo ampie reti distributive e che, ciononostante, operi in base al regime della libera prestazione di servizi. Se tale inquadramento ha conseguenze sull'applicazione della disciplina prudenziale, non ha invece effetti nell'applicazione della normativa antiriciclaggio, in virtù dell'introduzione, in tale corpus normativo, del concetto di stabilimento in forma diversa dalla succursale, di cui si è detto.

⁶⁹⁶ Già l'analisi nazionale dei rischi di riciclaggio (c.d. NRA) del 2014 aveva individuato una "vulnerabilità relativa molto significativa (...) imputabile a istituti di moneta elettronica (IMEL) e istituti di pagamento (IP) essenzialmente a causa di un quadro normativo comunitario in cui, attraverso la libera prestazione di servizi e processi di delocalizzazione, gli agenti possono operare nel nostro territorio al di fuori di un quadro adeguato di regolamentazione e controllo". Tale valutazione è stata poi confermata anche nell'ultimo NRA pubblicato nel 2019.

Nel recepire la quarta direttiva, il legislatore nazionale ha innanzi tutto individuato, tra i soggetti obbligati, non più gli agenti incaricati dagli IP comunitari, ma direttamente “gli intermediari bancari e finanziari (...) aventi sede legale e amministrazione centrale in un altro Stato membro, stabiliti senza succursale sul territorio della Repubblica italiana” (art. 3, comma 2, lett. u) e ha poi previsto, all’art. 43, comma 3. del D.lgs. 231/2007 che “i prestatori di servizi di pagamento e gli istituti di moneta elettronica aventi sede legale e amministrazione centrale in altro Stato membro e stabiliti sul territorio della Repubblica senza succursale, avvalendosi di soggetti convenzionati e agenti⁶⁹⁷, designano un punto di contatto centrale in Italia attraverso cui assolvono agli obblighi di cui al presente decreto”⁶⁹⁸.

Per rendere efficaci i controlli sulle reti distributive di tutti i PSP, italiani e comunitari, affidati alla Guardia di Finanza, la norma italiana ha introdotto un “Registro dei soggetti convenzionati ed agenti di prestatori di servizi di pagamento e istituti emittenti moneta elettronica” (art. 45), tenuto dall’Organismo degli agenti e dei mediatori (OAM), attribuendo al punto di contatto il compito di comunicare la composizione delle reti convenzionate dai PSP comunitari e di segnalare “a salvaguardia della correttezza e della legalità dei comportamenti degli operatori del mercato”, la “cessazione del rapporto di convenzionamento o del mandato, per motivi non commerciali”. In una sezione speciale di tale registro, l’OAM annota anche gli estremi identificativi del punto di contatto, l’avvio dell’operatività e ogni variazione ad essa attinente. Il decreto del Ministro dell’economia e delle finanze che disciplina le modalità tecniche di alimentazione e consultazione del registro è stato pubblicato in Gazzetta Ufficiale il 6 settembre 2022 e ne ha stabilito l’avvio nel dicembre 2022.

Lo strumento è disegnato per rendere efficace l’assetto dei controlli sulle reti distributive. Tenuto conto della capillarità delle reti, della pluralità degli operatori presenti nel mercato e della possibilità che ogni distributore possa essere convenzionato contemporaneamente da più PSP, il registro e, soprattutto, la sezione relativa alle cessazioni per motivi non commerciali, assume un rilievo fondamentale per evitare che un agente o un distributore, eliminato da una rete, ad esempio per violazioni di norme e procedure antiriciclaggio, continui ad operare sul mercato, mantenendo le altre convenzioni o potendo essere convenzionato da un nuovo mandante, italiano o comunitario.

Infine, le disposizioni emanate dalla Banca d’Italia ai sensi dell’art. 43, comma 4 del decreto, definiscono la struttura organizzativa e le risorse di cui il punto di contatto deve essere dotato per svolgere i compiti allo stesso assegnati dalla direttiva e dal regolamento.

In concreto, il ruolo di punto di contatto, che non può essere attribuito a una persona fisica, può essere affidato a una unità organizzativa dell’intermediario già presente in Italia e priva di rapporti con la clientela ovvero a una società comunque insediata in Italia⁶⁹⁹.

Per evitare la frammentazione delle competenze e la proliferazione di punti di interlocuzione tra le Autorità e l’ente comunitario, le disposizioni stabiliscono che quando sul territorio italiano è già presente una succursale della società, tale unità organizzativa venga designata quale punto di contatto centrale per l’attività svolta in Italia per il tramite di soggetti convenzionati e agenti. Con la stessa finalità, le disposizioni di vigilanza di IMEL e IP, nel dettare disposizioni per l’insediamento del punto di contatto competente per le materie di cui ai Titt. III e IV della PSD2 (trasparenza e diritti e obblighi delle parti), prevedono che, nel caso in cui sia insediato il punto di contatto centrale per le finalità antiriciclaggio, i due punti di contatto debbano coincidere.

Il punto di contatto, per poter svolgere i compiti che le norme gli attribuiscono, deve essere un’unità organizzativa strutturata, dotata quindi di risorse professionali, procedure e strumenti, anche informatici, idonei e proporzionati ai servizi offerti in Italia dall’intermediario comunitario per il tramite della rete. Rilevano a tal fine, in particolare, la dimensione e complessità della rete distributiva e l’esposizione al

⁶⁹⁷ L’art. 1, comma 2, lett. nn) definisce i soggetti convenzionati e agenti come “*gli operatori convenzionati ovvero gli agenti, comunque denominati, diversi dagli agenti in attività finanziaria iscritti nell’elenco di cui all’articolo 128-quater, commi 2 e 6, TUB, di cui i prestatori di servizi di pagamento e gli istituti emittenti moneta elettronica, ivi compresi quelli aventi sede legale e amministrazione centrale in altro Stato membro, si avvalgono per l’esercizio della propria attività sul territorio della Repubblica italiana*”.

⁶⁹⁸ La mancata istituzione del punto di contatto è sanzionata ai sensi dell’art. 62, comma 1. Con specifico riferimento alla moneta elettronica, la norma italiana, a differenza del regolamento comunitario, include tra i soggetti obbligati i soli istituti di moneta elettronica (IMEL) e non già la più ampia categoria degli emittenti di moneta elettronica, che include anche le banche. Tenuto conto che il regolamento prevede la mera facoltà e non l’obbligo per gli Stati membri di richiedere l’insediamento del punto di contatto (“*gli Stati membri possono imporre*”), si ritiene che tale misura non sia applicabile alle banche comunitarie che distribuiscono moneta elettronica sul territorio italiano.

⁶⁹⁹ L’intermediario, una volta designato il punto di contatto, deve eleggere domicilio presso lo stesso per tutti gli atti, gli obblighi e gli effetti previsti dal decreto antiriciclaggio e dalle relative disposizioni attuative.

rischio di riciclaggio dei servizi offerti in Italia. Deve essere altresì formalmente individuato e segnalato alla Banca d'Italia e alla UIF un responsabile del punto di contatto centrale, che deve essere in possesso dei requisiti previsti per il responsabile antiriciclaggio. Tale soggetto, in base al decreto antiriciclaggio, è individuato come responsabile delle segnalazioni di operazioni sospette e può eventualmente anche essere nominato responsabile antiriciclaggio.

Presso il punto di contatto devono inoltre essere disponibili documenti, dati e informazioni necessari alla Banca d'Italia e alla UIF per svolgere i controlli di competenza, anche ispettivi, sul rispetto degli obblighi antiriciclaggio.

Nella prassi applicativa, un certo grado di difficoltà nell'inquadramento delle varie fattispecie potrebbe derivare da taluni elementi di complessità presenti nelle norme, non ultimi, tra quelli già citati, il disallineamento presente nella disciplina transfrontaliera delle banche e degli altri PSP o la pluralità di figure e definizioni (agenti, italiani o comunitari, distributori, soggetti convenzionati per il solo incasso materiale ex art. 12, comma 2 del D.lgs. 141/2010⁷⁰⁰) che possono essere associate alla distribuzione di servizi di pagamento e di moneta elettronica. Un ulteriore elemento di complessità è dato dalla stessa evoluzione dei modelli distributivi, che alla progressiva sostituzione degli sportelli bancari con le reti commerciali di prossimità (tabaccai, edicole, supermercati e altri punti vendita della grande distribuzione, con una capillare presenza sul territorio) uniscono modalità innovative per lo svolgimento del servizio, grazie alle possibilità offerte dalle nuove tecnologie e all'ampia diffusione di strumenti di comunicazione connessi a internet. L'ibridazione nelle modalità di erogazione dei servizi – con ordini di pagamento originati *online*, direttamente dal cliente sul proprio *smartphone*, ma conclusi in prossimità con la mera consegna fisica ovvero con il prelievo del contante – potrebbe indurre a ritenere, erroneamente, l'operatività svolta in libera prestazione di servizi.

5. L'esercizio di autovalutazione (F. Lelli)

Il decreto antiriciclaggio introduce l'obbligo per i soggetti destinatari di effettuare una valutazione dei rischi di riciclaggio e finanziamento del terrorismo cui sono esposti (c.d. autovalutazione) al fine di facilitare l'approntamento di soluzioni organizzative e processi operativi commisurati a tali rischi. A questo fine, la legge rimette alla Banca d'Italia il compito di individuare per i soggetti vigilati soglie dimensionali e organizzative al di sotto delle quali l'obbligo di autovalutazione non si applica nonché di dettare criteri e metodologie per la conduzione dell'esercizio.

Prima dell'introduzione dell'obbligo di legge, le previgenti Disposizioni emanate dalla Banca d'Italia nel 2011 prevedevano che i soggetti obbligati valutassero il livello di rischio di riciclaggio e di finanziamento del terrorismo cui sono esposti al fine di predisporre procedure, strumenti e controlli appropriati. In particolare, spettava all'organo con funzione di supervisione strategica individuare politiche di governo di detti rischi adeguate all'entità e alla tipologia dei profili di rischio cui è concretamente esposta l'attività dell'intermediario. L'organo con funzioni di gestione doveva approntare le procedure necessarie per dare attuazione a tali politiche; la funzione antiriciclaggio ne avrebbe verificato nel continuo l'idoneità al fine di assicurare un adeguato presidio dei citati rischi. Limitatamente al settore bancario, l'obbligo di condurre un esercizio di autovalutazione era stato introdotto dalla Banca d'Italia nel 2015.

Per dare attuazione a quanto richiesto dal decreto, le nuove Disposizioni del 26 marzo 2019 richiedono a tutti i soggetti destinatari – ad accezione dei confidi minori – di dotarsi di procedure per effettuare l'autovalutazione dei rischi, in coerenza con la centralità assunta dal principio generale dell'approccio in base al rischio che governa la modulazione dei presidi organizzativi e procedurali antiriciclaggio.

L'introduzione dell'obbligo di autovalutazione mira ad accrescere la cultura antiriciclaggio dei soggetti vigilati, richiedendo loro di valutare almeno annualmente la propria esposizione ai rischi e il livello di vulnerabilità dei propri presidi, analogamente a quanto richiesto in ambito prudenziale. L'obiettivo ultimo non è l'azzeramento del rischio, quanto piuttosto la corretta gestione dello stesso, mediante l'adozione di assetti organizzativi e di misure di prevenzione idonee a mitigare la quota di rischio che l'intermediario si propone di tollerare nell'ambito della più ampia visione di tutti i rischi aziendali (*Risk Appetite Framework*).

⁷⁰⁰ Si tratta dei soggetti che svolgono l'attività "di incasso di fondi su incarico di soggetti autorizzati alla prestazione di servizi di pagamento" per i quali "non è necessaria l'iscrizione nell'elenco degli agenti in attività finanziaria, a condizione che detta attività sia svolta sulla base di un contratto di esternalizzazione, che ne predetermini le modalità di svolgimento, abbia carattere meramente materiale e in nessun caso sia accompagnata da poteri dispositivi". La norma introduce una deroga al regime applicabile ai soggetti convenzionati da PSP italiani, tenuti ad iscriversi nell'elenco degli agenti in attività finanziaria ex art. 128-*quater*, comma 2 del TUB tenuto dall'OAM e non ai soggetti convenzionati da PSP comunitari, già espressamente esclusi da tale obbligo.

Quanto ai criteri e alle metodologie per l'analisi e la valutazione dei rischi, le Disposizioni contengono una nuova sezione (la sezione VIII) che definisce la richiamata metodologia di autovalutazione e rappresenta pertanto il punto di partenza per la definizione da parte degli organi e delle funzioni aziendali – secondo le rispettive competenze e responsabilità – di politiche e strategie coerenti con i principi e le regole antiriciclaggio, per l'attuazione di misure organizzative, procedurali e operative atte a evitare il rischio di coinvolgimento in episodi di riciclaggio, assicurando i dovuti controlli sul rispetto della normativa e sull'adeguato presidio dei rischi.

Il decreto definisce i criteri metodologici per lo svolgimento dell'autovalutazione che si ripartisce in tre macro-attività: l'identificazione dei rischi attuali e potenziali cui l'intermediario è o può essere esposto in base alla natura e all'estensione dell'attività svolta (identificazione del rischio inerente); l'analisi dell'adeguatezza dell'assetto organizzativo e dei presidi aziendali rispetto ai rischi precedentemente identificati al fine di individuare eventuali vulnerabilità (analisi delle vulnerabilità); la conseguente determinazione del rischio residuo cui è esposto l'intermediario e delle relative modalità di mitigazione (determinazione del rischio residuo).

L'autovalutazione è svolta esaminando l'esposizione al rischio di coinvolgimento in fenomeni di riciclaggio per ogni linea di attività considerata rilevante. I criteri per l'individuazione delle linee d'attività sono definiti dai destinatari in ragione della propria natura, organizzazione, specificità e complessità operative, tenendo in considerazione i fattori di rischio individuati nelle Disposizioni. Per i soggetti caratterizzati da minore complessità operativa, la segmentazione in linee di attività può tenere conto del principio di proporzionalità, ferma restando la coerenza della segmentazione in relazione all'effettiva operatività svolta. Al riguardo, il documento di autovalutazione deve indicare i criteri che hanno determinato la scelta delle attività selezionate e il peso a ciascuna di esse attribuito nell'ambito dell'esercizio.

Determinato il livello di rischio residuo delle linee di attività e quello complessivo, i destinatari individuano le iniziative correttive o di adeguamento da adottare per prevenire e mitigare tali rischi residui; l'attribuzione del livello di rischio residuo viene accompagnata dalla descrizione degli elementi di valutazione considerati, delle analisi poste in essere e delle richiamate iniziative correttive o di adeguamento individuate. L'esercizio di autovalutazione è aggiornato con cadenza annuale dalla funzione antiriciclaggio ed è trasmesso alla Banca d'Italia unitamente alla relazione annuale della funzione antiriciclaggio, entro il 30 aprile dell'anno successivo a quello di valutazione.

6. Aspetti evolutivi: gli Orientamenti EBA sulle politiche e le procedure relative alla gestione della conformità e al ruolo del responsabile antiriciclaggio (A. Marrone)

Il quadro normativo nazionale sui controlli interni AML è mutato per effetto dell'entrata in vigore degli Orientamenti dell'Autorità bancaria europea (EBA) in materia di ruolo e funzioni del responsabile antiriciclaggio. Gli Orientamenti – indirizzati a tutti gli intermediari bancari e finanziari, incluse le imprese assicurative - sono stati pubblicati il 15 giugno 2022 e sono in vigore dal 1 dicembre 2022⁷⁰¹.

Essi specificano il ruolo, i compiti e le responsabilità del responsabile antiriciclaggio, dell'organo di gestione e dell'alto dirigente incaricato della conformità ai requisiti in materia di AML/CFT nonché le politiche, i controlli e le procedure interni ai sensi degli artt. 8, 45 e 46 della direttiva (UE) 2015/849⁷⁰².

Tra gli aspetti più significativi, rilevano l'obbligo di individuare all'interno dell'organo di vertice un responsabile per l'implementazione della normativa AML, in qualità di referente per i profili AML. La persona designata dovrebbe garantire che l'intero organo di gestione sia consapevole dell'impatto dei rischi di ML/TF sul profilo di rischio a livello di area di attività. Il membro dell'organo di gestione sarà il

⁷⁰¹ Si tratta di linee guida non previste espressamente dalla direttiva EU 849/2015. Esse sono elaborate dall'EBA d'iniziativa, a seguito di una richiesta della Commissione. In effetti, la necessità di una maggiore armonizzazione delle regole in materia di controlli interni AML è emersa con forza negli ultimi anni. In particolare, nel 2019 nel documento di Analisi Sovranazionale dei Rischi, la Commissione ha evidenziato come l'adozione di approcci divergenti nei diversi Stati europei e tra le diverse categorie di soggetti obbligati avesse creato delle lacune nei presidi AML/CFR dell'Unione.

⁷⁰² Cfr. F. Civale, *Antiriciclaggio: orientamenti EBA su politiche e procedure*, in www.dirittobancario.it, novembre 2022.

principale punto di contatto per il responsabile antiriciclaggio in seno alla dirigenza. Si tratta di un'importante innovazione per gli intermediari italiani, che attualmente non sono tenuti ad assegnare compiti specifici in materia AML ad un membro dell'organo con funzione di gestione, vigendo invece il principio della responsabilità collegiale dell'organo di vertice nel suo insieme per la definizione e l'implementazione delle *policy* AML.

Gli Orientamenti, inoltre, confermano l'obbligo di nominare, presso ciascun intermediario, un responsabile antiriciclaggio con il compito di assicurare l'efficiente gestione dei rischi di riciclaggio. Ogni intermediario è tenuto a nominare un responsabile, salvo eccezioni previste – in ossequio al principio di proporzionalità – per gli intermediari meno rischiosi. I compiti del responsabile antiriciclaggio, come descritti dagli Orientamenti, risultano in linea con quelli già allo stesso attribuiti nell'ordinamento nazionale in base alle Disposizioni della Banca d'Italia e dell'IVASS.

Gli Orientamenti individuano anche i requisiti di integrità e professionalità di cui deve essere dotato il soggetto designato come responsabile antiriciclaggio, che deve godere di una buona reputazione ed essere dotato di conoscenze, competenze ed esperienze adeguate per lo svolgimento dei compiti assegnati⁷⁰³.

Gli Orientamenti consentono di esternalizzare singoli compiti della funzione AML ma non la funzione nella sua interezza. Si prevede infatti che alcuni compiti (definiti strategici) non possono essere mai esternalizzati, nemmeno all'interno dei gruppi bancari e finanziari⁷⁰⁴. In tale contesto, va evidenziato che gli Orientamenti non distinguono tra l'esternalizzazione infragruppo e quella verso terzi, in tal modo replicando l'impostazione seguita dalla disciplina generale dell'EBA in materia di esternalizzazione. Con riferimento alla segnalazione di operazioni sospette, gli Orientamenti precisano che gli intermediari rimangono i responsabili finali della decisione di segnalare operazioni sospette all'UIF, anche laddove l'individuazione e la segnalazione di operazioni sospette è esternalizzata.

Le disposizioni EBA prevedono inoltre, in caso di gruppi, l'obbligo di nominare in ogni caso un responsabile antiriciclaggio di gruppo che avrebbe il compito di coordinare l'attività dei responsabili antiriciclaggio delle controllate e di assicurare una gestione integrata e consolidata del rischio di riciclaggio e di finanziamento del terrorismo.

Il 25 novembre 2022 la Banca d'Italia ha comunicato all'Autorità bancaria europea (EBA) l'intenzione di conformarsi agli orientamenti sulle politiche e le procedure relative alla gestione della conformità e al ruolo del responsabile antiriciclaggio. A tal fine la Banca si è impegnata a modificare le citate Disposizioni in materia di organizzazione, procedure e controlli interni antiriciclaggio del 26 marzo 2019. In attesa di queste modifiche, gli intermediari bancari e finanziari dovranno continuare ad applicare le disposizioni in vigore.

⁷⁰³ I controlli che le Autorità antiriciclaggio sono tenute ad effettuare in proposito sono descritti nella versione rivista degli Orientamenti EBA sulle caratteristiche di un approccio alla vigilanza antiriciclaggio basata sul rischio (EBA/GL/2021/16), in vigore dal 4 luglio 2022. In base a queste previsioni le Autorità AML sono tenute – in base al rischio – ad attivarsi per verificare il possesso dei richiamati requisiti, all'atto della nomina o successivamente alla stessa (ad es. fissando un incontro o richiedendo l'invio del curriculum vitae del responsabile). Qualora tali controlli evidenzino debolezze, l'Autorità AML è tenuta a comunicare le proprie valutazioni all'Autorità prudenziale. Nel caso in cui l'Autorità prudenziale non sia competente a valutare la suitability del responsabile antiriciclaggio (in quanto, ad esempio, la funzione antiriciclaggio non è accorpata ad altre funzioni di controllo, quale, ad esempio, la funzione di conformità), gli Orientamenti individuano (a titolo esemplificativo) alcune misure che l'Autorità AML potrebbe richiedere all'intermediario per il superamento delle debolezze riscontrate (si va dalla richiesta di sottoporre il responsabile AML a corsi di formazione supplementare o di perfezionamento delle qualifiche professionali alla richiesta, nelle ipotesi più gravi, di sostituire il responsabile stesso ovvero di nominare un ulteriore responsabile AML).

⁷⁰⁴ Più in dettaglio, in base agli Orientamenti, le decisioni strategiche in materia di AML/CFT non dovrebbero essere esternalizzate. Esse comprendono, in particolare: l'approvazione della valutazione del rischio di ML/TF a livello di area di attività; la decisione sull'organizzazione interna del quadro di AML/CFT dell'ente creditizio o dell'istituto finanziario; l'adozione di politiche e procedure interne in materia di AML/CFT; l'approvazione del metodo applicato per determinare il rischio di ML/TF insito in un determinato rapporto d'affari e l'attribuzione del profilo di rischio; l'approvazione dei criteri che l'ente creditizio o l'istituto finanziario deve applicare per individuare le operazioni sospette o anomale in relazione alle sue finalità di monitoraggio e/o segnalazione costanti.

CAPITOLO 6

Gli altri obblighi

(a cura di A.M.A. Carriero)

Premessa (A.M.A. Carriero)

I contributi racchiusi nel Capitolo 6 sono a commento di una miscellanea di obblighi in apparenza tra loro poco interrelati e, talora, secondari rispetto ai tradizionali pilastri della disciplina antiriciclaggio (obblighi di adeguata verifica, di conservazione e di segnalazione di operazioni sospette).

Per sgombrare il campo da equivoci, un discorso a sé merita il tema dello scambio di informazioni tra FIU dei diversi paesi; la cooperazione internazionale, infatti, è compresa tra le attività core delle FIU e riveste un'importanza cruciale nella prevenzione e nel contrasto al riciclaggio del denaro sporco e al finanziamento del terrorismo, il cui carattere è essenzialmente transnazionale.

Detto questo, è possibile individuare una comune matrice tra gli obblighi richiamati nel Capitolo, avendo a mente che il nocciolo duro della disciplina di prevenzione del riciclaggio e del finanziamento del terrorismo - per come si è andato formando nelle sedi sovranazionali - ben si presta a un percorso di arricchimento, nei singoli ordinamenti nazionali, ad opera di discipline convergenti – talora pur esse portate di direttive o regolamenti europei in materie complementari – o volte a declinare le specificità del contesto nazionale, che ne vanno a rafforzare l'impalcatura fondante in chiave anche complementare o strumentale.

Si pensi, anzitutto, alle Pubbliche amministrazioni, oggi destinatarie di obblighi di comunicazione alla UIF di operazioni sospette stabiliti in un articolo dedicato, ma che in Italia – sin dalla prima legge antiriciclaggio (L. 197/1991) – erano incluse tra i destinatari degli obblighi antiriciclaggio, pur se in un quadro precettivo carente, sino al 2015, di norme di attuazione. In questo caso si può, anzi, dire che i doveri si sono progressivamente meglio configurati e si colorano adesso di complementarità e peculiarità data la natura pubblica dei soggetti obbligati.

Un cenno meritano poi le limitazioni all'uso del contante, presenti anch'esse sin dalla prima legge antiriciclaggio italiana a completamento di una disciplina di prevenzione del riciclaggio impostata sulla canalizzazione dei flussi rilevanti di denaro contante attraverso intermediari c.d. abilitati. I conseguenti divieti di trasferimento di denaro contante tra privati (persone fisiche e giuridiche), non soltanto sono rimasti privi di forme concrete di *enforcement*, ma soprattutto, anche in virtù delle continue oscillazioni della soglia di riferimento, hanno progressivamente – secondo molti commentatori – subito uno sviamento dall'originaria finalità a obiettivi diversi, tra cui in primis il contrasto all'evasione fiscale. In materia si aprono prospettive di armonizzazione a livello europeo che vanno attentamente seguite.

Vanno considerate, inoltre, le comunicazioni oggettive, il cui principale scopo e utilizzo è quello di contribuire alle funzioni fondamentali delle FIU di analisi operativa e strategica; anche le disposizioni sul trasporto al seguito, che tendono a monitorare i passaggi di valori (oggi anche l'oro) alla frontiera, realizzano la dichiarata finalità di individuare possibili operazioni sospette che fa scattare il doveroso scambio informativo tra le Autorità doganali e la FIU.

Va da sé che, per ottenere segni tangibili del contributo in termini di efficacia degli obblighi compresi in questo Capitolo rispetto al sistema di prevenzione, occorre una piena integrazione delle informazioni che essi producono con i sistemi deputati a ricevere le segnalazioni di operazioni sospette e uno sfruttamento estensivo delle relative potenzialità nell'esercizio delle funzioni della UIF. Mi riferisco, soprattutto, alle informazioni delle basi dati ORO e SARA, nell'auspicio che le prime possano incrementare il loro valore aggiunto in virtù della prospettata riforma delle disposizioni della legge n. 7 del 2000 e le seconde possano continuare ad alimentare l'analisi strategica, gli studi e gli approfondimenti, il cui elevato valore qualitativo costituisce uno dei tratti peculiari della UIF oggetto di riconoscimento a

livello europeo e internazionale (*according to the 2016 Mutual Evaluation Report on Italy and the 2019 Follow-up Report “The UIF is a well-functioning financial intelligence unit. It produces good operational and high-quality strategic analyses that add value to the STRs”*). Infine, non vi è chi non veda sul piano teorico l’aggancio alla prevenzione dell’antiriciclaggio nell’istituto del “whistleblowing” che, purtroppo, nel sistema dell’AML è privo dell’elemento, a giudizio di chi scrive, di maggiore efficacia, insito nella possibilità di portare la comunicazione della violazione “all’esterno”, cioè all’attenzione delle Autorità.

1. Le comunicazioni oggettive (*C. Bentivogli e K. Bucaioni*)

1.1. Le comunicazioni oggettive in ambito internazionale e comunitario

L’art. 47 del decreto antiriciclaggio, introdotto dall’art. 2 del D.lgs. 90/2017, prevede un nuovo flusso segnaletico a favore dell’Unità d’Informazione Finanziaria per l’Italia, le comunicazioni oggettive, che – in linea con quanto previsto da altri ordinamenti europei ed extra-europei – è volto ad arricchire il patrimonio informativo delle unità d’intelligence finanziaria ai fini della prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo.

Si tratta di un flusso informativo contemplato dagli stessi standard internazionali emanati dal GAFI⁷⁰⁵, in base ai quali le FIU, “*oltre alle segnalazioni di operazioni sospette, ricevono altre informazioni rilevanti per il riciclaggio, i reati-presupposto e il finanziamento del terrorismo*” e, in questo ambito, sono menzionate a titolo esemplificativo “*comunicazioni relative a transazioni in contante, bonifici o altre dichiarazioni “basate su soglia”*”. In analogia con le segnalazioni di operazioni sospette, le comunicazioni oggettive sono, pertanto, flussi informativi che si riferiscono a operazioni a carattere nominativo e non di natura aggregata, trasmessi da operatori privati (per lo più intermediari) alle *financial intelligence units*. Al contempo, tali flussi si distinguono marcatamente dalle segnalazioni, in quanto riguardano operazioni che non sono individuate a valle di un complesso percorso valutativo finalizzato a sostanziarne la presunta natura sospetta, ma, al contrario, sono il frutto di un’elaborazione automatica e meccanicistica effettuata al ricorrere dei presupposti e delle soglie rilevanti definiti dai diversi ordinamenti nazionali. Il GAFI peraltro, pur riconoscendo il possibile apporto delle comunicazioni oggettive nel sistema di prevenzione, a differenza di quanto contemplato per le segnalazioni di operazioni sospette, ne tratteggia solo in modo esemplificativo caratteristiche e tipologia, rimettendo alla piena discrezionalità degli Stati membri l’opportunità di prevederne l’introduzione e, in tal caso, di individuarne i presupposti, definendo le tipologie di operazioni e le soglie rilevanti, come pure di configurare il novero dei soggetti tenuti alla loro trasmissione.

Ne discende una forte eterogeneità negli approcci adottati dai diversi Stati membri, come riscontrato dallo stesso Gruppo Egmont⁷⁰⁶, che, rispetto alla funzione di ricezione delle FIU, oltre alle segnalazioni di operazioni sospette, menziona le “*objective or threshold-based disclosures*” inoltrate dai soggetti obbligati relative al riciclaggio e al finanziamento del terrorismo, ma al contempo sottolinea anche che “*the scope and implementation of these reporting obligations will vary from one country to another based on national systems and obligations*”.

In linea di continuità con tale approccio le comunicazioni oggettive non sono sottoposte a misure di armonizzazione nell’ambito della previsioni europee; tali flussi possono tuttavia essere ricompresi tra le ulteriori informazioni che, sulla base delle diverse normative nazionali, sono ricevute dalle FIU a supporto delle funzioni di analisi finanziaria⁷⁰⁷.

⁷⁰⁵ Raccomandazione GAFI 29 e relativa Nota Interpretativa: “(b) *other information relevant to money laundering, associated predicate offences and terrorist financing*”. In particolare, la nota interpretativa rispetto alla funzione di “ricezione” precisa che “*the FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/ disclosures)*”.

⁷⁰⁶ Egmont Group of Financial Intelligence Units, *Operational Guidance for FIU activities and the exchange of information*, 2013, revised in 2017.

⁷⁰⁷ Ai sensi dell’art. 32, comma 3 della direttiva UE/2015/849.

In assenza di standard internazionali e disposizioni europee stringenti diversi ordinamenti hanno introdotto comunicazioni della specie, non ancorate a valutazioni di carattere discrezionale del segnalante; si tratta di flussi attinenti a specifiche categorie di transazioni, per lo più riferite al contante, atteso l'elevato rischio di riciclaggio di tale strumento di pagamento, per importi superiori a soglie fissate per legge.

In ambito extra-europeo, ad esempio, tra gli ordinamenti che hanno introdotto comunicazioni di natura oggettiva si annoverano gli Stati Uniti⁷⁰⁸, il Canada⁷⁰⁹ e l'Australia⁷¹⁰; si tratta di flussi che fanno riferimento a transazioni in contante effettuate con una o più operazioni eseguite nell'arco della stessa giornata e riferite a soglie particolarmente elevate.

In aggiunta a tali tipologie di flussi sono state peraltro progressivamente introdotte ulteriori tipologie di comunicazioni oggettive riferite a diverse categorie di operatori e strumenti: l'ordinamento canadese, ad esempio, ha previsto anche comunicazioni di tipo automatico alla FIU canadese (il FINTRAC) da parte dei casinò riferite a qualsiasi esborso⁷¹¹ (non necessariamente in contanti) effettuato da tali operatori per importi pari o superiori ai 10.000 dollari canadesi. A partire dal 1° giugno 2021⁷¹² è inoltre entrato in vigore l'obbligo per tutte le categorie di destinatari della normativa antiriciclaggio di comunicare al FINTRAC le *Large Virtual Currency Transactions Reports* inerenti a depositi o altre forme di pagamento in valute virtuali d'importo pari o superiore a 10.000 dollari canadesi.

In ambito europeo è di particolare interesse il caso francese anche per le modalità più articolate di calcolo della soglia di rilevanza rispetto alle operazioni prese in considerazione ai fini dell'individuazione di comunicazioni oggettive.

La Legge n. 2013-100 del 28 gennaio 2013 e n. 2013-672 del 26 luglio 2013 hanno introdotto per le banche, gli istituti di pagamento e gli IMEL un obbligo di "*Communication Systématique d'Informations*" (COSI) alla FIU francese, il TRACFIN, rispetto a determinate operazioni identificate per decreto come ad alto rischio di riciclaggio e finanziamento del terrorismo in ragione dei paesi, origine e destinazione dei fondi. La prima tipologia di comunicazioni oggettive ha riguardato le operazioni di trasferimento fondi effettuate a partire da un versamento in contanti o con moneta elettronica per importi superiori a 1.000 o 2.000 euro cumulati per cliente in un mese. Un successivo decreto del 25 marzo 2015 ha previsto un ulteriore flusso informativo a carico delle banche, inerente alle operazioni di deposito o i prelievi di contante che, cumulati, superano i 10.000 euro in un mese solare.

In Spagna determinate categorie di soggetti obbligati sono tenuti a comunicare al Sepblac, con periodicità mensile, le transazioni indicate nel regolamento della L. 10/2010, approvata con Regio Decreto 304/2014. Si tratta di un insieme di flussi di tipo automatico, tra i quali rientrano le operazioni superiori ai 30.000 euro con determinate caratteristiche, le operazioni di money transfer superiori ai 1.500 euro, le transazioni verso determinati paesi superiori ai 30.000 euro.

Tra gli Stati, anche in ambito europeo, si registra pertanto una certa eterogeneità nella definizione normativa di tali comunicazioni riguardo all'individuazione del novero dei soggetti obbligati, alla tipologia di operazioni considerate, alle soglie rilevanti, sebbene si tratti di flussi per lo più riferiti a transazioni in contanti, bonifici esteri e, in taluni casi, a specifiche operatività poste in essere presso casinò e operatori di gioco.

I limiti di tale eterogeneità sono peraltro stati rilevati nell'ambito degli approfondimenti condotti dalla Piattaforma delle FIU con il Mapping Exercise sulle caratteristiche, i poteri e la collaborazione delle FIU europee: proprio le comunicazioni oggettive ricevute dalle FIU sulla base delle diverse legislazioni nazionali sono considerate tra le fonti informative che dovrebbero essere oggetto di maggiore armonizzazione. Occorre infatti considerare che l'adozione di diversi presupposti e contenuti per le comunicazioni della specie impatta negativamente sulla qualità del patrimonio informativo che le FIU detengono a supporto delle analisi e della collaborazione internazionale; di qui la necessità di previsioni in ambito europeo che ne definiscano in modo convergente tipologie e contenuti⁷¹³.

⁷⁰⁸ Le Currency Transaction Reports sono inoltrate dagli intermediari in relazione a qualsiasi transazione in contante di importo superiore a \$10.000 effettuata da o per conto di un soggetto, anche con più operazioni aggregate nell'arco di un solo giorno.

⁷⁰⁹ Le Large Cash Transactions si riferiscono a operazioni in contante d'importo pari o superiore a CAD10.000 effettuate con un'unica transazione o più operazioni effettuate entro 24 ore consecutive dalla stessa persona o entità (Proceeds of Crime (Money Laundering) and Terrorist Financing Act).

⁷¹⁰ Le Threshold Transaction Reports sono riferite a operazioni in contante d'importo pari o superiore a AUD 10.000 effettuate con un'unica transazione o più operazioni frazionate. Cfr. Part 3, Division 3 (Sections 43 and 44) of the AML/CTF Act.

⁷¹¹ I Casino disbursement comprendono, tra l'altro, rimborsi di biglietti di slot, tokens o gettoni, prelievi di contante, anticipi su qualsiasi forme di crediti, pagamenti di scommesse inclusi i jackpots delle slots. Cfr. FINTRAC, [Guideline 10A: Submitting Casino Disbursement Reports to FINTRAC Electronically](#) and [Guideline 10B: Submitting Casino Disbursement Reports to FINTRAC by Paper](#).

⁷¹² Cfr. Regulations Amending the Regulations Amending Certain Regulations Made Under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2019: SOR/2020-112, Canada Gazette, Part II, Volume 154, No. 12.

⁷¹³ Cfr. C. Clemente, [Audizione sul Piano d'Azione della Commissione europea](#), tenutasi il 13 ottobre 2020 presso la Camera dei Deputati

Proprio in occasione dell'ampia riforma del sistema antiriciclaggio europeo avviata con la pubblicazione da parte della Commissione dell'*AML Package*, la proposta di regolamento relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo⁷¹⁴ introduce una tipologia di comunicazione oggettiva armonizzata che gli intermediari sono tenuti a inoltrare alle FIU. La disposizione che introduce limitazioni all'uso del contante per le operazioni di importo superiore ai 10.000 euro (art. 54 della proposta di regolamento) stabilisce infatti che, ai sensi del comma 4, lett. b), gli enti creditizi segnalino alla FIU *“i pagamenti o i depositi effettuati al di sopra di tale limite”*. L'intervento normativo in questa materia non appare tuttavia ispirato a una sistematica trattazione delle comunicazioni oggettive volta a disciplinarne in modo compiuto i presupposti, le condizioni, le caratteristiche distintive rispetto alle segnalazioni di operazioni sospette e le finalità, nonché le modalità di utilizzo e integrazione di tali flussi informativi nel processo di analisi finanziaria operativa e strategica condotta dalle FIU.

In chiave prospettica, il futuro Meccanismo di supporto e coordinamento delle FIU, che sarà collocato presso l'AMLA, potrebbe tuttavia acquisire un ruolo di catalizzatore nel favorire l'armonizzazione di tali tipologie di flussi informativi, nell'ambito del più ampio mandato volto, tra l'altro, a promuovere la convergenza operativa delle FIU. Il Meccanismo può infatti costituire la sede per valorizzare le modalità di sfruttamento di tali tipologie di flussi nel processo di analisi finanziaria tattica e strategica, favorendo così un processo di convergenza normativa volto ad armonizzare anche in questa area il patrimonio informativo delle FIU, con evidenti positive ripercussioni sul fronte dell'efficacia degli scambi informativi.

1.2. La scelta del legislatore nazionale: l'articolo 47 del D.lgs. 231/2007

Con il decreto di recepimento della direttiva UE/2015/849 (art. 2 del D.lgs. 90/2017) e in linea con la scelta compiuta da altri ordinamenti, l'art. 47 arricchisce il patrimonio informativo a disposizione della UIF con l'introduzione delle comunicazioni oggettive. Secondo tale previsione i soggetti obbligati, fermi gli obblighi di segnalazioni di operazioni sospette, sono infatti tenuti a trasmettere periodicamente alla UIF *“dati e informazioni individuati in base a criteri oggettivi, concernenti operazioni a rischio di riciclaggio e finanziamento del terrorismo”*.

Il legislatore nazionale, dopo aver definito la natura oggettiva di tali flussi e il loro carattere periodico, non ne disciplina puntualmente i contorni nella normativa primaria, ma rimette alla stessa UIF, sentito il Comitato di Sicurezza Finanziaria, il compito di individuare, con proprie istruzioni, le operazioni oggetto di tale comunicazione tra quelle *“a rischio di riciclaggio o di finanziamento del terrorismo”*, come pure il contenuto e la modalità di inoltro delle comunicazioni medesime.

Si tratta di un approccio che evidentemente privilegia una maggiore flessibilità nella definizione delle comunicazioni oggettive, per far sì che tali flussi segnaletici, anche in una prospettiva evolutiva, siano pienamente coerenti con le esigenze informative della FIU e, sulla base di compiute valutazioni della stessa Autorità tecnica, possano prontamente allinearsi al mutamento di tali esigenze in virtù della stessa evoluzione dei rischi di riciclaggio e finanziamento del terrorismo e, conseguentemente, siano *“ingaggiate”* le tipologie di soggetti obbligati in relazione alle diverse categorie di operazioni valutate come rilevanti.

La consultazione del Comitato di Sicurezza Finanziaria nella procedura di emanazione delle Istruzioni è chiaramente volta a garantire che le scelte della UIF siano opportunamente condivise con le altre Autorità competenti nella prevenzione e contrasto del riciclaggio e, segnatamente, con le controparti investigative dell'Unità, che beneficiano di tali informazioni nella fase d'indagine.

- Commissioni riunite Giustizia (II) e Finanze (V): *“Ancora maggiori sono le differenze attualmente esistenti per le comunicazioni relative a operazioni con determinate caratteristiche oggettive (soglie di importo, tipologie o forme tecniche, Paesi coinvolti) che le FIU ricevono a supporto delle loro analisi. La varietà di presupposti e contenuti delle comunicazioni oggettive si traduce in diversità del patrimonio informativo disponibile e degli strumenti per l'analisi. Va superato l'attuale vuoto normativo europeo mediante indicazioni armonizzate sulle tipologie significative di operazioni oggetto di comunicazione”*.

⁷¹⁴ Cfr. *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo*, 20 luglio 2021, COM (2021) 420 final.

Un ulteriore aspetto rimesso alle Istruzioni della UIF è quello di *“individuare espressamente le ipotesi in cui l’invio di una comunicazione oggettiva esclude l’obbligo di segnalazione di operazione sospetta, ai sensi dell’articolo 35”*. Sotto un profilo generale la finalità della disposizione appare evidente: le comunicazioni oggettive possono infatti contribuire a depurare il canale delle segnalazioni di operazioni sospette da segnalazioni cautelative, in quanto prive di circostanziati motivi di sospetto, ma riferite a operazioni a rischio di riciclaggio e finanziamento del terrorismo comunicate all’Unità in modo pressoché automatico.

Nondimeno, la disposizione pone per la sua stessa formulazione diverse criticità interpretative, proprio tenuto conto della distinzione ontologica tra segnalazioni di operazioni sospette e comunicazioni oggettive, distinzione confermata dallo stesso incipit del comma 1 dell’articolo in commento che, nell’introdurre l’obbligo di comunicazioni oggettive, ribadisce che restano fermi *“gli obblighi di cui al Titolo II, Capo III”*, ovvero gli obblighi di segnalazione di operazioni sospette di cui all’art. 35 e seguenti del decreto antiriciclaggio.

Rispetto alle finalità delle comunicazioni oggettive, il D.lgs. 90/2017 configura le medesime come un flusso segnaletico da sfruttare per finalità di analisi operativa in sede di approfondimento delle segnalazioni di operazioni sospette da parte della UIF e per l’effettuazione dell’analisi strategica. In sostanza le comunicazioni oggettive, in quanto costituite da dati a carattere nominativo, a differenza dei dati aggregati ricevuti dalla UIF ai sensi dell’art. 33 del D.lgs. 231 del 2007, possono essere sfruttate nella fase di arricchimento delle segnalazioni di operazioni sospette, integrando il quadro informativo sull’operatività inerente a soggetti segnalati, oltre che per condurre analisi specifiche su flussi finanziari potenzialmente anomali.

Con il D.lgs. 125/2019, entrato in vigore il 10 novembre 2019, è stato successivamente emendato il comma 2 dell’art. 47, per esplicitare, come richiamato nella stessa Relazione Illustrativa del predetto decreto, che tali comunicazioni sono utilizzate, oltre che per effettuare analisi di fenomeni o tipologie di riciclaggio o di finanziamento del terrorismo e per l’analisi finanziaria di operazioni sospette, anche per il loro approfondimento investigativo. Nell’ambito della collaborazione tra UIF, controparti investigative (Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e Direzione Investigativa Antimafia), e Direzione Nazionale Antimafia, l’utilizzo delle informazioni contenute nelle comunicazioni oggettive era stato espressamente richiamato nel Provvedimento emanato dall’Unità in un contesto che ne assicurasse elevati presidi di riservatezza, proprio attesa la natura di tali flussi informativi.

1.3. La scelta compiuta dalla UIF nelle Istruzioni

L’Unità d’Informazione Finanziaria ha definito le operazioni rilevanti e i soggetti tenuti alla trasmissione del nuovo flusso informativo con le Istruzioni pubblicate il 28 marzo 2019 sul sito internet della UIF e il successivo 15 aprile in Gazzetta Ufficiale⁷¹⁵.

Il 14 novembre 2018 il Provvedimento è stato sottoposto per il previo parere al Comitato di Sicurezza Finanziaria che, a seguito di un’interlocuzione scritta con le diverse Autorità interessate, si è espresso positivamente il 20 marzo 2019.

In coerenza con le evidenze del Supra-National Risk Assessment condotto dalla Commissione e del Risk Assessment nazionale sono sottoposte agli obblighi di comunicazione le operazioni in contante, categoria a elevato rischio di riciclaggio e finanziamento del terrorismo *“in quanto caratterizzate da non tracciabilità e anonimato negli scambi”*. Ai fini della rilevazione è stato stabilito il superamento di una soglia di importo pari o superiore a 10.000 euro, calcolato su base mensile e prendendo in considerazione

⁷¹⁵ Rispetto alla procedura di emanazione giova ricordare che, sebbene non fosse richiesto, lo schema di provvedimento, unitamente all’appendice tecnica, è stato posto in consultazione pubblica, al fine di garantire una piena trasparenza e condivisione delle scelte effettuate dalla UIF data la rilevanza degli adempimenti introdotti a carico degli operatori. La consultazione si è aperta nel luglio 2018 e si è conclusa il 10 agosto 2018. Come rilevato nel Rapporto Annuale dell’Unità la consultazione *“ha registrato un ampio e proficuo coinvolgimento degli operatori, che ha dato luogo a chiarimenti e anche ad alcuni limitati interventi di precisazione e rettifica del testo normativo e della sua appendice tecnica”*.

anche eventuali operazioni cumulate nel medesimo periodo, singolarmente pari o superiori a 1.000 euro ed effettuate dallo stesso cliente o esecutore (art. 3 delle Istruzioni).

Occorre sottolineare che, per quanto riguarda il criterio di calcolo delle operazioni cumulate, la scelta compiuta, in una prospettiva comparativa con analoghe tipologie di comunicazioni previste in altri ordinamenti, appare fortemente improntata a garantire il necessario bilanciamento tra la necessità di catturare possibili frazionamenti dell'operatività rilevante e l'opportunità di contenere al contempo eccessivi oneri, anche in termini di volume dei dati da gestire. Un eventuale frazionamento dell'operatività sotto la soglia dei 1.000 euro, volto ad eludere l'obbligo di comunicazione da parte del cliente, potrà essere rilevato dagli stessi intermediari in sede di valutazione delle operazioni sospette.

I nuovi obblighi di comunicazione si applicano a banche, Poste Italiane, IMEL, IP, succursali di tali intermediari di paesi comunitari e di Paesi terzi, nonché a IP e IMEL di paesi comunitari tenuti a designare un punto di contatto centrale (art. 2 delle Istruzioni)⁷¹⁶.

Rispetto alla definizione delle ipotesi in cui l'inoltro della comunicazione oggettiva esenta dalla segnalazione di operazione sospetta, le Istruzioni, dopo aver ribadito che le operazioni oggetto di comunicazione fanno parte del patrimonio informativo alla base delle valutazioni effettuate dagli intermediari, individuano due criteri di esclusione, rispettivamente di natura oggettiva e soggettiva (art. 4). Si fa infatti riferimento al fatto che l'operazione *“non presenta collegamenti con operazioni di diversa tipologia che facciano desumere una complessa operatività sospetta”*, ovvero che *“l'operazione non è effettuata da clienti con profilo soggettivo marcatamente anomalo”*.

Sotto questo profilo l'esenzione è stata evidentemente configurata tenendo conto dell'esperienza di analisi finanziaria e, in particolare, del fatto che la significatività di un'operazione in contanti ai fini di una rilevazione di possibile operazione sospetta si riscontra quando la stessa è riconducibile a fattispecie articolate di operazioni, o al profilo del soggetto (a rischio elevato, quale ad esempio una persona politicamente esposta o un soggetto indagato).

Nel corso della consultazione è stato altresì chiarito che, in caso di violazione del limite all'uso del contante di cui all'art. 49 del D.lgs. 231/2007, l'invio di una comunicazione oggettiva non esonera i destinatari del provvedimento dall'inoltro della relativa comunicazione al Ministero dell'Economia e delle finanze. Tale possibilità, ai sensi delle attuali disposizioni normative del D.lgs. 231/2007, è stata infatti contemplata solo in relazione alla trasmissione di segnalazioni di operazioni sospette (art. 51, comma 3, del D.lgs. 231/2007).

1.4. Le ragioni di un monitoraggio del contante

La scelta della UIF di focalizzare l'attenzione sul contante riflette i rischi peculiari del suo impiego. Il denaro contante è facilmente utilizzabile e, soprattutto nelle operazioni esterne ai circuiti finanziari, non è tracciabile e assicura l'anonimato degli scambi. Questa sua caratteristica lo rende uno strumento di elezione per occultare e riciclare i proventi di reati.

Uno studio sull'impatto di restrizioni ai pagamenti in contanti svolto per conto della Commissione UE conferma che, sebbene nelle attività di riciclaggio si utilizzino spesso schemi anche molto complessi, l'utilizzo del contante è significativo perché molte delle attività illegali sottostanti generano a loro volta profitti che affluiscono ai criminali sotto forma di denaro contante⁷¹⁷.

Numerose sono le attività illegali che producono ricavi ad alta intensità di contante. Fra queste rientrano lo spaccio di stupefacenti, il traffico di migranti e il traffico di esseri umani. L'analisi delle segnalazioni di operazioni sospette e le indagini delle forze dell'ordine mostrano come in tutte le fasi del riciclaggio l'utilizzo del contante sia ancora molto diffuso⁷¹⁸.

⁷¹⁶ Tenuto conto della tipologia delle operazioni da censire, non si è reputato di estendere l'obbligo a tutti i destinatari degli obblighi di collaborazione attiva.

⁷¹⁷ Commissione europea, *Relazione della Commissione al Parlamento europeo e al Consiglio sulle restrizioni ai pagamenti in contanti*, giugno 2018; ECORYS, *Study on an EU initiative for a restriction on payments in cash - Final Report*, December 2017.

⁷¹⁸ Europol, *Why cash is still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*, February 2015. Cfr. anche la sez. 6.1.5.

Nel Rapporto *Why is cash still king?*, Europol conferma che, nonostante il crescente utilizzo di strumenti digitali nelle transazioni, il contante continua a rappresentare uno strumento importante negli schemi di riciclaggio individuati⁷¹⁹.

Per l'Unione europea nel suo insieme, il *Supranational risk assessment* (SNRA)⁷²⁰ – elaborato dalla Commissione UE nel 2019 sulla base delle previsioni della quarta direttiva antiriciclaggio⁷²¹ – ha individuato e valutato i rischi di riciclaggio determinati dalle interrelazioni di minacce e vulnerabilità presenti in diversi Stati membri. Nel documento la Commissione identifica il contante come lo strumento preferito per il riciclaggio. Le sue caratteristiche rendono semplice, ad esempio, il rapido trasferimento da un paese ad un altro dove è più agevole la sua integrazione nei circuiti legali.

In generale, i settori con una porzione elevata di pagamenti in contanti, in particolare quelli del commercio che accettano pagamenti con banconote di grosso taglio, sono ritenuti particolarmente esposti al rischio di riciclaggio. Oltre all'esposizione al rischio, il *Supranational risk assessment* evidenzia l'importanza della diffusione della consapevolezza del rischio stesso e dell'adeguatezza del quadro normativo. Un limite legale alle transazioni in contanti rappresenta una forma di mitigazione di queste vulnerabilità. Fra le misure di contrasto previste dalla quarta direttiva rientrano gli obblighi di segnalazione da parte di commercianti in beni (ad esempio pietre e metalli preziosi), qualora i pagamenti siano effettuati in contanti per importi pari o superiori a 10.000 euro.

L'*Analisi nazionale sui rischi di riciclaggio e finanziamento del terrorismo* (National Risk Assessment - NRA) effettuata dal Comitato di sicurezza finanziaria istituito presso il MEF⁷²², offre una valutazione dei rischi nella specifica realtà italiana. Il rapporto evidenzia come l'elevato utilizzo del contante e la dimensione dell'economia non osservata rappresentino elementi di criticità molto significativi del sistema economico e sociale italiano.

Fra i paesi dell'area dell'euro oggetto dell'indagine SPACE della Banca centrale europea, l'Italia si colloca nel gruppo di quelli con maggiore utilizzo del contante nei pagamenti al dettaglio e nelle operazioni fra individui, con l'82% delle operazioni e il 58% del relativo valore⁷²³.

L'impiego del contante nei pagamenti è correlato negativamente agli importi pagati, con valori medi che per l'Italia si collocano lievemente al di sotto dei 20 euro. Le banconote di grosso taglio sono invece utilizzate nell'economia legale prevalentemente come riserva di valore, mentre sono ampiamente sfruttate nelle attività illecite a causa del contenuto volume e dell'alto valore, e in particolare facilitano il riciclaggio e l'evasione fiscale⁷²⁴. La decisione della BCE di interrompere l'emissione del taglio da 500 euro nel 2019 riflette la consapevolezza di questi rischi da parte delle Autorità europee.

Le stime più recenti dell'Istat (2020) sull'economia non osservata (sommerso economico ed attività illegali⁷²⁵) indicano che essa rappresenterebbe il 10,5% del PIL.

Il peso del sommerso economico sul valore aggiunto risulterebbe particolarmente elevato in settori ad alto utilizzo del contante: gli altri servizi alle persone (34,2%), il commercio, trasporti, alloggio e ristorazione (22,1%) e le costruzioni (19,3%). La rilevante dimensione dell'economia non osservata e la diffusione nell'uso del contante, insieme con le inefficienze dei mercati, delle imprese e della Pubblica amministrazione, svolgono un involontario schermo all'evasione fiscale e alle attività criminali, rendendole meno facilmente individuabili⁷²⁶.

La rilevazione delle operazioni in contanti effettuata dalla UIF con le comunicazioni oggettive si propone dunque di focalizzare meglio l'utilizzo di questo strumento di pagamento nel nostro Paese, per evidenziarne gli elementi di anomalia.

⁷¹⁹ Europol, 2015, cit.

⁷²⁰ Commissione europea, *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, luglio 2019. Da ultimo la terza edizione del *Supranational risk assessment*, pubblicata nell'ottobre del 2022, conferma che l'economia criminale rimane fortemente basata sull'utilizzo del contante, esponendo la UE a significativi rischi di riciclaggio e di finanziamento del terrorismo.

⁷²¹ Direttiva (UE) 849/2015.

⁷²² MEF, Dipartimento del Tesoro, *Analisi nazionale dei rischi di riciclaggio di denaro e di finanziamento del terrorismo elaborata dal Comitato di sicurezza finanziaria - Aggiornata al 2018 – Sintesi*, 2019. Anche il NRA è previsto dalla quarta direttiva antiriciclaggio UE.

⁷²³ Solo Malta, Cipro e Spagna effettuano una quota maggiore di operazioni in contanti rispetto all'Italia. I Paesi Bassi sono il paese meno intensivo di contanti nei pagamenti (34% del numero delle operazioni e 22% del valore). BCE, *Study on the payment attitudes of consumers in the euro area (SPACE)*, December 2020.

⁷²⁴ K. S. Rogoff, *The curse of cash*, Princeton University Press, 2016.

⁷²⁵ Nelle attività illegali sono inclusi dall'Istat la produzione e traffico di stupefacenti, i servizi di prostituzione e il contrabbando di tabacco.

⁷²⁶ G.M. Rey, *Interazioni fra economia criminale e economia legale*, Argomenti, n. 10, 2018, pp. 5-30.

1.5. Il contenuto della rilevazione

I segnalanti trasmettono i dati in via telematica tramite il portale Infostat-UIF della Banca d'Italia entro il giorno 15 del secondo mese successivo a quello di riferimento delle comunicazioni⁷²⁷.

Le informazioni richieste riguardano le operazioni in contanti di importo pari o superiore a 10.000 euro eseguite nel corso del mese solare, anche se realizzate attraverso più operazioni singolarmente pari o superiori a 1.000 euro. Le operazioni dovranno essere individuate considerando tutte le movimentazioni di denaro effettuate dal medesimo soggetto cliente o esecutore; le operazioni effettuate dall'esecutore sono imputate anche al cliente in nome e per conto del quale ha operato.

Ai sensi dell'art. 3, commi 2 e 3 del Provvedimento della UIF se, in un determinato mese, non hanno rilevato operazioni in contanti di importo superiore alla soglia, i segnalanti devono inviare una comunicazione negativa. I segnalanti che, per la propria tipologia di operatività, non effettuano mai operazioni da comunicare possono richiedere l'esonero dall'invio della comunicazione negativa mensile.

Le comunicazioni devono contenere, in forma strutturata, informazioni sulle operazioni, su tutti i soggetti coinvolti (persone fisiche e giuridiche) e sui rapporti movimentati⁷²⁸.

Il monitoraggio della qualità delle comunicazioni oggettive nei primi anni della rilevazione ha evidenziato diffuse criticità. In particolare sono state riscontrate errate comunicazioni delle operazioni in contante virtuale, mancate comunicazioni di operazioni in contanti riscontrabili, invece, nelle SOS trasmesse dai medesimi soggetti obbligati, informazioni obbligatorie mancanti e incoerenze fra i diversi campi delle operazioni o nei dati sulle caratteristiche dei soggetti.

Alla luce delle carenze riscontrate, la UIF ha sviluppato ulteriori controlli in fase di acquisizione dei dati e ha introdotto forme di verifica, anche ispettiva, degli interventi attuati dagli operatori. A supporto dei segnalanti è fornito un servizio di contatto diretto con i singoli operatori ed è disponibile un documento che fornisce chiarimenti sulle problematiche applicative più frequenti⁷²⁹.

1.6. Utilizzo delle comunicazioni oggettive

Le comunicazioni oggettive sono fondamentalmente diverse dalle segnalazioni di operazioni sospette perché le informazioni sono fornite sulla base delle caratteristiche dell'operazione (in contanti) e del raggiungimento delle soglie di importo prestabilite. A differenza delle segnalazioni di operazioni sospette, il soggetto obbligato non effettua valutazioni sulla presenza di elementi che facciano desumere attività di riciclaggio o di finanziamento del terrorismo.

Le informazioni raccolte con le due rilevazioni presentano, peraltro, ampie aree di sovrapposizione e di reciproco completamento, costituite da soggetti, da operazioni sospette che movimentano rilevanti importi di contante e dai rapporti su cui tali flussi di denaro insistono.

Il patrimonio informativo contenuto nelle comunicazioni oggettive, oltre a costituire una diretta fonte di arricchimento delle segnalazioni di operazioni sospette, consente l'esplorazione di flussi finanziari con strumenti statistici o di analisi delle reti/relazioni al fine di individuare operatività potenzialmente anomale e non ancora rilevate nelle SOS.

È in corso di completamento il progetto informatico per la disseminazione agli Organi investigativi dei dati delle comunicazioni oggettive sui soggetti presenti nelle SOS. I diversi filoni di indagine allo studio dell'Unità riguardano gli andamenti temporali dei flussi in specifici territori, le caratteristiche delle operazioni, gli attori delle stesse e i settori di attività economica in cui operano. L'individuazione di anomalie si basa sull'utilizzo di specifici indicatori semplici e compositi che utilizzano, oltre ai dati delle comunicazioni oggettive, anche le segnalazioni di operazioni sospette e basi dati esterne.

⁷²⁷ Informazioni dettagliate sulla procedura di registrazione e di invio delle Comunicazioni oggettive sono disponibili in UIF, *Comunicazioni oggettive - Manuale Utente*.

⁷²⁸ Lo schema segnaletico per le comunicazioni oggettive è descritto in UIF, *Istruzioni in materia di comunicazioni oggettive*, 28 marzo 2019. Le informazioni da trasmettere alla UIF sono descritte in dettaglio nel documento *Informazioni e dati contenuti nelle comunicazioni oggettive*.

⁷²⁹ UIF, *FAQ Comunicazioni oggettive (OGG)*.

2. Segnalazione dei dati aggregati e analisi strategica (M. Gara e S. Iezzi)

2.1. Definizione e obiettivi dell'analisi strategica

Gli standard internazionali collocano l'attività di analisi strategica tra le funzioni istituzionali delle FIU accanto all'analisi operativa (cfr. le note interpretative della Raccomandazione 29 del GAFI). L'analisi operativa ha natura prettamente finanziaria e consiste in una serie di attività concentrate su singoli casi o filoni di casi, tese a qualificare e ampliare l'originario contesto segnaletico, aumentando il patrimonio informativo di ciascuna segnalazione. Diversamente, l'analisi strategica ha la finalità di valutare l'esposizione al rischio di riciclaggio e di finanziamento al terrorismo del sistema economico-finanziario nel suo complesso, di specifiche aree geografiche del Paese, mezzi di pagamento o settori economici. In particolare, l'analisi strategica fa uso di un ampio bagaglio di informazioni disponibili al fine di identificare tendenze e fenomeni nel riciclaggio e nel finanziamento del terrorismo, identificare minacce e vulnerabilità del sistema economico-finanziario, e contribuire a determinare politiche e obiettivi per le FIU o, più in generale, per il sistema antiriciclaggio. Tra gli obiettivi dell'analisi strategica vi è anche l'individuazione, a partire dall'analisi massiva dei dati, di anomalie specifiche potenzialmente oggetto di approfondimenti mirati. Questa impostazione appare coerente con i più recenti orientamenti dell'*intelligence*, in cui l'attività di studio finalizzata a una migliore comprensione delle dinamiche associate al riciclaggio e al finanziamento del terrorismo, nonché del circostante contesto economico e regolamentare, è considerata uno strumento essenziale dell'apparato preventivo.

Di norma l'analisi strategica è organizzata in due filoni di attività distinti: 1) la rilevazione delle tipologie e degli schemi di condotte finanziarie anomale e 2) l'attività di osservazione e studio dei flussi finanziari e dei fenomeni di riciclaggio. L'obiettivo di individuare tendenze e criticità connesse al riciclaggio e al finanziamento del terrorismo viene perseguito, quindi, secondo due direttrici distinte: da un lato, soprattutto attraverso l'analisi massiva dei casi accertati di riciclaggio (ad esempio, quelli che emergono dalle segnalazioni di operazioni sospette), si mira a individuare le prassi e i comportamenti adottati in modo sistematico a fini di riciclaggio e finanziamento del terrorismo in modo da definire adeguati strumenti di prevenzione e contrasto; dall'altro, l'attività di studio e ricerca, anche mediante l'utilizzo di tecniche di analisi mutate dalle indagini statistiche ed economiche, ha lo scopo di fornire misure aggregate o di dettaglio del rischio di riciclaggio ed evidenziare tendenze anche a livello macro di natura economica e finanziaria collegate a tale fenomeno.

2.2. Il quadro normativo e gli orientamenti esteri

In linea con gli standard internazionali, anche la normativa europea (cfr. art. 32, par.8, direttiva (UE) 2015/849), fa rientrare l'analisi strategica tra le funzioni della FIU, definendo tale attività in base allo scopo perseguito, che è quello di individuare tendenze e schemi del riciclaggio e del finanziamento del terrorismo.

Più articolata è la previsione relativa a questa funzione nella normativa nazionale (D.lgs. 231/2007). L'art.6, comma 7, stabilisce che la UIF utilizza le informazioni raccolte nello svolgimento delle proprie funzioni anche per svolgere *“analisi e studi su singole anomalie, riferibili a ipotesi di riciclaggio e di finanziamento del terrorismo su specifici settori dell'economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realtà economiche territoriali”*.

L'attività di analisi strategica della UIF può essere anche effettuata su richiesta della DNAA (art. 8, comma 1, punto d). Con specifico riferimento alle Segnalazioni Antiriciclaggio Aggregate nell'art. 33, comma 1, si ribadisce che tali dati vengono impiegati dalla UIF per svolgere *“analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali”*. Quanto all'utilizzo delle analisi e degli studi svolti dalla UIF, la norma si limita a richiedere (art. 12, comma 5) che *“i risultati di carattere generale”* che emergono dagli stessi siano forniti alle altre Autorità e organi che

partecipano al sistema di prevenzione nazionale antiriciclaggio. Nella realtà i risultati di tale analisi trovano un utilizzo più ampio, come già detto in precedenza.

Prima di esaminare come viene tradotto in pratica il dettato della normativa anti-riciclaggio italiana, vale la pena di verificare come realizzano questa attività le principali organizzazioni internazionali attive nell'anti-riciclaggio (il Gruppo di Azione Finanziaria – GAFI e l'Egmont Group) e come viene declinata nelle FIU degli altri paesi.

L'attività di analisi strategica svolta dalle organizzazioni internazionali è essenzialmente concentrata sull'analisi e classificazione tipologica delle fattispecie di riciclaggio e finanziamento del terrorismo che vengono rilevate. La finalità di tale attività è quella soprattutto di rilevare l'emergere di nuove pratiche di riciclaggio e delle connesse minacce in modo da definire gli opportuni strumenti, prevalentemente normativi, ma anche di natura operativa, che i singoli stati sono poi incaricati di recepire nei propri ordinamenti, ovvero applicare nella prassi.

Nel GAFI è puntualmente definita la fase in cui viene inserita l'analisi strategica all'interno del "ciclo produttivo" in cui è organizzata l'attività dell'organizzazione. È compito infatti del *Risk, Trends and Methods Group* (RTMG) di individuare ed analizzare quei fattori critici connessi al riciclaggio ed al finanziamento del terrorismo che possano minacciare l'integrità del sistema finanziario. Nel corso degli anni sono stati trattati aspetti molto diversi, quali l'uso del contante, le criptovalute, i reati ambientali e il riciclaggio *trade-based*. Nei rapporti dell'RTMG vengono anche individuate *best practices* per il contrasto e la prevenzione delle varie minacce. Le indicazioni che provengono dalle analisi di questo gruppo possono essere recepite poi dal *Policy Development Group* (PDG) che ha il compito di aggiornare ed affinare le 40 Raccomandazioni proprio per tener conto delle nuove vulnerabilità che dovessero emergere, come è successo negli ultimi decenni per i professionisti (inclusi nel 2003 tra i destinatari degli obblighi anti-riciclaggio) e più di recente per gli intermediari che operano in *crypto-assets*. La filiera definita dal GAFI permette di individuare chiaramente qual è il ruolo dell'analisi strategica, intesa prevalentemente come analisi tipologica nell'economia dell'attività di contrasto al riciclaggio.

L'altra organizzazione internazionale di riferimento nel campo è l'Egmont Group, che raduna le FIU dei vari paesi. In tema di analisi strategica, l'Egmont è soprattutto impegnato in iniziative di assistenza tecnica e *capacity building* all'interno di un gruppo di lavoro, il *Technical Assistance and Training Working Group* (TATWG), appositamente costituito. In questo contesto, vengono forniti corsi di formazione mirati sull'analisi strategica che intendono individuare gli strumenti tecnici da utilizzare per questo tipo di analisi, i dati da impiegare, le varie fasi in cui deve essere strutturata ed infine gli esiti e gli utilizzi che essi possono avere all'interno di una FIU.

L'impostazione tipologico-centrica e dal carattere spiccatamente operativo che l'analisi strategica assume all'interno delle due principali organizzazioni internazionali nel campo dell'antiriciclaggio è un riflesso delle modalità in cui questa attività viene svolta nelle FIU dei principali paesi e, a sua volta, implica che questa sia l'impostazione più diffusa nello svolgimento dell'analisi strategica, con eccezioni molto isolate. È peculiare che la disponibilità di dati spesso molto dettagliati (come le segnalazioni *value-based* su operazioni in contante e bonifici esteri previste nella normativa anti-riciclaggio di molti paesi) non ispiri nelle FIU una diffusa applicazione di tecniche di *advanced data analytics* a fini di analisi strategica, oltre agli ovvi utilizzi a scopi più strettamente operativi.

Passando in rassegna i documenti disponibili in cui viene illustrata l'attività delle varie FIU (tipicamente i rapporti annuali, ma anche i rapporti di *mutual evaluation* del GAFI, oltre che altre pubblicazioni estemporanee) non emergono studi e analisi massive finalizzate all'esame di specifici fenomeni attraverso tecniche quantitative avanzate, quali quelle che la UIF da anni realizza. Oltre che in ragione di un acceso *focus* sull'attività operativa, come detto, ciò è anche conseguenza di carenze strutturali di *expertise* e capacità tecniche che caratterizzano molte FIU, soprattutto quelle di polizia, dato che le risorse per la realizzazione di questo tipo di analisi non sono sempre disponibili all'interno delle agenzie investigative.

2.3. L'analisi strategica nella UIF

Nell'ambito del primo filone di attività, a partire dall'analisi operativa svolta dalla UIF sulle segnalazioni di operazioni sospette, viene sviluppata un'attività di individuazione di condotte finanziarie ricorrenti poste in essere a fini di riciclaggio o di finanziamento del terrorismo. Attraverso la definizione delle tipologie, la UIF è in grado di classificare le segnalazioni e diffondere indicazioni aggiornate per agevolare l'identificazione delle operazioni sospette da parte dei soggetti obbligati. La diffusione dei risultati, a beneficio della collaborazione attiva, si realizza con la pubblicazione di casistiche di riciclaggio all'interno della Collana Analisi e studi dei Quaderni dell'Antiriciclaggio.

Negli ultimi anni l'utilizzo delle metodiche più consolidate per l'analisi delle SOS è stato, inoltre, accompagnato dall'impiego di strumenti che consentono l'analisi massiva delle segnalazioni. Tale approccio ha permesso di allargare la visione su un arco temporale esteso, rilevando così le ricorrenze degli attori coinvolti e le loro relazioni e connessioni, facendo emergere fenomeni rilevanti anche da operatività che, se esaminate singolarmente, appaiono poco significative. Tale modalità di analisi, utilizzata in particolare per le segnalazioni provenienti da soggetti operanti nel settore *money transfer*, è in corso di estensione ad altri settori caratterizzati dalla alta numerosità e frammentarietà delle operazioni e dalla pluralità di soggetti coinvolti, quali, ad esempio, quello delle transazioni con carte di pagamento e dei *virtual asset*.

L'analisi strategica del secondo filone di attività ha come obiettivo l'individuazione di fenomeni e tendenze del sistema finanziario, la valutazione del rischio del sistema economico-finanziario nel suo complesso, di specifiche aree geografiche, mezzi di pagamento o settori, nonché l'individuazione di anomalie specifiche. Le informazioni su cui poggia l'analisi derivano dall'insieme delle fonti informative raccolte dall'Unità, all'occorrenza integrate da dati di fonte interna ed esterna alla Banca d'Italia e da informazioni appositamente richieste agli intermediari. In questo caso l'analisi strategica impiega, in particolare, metodi quantitativi, quali tecniche statistico-econometriche e di intelligenza artificiale.

Le Segnalazioni Anti-Riciclaggio Aggregate (S.A.R.A.) rappresentano la principale fonte di informazione per la conduzione di tale tipologia di analisi. Le segnalazioni S.A.R.A. sono inviate mensilmente dagli intermediari finanziari e derivano dall'aggregazione di dati sulla loro operatività secondo criteri determinati dalla UIF con proprio Provvedimento. I dati S.A.R.A. coprono tutta la gamma degli strumenti di pagamento e delle operazioni finanziarie e, essendo segnalazioni che aggregano più operazioni aventi stesse caratteristiche, sono anonimi. Le aggregazioni dei dati riguardano principalmente il mezzo di pagamento utilizzato, l'ubicazione della dipendenza dell'intermediario segnalante, il settore di attività economica e la residenza del cliente. I dati si riferiscono sia alle operazioni in entrata sia a quelle in uscita e riportano separatamente l'eventuale ammontare delle transazioni effettuate in contante.

I dati ricevuti fino a dicembre 2020 riguardano tutte le operazioni disposte dalla clientela per importi (anche frazionati) pari o superiori a 15.000 euro. A partire da gennaio 2021 si applicano le nuove disposizioni attuative, che tengono conto delle principali novità introdotte dalla normativa primaria e secondaria, tra cui l'inclusione, tra i destinatari degli obblighi, di SICAF, punti di contatto di prestatori di servizi di pagamento e di IMEL comunitari, la riduzione della soglia minima per il censimento delle operazioni da 15.000 a 5.000 euro e l'eliminazione della soglia per le operazioni relative alla prestazione di servizi di pagamento e all'emissione e distribuzione di moneta elettronica; sono state inoltre introdotte modifiche volte ad accrescere il contenuto informativo dei dati inviati all'Unità⁷³⁰.

Per garantire la qualità dei dati S.A.R.A. e nel contempo contribuire a far emergere eventuali anomalie non individuate dagli operatori la UIF impiega un sistema automatico di controlli statistici che si attiva mensilmente e che permette di individuare circa 25 mila dati aggregati potenzialmente anomali ogni anno. Le segnalazioni aggregate così individuate sono comunicate agli intermediari ai fini di una loro verifica.

Tra gli strumenti di pagamento censiti nei flussi S.A.R.A. il bonifico riveste un'importanza centrale ai fini del contrasto alla criminalità finanziaria. Il contenuto informativo delle segnalazioni S.A.R.A. riferite ai bonifici è, infatti, ampio, includendo anche informazioni riguardanti il comune o paese estero di residenza della controparte e del suo intermediario. Tale ricchezza informativa consente all'Unità di impiegare una serie di strumenti statistici con l'obiettivo di misurare il rischio di riciclaggio insito nei flussi di bonifici tra l'Italia e i suoi paesi controparte e identificare anomalie specifiche.

Uno degli strumenti più evoluti di cui l'Unità dispone in tale ambito è un modello econometrico che permette di identificare la presenza di flussi potenzialmente illeciti a livello di comune, banca ricevente e paese estero di provenienza, attraverso il confronto tra i flussi osservati e quelli attesi sulla base dei "fondamentali" economici, finanziari e demografici dei comuni e dei paesi coinvolti. I flussi che hanno un volume significativamente superiore a quello previsto dal modello sono considerati anomali. Aggregando opportunamente le anomalie elementari per provincia di destinazione dei flussi, la metodologia consente, inoltre, di derivare indicatori territoriali di rischio di riciclaggio. L'aggregazione delle anomalie secondo il paese di provenienza permette, invece, di ottenere una classificazione di paesi a rischio di riciclaggio fondata su criteri quantitativi, che può affiancare la valutazione basata sul grado di conformità alle norme e agli standard internazionali.

⁷³⁰ Sono state introdotte nuove causali aggregate per la rilevazione delle rimesse di denaro e nuovi settori sintetici per la classificazione della clientela; sono invece state escluse dall'aggregazione, tra l'altro, le operazioni poste in essere con clientela costituita da banche e intermediari finanziari al ricorrere di determinate circostanze.

L'Unità dispone anche di una procedura statistica volta a monitorare semestralmente la dinamica macroeconomica dei flussi di bonifici tra l'Italia e ciascun singolo paese controparte. In particolare, la procedura permette di identificare due tipologie di fenomeni: una marcata e prolungata accelerazione (o decelerazione) dei flussi aggregati, oppure un repentino spostamento verso l'alto (o verso il basso) nei loro livelli. L'identificazione di tali discontinuità possono essere oggetto di interesse da parte dell'Unità in quanto potenzialmente connesse a fattori di rischio riferibili ad attività di riciclaggio internazionale.

All'interno dei dati S.A.R.A., le operazioni realizzate in contanti costituiscono, assieme ai bonifici, una delle informazioni più significative in un'ottica di prevenzione del riciclaggio, come emerge anche dall'ingente numero di SOS relative all'utilizzo di tale strumento. Nei flussi S.A.R.A. è riportato, oltre all'ammontare dei prelievi e dei versamenti di contante su conti correnti, anche l'importo regolato in contanti nelle altre tipologie di transazioni (quali compravendita di titoli ed emissione di certificati di deposito).

Le differenze territoriali nell'uso del contante in Italia sono riconducibili in gran parte a discrepanze strutturali del contesto socio-economico di riferimento e nella disponibilità e funzionalità dei servizi finanziari. D'altra parte, un ricorso significativo al contante non spiegabile da tali fattori socio-economici può essere indicativo di condotte illecite. A tale riguardo, l'UIF dispone di un modello econometrico⁷³¹ che, analogamente a quello dei bonifici internazionali, consente di stimare, a livello di singola banca in ciascun comune, la componente anomala della propensione all'uso di contante, che è quindi potenzialmente riconducibile a proventi di attività illecite. Aggregando i risultati è possibile derivare indicatori di rischio per singolo intermediario, oltre ad indicatori a livello comunale e provinciale.

Per lo svolgimento dei compiti di analisi strategica, la UIF impiega in modo estensivo anche dati di fonte esterna all'Unità. Un esempio rilevante è l'impiego dei dati dei bilanci delle imprese di fonte Cerved per la costruzione di un indicatore di rischio di infiltrazione mafiosa: a partire da una lista di imprese confiscate alla criminalità organizzata o i cui soci o amministratori risultano indagati per reati di criminalità organizzata, l'Unità ha impiegato tecniche di *Machine Learning* per sviluppare un algoritmo di apprendimento supervisionato, che, applicato all'universo delle imprese attive ad una certa data, consente di misurare il grado di rischio di infiltrazione mafiosa per ciascuna società di cui si dispone di dati di bilancio affidabili. Tale indicatore può essere impiegato – in modo complementare agli strumenti già in uso presso la UIF – nell'ambito dell'analisi operativa delle SOS, in analisi a carattere strategico come indicatore di rischio aggregato (geografico e settoriale), contribuendo a definire l'esposizione degli intermediari finanziari nei confronti di società a più elevato rischio di infiltrazione criminale.

L'UIF dispone anche di un modello econometrico per l'individuazione delle anomalie potenzialmente connesse al trasferimento all'estero di fondi di natura illecita sulla base delle statistiche bilaterali del commercio estero dell'Italia. La metodologia sviluppata⁷³² consente di individuare possibili irregolarità di natura dichiarativa e contabile (come la falsa dichiarazione del valore dei flussi commerciali o della residenza della controparte commerciale) riconducibili al fenomeno del cosiddetto *trade-based money laundering* (TBML). Sulla base dei risultati del modello è possibile stilare le graduatorie dei paesi partner commerciali dell'Italia e dei settori merceologici con valori di rischio statisticamente significativi.

Nel quadro della collaborazione tra la UIF e la Vigilanza della Banca d'Italia, da alcuni anni nell'attività di controllo si fa uso, prevalentemente in sede di valutazione del rischio degli intermediari bancari, di un modello di analisi che impiega, nella sua componente quantitativa, un sistema di indicatori che sfruttano i dati S.A.R.A. e le Segnalazioni creditizie e finanziarie.

Nel corso del 2020 è stata portata a termine la prima fase di definizione di un sistema di indicatori anche per alcune categorie di intermediari finanziari non bancari. L'approccio di calcolo degli indicatori adottato per questa tipologia di intermediari è quello della logica fuzzy, una tecnica mutuata dall'intelligenza artificiale, che comporta una serie di vantaggi quali una maggiore attendibilità dei risultati in presenza di dati imprecisi e incompleti, la possibilità di incorporare conoscenze aprioristiche o informazioni qualitative nel processo di definizione degli indicatori, e una più facile comprensione da parte

⁷³¹ G. Ardizzi, P. De Franceschi e M. Giammatteo, *Cash payment anomalies: An econometric analysis of Italian municipalities*, International Review of Law and Economics, 2018, 56, pp. 105-121; M. Giammatteo, *Cash use and money laundering: An application to Italian data at bank-municipality level*, UIF, Quaderni dell'antiriciclaggio, Analisi e studi, 2019, n. 13.

⁷³² M. Gara, M. Giammatteo e E. Tosti, *Magic mirror in my hand ... How trade mirror statistics can help us detect illegal financial flows*, The World Economy, 2019, 42 (11), pp. 3120-3147.

degli utenti finali delle regole di calcolo degli indicatori, facilitandone anche il coinvolgimento nella costruzione e manutenzione delle applicazioni.

Nell'ambito dell'analisi strategica, la UIF sviluppa anche attività di studio tese a migliorare la comprensione delle dinamiche associate alla criminalità finanziaria e verificare ipotesi di ricerca. In tale contesto si annoverano due recenti studi, entrambi sviluppati in collaborazione con il Dipartimento di Economia e statistica della Banca d'Italia.

Il primo⁷³³, utilizzando i dati sul numero di SOS ricevute dall'Unità, i dati SARA sull'operatività finanziaria degli intermediari bancari, nonché le informazioni sugli accessi ispettivi antiriciclaggio condotti dalla Vigilanza della Banca d'Italia e dalla UIF e sui relativi esiti, intende verificare empiricamente l'effetto sull'attività segnalatica delle banche derivante dall'attività ispettiva delle Autorità antiriciclaggio; l'analisi dimostra che le ispezioni inducono un aumento del numero di SOS e della probabilità che un'operazione sospetta sia segnalata. Il secondo studio⁷³⁴ propone una stima dell'effetto dell'utilizzo di contante sulla dimensione dell'economia sommersa; in particolare, impiegando dati provenienti da molteplici fonti, tra cui, in particolare, i dati S.A.R.A., per i prelievi e depositi di contante presso gli sportelli bancari, e le stime dell'economia sommersa limitatamente alla sotto-dichiarazione del fatturato da parte delle imprese, fornite dall'Istat, lo studio offre una robusta evidenza empirica in merito all'esistenza di un nesso di causalità tra l'impiego di contante e la scala delle attività economiche irregolari.

3. Limitazioni all'uso del contante, degli assegni e di altri valori (A. Baldassarre)

3.1. Il quadro sovranazionale

Sebbene il contante sia unanimemente considerato uno degli strumenti principali per il riciclaggio di capitali ed il finanziamento del terrorismo, nella disciplina sovranazionale manca un limite generalizzato all'utilizzo del contante analogo a quello previsto, a livello interno, dall'art. 49 del D.lgs. 231/2007. Nelle Raccomandazioni del GAFI, che rappresentano l'indiscusso standard internazionale nella lotta al riciclaggio ed al finanziamento del terrorismo, il contante viene preso in considerazione solo quale fattore di rischio in relazione al quale si chiede agli Stati l'adozione di misure di controllo aggiuntive⁷³⁵. In buona sostanza, il contante è considerato un campanello di allarme che deve mettere in allerta gli operatori, ma l'approccio seguito dagli standard internazionali non contempla alcun tipo di proibizione dell'uso del contante oltre una certa soglia.

Anche la normativa europea, pur riconoscendo l'elevato rischio di riciclaggio e di finanziamento del terrorismo associato ai pagamenti in contanti di importo elevato⁷³⁶, non ne preclude l'utilizzo a condizione che, nel caso di pagamenti in contanti per importi pari o superiori a 10.000 euro, siano osservati gli obblighi di adeguata verifica, registrazione e segnalazione delle operazioni sospette previsti dalla medesima direttiva⁷³⁷. Resta comunque salva la possibilità che gli Stati membri adottino misure più rigorose di controllo dell'uso del contante quali, ad esempio, l'adozione di "*soglie più basse*" rispetto a quella sopra indicata ovvero "*limitazioni supplementari di ordine generale*"⁷³⁸.

⁷³³ M. Gara, F. Manaresi, D.J. Marchetti e M. Marinucci, *The impact of anti-money laundering oversight on banks' suspicious transaction reporting: Evidence from Italy*, UIF, Quaderni dell'Antiriciclaggio, Analisi e studi n. 12.

⁷³⁴ M. Giammatteo, S. Iezzi e R. Zizza, *Pecunia olet. Cash usage and the underground economy*, in Questioni di Economia e Finanza, 2021, n. 649, Banca d'Italia.

⁷³⁵ La nota interpretativa alla raccomandazione n. 10 suggerisce di sottoporre a misure rafforzate di *customer due diligence* gli operatori che movimentano elevate quantità di denaro contante (settori c.d. cash intensive). Le raccomandazioni n. 22 e n. 23 prevedono che gli operatori che commerciano in metalli e pietre preziosi siano assoggettati agli obblighi antiriciclaggio qualora ricevano pagamenti in contante oltre la soglia di 15.000 USD/EUR. La medesima soglia viene presa in considerazione nella raccomandazione n. 32 quale limite oltre il quale gli Stati sono obbligati a prevedere un obbligo di dichiarazione o di denuncia dei trasporti transfrontalieri di danaro contante.

⁷³⁶ Cfr. considerando n. 6 della quarta direttiva antiriciclaggio.

⁷³⁷ L'art. 2, par. 1, n. 3, lett. e) della direttiva 2015/849/UE include nel perimetro degli obblighi previsti dalla direttiva tutti gli operatori economici che, a prescindere dall'attività esercitata, accettano pagamenti in contanti di importo pari o superiore a 10.000 euro, sia nel caso in cui il pagamento avvenga in un'unica soluzione, sia laddove lo stesso sia effettuato mediante una pluralità di operazioni fra loro collegate.

⁷³⁸ Cfr. sempre considerando n. 6 della direttiva 2015/849/UE. In mancanza di norme di armonizzazione minima sull'uso del contante, solo alcuni Stati membri hanno introdotto limiti massimi all'uso del contante, adottando peraltro soglie non omogenee. Queste asimmetrie, per un verso, incentivano comportamenti opportunistici, e per altro verso, non aiutano nemmeno i cittadini e le imprese,

A quest'ultimo proposito occorre tenere presente che, per gli Stati membri che adottano la moneta unica, la possibilità di introdurre limitazioni all'uso del contante trova un limite nella competenza esclusiva attribuita all'Unione europea riguardo alla politica monetaria. Ciò in quanto, nella complessa architettura costituzionale dell'Unione, ogni misura che tenda a circoscrivere l'uso del contante è il frutto del bilanciamento delle competenze proprie dell'Unione e di quelle spettanti agli Stati membri.

L'emissione e la disciplina del corso legale delle banconote e monete in euro rientrano nell'ambito della competenza esclusiva del diritto dell'Unione⁷³⁹, ragion per cui agli Stati membri è preclusa la possibilità di incidere, attraverso il diritto interno, sulla disciplina del corso legale dell'euro, e ciò anche in caso di inerzia del legislatore dell'Unione. Cionondimeno il considerando n. 19 del regolamento (CE) n. 974/98, relativo all'introduzione dell'euro, tempera la rigidità della predetta competenza esclusiva dell'Unione, prevedendo che *“le eventuali limitazioni di pagamento in banconote o monete metalliche, decise dagli Stati membri per motivi d'interesse pubblico, non sono incompatibili con il corso legale delle banconote e delle monete metalliche in euro, a condizione che esistano altri mezzi legali di estinzione dei debiti pecuniari”*⁷⁴⁰.

3.2. Le limitazioni all'uso del contante nella normativa nazionale

Nel nostro Paese le limitazioni all'uso del contante sono state originariamente introdotte dall'art. 1 del DL n. 143/1991, da cui poi sono transitate, mantenendo l'impostazione di base, nell'attuale art. 49 del D.lgs. 231/2007. Il comma 1 di quest'ultima disposizione vieta *“il trasferimento di denaro contante e di titoli al portatore in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, siano esse persone fisiche o giuridiche, quando il valore oggetto di trasferimento, è complessivamente pari o superiore a 3.000 euro”*. Il comma 3-bis però modifica la predetta soglia, stabilendo che *“A decorrere dal 1° luglio 2020 e fino al 31 dicembre 2022, il divieto di cui al comma 1 e la soglia di cui al comma 3 sono riferiti alla cifra di 2.000 euro. A decorrere dal 1° gennaio 2023, il predetto divieto di cui al comma 1 è riferito alla cifra di 5.000 euro”*⁷⁴¹.

Il divieto colpisce il *“trasferimento”* di denaro⁷⁴² o titoli al portatore⁷⁴³, ragion per cui la violazione si concretizza solo allorquando si verifichi una *traditio* tra due *“soggetti diversi”*, come precisa poco oltre la stessa disposizione, indipendentemente dal fatto che si tratti di persone fisiche o giuridiche. Non incorre nella violazione chi effettua un prelevamento in banca o presso sportelli bancomat di importo superiore alla soglia di legge, atteso che il successivo comma 13 prevede espressamente che il divieto non si applica ai trasferimenti di denaro o titoli al portatore in cui siano parte le banche, le Poste Italiane o gli istituti di

chiamati a districarsi fra le diverse discipline nazionali: v. *Commission Staff Working Document, Impact Assessment Accompanying the Anti-money laundering package, SWD(2021) 190 final*, che fornisce una fotografia aggiornata delle limitazioni all'uso del contante esistenti all'interno dell'Unione. Fra gli Stati membri solo 19, fra cui l'Italia, hanno introdotto limiti all'uso del contante, che spaziano dalla soglia di appena 500 euro prevista dalla Grecia ai 10.300 della Repubblica Ceca. La maggioranza degli Stati membri che prevedono limiti al contante (10 su 19) hanno adottato soglie inferiori ai 4.000 euro.

⁷³⁹ L'art. 128, par. 1, TFUE prevede: «La Banca centrale europea ha il diritto esclusivo di autorizzare l'emissione di banconote in euro all'interno dell'Unione. La Banca centrale europea e le banche centrali nazionali possono emettere banconote. Le banconote emesse dalla Banca centrale europea e dalle banche centrali nazionali costituiscono le uniche banconote aventi corso legale nell'Unione». Analoga è la previsione contenuta nell'art. 16, primo comma, del Protocollo n. 4 sullo Statuto del Sistema europeo di banche centrali e della Banca centrale europea.

⁷⁴⁰ La Corte di giustizia nella sentenza *Hessischer Rundfunk* ha ritenuto legittime le restrizioni ai pagamenti in contante in euro se le stesse rispondono a “motivi d'interesse pubblico”, dovendosi ricomprendersi sotto tale nozione sia le restrizioni giustificate da motivi di ordine pubblico relativi alla sicurezza o alla lotta contro la criminalità, sia quelle riconducibili a interessi pubblici di diversa natura (nel caso esaminato quello di assicurare una più efficace organizzazione dei pagamenti da parte della pubblica amministrazione), v. sentenza della Corte (Grande Sezione) del 26 gennaio 2021, cause riunite C-422/19 e C-423/19, *Hessischer Rundfunk*, ECLI:EU:C:2021:63.

⁷⁴¹ Il comma in esame è stato aggiunto dall'art. 18, comma 1, lett. a), del DL 26 ottobre 2019, n. 124, convertito con modificazioni dalla legge 19 dicembre 2019, n. 157 e successivamente modificato dall'art. 5-*quater*, comma 1, del DL 21 ottobre 2021, n. 146, convertito, con modificazioni, dalla legge 17 dicembre 2021, n. 215, dall'art. 3, comma 6-*septies*, del DL 30 dicembre 2021, n. 228, convertito con modificazioni dalla legge 25 febbraio 2022, n. 15 e, da ultimo, nuovamente modificato dall'art. 1, comma 384, lett. b), della legge 29 dicembre 2022, n. 197 (legge di bilancio 2023).

⁷⁴² L'art. 1, comma 2, lett. o), del D.lgs. 231/2007 fa ricadere nella definizione di “contante” le banconote e le monete metalliche, in euro o in valute estere, aventi corso legale.

⁷⁴³ Nelle definizioni dell'art. 1 del D.lgs. 231/2007 non è più contemplata quella relativa ai titoli al portatore originariamente prevista dall'art. 1, comma 2, lett. v), che definiva il “titolo al portatore” come il titolo di credito che legittima il possessore all'esercizio del diritto in esso menzionato in base alla mera presentazione e il cui trasferimento si opera con la consegna del titolo.

moneta elettronica. Parimenti sono esentati dal divieto, sempre in base al comma 13, i trasferimenti effettuati dai predetti soggetti vigilati allorché gli stessi operano fra loro direttamente o per mezzo di vettori specializzati nell'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate⁷⁴⁴.

Di contro, l'affidare somme liquide oltre la soglia di legge ad un terzo che le percepisce quale mero depositario è un atto dispositivo sufficiente a concretizzare la violazione del divieto in esame, a nulla rilevando che il depositario non abbia la disponibilità finale delle somme⁷⁴⁵. Nessuna valenza scriminante può essere attribuita alla circostanza che le dazioni di denaro contante siano state annotate nelle scritture contabili ovvero che avvengano in base a consuetudini commerciali tra imprese gestite da società del medesimo gruppo, posto che il divieto colpisce qualunque trasferimento effettuato tra soggetti dotati di distinta personalità giuridica ed autonomia patrimoniale⁷⁴⁶.

È inoltre irrilevante la finalità sottostante al trasferimento, come ben si evince dalla dizione “*a qualsiasi titolo*”, ragion per cui nessun rilievo assume, ad esempio, la provenienza lecita o illecita delle somme trasferite. La giurisprudenza ha chiarito che la disciplina in esame ha un carattere general-preventivo, in quanto mira a predisporre una difesa avanzata in relazione a rilevanti movimentazioni in contanti, le quali, per la spiccata attitudine ad eludere la tracciabilità dei passaggi, si prestano ad una molteplicità di fini illeciti; cionondimeno l'eventuale fine illecito perseguito non è elemento costitutivo della violazione, ma può semmai essere motivo di ulteriori illeciti, a seconda dei casi, di natura amministrativa, tributaria o penale⁷⁴⁷.

Il divieto non è circoscritto al solo contante espresso nella valuta dell'euro, ma abbraccia anche le valute diverse, in relazione alle quali occorrerà calcolare il controvalore della soglia, ed i titoli al portatore, anche in questo caso sia in euro che in valuta estera.

Allo scopo di evitare il facile aggiramento della disposizione, il comma 1 dell'art. 49 estende il divieto anche ai trasferimenti che appaiono artificiosamente frazionati ricorrendo ad una molteplicità di versamenti singolarmente inferiori alla soglia. Per stabilire se ricorra o meno la violazione occorre rifarsi all'art. 1, comma 2, lett. v), del D.lgs. 231/2007, che individua due indici del frazionamento, uno di natura “temporale”, dovendosi presumere come frazionate le operazioni effettuate in momenti diversi ed in un circoscritto periodo di tempo fissato in sette giorni, l'altro di natura “oggettiva”, che valorizza, anche al di fuori del predetto lasso temporale, il valore dell'intera operazione economica alla quale i singoli trasferimenti sono funzionali⁷⁴⁸.

L'aspetto più critico e al tempo stesso più controverso della disposizione in esame è rappresentato dal tetto all'uso del contante, che è stato oggetto di continui ripensamenti da parte del legislatore negli oltre venti anni trascorsi dalla sua introduzione⁷⁴⁹. Il percorso di progressivo abbassamento del tetto

⁷⁴⁴ Appare erroneo il richiamo contenuto nel comma 13 all'art. 3, comma 5, lett. e) atteso che i “vettori specializzati” di cui parla la disposizione sono annoverati nella successiva lett. f).

⁷⁴⁵ Cassazione civile, sez. II, 23 gennaio 2017, n. 1645.

⁷⁴⁶ Cassazione civile, sez. II, 21 gennaio 2016, n. 1080.

⁷⁴⁷ Cassazione civile sez. VI, 26 aprile 2018, n. 10147.

⁷⁴⁸ Cassazione civile sez. II, 23/06/2021, n. 1797. Si veda anche Tribunale Bari sez. III, 9 maggio 2018, n.1998 secondo cui con la nozione di trasferimento si intende non solo l'effettuazione di un determinato atto, ma l'insieme di tutti gli atti che siano tra loro funzionalmente ed economicamente collegati per realizzare una unica operazione di movimentazione di valuta.

⁷⁴⁹ La soglia era stata inizialmente fissata in lire 20.000.000 dall'art. 1, comma 1, DL 3 maggio 1991, n. 143, poi convertita in 10.329,14 a seguito dell'introduzione dell'euro. Successivamente l'importo era stato elevato a euro 12.500 con decreto 17 ottobre 2002 del Ministro dell'Economia e delle finanze. In occasione del recepimento della c.d. terza direttiva antiriciclaggio l'importo era stato ridotto a euro 5.000 dall'originario art. 49, comma 1, del D.lgs. 231/2007, ma la riduzione ha avuto vita brevissima, in quanto l'art. 32, comma 1, DL n. 112/2008 ha riportato la soglia a euro 12.500. È poi iniziato un periodo di graduale riduzione della soglia portata a euro 5.000 dall'art. 20, comma 1, del DL n. 78/2010, poi a euro 2.500 dall'art. 2, comma 4, del DL n. 138/2011 ed infine a euro 1.000 dall'art. 12, comma 1, del DL n. 201/2011. L'importo è tornato a salire con l'art. 1, comma 898, Legge n. 208/2015 (c.d. Legge di stabilità 2016) che ha riportato la soglia a 3.000 euro, per poi scendere nuovamente a euro 2.000 ai sensi del comma 3-bis, dell'art. 49, D.lgs. 231/2007, aggiunto dall'art. 18, comma 1, lett. a), del DL 26 ottobre 2019, n. 124. Non si è mai concretizzata l'ulteriore riduzione della soglia a 1.000 euro inizialmente prevista per l'1.1.2022 e poi fatta slittare all'1.1.2023 dall'art. 3, comma 6-septies, del DL 30 dicembre 2021, n. 228, convertito con modificazioni dalla Legge 25 febbraio 2022, n. 15.

all'uso del contante, avviato a partire dal 2018 si è interrotto con l'approvazione della legge di bilancio per il 2023 che, invertendo la tendenza in atto, ha riformulato il comma 3-*bis* prevedendo l'innalzamento del limite a 5.000 euro a partire dall'1° gennaio 2023⁷⁵⁰. Sarebbe auspicabile mettere fine all'altalena che ha finora connotato la disposizione in esame identificando un importo stabile nel tempo, che risulti efficace nell'azione di contrasto all'economia sommersa senza essere penalizzante per il nostro sistema economico⁷⁵¹. Solo dando stabilità alla soglia il limite all'uso del contante può risultare credibile e, quindi, efficace nella lotta alla criminalità ed al sommerso.

Ad accrescere la complessità del divieto contribuisce anche la previsione di soglie specifiche per talune attività, quale quella di 1.000 euro prevista per il servizio di rimesse di denaro (c.d. *money transfer*, v. art. 49, comma 2) e quella di 3.000 euro per i cambiavalute (comma 3). Ulteriori eccezioni sono state introdotte al fine di incentivare il turismo straniero, dal momento che gli operatori del settore del commercio al minuto e le agenzie di viaggio e turismo possono accettare pagamenti in contanti fino alla soglia di 15.000 euro dagli stranieri non residenti in Italia per la vendita di beni e l'erogazione di servizi legati al turismo, rispettando talune specifiche condizioni⁷⁵².

Sempre in tema di eccezioni al divieto, va segnalato che sono consentiti i trasferimenti di certificati rappresentativi di quote in cui siano parte le banche, le Poste Italiane, le SIM, le SGR, le SICAV, le SICAF e le imprese di assicurazione che operano in Italia nei rami vita, in quanto si tratta di trasferimenti che avvengono con l'intermediazione di un soggetto sottoposto all'osservanza dei presidi antiriciclaggio (art. 49, comma 14).

Il divieto non riguarda i pagamenti dello Stato e degli altri enti pubblici, né le erogazioni disposte dai predetti soggetti pubblici che restano regolati dalle rispettive disposizioni di settore. Sono altresì sottratti al divieto i pagamenti a mani dell'ufficiale giudiziario ai sensi dell'art. 494 c.p.c. che possono essere effettuati in contanti anche al di sopra della soglia di legge (art. 49, comma 15).

3.3. L'obbligo di utilizzare strumenti "tracciabili" per i trasferimenti soprasoglia

I trasferimenti di denaro o di titoli il cui valore eccede le soglie sopra indicate devono necessariamente essere effettuati avvalendosi di forme di pagamento "tracciabili". L'art. 49, comma 1, del D.lgs. 231/2007 prevede, infatti, l'obbligo di canalizzare le operazioni soprasoglia attraverso le banche, le Poste italiane, gli istituti di moneta elettronica e istituti di pagamento⁷⁵³.

L'obbligo di canalizzazione dei trasferimenti di denaro contante soprasoglia attraverso il sistema bancario e finanziario pone seri problemi di inclusione finanziaria in relazione a coloro che non hanno accesso a strumenti di pagamento tracciabili, essendo noto che una fascia purtroppo ancora ampia di popolazione non possiede un conto corrente o un conto di pagamento.

In relazione a queste situazioni, il legislatore italiano, già con la prima legge antiriciclaggio del 1991⁷⁵⁴ si è preoccupato di prevedere un meccanismo alternativo che consentisse di tracciare il trasferimento del contante soprasoglia, canalizzandolo attraverso quelli che all'epoca erano definiti "intermediari abilitati". La procedura, fatte salve le modifiche di carattere definitorio, è transitata, senza variazioni sostanziali, nel comma 1 dell'art. 49 del D.lgs. 231/2007 che al riguardo prevede che il trasferimento di contante soprasoglia possa essere effettuato per il tramite degli intermediari bancari e finanziari "*mediante disposizione accettata per iscritto dagli stessi, previa consegna ai medesimi intermediari della somma in contanti*". La somma trasferita diviene disponibile per il beneficiario "*a decorrere dal terzo giorno lavorativo successivo a quello dell'accettazione ... nella provincia del proprio domicilio*."

⁷⁵⁰ Cfr. art. 1, comma 384, lett. b, della legge 29 dicembre 2022, n. 197 (legge di bilancio 2023). Peraltro non si comprende perché il legislatore abbia lasciato invariato il comma 1 della disposizione in esame che continua a prevedere la soglia di 3.000 euro derogata dal successivo comma 3-*bis* che prevede il nuovo importo di 5.000 euro applicabile a partire dall'1.1.2023.

⁷⁵¹ Un recente studio della Banca d'Italia ha messo in luce che l'innalzamento del tetto del contante da 1.000 a 3.000 euro deciso dal legislatore a partire dal 2016 e motivato dall'esigenza di rilancio della spesa, ha avuto come effetto collaterale quello di incrementare l'economia sommersa, v. M. Giammatteo, S. Iezzi e R. Zizza, *Pecunia olet. Cash usage and the underground economy*, cit., pubblicato in *Journal of Economic Behavior & Organization*, vol. 204, December 2022, pp. 107-127.

⁷⁵² Cfr. art. 3 del DL 2 marzo 2012, n. 16, convertito, con modificazioni, dalla legge 26 aprile 2012, n. 44, e successive modificazioni.

⁷⁵³ Occorre fare attenzione però al servizio di rimessa di denaro al quale, anche se effettuato da istituti di pagamento, si applica comunque la già ricordata soglia di 1.000 euro.

⁷⁵⁴ Cfr. art. 1, comma 1-*bis*, del DL 3 maggio 1991, n. 143 conv. dalla l. 5 luglio 1991, n. 197.

La disposizione in esame si occupa di regolare anche gli effetti civilistici del meccanismo di trasferimento prevenendo che *“la comunicazione da parte del debitore al creditore della predetta accettazione produce gli effetti di cui all’articolo 1277, primo comma, del codice civile e, nei casi di mora del creditore, gli effetti di cui all’articolo 1210 del medesimo codice”*.

Al di là della farraginosità della procedura, la disposizione in esame non chiarisce se l’intermediario bancario o finanziario che effettua la procedura di trasferimento abbia diritto o meno a percepire un compenso per l’attività prestata e, eventualmente, quali siano i costi ed in che modo gli stessi debbano essere resi noti agli utenti. Il tema è piuttosto delicato in quanto la procedura, ideata come si è detto oltre venti anni fa con la prima legge antiriciclaggio, oggi viene a ricadere nel perimetro di applicazione della direttiva 2015/2366/UE configurando un vero e proprio servizio di rimessa di denaro⁷⁵⁵. Il che rende la disposizione in esame di dubbia compatibilità con l’assetto delineato dalla stessa direttiva 2015/2366/UE, dal momento che la disponibilità di fondi dal terzo giorno successivo non è in linea con la regola generale che impone al prestatore di servizi di pagamento di mettere a disposizione del beneficiario i fondi oggetto del trasferimento entro la fine della giornata successiva a quella in cui detti fondi sono stati versati⁷⁵⁶. Ma ciò che più preoccupa è che, inquadrando il meccanismo dell’art. 49 nello schema del servizio di rimessa di denaro, si viene presumibilmente a far gravare sull’utente un costo per il trasferimento che non verrebbe sostenuto in caso di utilizzo del contante, atteso che il citato art. 49 non prevede la gratuità del servizio.

3.4. Limiti all’utilizzo degli assegni, dei vaglia postali e cambiari e dei libretti di deposito

La disposizione in esame prevede, inoltre, talune specifiche disposizioni in tema di assegni, vaglia postali e cambiari, libretti di deposito e certificati rappresentativi di quote che mirano ad impedire che i predetti titoli, circolando quali strumenti al portatore, possano essere utilizzati quale surrogato del danaro contante.

Più specificamente, il comma 5 dell’art. 49 prevede che tutti gli assegni bancari o postali di importo pari o superiore 1.000 euro debbano essere emessi con la clausola “non trasferibile” e, nel contempo, debbano indicare il nome o la ragione sociale del beneficiario. Per rafforzare il divieto il comma 4 prevede che i moduli degli assegni bancari e postali sono rilasciati dalle banche e da Poste Italiane con prestampata la clausola di non trasferibilità, salva la possibilità del cliente di chiedere per iscritto il rilascio di moduli di assegni bancari e postali in forma libera, per i quali il richiedente è tenuto a corrispondere, a titolo di imposta di bollo, la somma di 1,50 euro per ciascun modulo (comma 10). In quest’ultimo caso, sarà onere del traente apporre la clausola di non trasferibilità sugli assegni emessi per importi pari o superiori alla soglia di legge. La circolazione degli assegni mediante girata viene pertanto ristretta agli assegni di importo inferiore alla soglia di 1.000 euro.

Sempre allo scopo di evitare che l’assegno possa essere utilizzato per aggirare il limite all’utilizzo del contante, il comma 6 dell’art. 49 prevede che gli assegni emessi all’ordine dell’emittente (vale a dire quelli che riportano le diciture “a me medesimo”, “m.m.”, “a me stesso”, etc.) possono essere girati unicamente per l’incasso a una banca o a Poste Italiane, venendo in tal modo preclusa qualsiasi possibilità che detti assegni possano circolare mediante girata a terzi, a prescindere dal loro importo.

Le stesse regole valgono anche per gli assegni circolari, i vaglia postali e cambiari in base al successivo comma 7, di modo che questi ultimi possono essere richiesti dal cliente in forma libera solo se di importo inferiore a 1.000 euro, corrispondendo per ciascun assegno o vaglia l’imposta di bollo di 1,50 euro. Per importi pari o superiori a 1.000 euro detti titoli possono essere emessi solo con la clausola di non trasferibilità e l’indicazione del nominativo o della ragione sociale del beneficiario. Nel caso in cui l’assegno circolare, il vaglia postale o cambiario non venga più negoziato, il cliente può ottenere il rimborso della provvista solo previa restituzione del titolo all’emittente (comma 9).

Allo scopo di scoraggiare ulteriormente l’uso di assegni e vaglia in forma libera, il comma 11 dell’art. 49 prevede che i soggetti autorizzati ad accedere all’anagrafe dei conti (fra cui Guardia di finanza, l’Agenzia delle entrate, la Direzione Investigativa Antimafia, l’Autorità giudiziaria, l’Unità di informazione finanziaria per l’Italia) possono chiedere alle banche e alle Poste italiane i dati identificativi e il codice fiscale dei soggetti ai quali siano stati rilasciati moduli di assegni bancari o postali in forma libera ovvero

⁷⁵⁵ Sul punto v. S. Vanini, *I nuovi limiti all’utilizzazione del denaro contante previsti dalla normativa antiriciclaggio e la disciplina sui servizi di pagamento*, in *Le Nuove Leggi Civili Commentate*, n. 6, 2020, p. 1317.

⁷⁵⁶ Cfr. artt. 78, par. 1, 83, par. 1, e 84 della direttiva 2015/2366/UE e artt. 20 e 21 del D.lgs. 11/2010.

che abbiano richiesto assegni circolari o vaglia postali o cambiari in forma libera nonché di coloro che li abbiano presentati all'incasso.

Il comma 12 della disposizione in esame vieta, infine, l'emissione di libretti di deposito, bancari o postali al portatore, in passato largamente utilizzati quale forma alternativa al trasferimento del contante. Detti libretti possono essere oggi emessi solo in forma nominativa, mentre per quelli al portatore già in circolazione il termine per la loro estinzione è scaduto il 31 dicembre 2018.

3.5. Prospettive di riforma

A fronte delle plurime modifiche intervenute nel tempo, è lecito domandarsi quale sia oggi la finalità perseguita dalla disposizione in esame, se essa assolva solo alla funzione di contrasto del riciclaggio che ne aveva giustificato l'introduzione, ovvero se abbia progressivamente acquisito ulteriori finalità, andando a rispondere anche ad esigenze diverse, quali *in primis* quella di contrasto dell'evasione fiscale. Tra gli elementi che militano a favore di questa seconda opzione figura innanzitutto il tetto di 5.000 euro che, seppure più alto rispetto al passato, resta distante dalle soglie previste dalla vigente normativa europea in materia antiriciclaggio ed antiterrorismo⁷⁵⁷, legittimando così la lettura secondo cui il divieto in esame assolve oltre che alla funzione di prevenzione del riciclaggio e del finanziamento del terrorismo, anche a quella di contrasto dell'economia sommersa, ossia di lotta all'evasione fiscale⁷⁵⁸.

Va però detto che la materia a livello europeo è in rapida evoluzione ed a breve sono attesi importanti cambiamenti. A luglio 2021 la Commissione europea ha approvato un pacchetto di proposte legislative che mirano a rafforzare la cooperazione in ambito europeo nel campo della lotta al riciclaggio ed al finanziamento del terrorismo. Nell'ambito di questo pacchetto è presente una proposta di regolamento sulla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio e di finanziamento del terrorismo⁷⁵⁹, nella quale è prevista l'armonizzazione a livello europeo della disciplina dei trasferimenti di denaro contante su cui, come si è detto, finora gli Stati membri si sono mossi in ordine sparso⁷⁶⁰.

L'art. 59 della proposta introduce un tetto massimo per i pagamenti in contanti valido per l'intero territorio dell'Unione, vietando il pagamento in contanti di beni e servizi per un valore superiore a 10.000 euro. La soglia è stata determinata in una misura ragionevolmente elevata, dovendosi tenere presente che la preoccupazione del legislatore è focalizzata essenzialmente sui pagamenti in contante di importo elevato, in relazione ai quali vengono ravvisati i maggiori elementi di vulnerabilità sotto il profilo antiriciclaggio e antiterrorismo. Al tempo stesso, prendendo atto della circostanza che alcuni Stati membri, come l'Italia, applicano soglie inferiori per il controllo del contante, la Commissione ha previsto la possibilità per gli Stati membri di mantenere le soglie esistenti o di ridurre il predetto importo.

La proposta circoscrive la predetta misura restrittiva ai soli pagamenti relativi alle cessioni di beni e servizi, quindi, in buona sostanza, ai pagamenti che vengono effettuati o ricevuti nell'ambito di attività commerciali svolte da operatori professionali. Sono invece espressamente esclusi dall'ambito di operatività del divieto i pagamenti che intervengono tra persone fisiche al di fuori di una specifica attività professionale⁷⁶¹. La proposta di regolamento non prevede, quindi, alcuna restrizione all'uso del contante laddove il trasferimento riguardi operazioni che siano effettuate al di fuori di una relazione professionale,

⁷⁵⁷ Si pensi ad esempio alla soglia di euro 10.000 prevista dall'art. 3 comma 5, lett. b), c) ed e), del D.lgs. 231/2007 ed a quella di 15.000 euro contemplata dall'art. 17, comma 1, lett. b), e dai successivi commi 5 e 6 del medesimo decreto.

⁷⁵⁸ Sono ormai numerose le opinioni che attribuiscono alle vigenti restrizioni all'uso del contante una finalità di ordine essenzialmente fiscale, v. G. Castaldi, *Limitazioni all'uso del contante: una normativa da riconsiderare*, in *Giurimetria*, n. 2/2015. In senso analogo si veda anche S. Capolupo, *Limite all'uso del contante, obbligo di tracciabilità e incentivi premiali*, in *Il fisco*, n. 43, 18 novembre 2019, p. 4115, il quale sottolinea come l'abbassamento delle soglie del contante sia coinciso temporalmente con tutta una serie di ulteriori misure finalizzate a disincentivare l'uso del contante da parte dei contribuenti, come nel caso delle lotterie nazionali finalizzate a premiare i pagamenti tracciabili ovvero l'introduzione dell'obbligo di accettazione di carte di pagamento da parte degli esercenti.

⁷⁵⁹ Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering, COM (2021) 420 final.

⁷⁶⁰ Il considerando n. 94 della proposta di regolamento sottolinea come i differenti approcci seguiti dagli Stati membri sul tema hanno determinato delle asimmetrie nel mercato interno a svantaggio degli operatori economici situati in Paesi con regimi più stringenti

⁷⁶¹ Cfr. art. 4, par. 4, lett. a) della proposta di regolamento.

in ciò differenziandosi dalla normativa italiana che vieta i trasferimenti a prescindere da ogni considerazione relativa alla natura del trasferimento (professionale o non professionale).

Si tratta di un aspetto su cui il legislatore italiano dovrà necessariamente compiere una riflessione. La proposta di regolamento, infatti, pur riconoscendo che possano esistere specificità nazionali che giustificano la conservazione o l'introduzione di soglie più basse rispetto a quella standard di 10.000 euro, sembra sottendere che tutte le restrizioni rientranti nel perimetro del regolamento stesso debbano essere ricondotte alle finalità di ordine pubblico associate al contrasto del riciclaggio di capitali illeciti e del finanziamento del terrorismo. Difficili da giustificare sembrerebbero, quindi, le restrizioni ulteriori contenute nella legislazione italiana nella parte in cui prevede l'estensione del divieto dell'uso del contante soprasoglia anche in relazione ai trasferimenti che avvengono per finalità diverse dal commercio di beni e servizi⁷⁶². Si tratta, infatti, di situazioni non coperte dalla proposta di regolamento e, forse, neppure facilmente giustificabili sotto il diverso interesse pubblico delle esigenze di contrasto del riciclaggio e dell'evasione fiscale⁷⁶³.

È assai probabile che l'adozione del regolamento europeo solleciterà una nuova riflessione sulla disposizione in esame, nella prospettiva di auspicata stabilità della norma a cui dovrebbe contribuire l'esigenza di armonizzazione manifestata dal legislatore europeo, che non a caso ha scelto lo strumento regolamentare per disciplinare i limiti ai pagamenti in contanti di importo elevato.

4. Le informative delle FIU estere (D. Bartolozzi)

La cooperazione internazionale costituisce una delle attività di principale importanza nell'ambito della prevenzione e del contrasto al riciclaggio del denaro sporco e al finanziamento del terrorismo, in considerazione del carattere essenzialmente transnazionale dei fenomeni criminali in questione, che richiedono scambi informativi rapidi ed efficaci fra Autorità di paesi diversi.

I principi che governano l'attività di cooperazione internazionale sono racchiusi nell'ultimo capitolo delle Raccomandazioni del GAFI (Raccomandazioni nn. 35-40) ed è su tale base che sono state redatte le norme delle Direttive europee e del decreto antiriciclaggio nazionale (D.lgs. 231/2007).

Tali principi, che ribadiscono la necessità per gli stati di aderire alle Convenzioni internazionali in materia e di darne efficace attuazione in concreto, si soffermano sui vari tipi di cooperazione internazionale, individuandone quattro forme principali: l'assistenza giudiziaria in materia di riciclaggio, delitti presupposto e finanziamento del terrorismo, quella relativa a sequestri e confische, quella relativa all'estradizione e, infine, le c.d. "altre forme di cooperazione internazionale", spesso identificate (a torto) come forme di "cooperazione informale" per distinguerle dalle precedenti che sono svolte in ambito giudiziario.

Rientrano in tale categoria residuale non solo la cooperazione fra *Financial Intelligence Units*, ma anche quella fra forze di polizia, fra Autorità di controllo dei flussi transfrontalieri di denaro contante e titoli assimilati, nonché fra Autorità di vigilanza degli operatori del settore finanziario e professionale, che sono assoggettati agli obblighi antiriciclaggio.

4.1. Le Raccomandazioni del GAFI sulla cooperazione internazionale

Il GAFI dedica l'ultima delle sue 40 raccomandazioni alle norme che devono regolare le c.d. "altre forme di cooperazione internazionale". In tale ambito, l'azione delle Autorità deve essere improntata a tre caratteristiche fondamentali: la rapidità, l'utilità e l'efficacia. I paesi sono tenuti a fornire tale

⁷⁶² Da parte di alcuni autori si sottolinea altresì la difficoltà dei controlli di trasferimenti di danaro contante che avvengano al di fuori di relazioni commerciali o professionali, v. ancora G. Castaldi, *op.cit.*, p. 39.

⁷⁶³ Eventuali scelte più rigorose, oltre la flessibilità prevista dalle disposizioni regolamentari, dovranno essere vagliate alla luce del principio di proporzionalità indicato dalla Corte di Giustizia nella sentenza *Hessischer Rundfunk* quale limite alla possibilità di prevedere limiti all'uso del contante.

cooperazione in tre specifici ambiti: il riciclaggio di denaro sporco, i delitti che ne costituiscono un presupposto e il finanziamento del terrorismo.

Va notato che le norme del GAFI disciplinano la materia della cooperazione internazionale esclusivamente in questi tre ambiti, e ciò nonostante il mandato del GAFI ricomprenda anche il contrasto del finanziamento della proliferazione delle armi di distruzione di massa. Il motivo di tale esclusione è da ricercarsi sia nella difficoltà di circoscrivere l'ambito della proliferazione (come dimostra il fatto che in molti casi il GAFI limita gli obblighi in materia alle sole misure di congelamento) sia nella mancanza di uno strumento cogente nel diritto internazionale, quali sono, appunto, le convenzioni internazionali sopra richiamate.

I caratteri e limiti della cooperazione internazionale sono stabiliti avendo presente l'esigenza principale che, come detto, è quella di facilitare gli scambi nella maniera più ampia possibile. Specifici obblighi sono, quindi, previsti in materia di rapidità e sicurezza: le Autorità devono adottare specifiche procedure operative in grado di individuare e trattare adeguatamente i casi urgenti (*prioritisation*), e impiegare sistemi e metodi finalizzati a salvaguardare la segretezza delle informazioni scambiate.

Per quanto attiene più specificamente agli scambi fra *Financial Intelligence Unit*, il GAFI adotta anche in tale ambito il principio di multidisciplinarietà delle FIU, richiedendo espressamente che tutti i poteri esercitabili a livello domestico debbano poter essere utilizzati anche per le esigenze delle controparti internazionali: discende da tale principio l'equiparazione fra segnalazioni di operazioni sospette (a livello domestico) e richieste di collaborazione (a livello internazionale). Sebbene tale principio fosse implicito già nelle precedenti raccomandazioni, le modifiche approvate nel 2012 hanno senz'altro contribuito a rafforzare l'equiparazione tra i casi domestici e quelli di fonte estera, assicurandone un trattamento paritario.

Sempre allo scopo di garantire una forma di assistenza più ampia ed efficace possibile, le raccomandazioni impongono ai paesi di non prevedere condizioni irragionevoli o eccessivamente restrittive per gli scambi.

In tal senso, come indicato nelle stesse Raccomandazioni e nelle relative Note interpretative, non è possibile rifiutare la collaborazione sulla base del fatto che la richiesta riguardi illeciti fiscali (il che è anche in linea con l'introduzione dei reati fiscali fra quelli presupposto di riciclaggio), né sulla base dell'esistenza di una tutela legale del segreto professionale (e in tal caso vale comunque l'eccezione per le professioni legali a tutela del diritto alla difesa). Sono anche vietate le limitazioni che fanno riferimento all'esistenza di un'indagine o un procedimento (e anche in tal caso è prevista un'eccezione qualora l'assistenza richiesta possa nuocere allo svolgimento degli accertamenti in corso) e i rifiuti opposti esclusivamente sulla base della diversa natura dell'Autorità richiedente rispetto a quella interpellata⁷⁶⁴.

L'assistenza può invece essere rifiutata quando l'Autorità richiedente non sia in grado di garantire un adeguato *livello* di sicurezza e confidenzialità alle informazioni scambiate.

Viene al riguardo precisato che gli scambi internazionali devono essere assistiti da adeguate regole di salvaguardia sulla sicurezza delle informazioni: tale salvaguardia si declina in due profili differenti, dei quali il primo tutela l'uso corretto delle informazioni, che possono essere utilizzate solo per le finalità per le quali sono state fornite, mentre il secondo tutela la segretezza delle informazioni scambiate. Gli scambi, infatti, devono avvenire per il tramite di canali sicuri ed *adeguatamente* protetti da accessi esterni, a tutela del buon andamento dell'analisi o dell'indagine in corso, e l'Autorità richiesta deve adottare almeno le stesse cautele che sono normalmente applicate nel trattamento delle informazioni domestiche (a conferma anche in tale caso dell'equiparazione fra segnalazioni domestiche e richieste internazionali).

Alcuni principi, infine, sono previsti specificamente in relazione al contenuto degli scambi informativi. La FIU richiedente è tenuta, infatti, *ex ante* a descrivere compiutamente il caso in analisi, indicando tutte le informazioni in proprio possesso, ivi comprese quelle sul collegamento con il paese richiesto⁷⁶⁵, ed *ex post* a fornire un *feedback* sull'utilità delle informazioni ricevute.

⁷⁶⁴ Si tratta, per esempio, del caso in cui una FIU amministrativa richieda informazioni a una FIU di polizia o viceversa: in entrambi i casi la natura dell'autorità è irrilevante dal momento che le FIU sono tenute a scambiarsi informazioni, a prescindere dalla loro organizzazione o caratteristiche interne.

⁷⁶⁵ Lo scopo, in tal caso, come espressamente previsto dai principi del gruppo Egmont, è quello di evitare richieste ingiustificate a tutte le FIU e concentrare invece gli scambi solo laddove si rendano veramente necessari e potenzialmente utili.

Per quanto riguarda la FIU ricevente, questa deve essere in grado di fornire alle proprie controparti tutte le informazioni cui ha normalmente accesso, diretto o indiretto, per le analisi domestiche, e di attivare i relativi poteri informativi.

Il contenuto delle raccomandazioni GAFI in materia di cooperazione internazionale è ampiamente ripreso e sviluppato nei principi adottati dal Gruppo Egmont (*Egmont Group of Financial Intelligence Units Principles for Information Exchange between Financial Intelligence Units*). Il rispetto di tali principi è obbligatorio per le FIU che aderiscono al Gruppo ed eventuali violazioni possono dare luogo all'attivazione di processi di *compliance* nei confronti della FIU che non li rispettano, con conseguenze che, a seconda dei casi, possono variare dall'adozione di un piano d'azione finalizzato all'introduzione di modifiche normative per la risoluzione delle lacune riscontrate, fino alla sospensione o radiazione dal Gruppo stesso.

4.2. La normativa europea

Le raccomandazioni GAFI, ivi comprese quelle in materia di cooperazione internazionale, sono alla base della direttiva europea relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (direttiva UE 2015/849). Rispetto ai principi già illustrati nel paragrafo precedente, vanno in questa sede messe in evidenza le peculiarità del sistema europeo che riguardano l'attività delle FIU.

Va fin da subito notato come la direttiva si occupa di disciplinare non solo i rapporti fra FIU e fra le FIU e le altre Autorità competenti, ma anche quelli fra le FIU e la Commissione europea.

Nelle more dell'introduzione delle nuove Autorità previste dal c.d. *AML Package*, la direttiva attribuisce alla Commissione un ruolo di assistenza a favore delle attività svolte dalle FIU, finalizzato non solo a favorire il coordinamento fra le FIU europee, ma anche e soprattutto ad agevolare lo scambio di informazioni. Lo strumento principale di cui si avvale la Commissione è la c.d. *Piattaforma delle FIU europee*, nata come gruppo informale di condivisione fra le FIU europee ed ora istituzionalizzata con la previsione di specifici compiti: la Piattaforma è infatti chiamata a svolgere la sua azione sia su temi di carattere generale (quali l'efficacia della cooperazione fra FIU), sia su aspetti di maggiore operatività, quali l'individuazione di operazioni sospette con carattere transfrontaliero, la standardizzazione dei formati delle segnalazioni oggetto di condivisione con altre FIU europee, l'analisi congiunta di casi di carattere transnazionale e l'identificazione di tendenze o fattori rilevanti per le valutazioni dei rischi di riciclaggio e di finanziamento del terrorismo. Il ruolo della Commissione in tali attività deve comunque intendersi limitato a quello di facilitatore, restando essa esclusa da ogni scambio di carattere operativo o avente ad oggetto l'esame di casi concreti.

Un ulteriore ruolo svolto dalla Commissione è quello relativo alla gestione dell'infrastruttura informatica FIU.net, utilizzata per gli scambi informativi fra FIU europee, a fianco dell'analoga rete mondiale gestita dal Gruppo Egmont; rispetto a quest'ultima, la rete Fiu.net prevede forme evolute di scambi, che consentono la condivisione in tempi rapidi di informazioni rilevanti aventi carattere transnazionale.

Di particolare rilievo è la norma che favorisce lo sviluppo di analisi congiunte, recependo a livello normativo una prassi adottata negli ultimi anni da numerose FIU europee.

Tali analisi consistono in una modalità particolarmente efficace di analisi di operatività sospetta transfrontaliera nella quale l'approfondimento dei casi non è svolto in maniera autonoma da ciascuna FIU sulla base delle informazioni ricevute e scambiate, bensì in maniera congiunta. Si tratta di una forma operativa particolarmente adatta per la trattazione di casi che presentano collegamenti con molteplici paesi e che non si prestano a essere trattati efficacemente mediante analisi condotte sul solo piano nazionale. Nelle analisi congiunte la condivisione delle informazioni disponibili o acquisibili a livello nazionale si accompagna all'esame di tali informazioni da parte di gruppi internazionali di analisti designati dalle FIU coinvolte, che in tal modo possono condividere l'intero processo di approfondimento, svolgendo un confronto sulle caratteristiche del caso e sulle relative conclusioni.

Una caratteristica precipua del sistema europeo va riscontrata, infine, nella previsione dell'art. 53 della direttiva: tale norma dispone, infatti, l'obbligo in capo alla FIU che riceve una segnalazione di

operazione sospetta che riguarda un altro Stato membro, di trasmetterla prontamente alla FIU di tale stato. Se gli standard del GAFI e del Gruppo Egmont si “limitano” a favorire gli scambi di informazione, la direttiva recepisce in pieno tale esigenza prevedendo per i casi della specie uno specifico obbligo informativo anziché la mera opportunità di inviare un’informativa spontanea.

In ossequio al principio secondo il quale le FIU devono scambiare le informazioni che sono in grado di ottenere a livello domestico, la direttiva prescrive anche le modalità con cui ottenere le informazioni in possesso di soggetti obbligati stabiliti presso uno Stato membro ma che operano in altri Stati membri in regime di libera prestazione di servizi: per questi casi l’art. 53 comma 2, dispone espressamente che spetta alla FIU del paese di stabilimento fornire le informazioni in possesso del soggetto obbligato su richiesta di altre FIU, e che è tenuta a provvedervi in maniera tempestiva.

4.3. La cooperazione fra FIU nella legislazione nazionale

I principi relativi al funzionamento della collaborazione internazionale fra FIU trovano la loro principale disciplina a livello nazionale nell’art. 13-*bis* del D.lgs. 231/2007, che recepisce la normativa europea e detta regole ulteriori per il funzionamento degli scambi tra la UIF e le FIU estere e per la trattazione dei successivi scambi con le competenti Autorità nazionali.

La normativa adottata in Italia appare in larga parte conforme ai principi del GAFI e del Gruppo Egmont e allo spirito della direttiva, sebbene lo scambio di informazioni di tipo investigativo rimanga di fatto limitato e, pertanto, possa limitare l’efficacia degli scambi da un punto di vista pratico.

Il nuovo art. 13-*bis* (introdotto con la riforma del novembre 2019) specifica nel dettaglio i poteri e le attività della UIF negli scambi con le proprie controparti. Rispetto alla previgente normativa, la norma attuale recepisce alcuni dei rilievi mossi dal GAFI in sede di *mutual evaluation* del sistema antiriciclaggio italiano e dalla Commissione europea in sede di recepimento della quarta direttiva, e prevede un esplicito riferimento alla possibilità per la UIF di scambiare informazioni, sia su richiesta, sia in maniera spontanea, in materia di informazioni collegate al riciclaggio, al finanziamento del terrorismo e ai soggetti coinvolti.

Sebbene sia nella norma italiana sia in quella europea manchi un esplicito riferimento ai delitti presupposto (che invece sono espressamente richiamati dal GAFI), si può ritenere che tali fattispecie siano già ricomprese implicitamente, dal momento che le FIU scambiano informazioni su casi di sospetto (e pertanto anche “potenziale” riciclaggio): è la stessa norma a precisare che l’accertamento sulla tipologia di reato presupposto non è richiesto ai fini dello scambio.

L’art. 13-*bis* fornisce anche una disciplina particolarmente dettagliata in merito alla trasmissione delle informazioni scambiate a favore di Autorità terze. Se infatti dal lato “passivo”, la UIF può trasmettere le informazioni ricevute ad altre Autorità nazionali solo previo consenso della FIU che ha fornito le informazioni stesse (e nel rispetto dei limiti o condizioni eventualmente posti da questa), dal lato “attivo” anche la UIF può fornire un analogo consenso alle FIU estere cui abbia fornito informazioni. Al riguardo, la norma specifica le condizioni tassative in cui tale consenso può essere rifiutato che, in aderenza a quanto stabilito dai principi internazionali, riguardano i casi in cui tale consenso possa pregiudicare lo svolgimento di indagini o sia in contrasto con norme costituzionali o con i principi fondamentali dell’ordinamento nazionale.

Il legislatore precisa espressamente che tale valutazione deve essere effettuata dalla UIF “in base alle evidenze disponibili”: a tutela, quindi, della speditezza degli scambi informativi deve ritenersi esclusa la necessità di una previa consultazione con Autorità terze, restando nella discrezionalità della UIF (e nei limiti di quanto risulta nel proprio patrimonio informativo) la valutazione circa l’esistenza di un tale impedimento. In tal senso risulta correttamente recepito lo spirito dei principi internazionali ed europei che individuano il diniego del consenso come una mera eccezione, peraltro da motivare adeguatamente.

Più difficile è configurare il caso in cui il diniego possa essere negato quando la sua concessione si ponga in contrasto con norme costituzionali o con i principi fondamentali dell’ordinamento. Una possibile ipotesi in tal senso potrebbe profilarsi laddove la legislazione dello stato estero prevedesse la pena di morte (e l’utilizzo delle informazioni da parte di Autorità investigative potrebbe portare a una condanna in tal senso) ovvero quando il soggetto cui si riferiscono le informazioni potrebbe essere sottoposto ad atti persecutori o discriminatori per motivi di razza, di religione, di sesso, di nazionalità, di lingua, di opinioni politiche o di condizioni personali o sociali ovvero a pene o trattamenti crudeli, disumani o degradanti o comunque ad atti che configurano violazione di uno dei diritti fondamentali della persona. Sebbene tale disciplina sia espressamente prevista in materia di estradizione dall’art. 698 c.p.p., i principi applicabili potrebbero ritenersi i medesimi.

Il tema delle informazioni investigative e dei rapporti fra UIF ed Autorità nazionali continua a costituire un elemento di non conformità della legislazione nazionale rispetto ai principi internazionali ed europei, con particolare riferimento all'accesso alle informazioni investigative per le esigenze di analisi delle FIU estere e all'attivazione della collaborazione internazionale fra FIU per esigenze di Autorità investigative nazionali.

Mentre i principi internazionali richiedono alle FIU di scambiare rapidamente le informazioni cui hanno accesso (a prescindere dalla natura amministrativa, finanziaria o investigativa delle stesse informazioni), in mancanza di accesso diretto della UIF alle informazioni investigative, la loro trasmissione da parte dei competenti organismi investigativi deve ritenersi soggetta ai limiti previsti dall'art. 12, comma 4, del D.lgs. 231/2007 relativamente alla previa autorizzazione dell'Autorità giudiziaria procedente.

Tale limitazione opera non solo quando l'indagine è coperta da segreto investigativo⁷⁶⁶, ma anche nei casi in cui sia stata trasmessa un'informativa all'Autorità giudiziaria e questa non abbia ancora assunto le proprie decisioni in materia di esercizio dell'azione penale. Sebbene la norma preveda anche l'adozione di modalità concordate che garantiscano la tempestiva disponibilità delle informazioni investigative, è di tutta evidenza come tale preventivo coordinamento, anche in considerazione del numero di Autorità coinvolte⁷⁶⁷, possa in concreto frustrare le esigenze di celerità sopra menzionate.

Va quindi evidenziato che, nonostante le raccomandazioni del GAFI e la direttiva europea limitino i casi di rifiuto alle sole ipotesi in cui sussista un rischio concreto di compromissione delle indagini, di fatto la normativa italiana pone una presunzione che di fatto equipara la mera esistenza di un'indagine in corso all'esistenza di un tale rischio. Inoltre, mentre la normativa internazionale ammette il rifiuto solo in relazione alla possibilità di trasmettere a terzi le informazioni scambiate tra FIU, la normativa italiana limita anche l'accesso della UIF a dette informazioni, e quindi introduce di fatto l'impossibilità per la UIF di scambiare informazioni in tale materia con le proprie controparti, anche quando tale informazione sarebbe destinata a restare nel solo patrimonio informativo della FIU estera.

Per quanto riguarda, infine, le forme di collaborazione "diagonale", un'ulteriore limitazione operativa è quella recentemente statuita dal D.lgs. 186/2021, che ha recepito la direttiva 1153/2019, il cui scopo era proprio quello di agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati.

Gli art. 5 e 7 di tale decreto, infatti, individuano quali unici interlocutori della UIF il Nucleo Speciale di Polizia Valutaria e la Direzione Investigativa Antimafia, prevedendo, nel caso in cui sia necessario, che siano questi ultimi a interessare ulteriori organi delle indagini: si viene in questo modo a creare un ulteriore "passaggio informativo", che non può non influire sulle esigenze di celerità degli scambi fra FIU e che, oltretutto, si pone in contrasto con le raccomandazioni che il GAFI medesimo aveva formulato all'Italia nel corso dell'ultima valutazione antiriciclaggio.

5. I movimenti transfrontalieri di contante: obblighi dichiarativi previsti dal D.lgs. 195/2008, evoluzione normativa e stato dell'arte (A. Cuzzocrea)

Il sistema dei controlli sui movimenti transfrontalieri di denaro, titoli e valori è stato introdotto nel nostro ordinamento dal decreto legge 28 giugno 1990, n. 167⁷⁶⁸, che prevedeva, tra l'altro, la canalizzazione, attraverso gli intermediari abilitati, dei predetti trasferimenti da e per l'estero nonché il relativo divieto di esportazione o importazione per importi eccedenti i venti milioni di lire. Tale sistema è stato, però, ritenuto in contrasto con il principio della libera circolazione dei capitali previsto dal Trattato di Roma del 1957.

⁷⁶⁶ Tale limitazione opererebbe fino a quando l'indagato non possa averne conoscenza o, comunque fino alla chiusura delle indagini preliminari, fatto salvo quanto previsto dall'art. 329 c.p.p.

⁷⁶⁷ Tale assunto deriva anche dalla scelta del legislatore (cfr. art. 7 del D.lgs. 186/2021, di recepimento della direttiva UE 1153/2019) di prevedere che in tale materia la UIF possa richiedere informazioni solo alla DIA e al NSPV, le quali a loro volta devono attivarsi presso gli altri organi delle indagini.

⁷⁶⁸ Convertito con modificazioni dalla legge 4 agosto 1990, n. 227.

Pertanto, successivamente, veniva emanato il D.lgs. 30 aprile 1997, n. 125 che, modificando il DL 167/1990 e in attuazione della direttiva 91/308/CEE (c.d. prima direttiva comunitaria antiriciclaggio), ha sostituito il regime di canalizzazione dei movimenti valutari superiori a venti milioni di lire con il sistema della dichiarazione dei trasferimenti al seguito, nel rispetto del principio comunitario della libertà dei trasferimenti transfrontalieri di denaro, titoli ed altri valori.

Il 15 dicembre 2005 è entrato in vigore il regolamento (CE) 1889/2005 concernente i controlli sul denaro contante in entrata nella Comunità o in uscita dalla stessa. Tale regolamento ha avuto come esplicita finalità l'integrazione delle disposizioni della direttiva 2005/60/CE del 26 ottobre 2005 (terza direttiva antiriciclaggio), considerata l'opportunità di realizzare a livello comunitario un sistema di sorveglianza sul denaro contante che assolvere al compito di arginare, anche mediante i controlli doganali, l'utilizzo del contante nell'economia criminale⁷⁶⁹.

L'art. 15 della legge 25 febbraio 2008, n. 34 (legge comunitaria 2007) ha delegato il Governo ad adottare, secondo i principi e criteri direttivi ivi previsti, uno o più decreti legislativi per consentire la piena applicazione del regolamento 1889/2005 nel nostro ordinamento. Ciò è avvenuto con il D.lgs. 19 novembre 2008, n. 195 recante "Modifiche ed integrazioni alla normativa in materia valutaria in attuazione del regolamento (CE) n. 1889/2005".

Le finalità del decreto legislativo del 2008 consistono nel contrasto all'introduzione dei proventi di attività illecite nel sistema economico e finanziario a tutela dello sviluppo armonioso equilibrato e sostenibile delle attività economiche e del corretto funzionamento del mercato interno, nonché nel coordinamento della disciplina recata dal predetto regolamento comunitario con la normativa antiriciclaggio contenuta nel D.lgs. 21 novembre 2007, n. 231 e successive modificazioni, per impiantare un adeguato sistema di sorveglianza sui movimenti transfrontalieri di denaro contante (art. 2 del D.lgs. 195/2008).

Rispetto al regime precedente, che limitava i propri effetti ai trasferimenti concernenti denaro, titoli e valori mobiliari, la nuova normativa propone una definizione notevolmente ampliata di denaro contante, integralmente ripresa dall'art. 2 del regolamento 1889/2005, prevedendo che nella dichiarazione debbono essere inseriti tutti gli strumenti non tracciabili utilizzati come mezzi di pagamento. In particolare, per denaro contante si intendono: le banconote e le monete metalliche aventi corso legale; gli strumenti negoziabili al portatore, compresi gli strumenti monetari emessi al portatore quali travellers cheque; gli strumenti negoziabili, inclusi assegni, effetti all'ordine e mandati di pagamento, emessi al portatore, girati senza restrizioni, a favore di un beneficiario fittizio o emessi altrimenti in forma tale che il relativo titolo passi alla consegna; gli strumenti incompleti, compresi assegni, effetti all'ordine e mandati di pagamento, firmati ma privi del nome del beneficiario (art. 1 del D.lgs. 195/08).

In sintesi, ai sensi dell'art. 3, chiunque entra nel territorio nazionale o ne esce, con qualsiasi modalità (aerea, stradale, ferroviaria o marittima), e trasporta denaro contante di importo pari o superiore a 10.000 euro, deve dichiarare tale somma all'Agenzia delle dogane e dei monopoli (ADM). L'obbligo di dichiarazione è diventato lo strumento principale per realizzare il sistema di sorveglianza sui movimenti transfrontalieri di denaro contante.

Nella dichiarazione devono essere riportati i dati essenziali al fine di identificare sia il dichiarante e/o il soggetto per conto del quale viene effettuato il trasferimento, sia i valori che si trasportano con l'itinerario seguito e il mezzo di trasporto utilizzato. Tutte queste informazioni sono indispensabili per la ricostruzione dei passaggi dei flussi finanziari, per consentire il contrasto a eventuali fenomeni di riciclaggio e/o traffici illeciti internazionali.

Sotto il profilo operativo, la dichiarazione transfrontaliera di cui all'art. 3, comma 2, del D.lgs. 195/2008 può essere anche trasmessa telematicamente, prima dell'attraversamento della frontiera, secondo le modalità pubblicate nel sito dell'ADM. Il dichiarante deve recare al seguito copia della dichiarazione e il numero di registrazione attribuito dal sistema telematico doganale, sia nei passaggi in entrata che in quelli in uscita dal territorio dello Stato⁷⁷⁰.

⁷⁶⁹ Il considerando n. 4 del citato regolamento richiamava "le iniziative complementari in corso in altri organismi internazionali, come ad esempio il gruppo di azione finanziaria internazionale sul riciclaggio dei capitali (GAFI), istituito dal vertice del G7 tenutosi a Parigi nel 1989. La raccomandazione speciale IX del GAFI del 22 ottobre 2004 esorta i governi ad attuare provvedimenti per l'individuazione dei movimenti materiali di denaro contante, compreso un sistema di dichiarazione o altro obbligo di divulgazione".

⁷⁷⁰ Nel caso di trasferimenti effettuati mediante plico postale o equivalente, la dichiarazione deve essere consegnata a Poste italiane Spa o ai fornitori di servizi postali ai sensi del D.lgs. 22 luglio 1999, n. 261, al momento della spedizione o nelle 48 ore successive al ricevimento.

Le disposizioni sui movimenti transfrontalieri di valuta non si applicano ai trasferimenti di vaglia postali o cambiari, ovvero di assegni postali, bancari o circolari, tratti su o emessi da banche o Poste italiane Spa che rechino l'indicazione del nome del beneficiario e la clausola di non trasferibilità, in quanto si tratta di strumenti tracciabili dal sistema degli intermediari.

I poteri di accertamento delle infrazioni alle norme del D.lgs. 195/2008 sono assegnati ai funzionari dell'ADM e ai militari della Guardia di finanza (GdF).

In particolare, la GdF trasmette i verbali di contestazione elevati sia all'ADM che al Ministero dell'Economia e delle finanze (MEF) ai fini del procedimento sanzionatorio disciplinato dal medesimo D.lgs. Alle contestazioni in argomento si applicano le disposizioni degli artt. 28 e 29 del decreto del Presidente della Repubblica 31 marzo 1988, n. 148⁷⁷¹. I poteri di svolgimento dell'istruttoria e di irrogazione delle sanzioni sono attribuiti al MEF, al quale spetta emettere l'eventuale decreto sanzionatorio avverso cui può essere proposta opposizione ai sensi degli artt. 22 e ss. della legge 24 novembre 1981, n. 689.

La disciplina delle sanzioni è contenuta nell'art. 9 del D.lgs. 195/2008, che è stato sostituito dall'art. 7 del D.lgs. 90/2017 al fine di ridurre, in caso di dichiarazione inesatta o incompleta, la soglia inferiore della sanzione e di prevedere specifici criteri per la graduazione della stessa in relazione alla effettiva gravità della violazione⁷⁷².

Una importante disposizione del decreto 195, tesa a realizzare la dichiarata finalità di coordinamento con la normativa antiriciclaggio di cui al D.lgs. 231/2007, è contenuta nell'art. 4, comma 7, del decreto stesso, in base al quale, ove nel corso degli accertamenti emergano fatti e situazioni che potrebbero essere correlati al riciclaggio e al finanziamento del terrorismo, anche se le somme di denaro contante al seguito siano inferiori alla soglia fissata di 10.000 euro, l'ADM fornisce notizie e dati all'Unità di informazione finanziaria (UIF) per l'adempimento delle proprie funzioni istituzionali⁷⁷³.

Più in generale, l'art. 5 del decreto 195/2008 prevede forme di collaborazione e di scambio di informazioni tra l'ADM e la GdF con le omologhe Autorità di altri Stati membri, qualora emergano fatti e situazioni da cui si evinca che somme di denaro contante sono connesse ad attività di riciclaggio e di finanziamento del terrorismo⁷⁷⁴. Sotto altro profilo, le informazioni raccolte mediante le dichiarazioni e nell'esercizio dei poteri di accertamento e contestazione, sono trasmesse per via telematica dall'ADM all'Agenzia delle entrate e alla GdF, secondo modalità e termini stabiliti con decreto del MEF.

Inoltre, la GdF e l'ADM forniscono al Comitato di Sicurezza Finanziaria (CSF), entro il 30 marzo di ogni anno, relazioni sulle attività rispettivamente svolte per prevenire e accertare le violazioni alle norme in materia di circolazione transfrontaliera dei capitali. Il CSF utilizza le informazioni in questione al fine della predisposizione della relazione al MEF, ex art. 5, del D.lgs. 231/2007.

Le informazioni sono trasmesse altresì alla Commissione europea se i fatti e le situazioni hanno ad oggetto somme di denaro contante afferenti frodi o qualsiasi altra attività illecita lesiva degli interessi finanziari dell'Unione europea.

⁷⁷¹ Il pagamento può essere effettuato alternativamente con due modalità: all'ADM o alla GdF, all'atto della contestazione; al MEF tramite specifica richiesta entro 10 giorni dalla data di contestazione. Il pagamento in misura ridotta (c.d. oblazione) estingue l'illecito. Nel caso di pagamento contestuale non si procede al sequestro; qualora il pagamento avvenga nei 10 giorni dalla contestazione, il MEF dispone la restituzione delle somme sequestrate entro 10 giorni dal ricevimento della prova dell'avvenuto pagamento.

⁷⁷² Ai sensi del novellato art. 9, comma 3, del D.lgs. 195/2008, nella determinazione del quantum della sanzione da irrogare, l'amministrazione procedente dovrà utilizzare una serie di criteri, che si aggiungono a quelli ordinariamente previsti dalle disposizioni generali che regolano la materia, relativi: all'entità dell'importo trasferito o che si tenta di trasferire in eccedenza rispetto alla soglia di 10.000 euro, prevista dall'art. 3; all'entità dell'importo non dichiarato in termini assoluti; all'entità dell'importo non dichiarato in termini percentuali rispetto all'intera somma trasportata.

⁷⁷³ In attuazione di tale previsione, il 13 dicembre 2013 l'ADM e l'UIF hanno sottoscritto un protocollo d'intesa per realizzare forme di collaborazione reciproca, poi rinnovato il 28 ottobre 2021 per tenere conto del regolamento (UE) n. 1672/2018.

⁷⁷⁴ Tale norma è stata poi modificata dall'art. 9, comma 1, del D.lgs. 25 maggio 2017, n. 90, in base al quale *“resta fermo quanto previsto dal decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni in materia di collaborazione e scambio di informazioni e cooperazione internazionale”*.

Il quadro dei controlli transfrontalieri fin qui descritto è destinato a subire modifiche a seguito della emanazione del regolamento (UE) 1672/2018 del 23 ottobre 2018, relativo ai controlli sul denaro contante in entrata o in uscita nell'Unione⁷⁷⁵ e che abroga il regolamento (CE) n. 1889/2005⁷⁷⁶.

L'intervento si inserisce nel quadro delle norme dell'Unione europea e internazionali per la lotta al riciclaggio dei proventi di attività criminose e al finanziamento del terrorismo. A livello internazionale, esso tiene conto della Raccomandazione 32 del GAFI riguardante i movimenti transfrontalieri di denaro contante. In ambito europeo, il regolamento intende allineare la legislazione dell'Unione alle norme e alle migliori prassi internazionali per la lotta al riciclaggio dei proventi di attività criminose e al finanziamento del terrorismo, completando il quadro giuridico AML/CFT di cui alla direttiva 2015/849/UE⁷⁷⁷. Il nuovo regolamento, entrato in vigore il 2 dicembre 2018, si applica a decorrere dal 3 giugno 2021, fatta eccezione per l'art. 16 ("Atti di esecuzione") già valido dall'entrata in vigore. Con il successivo regolamento di esecuzione della Commissione n. 2021/776/UE, dell'11 maggio 2021, sono stabiliti i modelli e le norme tecniche per l'efficace scambio di informazioni a norma del citato regolamento (UE) 1672/2018.

Le principali questioni che il regolamento 1672 intende risolvere, come specificato nella relativa proposta elaborata dalla Commissione, sono: a) la non perfetta copertura dei movimenti transfrontalieri di denaro contante (il regolamento 1889/2005 non contemplava i casi di denaro contante inviato per posta, come merce o con corriere); b) le difficoltà nello scambio di informazioni tra autorità (il regolamento 1889/2005 prevedeva che le autorità competenti di ciascuno Stato membro mettessero semplicemente "a disposizione" i dati contenuti nella dichiarazione, senza l'obbligo di trasmettere tali informazioni alle autorità competenti di altri Stati membri); c) l'impossibilità per le autorità competenti di trattenere temporaneamente importi inferiori alla soglia prevista in presenza di indizi di attività illecite; d) l'imperfetta nozione di denaro contante. Questo era definito come "strumenti negoziabili al portatore" ovvero "banconote e monete in circolazione come mezzo di scambio", senza considerare i casi in cui i soggetti criminali possano fare uso di altre riserve di valore altamente liquide, quali l'oro, nonché l'aumento della criminalità informatica, delle frodi via internet e dei mercati illeciti online; e) la divergenza nelle sanzioni irrogate dagli Stati membri per omessa dichiarazione; f) il problema di garantire "coerenza attuativa ed efficacia valutativa" tra gli Stati membri e di informare i destinatari dei loro obblighi.

Il regolamento, ancorché direttamente applicabile, necessita di adeguamento a livello nazionale⁷⁷⁸. Il regolamento 1672/2018 presenta infatti talune novità di rilievo volte ad ampliare la stessa nozione di denaro contante nonché l'ambito degli obblighi dichiarativi e i relativi flussi informativi tra le autorità competenti⁷⁷⁹.

In primo luogo, la nozione di "denaro contante" (art. 2) comprende, oltre alla "valuta", gli strumenti negoziabili al portatore, i beni utilizzati come riserve altamente liquide di valore e le carte prepagate⁷⁸⁰.

La "valuta" include banconote e monete attualmente in circolazione come mezzo di scambio ovvero la cui circolazione è sospesa, ma che possono ancora godere del rapporto di cambio con banconote e monete a corso legale tramite istituti finanziari ovvero banche centrali.

La categoria degli "strumenti negoziabili al portatore" comprende i mezzi diversi dalla valuta che autorizzano i portatori a esigere il pagamento di una somma di denaro dietro la loro presentazione senza dover provare il diritto a disporne o la

⁷⁷⁵ Al riguardo, si ha presente che il considerando (9) del Reg. (UE) 1672/2018 non pregiudica la possibilità per gli Stati membri di prevedere, nell'ambito del diritto nazionale, controlli nazionali supplementari per i movimenti di denaro contante all'interno dell'Unione.

⁷⁷⁶ La Commissione (COM 2016/825) ha ritenuto l'intervento conforme al principio di sussidiarietà in quanto il riciclaggio dei proventi delle attività illecite e del finanziamento del terrorismo mediante il traffico di denaro contante è un problema transnazionale che non può essere trattato solo a livello domestico ma richiede l'introduzione di misure armonizzate tra i vari Stati membri.

⁷⁷⁷ Esso intende inoltre attuare alcune delle misure individuate nel "Piano d'azione per rafforzare la lotta contro il finanziamento del terrorismo" (COM(2016)50), presentato dalla Commissione europea il 2 febbraio 2016.

⁷⁷⁸ Oltre al D.lgs. 195/2008 e al D.lgs. 231/2007, il regolamento presenta implicazioni anche per la normativa nazionale in materia di oro di cui alla legge 17 gennaio 2000, n. 7 nonché, sotto il profilo sanzionatorio, per il D.P.R. n. 148/1988.

⁷⁷⁹ Ai sensi dell'art. 2, comma 1, lett. g), del regolamento 1672/2018, sono autorità competenti le autorità doganali degli Stati membri e qualunque altra autorità autorizzata dagli Stati membri ad applicare il presente regolamento.

⁷⁸⁰ L'art. 14 del regolamento conferisce alla Commissione il potere di adottare atti delegati che le consentiranno di modificare l'allegato I, in cui sono elencati i prodotti rientranti nella definizione di "denaro contante". Tale flessibilità è ritenuta necessaria al fine di tener conto delle nuove tendenze nel riciclaggio o nel finanziamento del terrorismo, delle migliori prassi nel prevenire il riciclaggio o il finanziamento del terrorismo, ovvero allo scopo di impedire l'utilizzo criminoso di strumenti negoziabili al portatore, di beni come riserve altamente liquide di valore o di carte prepagate per eludere gli obblighi di cui agli artt. 3 e 4.

propria identità: ad esempio gli assegni turistici (o travellers cheque), gli assegni, i vaglia cambiari o gli ordini di pagamento emessi al portatore che siano firmati ma privi del nome del beneficiario, girati senza restrizioni, a favore di un beneficiario fittizio, ovvero emessi in forma tale che il relativo titolo si trasferisca all'atto della semplice consegna. Gli strumenti negoziabili al portatore risultano pertanto simili alla valuta in termini di liquidità, anonimato e rischio abusivo, consentendo al detentore di esigere il pagamento di una somma di denaro senza che la transazione sia tracciata.

I “beni utilizzati come riserve altamente liquide di valore” sono stati puntualmente elencati nell'allegato I al regolamento in esame, ferma restando la caratteristica di presentare un rapporto elevato tra il relativo valore e la potenzialità ad essere facilmente convertiti in valuta nei mercati accessibili, con costi di transazione assolutamente modesti. Si tratta, più in dettaglio, di monete con un tenore d'oro di almeno il 90% e lingotti sotto forma di barre, pepite o aggregati con un tenore in oro di almeno il 99,5%⁷⁸¹.

Per quanto concerne le “carte prepagate”, esse devono intendersi quali carte non nominative, non collegate ad un conto corrente, che contengono un valore in moneta o liquidità ovvero che danno accesso a detti valori per operazioni di pagamento, per l'acquisto di beni o servizi ovvero per la restituzione di valuta. Tra queste vanno ricomprese le carte prepagate anonime previste dalla direttiva (UE) 843/2018 (c.d. quinta direttiva antiriciclaggio), che ha ridotto le soglie preesistenti per l'uso di tali carte anonime, da 250 a 150 euro.

La nuova disciplina europea non prende in considerazione le valute virtuali, nonostante l'elevata minaccia evidenziata nella relazione della Commissione del 26 giugno 2017 sulla valutazione dei rischi ML/FT connessi ad attività transfrontaliere. Ciò è stato determinato anche dalla mancanza di specifiche *expertise* in materia da parte delle Autorità doganali (così il considerando (13) del regolamento). Tuttavia, il tema delle valute virtuali è stato già affrontato dal legislatore europeo nella citata quinta direttiva antiriciclaggio, con stringenti ricadute normative sulla disciplina nazionale di cui al D.lgs. 231/2007.

Ai fini dell'obbligo dichiarativo viene mantenuta la soglia di 10.000 euro; difatti, ai sensi dell'art. 3 del regolamento 1672/2018, il portatore che rechi con sé, nel bagaglio o nel mezzo di trasporto, denaro contante di valore pari o superiore a tale importo, deve dichiararlo alle Autorità competenti dello Stato membro attraverso il quale entra o esce dall'Unione e metterlo a loro disposizione a fini di controllo. L'obbligo dichiarativo non si ritiene assolto se le informazioni fornite sono scorrette o incomplete ovvero se il denaro contante non è messo a disposizione a fini di controllo.

La dichiarazione in parola deve fornire dettagli (dati anagrafici e indirizzi di contatto) riguardanti: il portatore; il proprietario del denaro contante; il destinatario del denaro contante, qualora disponibile; la natura e l'importo o il valore nonché la provenienza economica e l'uso del denaro contante; l'itinerario seguito e il mezzo di trasporto impiegato. Tali informazioni sono fornite per iscritto o per via telematica, utilizzando il modulo di dichiarazione conforme al modello di cui all'allegato I, parte 1, del citato regolamento 2021/776/UE.

È stato previsto l'obbligo di informativa per il denaro contante non accompagnato da un portatore (pacchi postali, spedizioni di merci o bagagli, container), sempre per importi pari o superiori a 10.000 euro (art. 4). In particolare, le Autorità competenti possono imporre al mittente ovvero al destinatario del denaro contante o a un rispettivo rappresentante, a seconda del caso, di presentare – entro il termine di 30 giorni – una dichiarazione a scopo informativo.

L'art. 5 conferisce poteri di controllo alle autorità competenti, al fine di verificare la corretta osservanza degli obblighi dichiarativi, conformemente alle condizioni previste dal diritto nazionale.

L'art. 6 prevede che le autorità competenti registrino le informazioni sui movimenti di denaro contante di importo inferiore alla soglia prevista per l'attivazione dell'obbligo di dichiarazione o di informativa, qualora vi siano indizi che denotano che tale denaro è correlato ad attività criminose (si applicherebbe in tal caso la definizione di “attività criminosa” contenuta nella quarta direttiva antiriciclaggio).

Il regolamento disciplina in modo maggiormente strutturato, rispetto al passato, il c.d. “trattenimento temporaneo” del denaro contante, lasciando però a ciascuno Stato membro il compito di disciplinare l'attuazione pratica di tale istituto. Secondo l'art. 7, le autorità competenti possono trattenere temporaneamente il denaro contante, con decisione amministrativa, qualora gli obblighi di dichiarazione o di informativa non siano stati assolti o vi siano indizi che denotano che tale denaro è correlato ad attività criminose, indipendentemente dal fatto che esso sia trasportato da una persona fisica o sia non accompagnato.

La decisione amministrativa dovrà essere accompagnata da una motivazione, comunicata alla persona interessata nel momento in cui sarà emanata e impugnabile conformemente alle procedure previste dalla legislazione nazionale. Il regolamento specifica che la durata del trattenimento dovrà essere “strettamente limitata al tempo necessario affinché le autorità competenti stabiliscano se le circostanze specifiche giustificano o meno una sua eventuale proroga”. In ogni caso, la durata massima del trattenimento, stabilita dalla legislazione nazionale, non potrà protrarsi oltre i 30 giorni. Nel caso in cui non venga assunta alcuna decisione in merito alla proroga del trattenimento del denaro contante, ovvero se la decisione assunta stabilirà che le circostanze specifiche non giustifichino tale proroga, il denaro contante dovrà essere immediatamente rimesso a disposizione del dichiarante.

⁷⁸¹ Tale tipologia di oro rientra nell'oro da investimento di cui all'art 1, comma 1, lett. a) della legge 7/2000.

La Commissione sottolinea che si tratta di una “misura amministrativa strettamente cautelare, il cui unico obiettivo è permettere alle autorità competenti di trattenere il denaro contante tra il momento in cui esse rilevano un’anomalia e quello in cui altre autorità, quali le FIU o le autorità giudiziarie, decidono se vi sono o meno sufficienti motivi per procedere a un’indagine, alla confisca o al dissequestro delle somme trattenute”.

Il regolamento rafforza i flussi informativi tra le autorità competenti, ossia le autorità doganali e le altre autorità designate dagli Stati membri ai fini dell’applicazione del regolamento; tra queste sono senz’altro incluse le UIF dei vari Stati membri.

In particolare, l’art. 9 impone alle autorità in questione di trasmettere alla UIF le informazioni ottenute ai sensi degli artt. 3 e 4, dell’art. 5, par. 3, e dell’art. 6, ossia le dichiarazioni relative al trasporto di valori di importo pari o superiore a 10.000 euro, le informazioni relative a casi di sospetto di riciclaggio o finanziamento del terrorismo senza limiti di soglia e quelle relative all’ipotesi di violazione dell’obbligo di dichiarazione emerse nel corso dei controlli. Le predette informazioni dovranno essere trasmesse conformemente alle norme tecniche di cui all’art. 16, par. 1, lett. c)⁷⁸². Viene in tal modo valorizzato il ruolo centrale della UIF nella ricezione e gestione delle informazioni acquisite ai sensi del regolamento 1672/2018, consentendo alla stessa Unità di analizzare ulteriormente a fini AML/CFT, come previsto dalla direttiva (UE) 2015/849.

L’art. 10 prevede anche lo scambio tra autorità competenti e con la Commissione delle dichiarazioni d’ufficio di cui all’art. 5, delle informazioni raccolte ai sensi dell’art. 6, delle dichiarazioni ottenute ai sensi degli artt. 3 o 4 (qualora sussistano indizi di attività criminosa correlata al denaro contante) e delle informazioni anonime riguardanti eventuali rischi e i risultati delle analisi di rischio.

In virtù poi dell’art. 11, le Autorità competenti di ciascuno Stato membro comunicano agli omologhi organismi di tutti gli altri Paesi membri le dichiarazioni d’ufficio redatte, le informazioni ottenute nei casi di importi inferiori alla soglia di cui si sospetta la correlazione ad azioni illecite, le dichiarazioni e le informative ricevute, inerenti a indizi di attività criminosa correlata al denaro contante.

Qualora sussistano indizi di attività criminali che potrebbero arrecare pregiudizio agli interessi finanziari dell’Unione europea, le informazioni in parola sono trasmesse, nel più breve tempo possibile, anche alla Commissione, alla Procura europea dagli Stati membri che partecipano alla cooperazione rafforzata a norma del regolamento (UE) 1939/2017, e a Europol qualora ricorrano i presupposti di cui all’art. 3 del regolamento (UE) 794/2016.

Inoltre, nell’ambito dell’assistenza amministrativa reciproca, gli Stati membri e la Commissione possono comunicare le previste informazioni anche ad un Paese terzo, previa autorizzazione scritta dell’Autorità competente che ha ottenuto per prima l’informazione, purché tale comunicazione sia conforme al diritto pertinente, nazionale e dell’Unione, in materia di trasferimento dei dati personali ai Paesi terzi. Gli Stati membri hanno l’obbligo di notificare alla Commissione qualunque comunicazione di informazioni.

Il regolamento detta disposizioni volte a tutelare la sicurezza dei dati e delle informazioni (art. 12), a limitare il trattamento dei dati personali al solo scopo di prevenzione e di lotta alle attività criminali e a definire il periodo di conservazione dei dati contenuti nella dichiarazione fissandolo entro un massimo di cinque anni (art. 13).

Sotto il profilo sanzionatorio, l’art. 14 prevede che ogni Stato membro stabilisca le sanzioni da applicare in caso di inosservanza dell’obbligo di dichiarazione e che tali sanzioni siano “effettive, proporzionate e dissuasive”⁷⁸³.

Gli artt. da 15 a 18 disciplinano ulteriori poteri della Commissione. In particolare essa ha competenze di esecuzione per la definizione di misure volte a garantire l’applicazione uniforme dei controlli da parte delle autorità competenti, predisponendo i modelli di dichiarazione e le norme tecniche per lo scambio di informazioni (inclusa l’introduzione di un sistema elettronico appropriato), il modello dello stampato da utilizzare per lo scambio di informazioni nonché le norme e il formato che gli Stati membri saranno tenuti a utilizzare per trasmettere alla Commissione i dati statistici anonimi sulle dichiarazioni e sulle infrazioni. Viene inoltre istituito un comitato di controllo sul denaro contante (art. 16), con esperti nazionali nominati dagli Stati membri, che assisterà la Commissione nel predisporre gli atti esecutivi. L’art. 17 stabilisce gli obblighi di informazione alla Commissione e specifica che gli Stati membri, entro sei mesi dalla data di applicazione del regolamento, dovranno comunicare l’elenco delle autorità competenti, i dettagli delle sanzioni previste per omessa dichiarazione, nonché eventuali dati statistici anonimi riguardanti le dichiarazioni, i controlli e le infrazioni. Gli Stati membri dovranno inoltre notificare alla Commissione le modifiche successive. Infine, l’art. 18 specifica che la Commissione trasmetterà al Parlamento europeo e al Consiglio un’apposita relazione cinque anni dopo l’entrata in vigore del regolamento e, successivamente, con cadenza quinquennale.

⁷⁸² Il considerando (25) del regolamento precisa che al fine di garantire un flusso di informazioni efficace, le UIF dovrebbero essere collegate al Sistema informativo doganale (SID) istituito dal regolamento (CE) n. 515/97 del Consiglio e i dati prodotti o scambiati dalle autorità competenti e dalle UIF dovrebbero essere compatibili e comparabili.

⁷⁸³ Le criticità dell’attuale sistema sanzionatorio in materia di infrazioni agli obblighi di dichiarazione dei trasferimenti transfrontalieri di contante sono state oggetto di rilievo anche da parte del GAFI nell’ultima Mutual Evaluation, stante il carattere scarsamente dissuasivo ed efficace delle disposizioni vigenti.

6. Le dichiarazioni di operazioni in oro: la legge 17 gennaio 2000, n. 7 (*F. Di Natale e R. Coppola*)

La legge 17 gennaio 2000, n. 7, recante la disciplina del mercato dell'oro, ha abolito il monopolio dell'oro⁷⁸⁴, prima attribuito all'Ufficio italiano dei cambi⁷⁸⁵, adeguando la normativa italiana alle direttive comunitarie in materia di libera circolazione delle merci e di regime fiscale sulle operazioni in oro che varia a seconda della qualificazione dell'oro⁷⁸⁶.

La caduta del regime monopolistico ha determinato la generale liberalizzazione del commercio dell'oro con il solo limite, a fini fiscali, di ordine pubblico e antiriciclaggio, dell'obbligo di dichiarazione all'Ufficio Italiano dei Cambi⁷⁸⁷ degli acquisiti di valore superiore alla soglia⁷⁸⁸ (art. 1, comma 5).

L'obbligo dichiarativo è posto a carico di chi "dispone" o "effettua" il trasferimento di oro ovvero il commercio di oro; tale prescrizione, invero, lascia aperti dubbi interpretativi che nella fase di emanazione della normativa secondaria sono stati risolti inizialmente dall'UIC, nonché dalla Banca d'Italia e dalla UIF ponendo l'obbligo dichiarativo a carico dei soggetti "attivi" nell'azione del trasferimento, salvo alcune eccezioni. Dall'obbligo sono comunque escluse le operazioni effettuate dalla Banca d'Italia.

L'esercizio professionale del commercio di oro può essere svolto, oltre che dalle banche, da operatori professionali che siano in possesso di determinati requisiti che devono essere comunicati alla Banca d'Italia prima dell'avvio dell'attività. Ove non sussistano ragioni di impedimento derivanti da particolari esigenze di celerità, la Banca d'Italia, ricevuta la Comunicazione, rende noto l'avvio del procedimento ai soggetti interessati; il termine per la conclusione del procedimento è fissato in 120 gg. dalla data di ricezione della domanda di iscrizione. Entro il suddetto termine, la Banca, in presenza dei requisiti richiesti, comunica, con proprio provvedimento, il codice operatore attribuito al soggetto che ha effettuato la Comunicazione. La mancanza anche di un solo requisito richiesto per l'esercizio in via professionale del commercio di oro determina il rigetto dell'istanza⁷⁸⁹.

Sono esclusi dalla riserva di attività gli acquisti di oro destinato alla lavorazione industriale o artigianale dello stesso acquirente o affidato, esclusivamente in conto lavorazione, a un titolare del marchio di identificazione di cui al decreto legislativo 22 maggio 1999, n. 251.

Sono soggette a riserva di attività le operazioni finanziarie in oro secondo quanto previsto dal Testo unico della finanza e non sono soggette agli obblighi dichiarativi previsti dall'art. 1, comma 2. Tuttavia se le operazioni comportano la consegna dell'oro, ricadono sotto la previsione di cui al predetto art. 1, comma 2, e, pertanto, devono essere dichiarate alla UIF.

Per quanto riguarda le disposizioni di natura fiscale di cui all'art. 3 della legge 7/2000 – che ha apportato modifiche al decreto del Presidente della Repubblica 26 ottobre 1972, n. 633 – esse prevedono la distinzione tra l'oro da investimento e quello ad uso industriale come definiti dall'art. 1, comma 1 della legge 7/2000⁷⁹⁰.

⁷⁸⁴ Il monopolio dell'oro, stabilito dall'art. 2 del D.lgs.lgt. 17 maggio 1945, n. 331, era stato ribadito dall'art. 15 del testo unico delle norme in materia valutaria, approvato con decreto del Presidente della Repubblica 31 marzo 1988, n. 148.

⁷⁸⁵ L'Ufficio italiano dei Cambi è stato soppresso in base all'art. 62 del D.lgs. 231/2007, che ha disposto il trasferimento dei poteri e delle competenze alla Banca d'Italia.

⁷⁸⁶ Relativamente agli aspetti fiscali, è stata recepita nel nostro ordinamento la direttiva 98/80/CE (ora sostituita dalla direttiva 2006/112/CE relativa al sistema comune d'imposta sul valore aggiunto).

⁷⁸⁷ Ora all'Unità di Informazione Finanziaria per l'Italia, in base a specifica delega conferita dalla Banca d'Italia.

⁷⁸⁸ La soglia, derivata dalla normativa antiriciclaggio, era inizialmente pari a 20.000.000 di lire; è stata portata a 12.500 euro con Decreto del Ministro dell'Economia e delle finanze del 17 ottobre 2002.

⁷⁸⁹ Cfr. <https://www.bancaditalia.it/compiti/vigilanza/intermediari/op-oro/index.html#3>.

⁷⁹⁰ Le cessioni di oro da investimento, per espressa previsione del modificato art. 10, comma 1, n. 11, e le operazioni finanziarie, disciplinate all'art. 2 della legge 7/2000 sono esenti dall'imposta IVA. Con riferimento all'oro industriale, vale a dire il materiale d'oro diverso da quello da investimento, ad uso prevalentemente industriale, sia in forma di semilavorati di purezza pari o superiore a 325 millesimi, sia in qualunque altra forma e purezza, è disposto uno speciale regime di imponibilità ai fini IVA, ove l'imposta viene assolta dal cessionario, se soggetto passivo d'imposta nel territorio dello Stato italiano. In merito all'esatta nozione di materiale d'oro e di prodotti semilavorati di purezza pari o superiore a 325 millesimi, premessa la natura non fiscale di tale nozione, l'Agenzia delle entrate ha chiarito che, in linea

L'art. 4 regola il sistema sanzionatorio; il comma 1 riguarda l'abusivo esercizio dell'attività di commercio di oro prevista dall'art. 1, comma 3, e l'abusivo esercizio di attività aventi a oggetto operazioni finanziarie in oro. Al comma 2 sono prescritte le sanzioni nel caso di violazione degli obblighi dichiarativi. Per l'accertamento delle violazioni dell'obbligo di dichiarazione e per l'irrogazione delle relative sanzioni si applicano le disposizioni del testo unico delle norme di legge in materia valutaria, approvato con decreto del Presidente della Repubblica 31 marzo 1988, n. 148 e successive modificazioni. Si applicano, in quanto compatibili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni e non è ammesso il pagamento in misura ridotta previsto dall'art. 16 della predetta legge.

Nell'ambito dei procedimenti amministrativi relativi alle violazioni degli obblighi dichiarativi, l'Unità di informazione finanziaria per l'Italia svolge funzioni esclusivamente istruttorie; più in dettaglio, ai sensi dell'art. 31, comma 1, del testo unico delle norme di legge in materia valutaria alla UIF può essere richiesta un'audizione e/o possono essere inviati scritti difensivi. Inoltre, ai sensi dell'art. 31, comma 2, l'Unità redige la relazione al Ministero dell'Economia e delle finanze. Il Ministero commina la sanzione udito il parere della Commissione consultiva per le infrazioni valutarie che si esprime sulla sussistenza della violazione e propone l'importo delle sanzioni medesime. Alla UIF, inoltre, ai sensi dell'art. 28 del predetto testo unico, può essere proposta opposizione nel caso di sequestro amministrativo disposto nell'ambito del procedimento sanzionatorio.

Si osserva che la legge non disciplina puntualmente le fattispecie di violazione dichiarativa con particolare riferimento alle dichiarazioni tardive, delle quali non è chiara l'effettiva sanzionabilità. La normativa primaria, difatti, non stabilisce un preciso termine per l'adempimento dell'obbligo dichiarativo esplicitato solamente nelle disposizioni attuative. Il Provvedimento UIC del 14 luglio 2000 e la Comunicazione della UIF del 1° agosto 2014 prevedono che il termine per l'invio delle dichiarazioni è la fine del mese successivo a quello in cui è compiuta l'operazione.

Il quadro normativo sopra descritto è destinato a mutare a seguito dell'entrata in vigore – il 3 giugno 2021 – del regolamento (UE) 2018/1672 relativo ai controlli sul denaro contante in entrata nell'Unione o in uscita dall'Unione⁷⁹¹, in quanto nella nozione di denaro contante sono inclusi i beni utilizzati come riserve altamente liquide di valore, tra cui le monete con un tenore di oro di almeno il 90% e i lingotti sotto forma di barre, pepite o aggregati con un tenore in oro di almeno il 99,5%. Il regolamento è parte delle misure dell'UE volte a contrastare il finanziamento del terrorismo, il riciclaggio, l'evasione fiscale e altre attività criminali e prevede che chiunque entri nell'UE o esca dall'UE recando con sé denaro contante di valore pari o superiore a 10 000 euro deve dichiarare tale somma alle Autorità del relativo paese. L'obbligo dichiarativo previsto dal regolamento, pertanto, si sovrappone parzialmente agli obblighi già previsti dalla legge 7/2000 e sarà compito del legislatore italiano apportare le necessarie modifiche volte a coordinare i due provvedimenti normativi per evitare la duplicazione degli adempimenti dichiarativi riguardanti l'oro da investimento in entrata in Italia e in uscita dall'Italia in contropartita con paesi extra-UE tenendo altresì conto che la soglia dichiarativa è differente per i due provvedimenti. L'occasione potrebbe essere favorevole per conferire maggiore chiarezza al quadro normativo relativo alle transazioni in oro nonché, in tale ambito, al ruolo della UIF.

L'obbligo dichiarativo previsto dalla L. 7/2000 e dalle relative disposizioni di attuazione può essere declinato in termini di oggetto dell'operazione, soggetto obbligato a dichiararla e operatività rilevante⁷⁹².

Con riferimento all'oggetto, le categorie di oro rilevanti ai fini dichiarativi sono due: il cosiddetto *oro da investimento* e il *materiale d'oro ad uso prevalentemente industriale* (art. 1, comma 1, della L. 7/2000). Nella prima fattispecie rientra: l'oro sotto forma di lingotti o placchette di peso superiore ad 1 grammo e di purezza pari o superiore a 995 millesimi, rappresentato o meno da titoli; le monete d'oro di purezza pari

con quanto stabilito dall'Ufficio italiano dei cambi e dalla Banca d'Italia, il riferimento all'oro è da intendersi nella sua funzione prevalentemente industriale, ossia di materia prima destinata alla lavorazione e non di investimento. In tal senso, vi rientrano tutti i prodotti che non hanno una funzione individuale, ma che hanno bisogno di una trasformazione per essere successivamente utilizzati.

⁷⁹¹ Che abroga il regolamento (CE) n. 1889/2005.

⁷⁹² Cfr. [Comunicazione della UIF in tema di “dichiarazioni delle operazioni in oro” del 1° agosto 2014](#); [Chiarimenti della Banca d'Italia sulla disciplina degli operatori professionali in oro](#).

o superiore a 900 millesimi, coniate dopo il 1800. Appartiene, invece, alla seconda fattispecie il materiale d'oro impiegato prevalentemente in ambito industriale sia in forma di semilavorati di purezza pari o superiore a 325 millesimi sia in qualsiasi altra forma e purezza. Una definizione di "semilavorato" è contenuta nell'art. 1, comma 1, lett. c), n. 3 del DPR 150/2002, che annovera in questa tipologia i prodotti di processi tecnologici di qualsiasi natura meccanici e non, che pur presentando una struttura finita o semifinita non risultano diretti ad uno specifico uso o funzione, ma sono destinati ad essere intimamente inseriti in oggetti compositi, garantiti nel loro complesso dal produttore che opera il montaggio. Anche l'oro da investimento, se destinato a lavorazione e non a riserva di valore, muta la propria qualificazione ed è da considerarsi oro industriale.

Come precisato dai Chiarimenti della Banca d'Italia, per esclusione, l'obbligo dichiarativo non sussiste quando l'oggetto dell'operazione è costituito dal cosiddetto *oro da gioielleria* ad uso ornamentale (ad es., i gioielli e i monili), dall'oro per la *componentistica elettronica* (ad es., il materiale aureo di rivestimento delle superfici) o dall'oro per *scopi medici e diagnostici* (ad es., il materiale aureo per la realizzazione di otturazioni e ponti in odontoiatria). In particolare, l'esenzione vale non solo nel caso in cui l'oro sia in condizione di nuovo o di usato da lavorare e/o riparare, ma anche quando sia in condizioni di rottame o rifiuto da destinare a fusione per ricavarne oro diverso da quello rilevante ai fini della L. 7/2000. Al contrario, la fusione finalizzata ad ottenere oro da investimento (ad es. lingotti) e industriale (ad es. verghe) da gioielli, rottami o oro usato rende il materiale d'oro in essi contenuto rilevante ai fini della dichiarazione.

Per quel che concerne i soggetti obbligati, la L. 7/2000 dà un'indicazione molto generale, stabilendo che *chiunque*, a qualsiasi titolo, trasferisca l'oro è tenuto ad effettuare la dichiarazione. L'Unità di Informazione Finanziaria, in attuazione dell'art. 6 della stessa Legge, ha fornito specificazioni a tale indirizzo precisando in capo a chi ricade l'obbligo dichiarativo in diversi contesti non immediatamente riconducibile alla regola generale.

Nel caso di operazioni in oro compiute con soggetti non residenti, ad esempio, l'obbligo dichiarativo ricade sulla parte residente anche nel caso in cui non sia cedente ma cessionaria dell'oro. Analogamente, se una delle due parti di un'operazione è una banca o un operatore professionale in oro⁷⁹³, spetta ad essi l'obbligo dichiarativo, indipendentemente dal ruolo di cedente o cessionario assunto, salvo ritornare alla regola generale del "chi trasferisce" nel caso in cui l'operazione avvenga tra due operatori professionali o tra un operatore professionale e una banca⁷⁹⁴. Le banche e gli altri intermediari finanziari, inoltre, hanno l'obbligo di dichiarare le operazioni finanziarie in oro in cui il metallo viene consegnato ai propri clienti o ricevuto dagli stessi (c.d. "oro finanziario").

Un'ulteriore deroga è prevista per la successione *mortis causa*: la qualità di dichiarante è attribuita agli eredi, cioè a chi succede nella titolarità dell'oro, ciascuno *pro quota*⁷⁹⁵, mentre il *de cuius* è controparte dell'operazione.

Sono da inquadrarsi, invece, nella regola generale, ma con alcune precisazioni, i casi di trasferimento "puro"⁷⁹⁶ di oro da/verso l'estero e di operazioni che coinvolgono le società fiduciarie che operano per conto dei propri clienti. Nel primo caso, infatti, a rilevare è l'attraversamento fisico della frontiera con oro al seguito, non essendoci alcuna cessione dell'oro, e la dichiarazione del passaggio deve essere resa dal soggetto che ha il possesso dell'oro o dal soggetto per conto del quale il passaggio viene effettuato. Nel caso, invece, delle società fiduciarie che operano in oro per conto della propria clientela nell'ambito di mandati fiduciari in essere, l'obbligo dichiarativo, nei casi in cui è previsto, ricade sulle fiduciarie stesse che hanno posto in essere l'operazione⁷⁹⁷.

Infine, merita un discorso più articolato l'individuazione del soggetto obbligato nel caso di dichiarazione di operazioni che hanno ad oggetto materiale contenente oro destinato a fusione per ricavarne oro da investimento o industriale. Tale soggetto, infatti, coincide con il cedente quando la destinazione dell'oro risulti dalle fatture o da altra documentazione inerente alla cessione; l'obbligo dichiarativo spetta, invece, al cessionario laddove questi sia il solo ad avere disponibilità della documentazione da cui sia possibile desumere natura e destinazione dell'oro. Cionondimeno, anche in questa casistica, qualora parte dell'operazione sia una banca o un operatore professionale in oro, spetta a essi l'obbligo dichiarativo.

Il novero delle operazioni in oro comprese nell'obbligo di dichiarazione previsto dall'art. 1, comma 2, della Legge 7/2000 è ampio e al suo interno si possono individuare tre macro-categorie. Nella prima rientrano tutte le operazioni non finanziarie in oro, quali gli atti di disposizione sull'oro, come la

⁷⁹³ Art. 1, comma 3 della legge 7/2000.

⁷⁹⁴ Le operazioni in oro tra banche non sono soggette all'obbligo dichiarativo.

⁷⁹⁵ Resta ferma la soglia di 12.500 euro per quota affinché sussista l'obbligo di dichiarazione.

⁷⁹⁶ Il trasferimento al seguito da/verso l'estero che non avvenga in forza di un contratto di compravendita o di altro titolo traslativo.

⁷⁹⁷ Alle società fiduciarie è comunque richiesto di indicare i clienti per conto dei quali l'operazione in oro è stata compiuta (cfr. riferimento al Manuale e/o alle FAQ oro).

compravendita, il prestito d'uso, il conferimento in garanzia, il trasferimento a titolo di donazione o successione *mortis causa*. Le operazioni finanziarie in oro costituiscono la seconda macro-categoria sempre che esse comportino la consegna materiale del metallo (per es.: la consegna del materiale d'oro nello svolgimento di servizi di investimento). Infine, appartengono al terzo gruppo i trasferimenti di oro al seguito da o verso l'estero⁷⁹⁸. Specificamente per il trasferimento in uscita dall'Italia, è prevista una dichiarazione da rendere prima dell'attraversamento transfrontaliero (si parla di dichiarazione *preventiva*).

7. Whistleblowing (M. Siani)

Il termine *whistleblowing* indica l'attività di segnalazione di possibili illeciti e irregolarità da parte di un soggetto (*whistleblower*) che ne sia venuto a conoscenza nello svolgimento di un rapporto lavorativo pubblico o privato⁷⁹⁹. Il D.lgs. 90/2017, in attuazione degli obblighi imposti dall'art. 61, par. 3, della quarta direttiva antiriciclaggio, ha introdotto all'interno del D.lgs. 231/2007 specifiche disposizioni volte a disciplinare i meccanismi di segnalazione di violazioni della disciplina antiriciclaggio e a introdurre forme di tutela per il soggetto segnalante⁸⁰⁰.

L'art. 48, comma 1, del D.lgs. 231/2007 impone ai soggetti obbligati di adottare *“procedure per la segnalazione al proprio interno da parte di dipendenti o di persone in posizione comparabile di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo”*⁸⁰¹. La nozione di “dipendenti o di persone in posizione comparabile” va interpretata in senso ampio, al fine di ricomprendervi anche soggetti inseriti nell'organizzazione aziendale in forma diversa rispetto alla stretta fattispecie di rapporto di lavoro subordinato⁸⁰².

Tali meccanismi procedurali devono garantire, *in primis*, la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni (art. 48, comma 2, lett a).

Il dipendente che effettua la segnalazione, inoltre, deve essere adeguatamente posto al riparo da condotte c.d. di *“retaliation”*, ovvero quelle condotte *“ritorsive, discriminatorie o comunque sleali”* conseguenti alla segnalazione (art. 48, comma 2, lett b)). Il licenziamento ritorsivo o discriminatorio, il mutamento di

⁷⁹⁸ Per tali operazioni, attualmente gli obblighi dichiarativi ai fini della legge 7/2000 si sovrappongono a quelli previsti dal regolamento UE 1672/2018.

⁷⁹⁹ Tale termine è mutuato dal contesto e dalla legislazione anglosassone, ove l'attività di “whistleblowing” è stata originariamente incentivata e disciplinata, dapprima nel settore pubblico e, successivamente, in ambito privato. Per una ricostruzione più puntuale dell'istituto cfr. G. Amato, *Obbligo di segnalazione [c.d. Whistleblowing]*, https://www.treccani.it/enciclopedia/obbligo-di-segnalazione-cd-whistleblowing_%28Diritto-on-line%29/; R. Cantone, *Il dipendente pubblico che segnala illeciti. Un primo bilancio sulla riforma del 2017*, https://www.sistemapenale.it/pdf_contenuti/1593371098_cantone-2020b-whistleblowing-segnalazione-illeciti-dipendente-pubblico-primo-bilancio-riforma-2017.pdf; A.F. Masiero, *La disciplina del whistleblowing alla luce della direttiva 2019/1937/UE. Tra prevenzione dei fenomeni corruttori e tutela del denunciante*, <https://archiviopenale.it/File/DownloadArticolo?codice=2b16d7fb-05d7-46ad-9309-e087d1905808&idarticolo=24906>.

⁸⁰⁰ Per tutte le categorie di soggetti obbligati rilevano inoltre le disposizioni generali in materia di “whistleblowing” contenute negli artt. 2 e 3 della legge 179/2017, recante “Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato” e, ove applicabili, quelle contenute nell'art. 6, commi 2-*bis*, 2-*ter* e 2-*quater*, del D.lgs. 231/2001 in materia di responsabilità degli enti per gli illeciti amministrativi dipendenti da reato, introdotti dall'art. 2 della legge n. 179.

⁸⁰¹ Nei soggetti obbligati che, ai sensi dell'art. 6 del D.lgs. 231/2001, hanno adottato un modello (facoltativo) di organizzazione, gestione e controllo (“MOGC”) per prevenire la commissione di reati (tra cui il riciclaggio, come previsto dall'art. 25-*octies*), le procedure di “whistleblowing” introdotte dal D.lgs. 231/2007 si sovrappongono a quelle previste dal comma 2-*bis* dell'art. 6 del D.lgs. 231/2001, secondo il quale tali modelli devono prevedere uno o più canali che consentano “segnalazioni circostanziate di condotte illecite” fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente (per un approfondimento cfr. Associazione dei Componenti degli Organismi di Vigilanza, *Il ruolo dell'Organismo di Vigilanza*, <https://www.aodv231.it/images/pdf/3580-10-PP%20Antiriciclaggio.%20Il%20ruolo%20dell%E2%80%99Organismo%20di%20Vigilanza.pdf> e *Il Whistleblowing*, <https://www.aodv231.it/documenti-di-approfondimento/il-whistleblowing-3505/>).

⁸⁰² L'art. 6, comma 2-*bis*, del D.lgs. 231/2001 prevede che le segnalazioni possano essere effettuate dai soggetti indicati all'art. 5, comma 1, lett a) e b), vale a dire *“persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché persone che esercitano, anche di fatto, la gestione e il controllo dello stesso”* ovvero da persone sottoposte alla loro direzione o vigilanza. Tale nozione estensiva di “dipendente” legittimato al “whistleblowing” pare pienamente applicabile anche alle segnalazioni di violazioni in materia antiriciclaggio, argomentando, a fortiori, circa il preminente interesse pubblico sotteso a tali segnalazioni.

mansioni ai sensi dell'art. 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante, vengono colpiti con la sanzione civilistica della nullità⁸⁰³.

I soggetti obbligati sono altresì tenuti a sviluppare specifici canali di segnalazione, anonimi e indipendenti, proporzionati alla loro natura e dimensione (art. 48, comma 2, lett c). È opportuno, pertanto, che tali sistemi interni differiscano dalle ordinarie modalità di *reporting* aziendale.

L'identità del segnalante può essere rivelata solo con il suo consenso o nei casi in cui sia indispensabile per la difesa del segnalato. Risulta invece inapplicabile l'art. 15 del regolamento UE 2016/679 ("GDPR") che prevede il diritto dell'interessato (in questo caso il segnalato) di ottenere dal titolare del trattamento la conferma che sia in corso un trattamento dei dati personali che lo riguardano e, in tali casi, di ottenere l'accesso a tali dati⁸⁰⁴.

La presentazione della segnalazione non costituisce, di per sé, violazione degli obblighi derivanti dal rapporto contrattuale con il soggetto obbligato (art. 48, comma 3). Inoltre, la segnalazione effettuata nelle forme stabilite dalla legge costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli artt. 622 e 623 del codice penale e all'art. 2105 del codice civile⁸⁰⁵.

La protezione accordata al "*whistleblower*" copre le sole segnalazioni che riguardino fatti veri o comunque reputati ragionevolmente e in buona fede tali dal dipendente⁸⁰⁶; sono pertanto escluse dalla tutela le segnalazioni presentate con dolo o colpa grave⁸⁰⁷ nonché, secondo un orientamento giurisprudenziale, quelle effettuate a seguito di "attività investigativa" del dipendente in violazione di norme di legge⁸⁰⁸.

Stante il contenuto di questo tipo di segnalazioni, appare chiara la distinzione con le segnalazioni di operazioni sospette. Lo scopo del "*whistleblowing*" è infatti quello di far emergere violazioni della normativa di prevenzione e carenze nella collaborazione passiva e attiva; per contro, la finalità delle segnalazioni di operazioni sospette è quella di portare all'attenzione della funzione antiriciclaggio e, in caso di "fondatezza", della UIF, possibili attività di riciclaggio o di finanziamento del terrorismo compiute o tentate dalla clientela⁸⁰⁹.

L'art. 48 non prevede modalità di segnalazione "esterna" delle violazioni riscontrate. La scelta legislativa compiuta in sede di trasposizione di disciplinare il solo "*whistleblowing* interno" si discosta tuttavia dal contenuto dell'art.61 della richiamata direttiva n. 849, che prevede espressamente l'obbligo per gli Stati membri di prevedere anche forme di segnalazione "*extra moenia*"⁸¹⁰. L'art. 61, par.1, dispone

⁸⁰³ Dovrebbero infatti trovare applicazione le tutele previste dall'art. 6, comma 2-*quater*, del D.lgs. 231/2001, a prescindere dal fatto che il soggetto obbligato abbia predisposto un modello organizzativo di gestione. Il citato articolo prevede inoltre che, in caso di controversie, spetti al datore di lavoro l'onere di dimostrare che tali misure, adottate successivamente alla segnalazione, siano fondate su ragioni estranee alla medesima, essendo viceversa sufficiente per il dipendente la dimostrazione della consequenzialità tra la segnalazione e il provvedimento discriminatorio.

⁸⁰⁴ Cfr. Consiglio Nazionale dei Dottori Commercialisti ed Esperti Contabili e Fondazione Nazionale Commercialisti, *La disciplina del whistleblowing: indicazioni e spunti operativi per i professionisti*, <https://www.fondazioneNazionaleCommercialisti.it/> ove si osserva (p.11) che l'art. 7, comma 2, del D.lgs. 196/2003, richiamato dall'art. 48, comma 4, è stato abrogato dal D.lgs. 101/2018 e che, per effetto di quanto disposto da quest'ultimo decreto, i rinvii alle disposizioni del Codice della Privacy si intendono riferiti alle corrispondenti disposizioni del GDPR.

⁸⁰⁵ Art. 3, comma 1, della legge 179/2017. È dibattuto se la segnalazione effettuata nel rispetto dei requisiti stabiliti dalla legge costituisca causa di esclusione dell'antigiuridicità di un fatto che corrisponde, sotto il profilo oggettivo e soggettivo alla fattispecie tipica, ovvero se questa incida sulla stessa tipicità del fatto, in quanto non si configurerebbe l'offesa al bene giuridico tutelato dalla norma incriminatrice. Cfr. R. Cantone, *op. cit.*, p.14 e dottrina ivi richiamata. Per una puntuale disamina di tali reati cfr. A.F. Masiero, *op. cit.*, p. 18.

⁸⁰⁶ Cfr. R. Cantone, *op. cit.* p. 11.

⁸⁰⁷ L'art. 6, comma 2-*bis* del D.lgs. 231/2001 dispone che debbano essere predisposte adeguate sanzioni (interne) nei confronti di "chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate".

⁸⁰⁸ Cfr. Cass. Pen. Sez. V, 26 luglio 2018 (ud. 21 maggio 2018), n. 35792.

⁸⁰⁹ Le disposizioni in materia di "whistleblowing", pur essendo ispirate dalla medesima ratio di protezione del soggetto "referente", vanno pertanto tenute distinte da quelle previste dall'art. 38 del D.lgs. 231/2007 in materia di tutela dell'identità del segnalante e di riservatezza della segnalazione di operazione sospetta.

⁸¹⁰ La scelta compiuta dal legislatore delegato appare non condivisibile anche alla luce dei principi e dei criteri direttivi contenuti nella legge n.170/2016. L'art. 15, comma 2, lett. g), non prevedeva l'introduzione esclusiva di forme di segnalazione interna, ma si limitava a evidenziare la finalità di "incoraggiare le segnalazioni di violazioni potenziali o effettive della normativa di prevenzione dell'utilizzo del

infatti che *“gli Stati membri provvedono affinché le Autorità competenti mettano in atto meccanismi efficaci e affidabili per incoraggiare la segnalazione alle Autorità competenti di violazioni potenziali o effettive delle disposizioni nazionali di recepimento della presente direttiva”*⁸¹¹.

L'impostazione adottata nel D.lgs. 231/2007 risulta inoltre non in linea rispetto ad altre soluzioni in materia di *“whistleblowing esterno”* accolte in sede di trasposizione nell'ordinamento italiano di disposizioni euro-unitarie aventi medesimezza contenutistica rispetto al citato art. 61. Il riferimento è, nello specifico, all'approccio seguito dal legislatore nel recepimento dell'art. 71 della direttiva 2013/36/UE *“sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento”* (c.d. CRD IV), a tenore del quale *“Gli Stati membri assicurano che le Autorità competenti mettano in atto meccanismi efficaci e affidabili per incoraggiare la segnalazione alle Autorità competenti di violazioni potenziali o effettive delle disposizioni nazionali di recepimento della presente direttiva e del regolamento (UE) n. 575/2013”*⁸¹². Il D.lgs. 72/2015, con cui tale direttiva è stata recepita, ha infatti introdotto all'interno del D.lgs. 385/1993 (*“TUB”*) gli artt. 52-*bis* e 52-*ter*, i quali prevedono procedure di segnalazione sia *“interna”* agli intermediari⁸¹³ che *“esterna”*. In particolare, l'art. 52-*ter*, comma 1, dispone che la Banca d'Italia (nella veste di autorità di vigilanza prudenziale) possa ricevere, da parte del personale delle banche e delle relative capogruppo segnalazioni che si riferiscono a violazioni riguardanti le norme del titolo II e III del TUB, nonché riguardanti altri atti dell'Unione europea direttamente applicabili nelle stesse materie. Le informazioni trasmesse dal *“whistleblower”*, ove rilevanti, vengono adoperate dalla Banca esclusivamente nell'esercizio delle funzioni di vigilanza e per il perseguimento delle finalità previste dall'art. 5 (art. 52-*ter*, comma 3), vale a dire *“sana e prudente gestione dei soggetti vigilati, stabilità complessiva, efficienza e competitività del sistema finanziario, nonché osservanza delle disposizioni in materia creditizia”*⁸¹⁴.

Analoga impostazione, basata su un *“doppio binario segnaletico”* in favore del *“whistleblower”* è stata inoltre seguita nel D.lgs. 129/2017 di trasposizione della direttiva 2014/65/UE relativa ai mercati degli strumenti finanziari (*“MIFID II”*), che ha introdotto all'interno del D.lgs. 58/1998 (*“TUF”*) gli artt. 4-*undecies*, di disciplina delle segnalazioni *“interne”*, e 4-*duodecies* sulle segnalazioni *“esterne”*. Quest'ultimo articolo disciplina, segnatamente, le segnalazioni alla Banca d'Italia e alla Consob, stabilendo che le due autorità di vigilanza ricevono, ciascuna per le materie di propria competenza, da parte del personale dei soggetti vigilati, le segnalazioni che si riferiscono a *“violazioni delle norme del TUF nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie”*⁸¹⁵.

Alla luce delle finalità sottese alle menzionate direttive di settore, distinte ed autonome rispetto a quelle, trasversali, di prevenzione del sistema economico finanziario poste alla base della direttiva n.849, non può condividersi l'opzione ermeneutica secondo cui il *“whistleblowing esterno”* in materia di riciclaggio non sarebbe *“meritevole”* di una propria autonomia normativa in quanto *“assorbito”* nelle procedure previste dall'art. 52-*ter* del TUB, come invece sostenuto anche in sede di predisposizione del D.lgs.125/2019, di trasposizione della direttiva UE 2018/843 (quinta direttiva) e di parti della precedente direttiva n.849 non ricomprese nel D.lgs.90/2017. Nel relativo schema di decreto è stato infatti rimarcato che la previsione di *“meccanismi di reporting di eventuali violazioni commesse dai soggetti sottoposti alla vigilanza delle Autorità competenti risponde ad una esigenza che trascende la materia antiriciclaggio e interessa tutti gli ambiti della disciplina cui sono soggetti gli intermediari bancari e finanziari”* e che, pertanto, *“con riguardo alla disciplina antiriciclaggio, si ritiene che il meccanismo per il “whistleblowing” previsto dalla disciplina bancaria rappresenti un canale idoneo ad assicurare agli intermediari obbligati anche la comunicazione delle violazioni rilevanti della disciplina antiriciclaggio”*.

sistema finanziario a scopo di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo”.

⁸¹¹ La mancata attuazione di norme di incoraggiamento del *“whistleblowing”* contenute nell'art. 61, par.1 e par.2 è stata censurata dalla Commissione europea nell'ambito della procedura di infrazione ex art. 258 TFUE avviata nei confronti dell'Italia con lettera di costituzione in mora del 7 marzo 2019 per l'incompleto recepimento della quarta direttiva; cfr. il dossier delle Camere del 15 luglio 2019 <https://www.senato.it/service/PDF/PDFServer/BGT/01118721.pdf>.

⁸¹² Anche la disposizione di cui al par. 3 dell'art. 71 risulta sovrapponibile a quella contenuta nell'analogo paragrafo dell'art. 61 della quarta direttiva; entrambe, infatti, impongono l'obbligo di predisporre procedure di segnalazioni interne attraverso canali *“specifici, autonomi e indipendenti”*.

⁸¹³ Nel dettaglio, l'art. 52-*bis* dispone che le banche e le relative capogruppo adottino procedure specifiche *“per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria”*. Disposizioni attuative di tale articolo sono contenute nella Circolare n.285/1993 della Banca d'Italia.

⁸¹⁴ L'art. 52-*ter* è stato da ultimo novellato dal D.lgs. 223/2016, con il quale è stato introdotto il comma 4-*bis*, che prevede scambi di informazioni reciproci tra la Banca d'Italia e la BCE sulle segnalazioni ricevute.

⁸¹⁵ Si evidenzia che un'analoga impostazione è stata infine seguita anche in sede di attuazione delle procedure di segnalazione previste dalla direttiva UE) 2016/97 di disciplina del settore assicurativo. Il D.lgs. 68/2018 ha infatti introdotto al riguardo gli artt. 10-*quater* (segnalazioni interne) e 10-*quinqies* (segnalazioni all'IVASS) all'interno del D.lgs. 209/2005 (*“Codice delle assicurazioni”*).

La descritta impostazione, oltre a non essere aderente alla lettera dello stesso art. 52-ter, espressamente incentrato sulla segnalazione di violazioni afferenti la normativa *latu sensu* “prudenziale”, si discosta dall’art. 61 della quarta direttiva laddove procede ad una non corretta sovrapposizione tra “Autorità competenti” in materia di riciclaggio, deputate a ricevere le segnalazioni di violazioni e “autorità di vigilanza di settore”. Pur volendo infatti accettare tale “forzatura” del dato normativo con riferimento alla possibilità di inoltrare segnalazioni in materia di violazione della disciplina antiriciclaggio alle autorità di vigilanza di settore, facendo leva sulle rispettive procedure di segnalazione “esterna” già esistenti, resterebbe in ogni caso pregiudicata la possibilità di uno “sbocco” esterno per le segnalazioni dei dipendenti dei soggetti obbligati non vigilati⁸¹⁶, in contrasto con il contenuto della direttiva.

È pertanto auspicabile, *de iure condendo*, un intervento legislativo che introduca disposizioni comuni a tutti i soggetti obbligati in materia di segnalazione “esterna” delle violazioni della disciplina antiriciclaggio e che individui un’Autorità destinataria unica per tutti i soggetti, quantomeno con riferimento ad alcuni tipi di violazione. Le modifiche all’art. 61 introdotte dalla direttiva 2018/843, peraltro, sembrano riconoscere con maggiore nettezza che tali segnalazioni possano essere indirizzate anche alle FIU⁸¹⁷.

Si evidenzia infine che la direttiva UE 2019/1937, non ancora recepita in Italia, ha introdotto disposizioni armonizzate riguardanti “la protezione delle persone che segnalano violazioni del diritto dell’Unione”. L’ambito di applicazione della direttiva risulta tuttavia residuale rispetto alle citate direttive di settore⁸¹⁸.

8. Le comunicazioni della Pubblica amministrazione (R. Lo Santo e I. Cosenza)

L’art. 10 del D.lgs. 231/2007 disciplina il ruolo delle Pubbliche amministrazioni all’interno del sistema di prevenzione del riciclaggio e del finanziamento del terrorismo.

Nel vigente quadro normativo, le Pubbliche amministrazioni sono infatti tenute a collaborare attivamente con le Autorità preposte alla prevenzione del riciclaggio, in quanto ritenute in posizione privilegiata per individuare, e quindi prevenire, fenomeni illeciti⁸¹⁹. L’attività amministrativa, volta al perseguimento del pubblico interesse, porta gli uffici pubblici a operare in contatto con soggetti esterni, portatori di propri interessi di carattere privato, imprenditoriale o professionale. È su questo rapporto con l’esterno che la normativa antiriciclaggio pone la propria attenzione: il *modus operandi* del soggetto con cui l’amministrazione entra in relazione, può presentare profili di anomalia tali da destare il “sospetto” che il soggetto medesimo sia coinvolto in attività di riciclaggio ovvero stia utilizzando fondi provenienti da attività criminosa. Peraltro, i procedimenti amministrativi hanno spesso ad oggetto la gestione di somme di denaro anche ingenti, come tali particolarmente appetibili da parte di criminali e potenzialmente oggetto di attività illecite (tramite condotte distrattive o corruttive), che possono

⁸¹⁶ Ad esempio, il “whistleblowing esterno” sarebbe precluso al dipendente che opera presso un prestatore di servizi in materia di valute virtuali (c.d. VASP).

⁸¹⁷ Il novellato art. 61 oltre ad ammettere la possibilità di inoltro delle segnalazioni agli organismi di autoregolamentazione (par. 1), dispone infatti che “*gli Stati membri garantiscono che le persone, inclusi i lavoratori dipendenti e i rappresentanti del soggetto obbligato, che segnalano un caso sospetto di riciclaggio o di finanziamento del terrorismo, internamente o alla FIU, siano tutelati legalmente da qualsiasi minaccia o atto ostile o di ritorsione, in particolare da atti avversi o discriminatori in ambito lavorativo*”, nonché che questi abbiano “*diritto a presentare una denuncia in condizioni di sicurezza*” e “*godano del diritto a un ricorso effettivo per tutelare i loro diritti*” (par.3). Pare plausibile ritenere che le disposizioni di recente introduzione riguardino la tutela da accordare al “whistleblower” che denuncia una violazione alla FIU e non al soggetto che segnala un’operazione sospetta; non si spiegherebbe, altrimenti, la contestuale introduzione di garanzie pressoché identiche anche all’interno dell’art. 38 della direttiva al fine di rafforzare i presidi di confidenzialità e riservatezza in favore del segnalante.

⁸¹⁸ L’art. 3, par. 1, stabilisce infatti che “*laddove siano previste norme specifiche sulla segnalazione delle violazioni negli atti settoriali dell’Unione elencati nella parte II dell’allegato si applicano tali norme*”; tra questi viene ricompresa la direttiva 2015/849. Il legislatore italiano ha tardivamente definito principi e criteri direttivi di trasposizione della direttiva n. 1937 all’interno dell’art. 13 della Legge n.127/2022.

⁸¹⁹ La previsione di obblighi di collaborazione attiva a carico degli uffici della Pubblica amministrazione è presente sin dalle origini della normativa antiriciclaggio. Già il DL 3 maggio 1991, n. 143 (convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197) includeva tra i destinatari degli obblighi anche gli “uffici della Pubblica amministrazione, ivi compresi gli uffici postali”. Con il successivo D.lgs. 20 febbraio 2004, n. 56, il legislatore esonerava gli uffici delle Pubbliche amministrazioni dall’applicazione delle disposizioni in materia di identificazione e registrazione, mantenendo tuttavia in capo agli stessi l’obbligo di segnalazione delle operazioni sospette. Tale impostazione è rimasta inalterata anche a seguito dell’emanazione del D.lgs. 231/2007, adottato in attuazione della terza direttiva antiriciclaggio. In attuazione della previgente normativa, il Decreto del Ministero dell’Interno, emanato, su proposta della UIF, il 25 settembre 2015 dettava rilevanti specificazioni di ordine organizzativo e operativo per l’applicazione dei presidi e recava un elenco di indicatori di anomalia destinati ad agevolare l’individuazione delle operazioni sospette di riciclaggio e di finanziamento del terrorismo da parte degli uffici della Pubblica amministrazione.

costituire il presupposto di attività di riciclaggio. Si richiede pertanto ai soggetti pubblici che gestiscono tali risorse di innalzare la soglia di attenzione per preservarne il corretto utilizzo.

La scelta di estendere anche agli uffici pubblici l'applicazione dei presidi antiriciclaggio scaturisce dunque dall'esigenza di far fronte al rischio che l'amministrazione venga in contatto con soggetti coinvolti in attività criminali e che l'azione pubblica, di conseguenza, concorra involontariamente ad alterare il fisiologico funzionamento dei circuiti economici. La normativa antiriciclaggio, inoltre, viene a collocarsi nel più ampio alveo delle regole tese a tutelare l'integrità e la legalità dell'attività amministrativa e a garantirne l'efficienza anche in termini di corretta allocazione dei flussi di spesa pubblica.

In occasione del recepimento della quarta direttiva antiriciclaggio, il D.lgs. 25 maggio 2017, n. 90, ha ridefinito il perimetro e il ruolo degli uffici pubblici all'interno del sistema di prevenzione. Nel novellato quadro normativo, le Pubbliche amministrazioni non sono più formalmente incluse nel novero dei soggetti obbligati, ma sono comunque chiamate a fornire un contributo attivo al sistema, mediante la "comunicazione" alla UIF di "*dati e informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell'esercizio della propria attività istituzionale*". Il legislatore ha scelto così di collocare le amministrazioni su un piano diverso rispetto ai soggetti obbligati, pur confermando l'importante apporto che esse possono offrire al sistema antiriciclaggio⁸²⁰.

Il comma 1 dell'art. 10 individua gli uffici delle Pubbliche amministrazioni⁸²¹ tenuti a prestare la propria "collaborazione attiva" all'interno del sistema di prevenzione. In particolare, vengono richiamati gli uffici pubblici competenti allo svolgimento di compiti di amministrazione attiva o di controllo, nell'ambito di: procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione; procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al codice dei contratti pubblici; procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati. Il legislatore ha ritenuto i procedimenti amministrativi sopra elencati i più esposti a rischi di illecito, anche in ragione del rilevante legame che essi comportano tra l'amministrazione competente e l'economia e il mercato.

Il comma 2 dell'art. 10 consente poi al CSF di individuare, in funzione del rischio di riciclaggio o di finanziamento del terrorismo, anche sulla base dell'analisi nazionale del rischio, ulteriori procedimenti ai quali estendere l'applicazione degli obblighi di collaborazione attiva. Analogamente, il CSF può enucleare categorie di attività amministrative svolte dalle Pubbliche amministrazioni responsabili dei procedimenti di cui al comma 1 da escludere dall'ambito di applicazione della disposizione in esame, in quanto ritenute non a rischio⁸²².

Agli uffici pubblici così delimitati, il comma 3 richiede, innanzitutto, di mappare e valutare i rischi di riciclaggio e di finanziamento del terrorismo cui sono esposti secondo le Linee Guida elaborate dal CSF, nonché di adottare procedure interne, proporzionate alle proprie dimensioni organizzative e operative, idonee a valutare il livello di esposizione al rischio, e di indicare le misure necessarie a mitigarlo.

⁸²⁰ Il D.lgs. 90/2017, nel prevedere un dovere di "comunicazione" (e non di "segnalazione") nei confronti della UIF, ha dettato per le Pubbliche amministrazioni una disciplina ad hoc, di regime differenziato; si pone pertanto il dubbio circa la possibilità di estendere, in via interpretativa, a tali comunicazioni norme di fondamentale importanza previste per le segnalazioni di operazioni sospette. Inoltre, è rimasto aperto il tema della possibilità, per le amministrazioni, non tenute agli obblighi di adeguata verifica ma solo a quelli di comunicazione delle operazioni sospette, di identificare la titolarità effettiva delle proprie controparti al fine di garantire la massima trasparenza nelle interlocuzioni tra amministrazioni e privati, possibilità che darebbe all'azione amministrativa garanzie più profonde ed efficaci di intercettazione di fenomeni criminali e di ammissione alle procedure pubbliche di soggetti affidabili.

⁸²¹ Il decreto antiriciclaggio contiene, all'art. 1, comma 2, lett. hh), una propria definizione di "Pubbliche amministrazioni", che include "*le amministrazioni Pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, gli enti pubblici nazionali, le società partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'articolo 2359 del codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea e i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica*". Si tratta di una definizione ampia, che comprende un esteso numero di soggetti pubblici e che assume rilievo, tra l'altro, al fine di individuare i soggetti cui la UIF, ai sensi degli artt. 6, comma 5, lett. b) e 40, comma 2, del decreto può chiedere informazioni nell'ambito della propria attività di analisi delle segnalazioni (e delle comunicazioni) di operazioni sospette.

⁸²² La puntuale delimitazione del novero degli uffici pubblici tenuti ad effettuare le comunicazioni alla UIF implica che non è opevita per altri soggetti, operanti in settori non richiamati dall'art. 10 del decreto, la possibilità di portare all'attenzione della UIF eventuali situazioni a rischio intercettate tramite lo strumento della comunicazione. Si rischia, così, di escludere a priori soggetti pubblici ed attività amministrative che potrebbero, invece, fornire un concreto contributo alla prevenzione di fenomeni criminali in altri ambiti ritenuti a rischio. Resta da auspicare, sotto tale profilo, che il CSF utilizzi la facoltà (ad oggi mai esercitata) di ampliare il novero di attività pubbliche cui applicare la normativa antiriciclaggio.

In ragione della forte eterogeneità dei soggetti pubblici coinvolti, il legislatore ha ritenuto di non adottare regole organizzative dettagliate e di prediligere un approccio “funzionale”, rimettendo la scelta dei presidi interni alle singole amministrazioni nell'esercizio della propria autonomia organizzativa⁸²³.

A prescindere dall'organizzazione interna prescelta, alle Pubbliche amministrazioni si chiede di individuare, con provvedimento formalizzato, un “gestore”, quale soggetto delegato a valutare ed eventualmente effettuare le comunicazioni alla UIF. Nel Provvedimento del 23 aprile 2018, la UIF ha infatti specificato che *“al fine di garantire efficacia e riservatezza nella gestione delle informazioni, la UIF considera quale proprio interlocutore per tutte le comunicazioni e i relativi approfondimenti la persona individuata quale “gestore” e la connessa struttura organizzativa indicate in sede di adesione al sistema di comunicazione on-line”*. Tramite l'iscrizione al Portale della Banca d'Italia, Infostat-UIF, le amministrazioni si pongono materialmente in condizione di inviare alla UIF le comunicazioni di operazioni sospette e attraverso l'indicazione del “gestore”, si consente altresì all'Unità di individuare un interlocutore di riferimento al quale inoltrare eventuali richieste di informazioni necessarie per l'approfondimento finanziario delle segnalazioni.

Il principale contributo richiesto agli uffici pubblici nell'ambito dei procedimenti elencati nel comma 1 dell'art. 10 consiste nel comunicare alla UIF *“dati e informazioni concernenti le operazioni sospette di cui vengano a conoscenza nell'esercizio della propria attività istituzionale”*, al fine di *“consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio”* (art. 10, comma 4).

Analogamente alla segnalazione di operazioni sospette, la comunicazione è sempre il risultato di un autonomo processo valutativo che l'operatore è chiamato a svolgere sulla base del patrimonio informativo a sua disposizione, tenendo conto degli elementi soggettivi e oggettivi della fattispecie concreta che ha di fronte. Ciò che, in particolare, si richiede agli uffici pubblici è di esaminare il vasto corredo informativo raccolto ai fini dell'istruttoria procedimentale con “approccio critico”, focalizzando la propria attenzione sulle eventuali anomalie che possono indurre a considerare una determinata operazione come sospetta, anche integrando dati acquisiti per finalità diverse e spesso conservati presso archivi o uffici separati. Un simile “approccio critico” può essere sviluppato dai singoli operatori solo grazie ad una *expertise* che matura nel tempo, ma un forte ausilio può derivare dall'attività di formazione che le amministrazioni pubbliche sono tenute a organizzare a favore del personale⁸²⁴, così come dallo sfruttamento degli strumenti di supporto elaborati dalla UIF (tra cui gli indicatori di anomalia).

La comunicazione di operazioni sospette alla UIF è adempimento diverso e distinto dalla denuncia di reato all'Autorità giudiziaria che pubblici ufficiali e incaricati di pubblico servizio sono tenuti a effettuare, in base all'art. 331 del Codice di procedura penale, quando, per le informazioni acquisite nell'esercizio della funzione ovvero a causa delle funzioni o del servizio, *“hanno notizia di un reato perseguibile d'ufficio”* e che si fonda sull'individuazione di fatti specifici corrispondenti a una fattispecie penalmente rilevante. L'eventuale invio di una comunicazione alla UIF in relazione ai medesimi fatti non esclude l'obbligo di effettuare la denuncia in presenza dei citati presupposti.

Il comma 4, dell'art. 10 del decreto antiriciclaggio, stabilisce inoltre che *“la UIF, in apposite istruzioni, adottate sentito il Comitato di sicurezza finanziaria, individua i dati e le informazioni da trasmettere, le modalità e i termini della relativa comunicazione nonché gli indicatori per agevolare la rilevazione delle operazioni sospette”*. In attuazione di tale disposizione l'Unità, sentito il CSF, il 23 aprile 2018 ha adottato un Provvedimento nel

⁸²³ Sotto il profilo dei modelli organizzativi, è frequente l'integrazione tra presidi antiriciclaggio e presidi anticorruzione, con la nomina in qualità di “gestore” del medesimo soggetto che svolge la funzione di “Responsabile della prevenzione della corruzione e della trasparenza”. La scelta, di per sé legittima e in qualche modo suggerita dal previgente DM del 25 settembre 2015, non deve tuttavia indurre a percepire i presidi antiriciclaggio come sovrapponibili a quelli anticorruzione. Mentre le misure anticorruzione chiedono agli uffici pubblici di focalizzare l'attenzione al proprio interno, al fine di prevenire possibili abusi a scopo corruttivo, la disciplina antiriciclaggio richiede uno sguardo più ampio: le analisi a fini antiriciclaggio devono essere orientate alla valutazione del rischio dell'operatività dell'utente che entra in relazione con l'ufficio pubblico e riferite a tutte le attività potenzialmente rilevanti, anche a prescindere dall'eventuale ricorrenza episodi corruttivi. D'altro canto, tra i sistemi di prevenzione del riciclaggio e della corruzione sussistono evidenti interrelazioni che possono – e devono – essere valorizzate. La prevenzione, che costituisce uno dei concetti fondamentali su cui entrambi gli apparati si reggono, si accompagna al principio-guida dell'integrità intesa quale garanzia di tutela dei soggetti coinvolti (intermediari e altri operatori, nel caso dell'antiriciclaggio; Pubbliche amministrazioni, nel caso dell'anticorruzione) da illecite infiltrazioni. Inoltre, entrambi i sistemi poggiano sul concetto di rischio, quale parametro in base al quale calibrare le misure preventive, e richiedono alle singole amministrazioni di esplorare le proprie aree di vulnerabilità e di adottare le misure di mitigazione ritenute di volta in volta più appropriate. Questa attività di analisi può essere condotta in modo unitario, in una logica di “valutazione e gestione integrata dei rischi” di corruzione e di riciclaggio cui le amministrazioni sono esposte.

⁸²⁴ In base al comma 5, le Pubbliche amministrazioni devono adottare, nel quadro dei programmi di formazione continua del personale (realizzati ex art. 3 del D.lgs. 1° dicembre 2009, n. 178), misure idonee ad assicurare il riconoscimento, da parte dei propri dipendenti delle fattispecie meritevoli di essere comunicate alla UIF.

quale vengono fornite specifiche indicazioni in ordine al contenuto e alle modalità di inoltro alla UIF delle comunicazioni.

Il citato Provvedimento reca, in allegato, un elenco di indicatori di anomalia volti ad agevolare la rilevazione delle operazioni sospette da parte degli uffici delle Pubbliche amministrazioni. Tali indicatori, che riprendono in larga parte quelli già emanati con il decreto del Ministero dell'Interno del 25 settembre 2015, sulla base delle previgenti previsioni normative in materia di obblighi antiriciclaggio della P.A., sono suddivisi in 3 macro-categorie: indicatori a carattere soggettivo, connessi con l'identità o il comportamento del soggetto cui è riferita l'operazione; indicatori a carattere oggettivo, connessi con le modalità (di richiesta o esecuzione) delle operazioni; indicatori specifici per settore di attività (appalti e contratti pubblici; finanziamenti pubblici; immobili e commercio).

Le informazioni provenienti dagli uffici pubblici, una volta trasmesse tramite il portale Infostat-UIF, vanno ad alimentare il patrimonio informativo dell'Unità e costituiscono oggetto di analisi. Con la riforma del 2019, il legislatore è intervenuto sull'art. 40 del decreto antiriciclaggio al fine di precisare che le comunicazioni delle Pubbliche amministrazioni, analogamente alle segnalazioni di operazioni sospette trasmesse dai soggetti obbligati, sono esaminate dalla UIF sotto il profilo finanziario e poi trasmesse agli organi competenti per i successivi approfondimenti investigativi.

Delicato e denso di problematiche applicative è, infine, il tema delle conseguenze del mancato adempimento dei doveri antiriciclaggio da parte degli uffici delle Pubbliche amministrazioni. Nell'attuale quadro normativo mancano infatti disposizioni sanzionatorie efficaci, che "incentivino" la corretta applicazione della normativa nel settore pubblico, così come avviene per i soggetti obbligati.

In base al comma 6 dall'art. 10 del D.lgs. 231/2007, l'inosservanza degli obblighi previsti dal medesimo art. 10 assume rilievo ai fini della responsabilità dirigenziale di cui all'art. 21, comma 1-*bis*, del D.lgs. 165/2001 e può, dunque, comportare una decurtazione fino all'ottanta per cento della retribuzione di risultato del dirigente responsabile della violazione. Si tratta di una misura che appare oggi di difficile attuazione, stante la ancora scarsa consapevolezza della materia all'interno del comparto pubblico, ma che dovrà essere valorizzata per conseguire l'efficace implementazione dei presidi antiriciclaggio, rendendone effettiva l'applicazione nei casi di mancata attivazione della collaborazione attiva.

Le comunicazioni del settore pubblico rappresentano infatti un flusso informativo ancora molto contenuto. I controlli antiriciclaggio, anche laddove effettuati, vengono spesso intesi in modo formale e ridotti alla mera compilazione di *check list* costruite sulla base degli indicatori di anomalia che, pur funzionali all'avvio della collaborazione, rischiano di burocratizzare e rendere automatico l'invio della comunicazione alla UIF, in contrasto con lo spirito della normativa e con il significato stesso e la portata degli indicatori. L'esiguità del flusso di comunicazioni della PA è indicativa di una consapevolezza ancora ridotta del contributo che essa può dare all'azione di prevenzione come fonte preziosa di informazioni per intercettare fattispecie a rischio di riciclaggio e per arricchire il patrimonio informativo della UIF, di cui beneficia anche l'analisi delle segnalazioni provenienti da altri attori del sistema di prevenzione del riciclaggio. D'altro canto, l'implementazione di procedure specifiche nell'ambito delle attività amministrative potrebbe rappresentare un importante fattore di miglioramento della qualità dell'azione amministrativa.

CAPITOLO 7

La prevenzione e il contrasto del finanziamento del terrorismo e dell'attività dei paesi che minacciano la pace e la sicurezza internazionale

(a cura di G. Ilacqua)

Premessa (A. Cassetta e L. Baron)

Il contrasto al finanziamento del terrorismo rappresenta una componente essenziale della strategia internazionale di lotta al terrorismo, la cui complessità richiede necessariamente un approccio integrato “multidimensionale” (attività di indagine e di intelligence, dialogo interculturale e interreligioso, contrasto finanziario, sicurezza dei trasporti, strategia di prevenzione della radicalizzazione).

Le organizzazioni terroristiche e i singoli terroristi hanno costante bisogno di finanziamenti: per sostenere le proprie reti, per la propaganda e il reclutamento, per le spese logistiche (trasporti, alloggi, documenti, armi ed equipaggiamenti) finalizzate al compimento degli atti terroristici. Diventa fondamentale per l'attività di prevenzione e contrasto bloccare le fonti di finanziamento e utilizzare in modo ottimale ogni informazione finanziaria utile per smantellare le organizzazioni terroristiche.

Il sistema di prevenzione del finanziamento del terrorismo si basa su strutture, regole e metodologie coincidenti con quelle che formano il sistema di prevenzione del riciclaggio. La ragione di questa impostazione si fonda su un'analogia di fondo tra i due fenomeni: il riciclaggio e il finanziamento del terrorismo rappresentano entrambi momenti di interazione delle attività criminali con il sistema economico-finanziario; nel primo caso, in genere, “a valle” del reato, per occultare o godere dei proventi di origine illecita; nel secondo, “a monte” del reato, per l'approvvigionamento delle risorse finanziarie necessarie a sostenere le azioni e le organizzazioni terroristiche. Questa interazione rappresenta, tanto per il riciclaggio che per il finanziamento del terrorismo, un momento di emersione e, quindi, di vulnerabilità che le Autorità devono saper sfruttare per intercettare e indagare i fenomeni criminali con la collaborazione attiva del settore privato.

Analogamente al riciclaggio, il finanziamento del terrorismo costituisce una grave minaccia per l'economia legale e può determinare effetti destabilizzanti, soprattutto per il sistema bancario e finanziario; la natura mutevole della minaccia, facilitata anche dalle innovazioni dei servizi finanziari e dall'evoluzione tecnologica, richiede un costante adattamento dei presidi di prevenzione e contrasto.

L'estensione delle misure antiriciclaggio si è affiancata all'azione specifica di contrasto del terrorismo imperniata sulle liste pubbliche dei soggetti “designati” dalle istituzioni internazionali e sulle misure di “congelamento delle loro risorse”. Il processo di integrazione tra sistemi di contrasto al riciclaggio e al finanziamento del terrorismo è stato realizzato a partire dagli anni 2000, traendo impulso dai gravi attentati terroristici del 2001 negli Stati Uniti e ha trovato base regolamentare in un'articolata sequenza di iniziative e provvedimenti delle Nazioni Unite, dell'Unione europea, del Gruppo di Azione Finanziaria Internazionale.

Negli ultimi anni la minaccia terroristica si è manifestata con crescente, drammatica intensità, assumendo molteplici forme, con la compresenza di organizzazioni terroristiche che controllano territori, organizzazioni affiliate ad articolati network, cellule di dimensioni ridotte, terroristi individuali, con riflessi sotto il profilo dei fabbisogni e delle fonti di finanziamento. In risposta, gli organismi internazionali hanno adottato una serie di iniziative volte a potenziare il sistema di prevenzione, rafforzando la condivisione di informazioni tra le Autorità e agevolando la collaborazione degli operatori.

1. Il quadro normativo internazionale (A. Cassetta e L. Baron)

Le prime linee strategiche nel contrasto finanziario al terrorismo internazionale sono state tracciate dall'ONU, con la *Convenzione di New York* (1999), che per la prima volta ha riconosciuto una rilevanza autonoma alla nozione di finanziamento del terrorismo rispetto a quella di terrorismo internazionale, ponendo le basi giuridiche per la successiva “criminalizzazione” del reato. Con la stipula della Convenzione sono state infatti poste le basi a livello internazionale per la repressione penale del fenomeno e per la successiva estensione al medesimo del sistema di presidi già esistente per la prevenzione e il contrasto del riciclaggio.

Il provvedimento ha preso forma in un contesto storico particolare, in cui la comunità internazionale era stata da poco scossa dagli attentati terroristici alle sedi diplomatiche statunitensi in Kenya e Tanzania, che causarono centinaia di vittime; si rafforzò in quel periodo la consapevolezza che il terrorismo di *Al-Qaeda* e Bin Laden era ormai diventato una minaccia globale, da contrastare necessariamente anche sul piano finanziario, con un'attività coordinata e sinergica tra tutti i paesi e le Autorità coinvolte.

A quel periodo risalgono anche le prime misure adottate dal Consiglio di Sicurezza dell'ONU per il “congelamento” dei fondi e delle attività detenute dai terroristi; si tratta, in particolare, della Risoluzione n. 1267 (1999), relativa ai soggetti ed entità collegati all'organizzazione *Al-Qaeda* e ai *Talebani*⁸²⁵, e della Risoluzione 1373 (2001), che ne ha significativamente ampliato la portata applicativa, estendendo queste misure a tutti i soggetti coinvolti in attività terroristiche individuati dai Paesi membri, indipendentemente dall'affiliazione ideologica e dall'ambito territoriale di azione⁸²⁶.

Il meccanismo delle liste di “congelamento” costituisce il primo dei due “pilastri” su cui è fondato il sistema internazionale di prevenzione e contrasto del finanziamento del terrorismo; si tratta di un presidio preventivo interdittivo funzionale a bloccare ogni forma di utilizzo o di trasferimento di fondi – o di ogni altro bene suscettibile di produrre ricchezza – da parte di soggetti o entità elencati nelle *blacklist* pubbliche; il medesimo presidio è stato peraltro esteso dall'ONU anche ad altre fattispecie rilevanti per la minaccia della pace e della sicurezza internazionale, per contrastare, ad esempio, le attività dei regimi accusati di gravi violazioni dei diritti umani o di non rispettare i trattati internazionali, anche in tema di proliferazione nucleare.

Le Risoluzioni del Consiglio di Sicurezza dell'ONU, hanno trovato recepimento nello spazio europeo attraverso una serie di Posizioni e Decisioni Comuni e di Regolamenti esecutivi, che trovano immediata applicazione tra i Paesi membri; rilevano in particolare il regolamento CE n. 337/2000 (Risoluzione n. 1267/1999)⁸²⁷ e il regolamento CE n. 2580/2001 (Risoluzione n. 1373/2001). Il meccanismo di aggiornamento delle liste avviene attraverso provvedimenti emendativi dei predetti Regolamenti, che alimentano la lista consolidata europea (*Financial Security Database*).

Il quadro comunitario in materia penale è stato armonizzato per la prima volta con la Decisione Quadro 2002/475/GAI, adottata dal Consiglio europeo in seguito agli attentati dell'11 settembre, che, nel tipizzare i reati terroristici, ha richiesto agli Stati membri di allineare le loro normative e introdurre pene adeguate⁸²⁸. L'intero sistema di misure di prevenzione in materia di contrasto al riciclaggio è stato poi esteso al contrasto al finanziamento del terrorismo in occasione della direttiva 2005/60/CE (terza direttiva antiriciclaggio).

La nuova fase del terrorismo *jihadista* e della minaccia dell'ISIL, caratterizzata dall'occupazione da parte dell'organizzazione terroristica di interi territori in Medio Oriente e da una nuova scia di attentati in Europa, tra il 2015 e il 2016 (attentati di Parigi, Bruxelles, Nizza e Berlino), ha portato a un generale lavoro di revisione e rafforzamento delle misure di contrasto al finanziamento del terrorismo, anche per

⁸²⁵ La Risoluzione 1267/1999 è stata in seguito “scissa” in due provvedimenti separati per distinguere *Al-Qaeda* (Risoluzione n. 1988/2011) e i *Talebani* (Risoluzione n. 1989/2011).

⁸²⁶ Con le due Risoluzioni citate sono stati creati, tra l'altro, appositi Comitati (1267 Committee e Counter Terrorism Committee), incaricati di gestire i processi di gestione delle liste (c.d. “listing” e “delisting”) e di monitorare l'effettiva applicazione delle sanzioni internazionali emanate. Con le Risoluzioni ONU n. 2082/2012 e n. 2083/2012 sono stati in seguito rivisti i criteri per la designazione e per la gestione delle liste.

⁸²⁷ In seguito abrogato dal regolamento CE n. 467/2001, che è stato a sua volta sostituito dal regolamento CE n. 881/2002.

⁸²⁸ La Decisione è stata in seguito modificata attraverso la Decisione Quadro 2008/919/GAI, che ne ha ampliato la portata definendo nuove condotte terroristiche.

tenere conto delle nuove forme del fenomeno, in particolare quello dei “combattenti terroristi stranieri” (*foreign terrorist fighters*) e delle relative forme di sostegno materiale e finanziario.

La risposta internazionale si è tradotta in una nuova serie di Risoluzioni del Consiglio di Sicurezza dell'ONU: nel condannare fermamente le azioni dell'ISIL nei territori occupati, le Risoluzioni n. 2170/2014 e n. 2178/2014 hanno esteso agli affiliati all'ISIL e al Fronte *al-Nusra* le sanzioni finanziarie già imposte ai membri di Al-Qaeda, e richiesto ai Paesi membri di adottare misure specifiche per contrastare il fenomeno dei *foreign terrorist fighters*; le Risoluzioni n. 2199/2015 e n. 2253/2015 hanno sistematizzato e rafforzato il sistema sanzionatorio esistente e introdotto misure volte a bloccare i flussi di finanziamento dell'ISIL derivanti dalle attività di controllo dei territori occupati, quali i rapimenti a scopo di riscatto, il commercio del petrolio e quello dei beni archeologici trafugati; le Risoluzioni n. 2322/2016 e n. 2341/2017 hanno infine dato centralità alle attività di scambio di informazioni e alla collaborazione tra gli Stati e le Autorità a vario titolo coinvolte nel contrasto al fenomeno.

Sul piano europeo, la Commissione, nel febbraio del 2016, ha presentato un *Piano d'Azione* per rafforzare la lotta contro il finanziamento del terrorismo, delineando una serie di interventi mirati anche per il presidio dell'utilizzo degli strumenti di pagamento esposti a maggiore rischio e per il potenziamento dei poteri delle Autorità coinvolte e degli scambi informativi. La nuova direttiva 2017/541/UE sulla lotta contro il terrorismo ha sostituito la Decisione 2002/475/GAI.

Il secondo pilastro nella lotta al finanziamento del terrorismo è costituito dalla estensione a questo fenomeno del sistema di presidi già esistenti per il contrasto al riciclaggio.

In risposta agli attentati alle Torri Gemelle dell'11 settembre 2001, il GAFI ha allargato prontamente il proprio mandato al contrasto del finanziamento del terrorismo, elaborando alcune linee di indirizzo, anche per dare rapida e concreta attuazione alle Risoluzioni dell'ONU.

In tale ambito, a poche settimane di distanza dai drammatici eventi (ottobre 2001), il GAFI ha emanato le 9 *Raccomandazioni Speciali* specificamente dedicate al finanziamento del terrorismo⁸²⁹. Le Raccomandazioni Speciali, oltre a delineare gli ambiti di applicazione operativa delle Risoluzioni ONU, definivano alcuni *standard* regolamentari per rafforzare i presidi normativi di alcuni settori o ambiti di operatività maggiormente esposti al rischio di finanziamento del terrorismo, quali i *money transfer*, i bonifici transfrontalieri, i trasferimenti di contante al seguito e le organizzazioni *non-profit*.

In occasione della revisione generale degli *standard*, le Raccomandazioni Speciali sono state integrate nelle “nuove” 40 Raccomandazioni (febbraio 2012), regolarmente aggiornate, il cui campo d'azione include tutti gli ambiti di competenza del FATF/GAFI (prevenzione e contrasto del riciclaggio, del finanziamento del terrorismo e del finanziamento dei programmi di proliferazione delle armi di distruzione di massa). Le Raccomandazioni trattano in una sezione dedicata al finanziamento del terrorismo i temi della criminalizzazione del fenomeno (*terrorist financing offence*), l'applicazione delle sanzioni finanziarie internazionali (*targeted financial sanctions*) e delle organizzazioni no-profit (*Non-profit organisations*). Le indicazioni del GAFI su questi temi, oltre alle note interpretative, sono state integrate nel tempo da *guidance, guidelines e best practices*⁸³⁰.

2. La normativa nazionale (A. Cassetta e L. Baron)

La normativa nazionale si è adeguata nel tempo alla evoluzione del quadro giuridico internazionale. A breve distanza dagli attentati del 2001, il decreto legge n. 374/2001 (convertito dalla legge n. 438/2001), in linea con quanto imposto dalla *Convenzione di New York* e dalle *Raccomandazioni Speciali*, ha rinnovato l'art. 270-bis c.p. (associazione con finalità di terrorismo) e introdotto l'art. 270-ter c.p. (assistenza agli associati), integrando nelle condotte perseguite anche il finanziamento delle organizzazioni terroristiche. Con il decreto legge n. 369/2001 (convertito con legge n. 431/2001) sono state fornite istruzioni per dare concreta esecuzione alle misure di congelamento, istituendo il Comitato di Sicurezza Finanziaria (CSF) quale organismo di coordinamento tra le Autorità e le forze di polizia impegnate nell'attività di prevenzione e contrasto, le cui funzioni sono poi state estese anche alla materia del riciclaggio.

Un primo pacchetto di misure di rafforzamento è stato varato nel 2005 (a ridosso degli attentati di Londra) con il decreto legge n. 144/2005 (convertito con legge n. 155/2005), che ha ampliato, tra l'altro, le condotte delittuose, includendo l'arruolamento con finalità di terrorismo (art. 270 *quater, quinques* e

⁸²⁹ La IX Raccomandazione è stata aggiunta nel 2004.

⁸³⁰ *Guidance on Criminalising Terrorist Financing* (2015); *International best practices- targeted financial sanctions related to terrorism and terrorist financing* (2013); *Best Practices Paper on Combating the Abuse of Non-Profit Organisations* (2015).

sexies c.p.), e ha potenziato gli strumenti di indagine, controllo e prevenzione, estendendo l'impiego di alcuni presidi già utilizzati con successo per il contrasto alla criminalità organizzata.

Le nuove misure internazionali adottate in risposta alla minaccia dell'ISIS hanno trovato applicazione nel decreto legge 7/2015 (convertito con legge 43/2015), contenente un pacchetto di misure di rafforzamento dei presidi di prevenzione e contrasto.

Il provvedimento, sul piano penale, ha introdotto nuove figure di reato, quali l'organizzazione di viaggi e l'addestramento per finalità di terrorismo, incluso il loro finanziamento (art. 270-*quater*.1). In occasione della ratifica di alcune convenzioni internazionali in materia⁸³¹, con la legge 153/2016, sono state ulteriormente ampliate le fattispecie di finanziamento con finalità di terrorismo (art. 270-*quinquies*.1, c.p.).

La disciplina nazionale in tema di contrasto al finanziamento del terrorismo ha trovato organica sistemazione nel 2007, attraverso i decreti emanati in attuazione della direttiva 2005/60/CE. Il decreto legislativo 22 giugno 2007, n. 109, recante “misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei paesi che minacciano la pace e la sicurezza internazionale” costituisce sostanzialmente la cornice che da attuazione alla normativa internazionale in tema di “congelamenti”, disciplinando obblighi e adempimenti degli operatori, competenze e ruoli delle diverse Autorità coinvolte, nonché ulteriori dettagli amministrativi e sanzionatori.

Il decreto anzitutto fornisce una definizione normativa del finanziamento del terrorismo, come “qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi e risorse economiche, in qualunque modo realizzata, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzati per il compimento di una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette”.

Il decreto chiarisce poi, attraverso definizioni precise (art. 1) il significato dei congelamenti di fondi e di risorse economiche. Il “congelamento dei fondi”, secondo il dettato normativo, comporta “il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consenta l'uso dei fondi, compresa la gestione di portafoglio”⁸³².

Il “congelamento delle risorse economiche” determina “il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, l'utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia”⁸³³.

Il congelamento pertanto consiste sostanzialmente nel blocco automatico delle disponibilità finanziarie ed economiche di soggetti coinvolti in fatti di terrorismo, per la sola circostanza che gli stessi siano stati inseriti (“designati”) nelle liste antiterrorismo previste dal decreto. È fatto infatti divieto sia di mettere, direttamente o indirettamente, a disposizione dei soggetti designati fondi o risorse economiche o di stanziarli a loro vantaggio, sia di partecipare consapevolmente e deliberatamente ad attività aventi l'obiettivo o il risultato, diretto o indiretto, di aggirare le misure di congelamento.

Circa gli effetti del congelamento, il decreto 109/2007 stabilisce che i capitali liquidi e i beni mobili ed immobili, società ed aziende sottoposte al blocco non possono costituire oggetto di atti di trasferimento, disposizione o utilizzo. In tal senso, viene sancita la nullità degli atti compiuti in violazione di tale prescrizione.

Nell'ambito dei “congelamenti” riveste un ruolo fondamentale il Comitato di Sicurezza Finanziaria (CSF), di cui il decreto definisce, in una rinnovata formulazione, la composizione e le competenze (art. 3 del D.lgs. 109/2007). Si tratta dell'organismo nazionale a cui sono attribuiti in particolare i poteri di formulare le proposte di designazione nelle liste ai competenti organismi delle Nazioni Unite e dell'Unione europea, nonché tutti gli altri adempimenti connessi (esenzioni, *delisting*, scambio di informazioni tra le Autorità che vi partecipano etc.).

⁸³¹ Convenzione del Consiglio d'Europa per la prevenzione del terrorismo (Varsavia, 16 maggio 2005) e Convenzione internazionale per la soppressione di atti di terrorismo nucleare (New York, il 14 settembre 2005).

⁸³² Per “fondi” il decreto intende “attività ed utilità finanziarie di qualsiasi natura, possedute anche per interposta persona fisica o giuridica, compresi a titolo meramente esemplificativo: 1) i contanti, gli assegni, i crediti pecuniari, le cambiali, gli ordini di pagamento e altri strumenti di pagamento; 2) i depositi presso enti finanziari o altri soggetti, i saldi sui conti, i crediti e le obbligazioni di qualsiasi natura; 3) i titoli negoziabili a livello pubblico e privato nonché gli strumenti finanziari come definiti nell'articolo 1, comma 2, del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58; 4) gli interessi, i dividendi o altri redditi ed incrementi di valore generati dalle attività; 5) il credito, il diritto di compensazione, le garanzie di qualsiasi tipo, le cauzioni e gli altri impegni finanziari; 6) le lettere di credito, le polizze di carico e gli altri titoli rappresentativi di merci; 7) i documenti da cui risulti una partecipazione in fondi o risorse finanziarie; 8) tutti gli altri strumenti di finanziamento delle esportazioni; 9) le polizze assicurative concernenti i rami vita di cui all'articolo 2, comma 1, del decreto legislativo 7 settembre 2005, n. 209, recante il Codice delle assicurazioni private”.

⁸³³ Per “risorse economiche” il decreto intende “le attività di qualsiasi tipo, materiali o immateriali, mobili o immobili, ivi compresi gli accessori, le pertinenze e i frutti, che non sono fondi ma che possono essere utilizzate anche per interposta persona fisica o giuridica per ottenere fondi, beni o servizi”.

Sotto il profilo procedurale, il decreto prevede specifici oneri di comunicazione a carico degli intermediari finanziari e degli altri soggetti tenuti agli obblighi di collaborazione attiva, i quali devono segnalare (entro 30 giorni) l'avvenuta applicazione delle misure previste, ovvero l'esistenza di fondi e risorse economiche "congelati", all'Unità di Informazione Finanziaria e, limitatamente alle risorse economiche, anche al Nucleo Speciale Polizia Valutaria (artt. 6 e 7 del D.lgs. 109/2007)⁸³⁴.

Il decreto ripartisce i compiti tra Unità di Informazione Finanziaria, Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e Agenzia del Demanio, ai fini della esecuzione delle misure di congelamento (artt. 10, 11 e 12 del D.lgs. 109/2007). In particolare, la UIF riceve le comunicazioni relative ai congelamenti di fondi, agevola la diffusione delle *black list* dei soggetti e delle entità designate dalle istituzioni internazionali e a livello nazionale e verifica l'applicazione delle sanzioni; il NSPV riceve le comunicazioni relative alle risorse economiche congelate e riveste una funzione di interfaccia con le altre amministrazioni coinvolte, tra le quali, in particolare, con l'Agenzia del Demanio, cui compete la custodia, la conservazione e la gestione delle risorse congelate, e cura infine la notifica dell'avvenuta designazione ai diretti interessati.

Il D.lgs. 231/2007 ha armonizzato la normativa antiriciclaggio e antiterrorismo, estendendo al finanziamento del terrorismo tutte le misure preventive del contrasto al riciclaggio e, in particolare, l'adeguata verifica della clientela, la conservazione dei documenti, la segnalazione delle operazioni sospette, i controlli interni e la valutazione e gestione del rischio.

Tra gli obblighi sopra richiamati, particolare rilevanza rivestono quelli in materia di segnalazione di operazioni sospette, che attribuiscono agli intermediari finanziari un ruolo attivo e determinante nel contrasto al terrorismo, in quanto viene loro richiesto di identificare e segnalare quei comportamenti ritenuti anomali posti in essere da clienti potenzialmente ricollegabili al finanziamento del terrorismo. Si tratta di un'attività difficile in assenza di riferimenti "soggettivi" precisi e in considerazione delle caratteristiche "mimetiche" del fenomeno.

Un ruolo fondamentale nell'individuazione e segnalazione delle operazioni sospette da segnalare rivestono gli indicatori di anomalia (in particolare quelli specifici per il finanziamento del terrorismo contenuti nel provvedimento della Banca d'Italia del 2010) che pongono particolare attenzione al profilo soggettivo (liste), alla localizzazione delle controparti (aree a rischio), e agli istituti non profit. Ulteriori indici di rischio sono contenuti nei Comunicati pubblicati dalla UIF in materia nel 2016 e 2017.

3. Il finanziamento del terrorismo: tratti caratteristici del fenomeno (A. Cassetta e L. Baron)

L'avvenuta integrazione tra finanziamento del terrorismo e riciclaggio – pur mantenendo alcune specificità, segnatamente il regime dei "congelamenti" – si giustifica per le caratteristiche che accomunano i due fenomeni, in particolare nelle manifestazioni finanziarie, nonostante le differenze concettuali nella loro natura e struttura.

Il passaggio dei fondi attraverso il sistema finanziario rappresenta per il riciclaggio una fase funzionale e necessaria alla successiva integrazione nel sistema economico ufficiale di fondi che, per definizione, sono di origine illecita (dall'*economia illegale* all'*economia legale*), mentre per il finanziamento del terrorismo costituisce una modalità per consentire ai fondi – la cui origine può essere indifferentemente lecita o illecita – di raggiungere i beneficiari che li utilizzeranno per finalità attinenti alla sfera del terrorismo.

Nella definizione normativa di finanziamento del terrorismo del D.lgs. 109/2007 non ci si riferisce solo alla realizzazione diretta di attentati terroristici, ma anche a ogni forma di supporto o sostegno finanziario delle attività delle organizzazioni (es: logistica, documenti, armi, propaganda, etc.) o di singoli membri delle stesse ovvero di individui che agiscono in maniera isolata ("lupi solitari"), nell'ambito di una qualsiasi delle condotte previste dall'art. 270 c.p. (es: arruolamento, addestramento, organizzazione di viaggi, etc.).

⁸³⁴ Le comunicazioni devono indicare i nominativi coinvolti, l'ammontare e la natura dei fondi o delle risorse economiche; le operazioni, i rapporti e ogni altra informazione disponibile, riconducibile ai soggetti designati nelle liste, nonché ai soggetti in via di designazione. Si tratta di due distinti tipi di comunicazione, funzionali a tenere informate le autorità, da un lato, circa le misure di congelamento applicate, dall'altro, circa le operazioni, i rapporti o ogni altra informazione finanziaria conosciuta relativamente ai soggetti designati nelle liste ovvero in via di designazione.

Questa diversità nella funzione svolta dal passaggio attraverso il sistema finanziario è evidenziata anche dalla diversa qualificazione delle fasi in cui si articolano i due fenomeni: nel riciclaggio tutte le fasi (*placement, layering, integration*) sono definite proprio in funzione del rapporto dei fondi con il sistema finanziario ufficiale (rispetto al quale rappresentano rispettivamente i momenti di ingresso, transito e uscita); nel finanziamento del terrorismo, invece, le tre fasi del processo (raccolta, trasferimento, utilizzo) rappresentano altrettanti stadi del “ciclo di vita” dei fondi stessi rispetto alla finalità da perseguire. Altro elemento distintivo tra i due fenomeni è che, per quanto concerne il finanziamento del terrorismo, spesso vengono utilizzati circuiti informali di trasferimento di disponibilità (es: *hawala*).

Ulteriore differenza fondamentale nella struttura dei due fenomeni risiede nel fatto che, pur prevedendo entrambi, per definizione, la presenza di un atto illecito, questo si colloca: per il riciclaggio, all’*origine* dei flussi finanziari, a seguito del “reato presupposto”, i cui proventi dovranno essere introdotti nel circuito dell’economia legale; per il finanziamento del terrorismo, nella fase terminale, cioè nella *destinazione* (utilizzo) dei fondi per una delle finalità ricadenti nella sfera dei reati di terrorismo.

Proprio perché l’illecito che qualifica il finanziamento del terrorismo attiene alla fase di utilizzo dei fondi, è irrilevante se i fondi stessi siano di origine lecita oppure illecita, ben potendo accadere che la fase di raccolta avvenga all’interno dell’economia legale; si pensi, a titolo esemplificativo, alla raccolta di donazioni a fini umanitari trasferite, da ultimo, a organizzazioni terroristiche (anche) nella completa inconsapevolezza dei donanti e dei responsabili dell’organizzazione. La differenza fra riciclaggio e finanziamento del terrorismo può essere emblematicamente rappresentata attraverso i due concetti di *money laundering* (fondi di origine illecita che vengono “ripuliti”, finendo utilizzati per uno scopo lecito nell’economia legale) e *money dirtying* (fondi di origine lecita, che vengono “sporcati” da un utilizzo finale illegale).

Un ulteriore tratto distintivo, che deriva dalla definizione normativa di finanziamento del terrorismo, è che mentre per il riciclaggio, affinché i fondi che alimentano il processo possano qualificarsi come proventi di reato, è necessario che questo (“reato presupposto”) si sia consumato, non è così per il finanziamento del terrorismo, laddove l’illecito qualificante può anche non essersi ancora tradotto in realtà, ma esser rimasto allo stato potenziale o anche solo intenzionale; ciò che rileva infatti è la “finalità di utilizzo” dei flussi, indipendentemente dal loro effettivo impiego.

A fronte di questa articolazione generale della struttura del fenomeno del finanziamento del terrorismo, le forme che esso concretamente assume nelle sue interazioni con il sistema finanziario dipendono dalla modalità di realizzazione di ciascuna delle tre fasi costitutive (raccolta, trasferimento, utilizzo): queste, a loro volta, riflettono il tipo di obiettivi che i gruppi terroristici si propongono di raggiungere e la forma stessa della loro organizzazione interna, determinante per l’individuazione degli specifici fabbisogni finanziari.

Esemplare è il confronto fra le modalità di finanziamento delle organizzazioni terroristiche “tradizionali” (*Al Qaeda* e tutte le altre organizzazioni affiliate), nei primi anni duemila, la cui attività ha originato sostanzialmente l’attuale assetto di contrasto al finanziamento del terrorismo, e quelle più recenti che hanno caratterizzato altre organizzazioni (*ISIS e Al-Nusra*).

L’originaria organizzazione di Al-Qaeda era di tipo gerarchico, con una struttura centrale che pianificava le azioni eseguite in diverse aree del mondo da cellule locali sottoposte al suo “controllo”, spesso segregate fra loro (al fine di garantire la compartimentazione delle informazioni e dei rischi in caso di cattura); la struttura centrale oltre a coordinare le attività, provvedeva anche a fabbisogni materiali (finanziari) delle cellule, con uno sviluppo “reticolare” dell’organizzazione, che restava ancorato a una organizzazione verticistica.

I canali finanziari utilizzati riflettevano questa struttura organizzativa e gestionale, in particolare nelle fasi di raccolta e di trasferimento dei fondi: infatti, dato che il livello centrale era responsabile di reperire le risorse finanziarie per l’intera organizzazione, era ragionevole attendersi che questo ricorresse a modalità che gli consentissero di raccogliere volumi consistenti di denaro, anche di origine lecita. Quanto detto avveniva attraverso il coinvolgimento di imprese e di *charity* di rilevanti dimensioni, anche collegate direttamente o indirettamente a Stati “simpatizzanti” e richiedeva il trasferimento dei flussi finanziari attraverso canali adeguati sia al volume degli stessi sia alla fonte di provenienza (tipicamente: bonifici scambiati sul circuito bancario internazionale).

Con l’ingresso sulla scena dell’ISIS si è affermato un modello organizzativo profondamente diverso. Anzitutto, questa organizzazione è arrivata ad acquisire (a partire dal 2014) il controllo completo di territori estesi (in Siria e Iraq in particolare), esercitandovi (fino alla successiva sconfitta contro la coalizione Occidentale) un’autorità quasi “statuale” (il c.d. “Stato islamico”). Ciò ha determinato notevoli mutamenti nella morfologia della minaccia terroristica e, conseguentemente, dei suoi

risvolti finanziari; in particolare le esigenze di finanziamento (connesse con il mantenimento dell'apparato "statale" e dei servizi) e la conseguente necessità di "diversificazione" delle fonti. Un fenomeno peculiare emerso nel periodo di dominio territoriale dell'ISIS, inoltre, è quello dei c.d. *foreign terrorist fighters* (FTFs), ovvero soggetti che, spinti da un forte richiamo ideologico, si recavano da ogni parte del mondo verso i territori controllati per unirsi alle milizie dell'ISIS e aderire alla "causa" del sedicente "Stato Islamico", non di rado del tutto isolati da qualsiasi organizzazione, con percorsi di radicalizzazione e di finanziamento autonomi.

In generale, si è venuta a delineare una marcata separazione tra l'entità centrale e tutte le altre forme di terrorismo più o meno strutturate (organizzazioni locali affiliate, micro-cellule), dal punto di vista operativo e di conseguenza finanziario. Da un lato, l'entità quasi-statale che si finanziava attraverso forme di sfruttamento delle risorse fisiche presenti sul territorio (dalla vendita del petrolio all'esportazione di reperti archeologici) e di tassazione, per lo più indiretta, delle popolazioni locali e degli stranieri eventualmente presenti (incluso il pagamento di pedaggi e di "permessi" per l'esercizio delle attività economiche, fino al rapimento a scopo di estorsione); dall'altro, singole cellule operative al di fuori del territorio direttamente controllato, autonome sia dal punto di vista operativo che finanziario, le quali, chiamate ad agire di propria iniziativa e a proprie spese, in mancanza di risorse per attentati di grande impatto che avrebbero richiesto adeguata pianificazione e mezzi materiali, tipicamente ricorrevano ad armi di uso ordinario o a strumenti offensivi autoprodotti.

Quest'ultima connotazione del terrorismo, che costituisce oggi – come dimostrano gli episodi degli ultimi anni – la principale minaccia in Europa, assume una dimensione estrema con il fenomeno dei cosiddetti "lupi solitari" (*lone wolves*): singoli individui che agiscono in maniera del tutto isolata, spinti solo da una matrice "ideologica" – in una relazione di tipo spontaneo-imitativo – derivante da percorsi di indottrinamento spesso autonomi e repentini (favoriti anche da dinamiche di disagio sociale), la cui azione per questo è ancora più imprevedibile e invisibile, anche nei suoi risvolti finanziari. Questa forma di minaccia è stata rafforzata anche dal flusso dei *foreign terrorist fighters* rientrati dalle zone del conflitto (c.d. *returnees*), a seguito del ripiegamento dell'ISIS.

La differenziazione "morfologica" del terrorismo si riflette, oltre che nei fabbisogni finanziari, anche nelle fonti di finanziamento e nei canali finanziari utilizzati.

Le fonti lecite possono assumere diverse conformazioni: modalità di raccolta di denaro a titolo di contributo diretto da sovvenzionatori ("sponsor"), affiliati, simpatizzanti, ovvero di contribuzione indiretta attraverso forme associative senza scopo di lucro (*Non Profit Organisations*); attività economiche generatrici di profitto; ogni altra forma di "autofinanziamento" derivante da disponibilità proprie dei membri dell'organizzazione o di individui che agiscono isolatamente (redditi da lavoro, contributi statali, patrimoni individuali, rendite, liquidazione di attività).

Nella prima tipologia, una forma di sostegno finanziario è quella - tipica delle organizzazioni più complesse - che può provenire da governi di paesi islamici permeati da una cultura integralista, sulla base di ideologie antimperialiste o di interessi geo-politici locali⁸³⁵, ovvero da persone di fede islamica dotate di grosse disponibilità economiche, mosse da motivazioni ideologiche (es: "sceicchi del terrore"). Tali forme di contributo, che possono raggiungere dimensioni anche rilevanti, per effetto del forte richiamo indotto dalla componente religiosa e ideologica, sono spesso richiamate in letteratura come casi "accademici" e sono tuttavia poco adattabili alla realtà europea. Una seconda forma è costituita dalle raccolte di fondi tra fedeli e simpatizzanti, sotto forma di offerte e donazioni individuali. In tale ambito, assumono un rilievo fondamentale i centri di aggregazione e di culto e le organizzazioni no-profit (comunità islamiche, moschee, istituti culturali islamici).

Una seconda tipologia di fonte di finanziamento legale è costituita dalla attività economiche regolari che, oltre a costituire un possibile canale di approvvigionamento, costituiscono uno strumento versatile che consente di accedere al sistema finanziario senza dare nell'occhio e al tempo stesso dissimulare con maggiore facilità – ad esempio, attraverso la copertura di operazioni apparentemente commerciali – le finalità illecite di impiego dei fondi.

Una terza forma di finanziamento, più diffusa nelle organizzazioni meno strutturate e nel caso di micro-cellule e individui isolati, è quella che deriva direttamente dagli affiliati, che oltre a partecipare alle attività di questa la sostengono anche dal punto di vista finanziario, attingendo alle proprie disponibilità, garantendone l'autofinanziamento.

⁸³⁵ Specie con riferimento alle regioni della Penisola araba e, più di recente, del Medio Oriente, è frequente il richiamo a ipotesi di foraggiamento delle organizzazioni terroristiche locali da parte dei governi dei Paesi confinanti per favorire cambiamenti di regime. Iene frequentemente richiamato, il foraggiamento da parte di Paesi di organizzazioni terroristiche locali per favorire cambiamenti di regime.

Le fonti illegali ricomprendono astrattamente qualsiasi attività criminosa idonea a produrre ricchezza; tuttavia le più impiegate, per una serie di fattori socioeconomici, di complessità finanziaria, di “contiguità” con altri fenomeni illeciti di tipo associativo, sono quelle derivanti da traffici illeciti (sostanze stupefacenti, armi, prodotti contraffatti), estorsioni e da sfruttamento e traffico di esseri umani (*human trafficking* e *migrant smuggling*). È evidente, in tal senso, la sovrapposizione del fenomeno con la criminalità comune, laddove a una finalità di arricchimento può aggiungersi (o sostituirsi) quella di raccogliere e destinare risorse alla causa *jihadista*.

Per quel che riguarda i canali finanziari e le modalità di trasferimento, i flussi delle organizzazioni più complesse tendono ad assumere di frequente la forma di bonifici sul circuito bancario internazionale, che garantisce rapidità e sicurezza alle transazioni, se del caso con meccanismi di “triangolazione” con Paesi terzi o tecniche per dissimulare la natura dei flussi o aggirare i controlli⁸³⁶. In alternativa, le organizzazioni terroristiche anche più strutturate possono ricorrere anche a canali informali, come ai sistemi di tipo *hawala* o ai corrieri di valuta (*money mules*).

Nel caso delle cellule locali, i flussi destinati al loro finanziamento (anche in ragione della ridotta entità degli importi delle operazioni e della natura occasionale, specie nel caso di micro-cellule e individui che agiscono in maniera isolata) restano spesso al di fuori del circuito finanziario, restando confinati in trasferimenti di contante non tracciati o trovando collocazione nei canali informali indicati in precedenza.

Tipici della tradizione islamica, i circuiti alternativi informali sono particolarmente diffusi in diverse aree geografiche del mondo, specie in quelle con sistemi finanziari meno evoluti (Medio Oriente, Nord Africa, Corno d’Africa e Asia Meridionale). Uno dei più noti è costituito dall’*hawala*, un sistema di trasferimento di denaro di antiche radici che si avvale di una rete di mediatori (*hawala* o *hawaladars*) dislocati sul territorio che, in analogia con i sub-agenti, raccolgono le somme dai clienti e danno istruzione ai propri omologhi in altre città (o all’estero) di mettere i fondi a disposizione dei destinatari, dopo aver trattenuto una commissione. Periodicamente le reciproche posizioni degli *hawaladars* vengono saldate mediante una sorta di sistema di compensazione simile a quello dei *money transfer*, che può transitare o meno attraverso il sistema finanziario formale. Tali sistemi nel tempo hanno preso piede anche nei paesi sviluppati, in particolare all’interno di comunità di immigrati ove le componenti di clandestinità ovvero di appartenenza ad un determinato gruppo etnico, se non il minore costo dell’operazione, possono spingere a privilegiarli rispetto ai canali “ufficiali”. Tali sistemi, sfuggendo a qualsiasi forma di regolamentazione e controllo, possono essere utilizzati anche per canalizzare flussi di cui si intenda evitare la tracciabilità e, pertanto, risultano appetibili per le organizzazioni criminali e organizzazioni terroristiche.

Nel caso invece dei canali finanziari formali è frequente l’utilizzo di quelli che sono facilmente accessibili a soggetti poco o per nulla “bancarizzati”, come i circuiti *money transfer* e le carte di pagamento. Il canale dei *money transfer* presenta alcuni elementi di rischio, che lo espongono a possibili utilizzi di natura illecita tra cui il finanziamento del terrorismo.

Diversamente dal circuito bancario, il punto di contatto con la clientela è infatti costituito da operatori (agenti) meno professionalizzati, che di norma svolgono contestualmente attività di natura commerciale, e costituiscono un possibile anello debole del sistema per la minore cultura, sensibilità ed esperienza in materia di antiriciclaggio. Inoltre, il rapporto con la clientela è più sfumato, in quanto è riferibile a operazioni occasionali, che non consentono una adeguata applicazione del principio *know your customer* applicato dalle banche. È per questi motivi che la normativa antiriciclaggio ha previsto un limite stringente sull’importo trasferibile per operazione (1.000 euro). Alcuni strumenti di moneta elettronica, come ad esempio le carte prepagate, possono costituire un ulteriore mezzo per trasferire fondi per finalità illecite, anche grazie ad alcune loro caratteristiche che consentono di dissimulare la reale intestazione della carta, e di utilizzarle come un vero e proprio sistema di trasferimento di denaro in un *network* di soggetti, ad esempio mediante i meccanismi delle ricariche seguite da prelievi di contante.

Negli ultimi anni, con l’evoluzione della tecnologia applicata ai sistemi finanziari, l’attenzione delle Autorità di prevenzione e contrasto si è focalizzata sui nuovi fenomeni delle valute virtuali e delle piattaforme di raccolta online (*crowdfunding*, *fundraising* e altre forme assimilabili).

4. Gli indicatori di anomalia e le comunicazioni della UIF (A. Cassetta e L. Baron)

Le indicazioni fornite dalle Autorità, nazionali e internazionali, per contribuire a intercettare e bloccare i flussi del finanziamento del terrorismo si sono adeguate, nel tempo, all’evoluzione dello

⁸³⁶ In tale ambito, le tecniche di dissimulazione non sono diverse da quelle del riciclaggio e, possono ricomprendere, a titolo esemplificativo: il frazionamento di operazioni; l’occultamento dei titolari delle operazioni o rapporti mediante l’utilizzo di intestazioni fiduciarie o di “prestanome”, trust o enti senza scopo di lucro; operazioni simulate e in generale ogni altro genere di condotta artificiosa, anche mediante l’utilizzo – specie nelle organizzazioni più complesse – di schemi finanziari e societari sofisticati.

scenario descritto precedentemente, anche sulla base delle conoscenze maturate in occasione degli eventi terroristici.

Le prime istruzioni in materia risalgono al 2001, allorché l'Ufficio Italiano Cambi (UIC), allineandosi alle indicazioni del GAFI, a poche settimane dagli eventi di New York diede istruzione di segnalare le operazioni sospette di finanziamento del terrorismo, anche in quanto direttamente o indirettamente riconducibili ai soggetti designati nelle "liste" diffuse agli intermediari⁸³⁷. Queste indicazioni sono state poi integrate nel Provvedimento della Banca d'Italia recante gli indicatori di anomalia per gli intermediari (2010), che riporta una serie di indicatori specifici volti alla individuazione delle fattispecie di finanziamento del terrorismo. Gli indicatori, ritagliati essenzialmente sulle Raccomandazioni "speciali" e sugli altri documenti del GAFI a quel tempo disponibili⁸³⁸, richiamano l'attenzione in particolare su: elementi di rischio "soggettivi" (operazioni con soggetti designati nelle liste o coinvolti in fatti di terrorismo); fattori di rischio "geografici" (operazioni con paesi a rischio terrorismo); operatività anomala riferibile a organizzazioni non profit⁸³⁹.

Al finanziamento del terrorismo sono comunque applicabili astrattamente tutti gli indicatori di carattere "generale", che rivestono in molti casi un ruolo neutrale rispetto alla qualifica del sospetto sottostante (riciclaggio o finanziamento del terrorismo).

A fronte delle nuove forme assunte dalla minaccia terroristica con l'affermazione dell'ISIS e con i fenomeni connessi, vi è stato un notevole sforzo sul piano internazionale volto ad aggiornare i risvolti finanziari del fenomeno e a rivedere gli schemi di contrasto per fronteggiare l'accresciuta minaccia. L'attenzione si è focalizzata sul tema dello scambio di informazioni tra i soggetti coinvolti (Autorità e settore privato) e su quello del potenziamento delle capacità dei soggetti obbligati di identificare e, quindi, di segnalare le attività sospette alle *Financial Intelligence Units*, anche in relazione alle accresciute connotazioni di "mimetismo" del fenomeno.

Con riguardo a quest'ultimo aspetto, nella prospettiva di costruire un sistema di indicatori più preciso, oltre a nuove fattispecie operative, sono stati tenuti in debita attenzione fattori di rischio connessi con l'adeguata verifica e il comportamento della clientela complessivamente inteso (finanziario e non), arrivando a delineare una sorta di "profilatura" e di schemi di condotte finanziarie assimilabili a quelle dei terroristi.

Questa attività ha dato origine, nell'ambito dei lavori del GAFI, a un "filone" di gruppi di studio che hanno approfondito, tra gli altri, tematiche riguardanti il rischio di abuso delle *non-profit organisations*, le fonti di finanziamento dell'ISIS e di altre organizzazioni terroristiche territoriali, i nuovi rischi connessi con il finanziamento del terrorismo, il finanziamento del reclutamento per attività terroristiche⁸⁴⁰.

In particolare, un fondamentale riferimento per gli indicatori di anomalia è il Report GAFI "Emerging Terrorist Financing Risk" (ottobre 2015). La pubblicazione, che ha aggiornato il precedente rapporto del 2008, passa in rassegna, accanto alle modalità di finanziamento qualificate come "tradizionali", tuttora valide, tutte le nuove forme emerse con il fenomeno dell'ISIS.

A margine dei lavori in ambito GAFI, la UIF ha diffuso ad aprile 2016 e ottobre 2017 due "Comunicazioni" in tema di finanziamento del terrorismo, dirette a sensibilizzare gli operatori e a fornire un quadro aggiornato di indicatori di rischio, che tengono conto anche delle modalità di finanziamento dell'ISIS, delle nuove minacce dei *foreign terrorist fighters* e dei *returnees*, dei rischi connessi con le nuove tecnologie.

Le comunicazioni richiamano anzitutto gli elementi di rischio "tradizionali", come le operazioni con soggetti "a rischio" (listati o legati a fenomeni di estremismo e radicalizzazione), i movimenti anomali riferiti a organizzazioni non lucrative, i trasferimenti di denaro (money transfer e bonifici esteri) con controparti insediate in paesi o aree che possano essere

⁸³⁷ Provvedimento UIC del 9 novembre 2001.

⁸³⁸ Report "Emerging Terrorist Financing Risks" (2008), contenente, tra l'altro, una serie di indicatori di rischio.

⁸³⁹ Per maggiori dettagli, cfr. Provvedimento della Banca d'Italia recante gli indicatori di anomalia per gli intermediari del 24.8.2010 (gruppi indicatori 20 e 21).

⁸⁴⁰ "Risk of terrorist abuse in non-profit organisations" (2014); "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant" (2015); "Emerging Terrorist Financing Risks" (2015); "Terrorist Financing in West and Central Africa" (2016); "Financing of Recruitment for Terrorist Purposes" (2018).

considerate a rischio “geografico”⁸⁴¹. L’attenzione degli operatori viene poi richiamata sul commercio illecito di beni e risorse provenienti da territori controllati dalle organizzazioni terroristiche (contrabbando di beni culturali e petrolio) e sulle tracce finanziarie e i comportamenti potenzialmente ricollegabili a quelli dei *foreign terrorist fighters* e dei *returnees* nelle diverse “fasi” (organizzazioni di viaggi, permanenza in paesi a rischio, passaggi in paesi di transito, rientri).

In tale ambito rilevano: i prelevamenti di contante volti ad azzerare le disponibilità dei rapporti; finanziamenti personali seguiti da inadempienze nei pagamenti, connesse con irreperibilità dei clienti; richieste inusuali di cambio di valuta; l’acquisto di titoli di viaggio, biglietti aerei o visti, ovvero di beni e servizi utilizzabili in quelle zone (articoli di equipaggiamento militare e sopravvivenza, servizi funzionali all’addestramento operativo); la riattivazione di rapporti mantenuti inattivi per lungo periodo; i versamenti di contante provenienti dall’estero; l’utilizzo di carte di pagamento o di portali di *home banking* in aree a rischio geografico; le attività di raccolta di fondi online, anche attraverso piattaforme di *crowdfunding*; e il ricorso anomalo a valute virtuali.

5. Le segnalazioni di operazioni sospette (A. Cassetta e L. Baron)

Le segnalazioni di operazioni sospette di finanziamento del terrorismo trasmesse dai soggetti obbligati risultano di numero esiguo, se rapportate a quelle di riciclaggio (meno dell’1% del totale delle segnalazioni nel 2021). Come riportato in precedenza, il finanziamento del terrorismo, oltre a essere un fenomeno di per sé meno ricorrente, presenta una serie di caratteristiche che ne rendono difficile la rilevazione; i flussi sono di importo contenuto, possono avere origine lecita e spesso sono canalizzati su circuiti finanziari informali, pertanto sfuggono facilmente ai sistemi di controllo.

L’andamento delle segnalazioni nel tempo è meno regolare rispetto a quelle di riciclaggio, essendo molto condizionato dalle dinamiche evolutive della minaccia e della sua percezione da parte dei soggetti obbligati. Nei momenti in cui vi è una percezione del rischio maggiore le segnalazioni aumentano in modo significativo, con picchi nei momenti immediatamente successivi agli attentati, come accaduto, ad esempio, nei primi anni duemila (attentati di Londra e Madrid) e, dieci anni più tardi, dopo la lunga scia di attentati in Europa. Nel periodo più recente, nel momento in cui le sorti belliche dell’ISIS hanno subito dapprima un rallentamento e poi un progressivo ripiegamento, l’attenzione anche mediatica nei confronti del fenomeno si è ridotta, e il flusso di segnalazioni si è stabilizzato.

Sulla crescita delle segnalazioni degli ultimi anni ha influito certamente anche la maggiore reattività degli operatori che, anche grazie alle istruzioni della UIF, hanno adeguato le procedure di rilevazione delle operazioni anomale e si sono mostrati in generale più attenti nella valutazione delle tracce finanziarie e di comportamenti, anche non finanziari, della propria clientela.

La qualifica di sospetto di finanziamento del terrorismo avviene nella maggior parte dei casi per fattori soggettivi, ovvero per la circostanza che l’operatività (non necessariamente connotata da anomalie finanziarie) riguardi soggetti coinvolti in fatti di terrorismo, o più o meno vicini a organizzazioni terroristiche o ad ambienti dell’estremismo; negli altri casi i fattori di rischio determinanti sono “geografici”, ovvero attinenti alla localizzazione delle operazioni o provenienza dei soggetti ai quali sono ricondotte le anomalie finanziarie.

Anche la qualità delle segnalazioni, come peraltro accaduto nel riciclaggio, ha beneficiato dell’attività di sensibilizzazione da parte della UIF, specie sotto il profilo della ricostruzione di contesti finanziari complessi con sviluppo “reticolare” (es: money transfer e carte prepagate).

Le casistiche segnalate possono essere inquadrate in tre grandi categorie, nelle quali il sospetto che innesci la segnalazione attiene rispettivamente: al profilo individuale dei soggetti coinvolti; all’operatività finanziaria complessivamente messa in atto; al coinvolgimento di organizzazioni non profit.

Nella prima categoria, che è la più ricorrente, rientrano le segnalazioni in cui il sospetto sul coinvolgimento di uno o più individui in attività ricollegabili al terrorismo deriva da corrispondenza dei loro nominativi con soggetti ricompresi nelle liste pubbliche di sanzioni (ONU, UE e OFAC) ovvero interessati da procedimenti giudiziari o attività di indagine di autorità di *law enforcement* italiane o estere per ipotesi di reato, che possono direttamente o indirettamente ricollegarsi a fattispecie di terrorismo.

⁸⁴¹ Da intendersi, a titolo di esempio, le aree di conflitto e le zone limitrofe e di transito, i paesi che finanziano o sostengono attività terroristiche o con una significativa incidenza di organizzazioni terroristiche, le giurisdizioni caratterizzate da carenze nei presidi di prevenzione e contrasto del finanziamento del terrorismo.

Tali situazioni emergono tipicamente da meccanismi di *data crossing* automatico con i sistemi aziendali, per i quali gli operatori – anche per adempiere agli obblighi di congelamento – si avvalgono generalmente del supporto di *provider* esterni specializzati o reagiscano a input esterni anche di fonte aperta, quali fatti di cronaca o richieste di informazioni da parte delle Autorità.

Il censimento nelle liste è certamente un indicatore di per sé robusto, anche in considerazione dei rigidi criteri per la designazione; tuttavia non di rado gli elementi anagrafici disponibili sui soggetti presenti nelle liste e/o su quelli coinvolti nell'operatività (in particolare, le controparti finanziarie dei clienti) risultano poco affidabili, generando in molti casi dei “falsi positivi” legati a fenomeni di omonimia. Nel caso di individui oggetto di indagini di polizia non sussistono problemi di ambiguità (le generalità sono note), tuttavia non sempre sono certe o note le circostanze relative al coinvolgimento dei soggetti segnalati in reati di finanziamento del terrorismo; le indagini, infatti, possono riguardare illeciti contigui o potenzialmente funzionali al terrorismo stesso (crimini violenti, abusivismo finanziario, sfruttamento di esseri umani) o individui il cui legame con i soggetti segnalati può essere “debole”, in quanto ad esempio sporadico e datato nel tempo o intermediato da terzi soggetti.

In tale ambito, una casistica particolarmente ricorrente è quella delle segnalazioni degli istituti di money transfer, avvantaggiati dalla capacità di disporre di una visione globale dei *network* nel proprio circuito, specie nel caso degli operatori di maggiori dimensioni. La presenza in gran parte dei paesi, ivi inclusi gli Stati a rischio terrorismo, consente loro di svolgere una funzione di collettore di richieste nominative da parte di Organi investigativi e, pertanto, di ricostruire, attorno a detti nominativi, le rispettive reti di operazioni transnazionali, comunicando le risultanze alle FIU per la parte di operatività rientrante nel territorio di competenza. Tale meccanismo offre alle Autorità un canale parallelo a quello tradizionale – costituito dagli scambi informativi bilaterali – per intercettare movimenti finanziari potenzialmente destinati al terrorismo nell'ambito di attività di indagine che hanno origine in altre giurisdizioni.

La seconda categoria ricomprende le segnalazioni che si focalizzano sulla operatività espressa dalla clientela e, quindi, prescindono dai nominativi o dai soggetti in sé (o dalle loro controparti finanziarie). In questo caso, il più frequente elemento di sospetto è l'elemento geografico, ovvero la presenza di un Paese a rischio terrorismo quale lo Stato di nascita o di residenza di alcuni dei soggetti ricompresi nella segnalazione, oppure come lo Stato di provenienza o di destinazione dei relativi flussi finanziari.

È evidente che il fattore geografico, se considerato isolatamente, è un elemento di sospetto generico. Spesso è il Paese di origine della clientela che, associato ad anomalie finanziarie, può indirizzare gli operatori verso un sospetto specifico, che può essere alimentato ad esempio dalle caratteristiche delle operazioni, come nel caso di prelevamenti di contante, ricariche di carte prepagate o bonifici tra una moltitudine di soggetti, ovvero dalla loro localizzazione, specie se in luoghi di transito o caratterizzati da un'alta densità di attività criminali “contigue” come lo sfruttamento degli esseri umani e il traffico dei migranti.

Infine, un terzo insieme di segnalazioni è quello avente a oggetto operatività anomala di organizzazioni non profit. Queste ultime ricomprendono un insieme variegato, che può assumere diversa forma (associazioni, fondazioni, centri culturali) e oggetto sociale (servizi per gli immigrati, diffusione della religione e realizzazione di luoghi di culto, finanziamento di progetti di assistenza anche all'estero). Tali organizzazioni sono da sempre costantemente all'attenzione delle Autorità di sicurezza e di *intelligence*, in quanto sono luoghi di aggregazione in cui possono svilupparsi fenomeni di radicalizzazione religiosa, che possono sfociare in azioni violente. Sotto il profilo finanziario, il GAFI mette in evidenza (Raccomandazione n. 8) come alcuni elementi, tra cui l'ampia fiducia di cui queste organizzazioni godono presso la collettività, la loro proiezione internazionale, l'utilizzo intensivo di contante, possano costituire degli importanti fattori di rischio, che le rendono vulnerabili ad “abuso” o infiltrazione da parte delle organizzazioni terroristiche.

Le segnalazioni traggono origine proprio dalle attività di monitoraggio rafforzato poste in essere dagli operatori sui rapporti finanziari riferiti a queste organizzazioni, tenendo conto degli indicatori di anomalia disponibili già dal 2010. Tra le anomalie più ricorrenti, figurano: versamenti o prelevamenti di contante anomali, per frequenza o importi; bonifici con persone fisiche o con altre associazioni che non appaiano riconducibili all'oggetto sociale o a raccolte di fondi tra gli associati; movimenti di denaro ingiustificati tra le associazioni e persone collegate (rappresentanti, tesorieri, esponenti religiosi). In diversi casi, il sospetto è riferito ad associazioni in via di costituzione o neo costituite, connotate da afflussi di fondi in contante o comunque di dubbia origine, motivati come raccolte per la realizzazione di centri di culto. In alcuni casi, il sospetto non nasce dal monitoraggio dei rapporti delle associazioni, ma da operazioni poste in essere da clienti a favore di queste, di importo o frequenza non giustificabili.

Con riferimento ai contributi segnaletici delle singole categorie di segnalanti si è assistito al progressivo consolidarsi di una situazione che vede circuiti money transfer e istituti emittenti di moneta elettronica come segnalanti di gran lunga maggioritari, facendo passare in secondo piano il contributo delle banche (il cui ruolo rimane invece non a caso tuttora preponderante nelle segnalazioni riferite alle onlus, quali soggetti strutturati finanziariamente ed integrati nel contesto del sistema dei pagamenti stabili associato a rapporti di durata). Ciò si è riflesso inevitabilmente anche sul piano della tipologia

delle operazioni segnalate, con i trasferimenti internazionali rappresentati prevalentemente dalle operazioni money transfer piuttosto che dai bonifici esteri, e quelli nazionali realizzati principalmente tramite ricariche di carte di pagamento piuttosto che tramite bonifici domestici, mentre rimane diffusa l'attenzione dei segnalanti alle transazioni in contante, sia in fase di alimentazione che di utilizzo.

L'approfondimento finanziario delle segnalazioni di finanziamento del terrorismo da parte della UIF si avvale di metodi, percorsi e strumenti di analisi analoghi a quelli dei contesti di riciclaggio, pur conservando alcune peculiarità dettate dalle caratteristiche del fenomeno che, diversamente dal riciclaggio, richiede la massima valorizzazione delle informazioni soggettive e di contesto (legami) e di alcuni elementi informativi che possono avere anche limitato spessore finanziario.

Dal momento che le segnalazioni, nella maggior parte dei casi, appaiono finanziariamente poco significative, le attività di analisi cercano spesso di valorizzare al massimo le informazioni soggettive, attraverso incroci di dati e interrogazioni delle banche dati, e si avvalgono di strumenti evoluti, utilizzando anche la *social network analysis* per i contesti con sviluppo reticolare.

L'attività della UIF nel tempo si è orientata a declinare sempre più il proprio approccio analitico in funzione delle caratteristiche delle segnalazioni e delle fonti di innesco, adattando prassi di approfondimento finanziario già sviluppate per il riciclaggio in funzione delle caratteristiche specifiche del finanziamento del terrorismo, al fine di produrre un valore aggiunto informativo utile per la successiva fase dell'analisi investigativa.

Le risultanze degli approfondimenti della UIF vengono prontamente messe a disposizione degli Organi investigativi. Le analisi finanziarie costituiscono un naturale complemento delle indagini investigative tradizionali, in quanto consentono di rilevare, anche a ritroso nel tempo, attraverso la lettura delle tracce finanziarie, comportamenti e collegamenti soggettivi. Le segnalazioni, tramite il NSPV, sono messe a disposizione anche del Procuratore Nazionale Antimafia e Antiterrorismo; le informazioni sui soggetti segnalati sono condivise con le altre Autorità di contrasto al terrorismo, sempre tramite il NSPV, anche nell'ambito del C.A.S.A. (Comitato Analisi Strategica Antiterrorismo).

6. Le sanzioni finanziarie “mirate” (D. Bartolozzi)

Con il termine “sanzioni finanziarie mirate” si indica generalmente una serie di misure sanzionatorie adottate a livello internazionale nei confronti di soggetti specificamente determinati, finalizzate a evitarne l'accesso a risorse finanziarie di qualsiasi tipo.

Nelle raccomandazioni del GAFI, per esempio, tali misure consistono nel congelamento di fondi e di risorse economiche e nei correlativi divieti di messa a disposizione nei confronti dei c.d. “soggetti designati” dall'ONU, cioè individuati come responsabili di attività di terrorismo (Raccomandazione n.6 del GAFI) e di proliferazione delle armi di distruzione di massa (Raccomandazione n. 7 del GAFI). A livello europeo, analoghe misure sono state introdotte in maniera autonoma (quindi a prescindere dall'adozione di una Risoluzione del Consiglio di Sicurezza delle Nazioni Unite), e prevedono l'interruzione o la riduzione, totale o parziale, delle relazioni economiche e finanziarie con uno o più paesi. In tal caso, le misure adottate possono prevedere non solo il blocco dei beni di specifici soggetti, ma anche restrizioni ai commerci, alla prestazione di servizi finanziari o ad altro tipo di servizi.

Le sanzioni finanziarie mirate costituiscono una categoria particolare di misure coercitive, di carattere amministrativo, che sono prive di una durata temporale predeterminata e sottoposte a una tutela giurisdizionale del tutto particolare, in gran parte sottratta al giudice ordinario. La natura “amministrativa” di tali misure può essere dedotta anche da altre disposizioni normative, che prevedono specifici meccanismi di esenzione dal congelamento (si veda, per esempio, l'art. 2-*bis* del regolamento UE 881/2002) e rinviando per la determinazione della specifica competenza all'autonomia di ciascuno Stato membro.

Resta, comunque, da escludere la configurabilità delle sanzioni in questione come misure coercitive di carattere penale o giudiziario.

Va a tal fine sottolineato, infatti, che il coinvolgimento dei soggetti designati in procedimenti penali (o in indagini per fatti di terrorismo o di finanziamento del terrorismo) è eventuale, seppur frequente, e non necessaria ai fini del loro inserimento nelle liste. L'adozione delle misure, infatti, si basa prevalentemente su una finalità preventiva piuttosto che repressiva, essendo le stesse adottate per impedire che risorse di qualsiasi tipo possano essere destinate o comunque gestite per finalità di terrorismo, di proliferazione o per attività che minacciano la pace o la sicurezza internazionale. Ne costituisce una riprova, ad esempio, l'art. 2 del regolamento UE 881/2002, che definisce i soggetti designati proprio come “associati alle organizzazioni dell'ISIL (Da'esh) o di Al-Qaeda”.

Infine, un ulteriore carattere che vale a distinguere le misure della specie da quelle proprie dell'ordinamento penale è la loro durata. Se, infatti, le sanzioni di tipo penale sono limitate nel tempo, agli obblighi di congelamento non è assegnata alcuna durata predeterminata (ad eccezione dei congelamenti nazionali, di cui al successivo par. 7.2.2) trovando essi efficacia per

effetto della pubblicazione dei regolamenti comunitari e dovendosi ritenere vigente l'obbligo di congelamento finché il regolamento stesso non venga abrogato oppure finché il nominativo del soggetto designato non venga cancellato dall'elenco medesimo⁸⁴².

Alla stessa conclusione circa la natura amministrativa delle sanzioni in esame dovrebbe giungersi anche per le c.d. misure di congelamento nazionali, introdotte dall'art. 4-*bis* del D.lgs. 109/2007.

La principale differenza con le altre "sanzioni finanziarie mirate" sta, infatti, nell'autorità che le dispone (il Ministro dell'Economia e delle Finanze, su proposta del Comitato di Sicurezza Finanziaria) e nel carattere strettamente temporaneo, che la legge nazionale limita a soli sei mesi. In tal caso la durata limitata del provvedimento si giustifica con l'esigenza di assicurare tempestivamente che i fondi e le risorse economiche non siano distratte, occultate o trasferite allo scopo di evitarne il congelamento. Va altresì messo in evidenza come il provvedimento di congelamento nazionale non costituisce un'autonoma designazione dell'Italia, ma deve comunque riferirsi a un provvedimento (di fonte ONU o europea) che sia in corso di adozione. Precisa, infatti, la norma, che tale provvedimento (che assume quindi, carattere anticipatorio, oltre che temporaneo) può essere adottato "nelle more dell'adozione dei provvedimenti di designazione da parte dell'Onu o dell'Unione europea". L'introduzione di tale norma risponde anche ai rilievi mossi dal GAFI nei confronti della legislazione italiana (e, in particolar modo di quella europea) che non prevedeva meccanismi idonei ad assicurare il congelamento dei beni dei terroristi designati dall'ONU in maniera sufficientemente tempestiva (al riguardo il GAFI richiede che l'attuazione di tali congelamenti avvenga *ideally within a matter of hours*, e cioè nell'arco di 24 ore circa, in modo da assicurare l'efficace attuazione dei congelamenti medesimi).

6.1. I congelamenti di fondi nelle Risoluzioni ONU e nei Regolamenti europei

Il sistema internazionale di prevenzione e contrasto al finanziamento del terrorismo, al finanziamento della proliferazione e all'attività dei paesi che minacciano la pace e la sicurezza internazionale prevede l'applicazione di misure restrittive di "congelamento" dei fondi e delle risorse economiche detenute da persone fisiche e giuridiche, gruppi ed entità specificamente individuati (c.d. soggetti designati). La designazione di tali soggetti avviene, a livello internazionale, in primo luogo da parte dell'Organizzazione delle Nazioni Unite, attraverso specifiche Risoluzioni del Consiglio di Sicurezza che individuano tali soggetti e chiedono agli stati di adottare misure nei loro confronti.⁸⁴³

Tali risoluzioni, tuttavia, non sono di per sé efficaci nei confronti dei soggetti privati, dal momento che obbligano gli Stati membri dell'Onu (ma non direttamente i rispettivi cittadini) ad applicare tali misure secondo gli strumenti legislativi propri di ogni paese e, quindi, a renderli obbligatori attraverso un provvedimento vincolante. Nei paesi dell'Unione europea tale esigenza è soddisfatta attraverso l'adozione di specifici regolamenti comunitari che, avendo efficacia diretta e vincolante, hanno piena forza legale *erga omnes* fin dal momento della loro pubblicazione nella Gazzetta Ufficiale dell'Unione europea.

Non si tratta, tuttavia, di una mera ripetizione delle norme previste dalle risoluzioni dell'ONU: infatti, nell'ambito della politica estera e di sicurezza comune, il trattato di funzionamento dell'Unione consente al Parlamento e al Consiglio di adottare misure di congelamento per la prevenzione e la lotta contro il terrorismo e le attività connesse (art. 75 del TFEU) e al Consiglio di adottare misure restrittive nei confronti di specifici individui o entità, in presenza di una decisione che preveda l'interruzione o la riduzione, totale o parziale, delle relazioni economiche e finanziarie con uno o più Paesi terzi (v. in particolare quanto previsto dall'art. 215 del TFEU). Per tale motivo, l'ambito sanzionatorio in vigore in Unione è più ampio rispetto a quello adottato dall'Onu e prevede, oltre a quelle stabilite dal Consiglio di Sicurezza, anche misure autonome.

Venendo all'esame del contenuto prescrittivo degli obblighi di congelamento, deve anzitutto porsi in evidenza come tali sanzioni prevedano due categorie distinte ma complementari di divieti. Da un lato, infatti, la normativa dispone il congelamento dei fondi e delle risorse economiche appartenenti,

⁸⁴² Ipotesi di "deroga" ai congelamenti sono previste dai regolamenti comunitari per soddisfare le esigenze di base delle persone fisiche e giuridiche, nonché per garantire il pagamento di spese ritenute ammissibili dall'ordinamento (quali il pagamento di onorari ragionevoli, l'adempimento di obbligazioni pregresse sorte in epoca antecedente alla designazione ecc. L'art. 4-*septies* del D.lgs. 109/2007 disciplina l'iter procedimentale stabilito in Italia per la gestione di tali procedure di esenzione.

⁸⁴³ Numerose sono le Risoluzioni del Consiglio di Sicurezza che prevedono l'implementazione di misure di congelamento di fondi e di risorse economiche. Fra queste merita senz'altro menzionare, pur senza carattere di esaustività, in materia di finanziamento del terrorismo le Risoluzioni 1267/1999 e 1373/2001 e, in materia di finanziamento della proliferazione, le Risoluzioni 1718/2006 e 1737/2006. Per quanto attiene la regolamentazione comunitaria, in materia di contrasto al finanziamento del terrorismo occorre citare il regolamento 881/2002 e il regolamento 2580/2001, adottati rispettivamente in esecuzione delle Risoluzioni 1267 e 1373, oltre al regolamento 1686/2016, che impone misure sanzionatorie aggiuntive e autonome rispetto a quelle adottate dalle Nazioni Unite.

possedute, detenute o controllate da soggetti designati, specificandosi che tale congelamento consiste nel blocco preventivo di qualsiasi operazione che possa comportare un utilizzo di detti fondi o risorse. Dall'altro lato, l'obbligo di effettuare il congelamento viene completato con il correlativo divieto di mettere a disposizione dei medesimi soggetti fondi o risorse economiche di qualunque tipo.

Tenendo conto del fatto che lo scopo del legislatore è quello di privare *in toto* i soggetti designati dall'accesso e dall'utilizzo di qualsiasi tipo di utilità economica, meritano particolare attenzione due aspetti della normativa appena descritta. Il congelamento opera di diritto e automaticamente per il solo fatto della pubblicazione del nominativo nella lista di soggetti designati. Infatti, il legislatore non impone un obbligo di fare (nella specie, di congelare), bensì dispone egli stesso il congelamento ("sono congelati tutti i fondi e le risorse economiche...", come recitano i regolamenti comunitari che istituiscono le sanzioni di questo tipo). Non è quindi richiesto al soggetto passivo un comportamento positivo che si estrinsechi in attività particolari sui fondi o risorse economiche (come, ad esempio, la nomina del custode nel caso del sequestro).

In secondo luogo i destinatari di tali obblighi (*rectius*: divieti) non sono definiti in maniera puntuale con il riferimento a una determinata categoria di attività. Infatti, sebbene la prassi operativa individui tali destinatari principalmente nelle banche e negli intermediari finanziari, in realtà i regolamenti comunitari si applicano nei confronti della generalità dei soggetti, e quindi, di fatto, deve ritenersi obbligato non solo il soggetto che per motivi professionali si ritrovi la disponibilità dei beni del soggetto designato⁸⁴⁴, ma chiunque abbia a qualsiasi titolo il possesso, la detenzione o comunque la disponibilità di fondi o risorse facenti capo al soggetto.

Infine, con il congelamento rimane vietato l'utilizzo dei fondi, ma non si determina un passaggio nella titolarità dei beni, che restano nella proprietà del soggetto designato, ancorché ne sia limitato l'utilizzo: ciò vale anche a differenziare i congelamenti da altro tipo di misure quali, ad esempio, la confisca prevista dall'art. 240 del codice penale.

Per quanto riguarda l'oggetto del congelamento, la scelta del legislatore è stata quella di ampliare il più possibile la natura dei beni da colpire, prevedendo due categorie: i fondi, da intendersi come disponibilità finanziarie e i proventi economici di qualsiasi tipo, per i quali è previsto un lungo elenco esemplificativo (ma non esaustivo) che comprende, fra l'altro, il denaro contante, gli assegni, i saldi dei conti correnti e, più in generale, i crediti e le obbligazioni; le risorse economiche, che costituiscono una categoria residuale nella quale sono ricomprese le disponibilità di qualsiasi tipo, anche intangibili, che non siano fondi, ma che possano essere utilizzate per ottenere fondi, beni o servizi.

Di fronte a una definizione così ampia, ben diversa e più ampia rispetto a quella di "beni" prevista dall'art. 810 del codice civile (che richiama la nozione di "cose", del tutto assente nella disciplina comunitaria), appare particolarmente arduo individuare un tipo di risorsa economica che possa essere sottratta all'obbligo di congelamento, specie considerando il riferimento alle disponibilità "intangibili" e alla natura residuale della categoria, il cui unico requisito distintivo consiste nell'astratta utilizzabilità per ottenere altri fondi, beni o servizi. Va anche rimarcato che tale astratta utilizzabilità non deve essere necessariamente correlata alle attività terroristiche (o alla minaccia della pace e della sicurezza internazionale), bensì è sufficiente che il soggetto designato ne possa avere la concreta disponibilità, anche per fini diversi e del tutto leciti. Se, quindi, non vi sono dubbi che vi rientrino le disponibilità dei conti correnti bancari, le azioni e le quote di società, nonché le aziende e i beni mobili registrati, come la prassi degli ultimi anni ha avuto modo di sperimentare, non sembrano sussistere dubbi nemmeno sulle nuove forme di fondi o risorse economiche, quali ad esempio, le valute virtuali.

6.2. Il ruolo dei soggetti obbligati

Se gli obblighi di congelamento sono disciplinati direttamente nei regolamenti europei, le normative nazionali dei Paesi membri possono prevedere disposizioni aggiuntive, in particolare per determinati operatori finanziari o commerciali, che sono maggiormente esposti al rischio di entrare in contatto con fondi e risorse da sottoporre a congelamento.

⁸⁴⁴ Più frequentemente la banca presso cui il designato è correntista, o l'assicuratore che deve risarcire un danno patrimoniale

Per quanto riguarda il nostro paese, la disciplina normativa è in gran parte prevista dal D.lgs. 109/2007⁸⁴⁵, che istituisce il Comitato di Sicurezza Finanziaria e che attribuisce specifiche competenze ad altre Autorità quali l'Unità di Informazione Finanziaria per l'Italia, il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e l'Agenzia del Demanio. L'art. 7 del decreto in questione attribuisce specifici compiti aggiuntivi, non previsti dalla normativa comunitaria, in capo ai c.d. soggetti obbligati, quelli cioè identificati come tali ai sensi del decreto antiriciclaggio.

Per tali soggetti, oltre all'obbligo di congelamento (e al correlativo divieto di mettere fondi e risorse economiche a disposizione dei soggetti designati) sono previsti due obblighi aggiuntivi di natura informativa. Tali obblighi consistono, rispettivamente nel dovere di: informare la UIF circa le misure di congelamento adottate entro i 30 giorni successivi all'adozione delle stesse, specificando i soggetti coinvolti, l'ammontare e la natura dei fondi o delle risorse economiche congelate; comunicare alla UIF, anche in assenza di misure di congelamento adottate, ogni informazione disponibile riconducibile ai soggetti designati (o in corso di designazione) con particolare riguardo ai dati relativi a operazioni o rapporti.

Le comunicazioni sopra menzionate devono essere considerate diverse e completamente autonome dalle segnalazioni di operazioni sospette previste dall'art. 35 del D.lgs. 231/2007: difatti, mentre queste trovano un presupposto nell'esistenza di un sospetto (o di motivi ragionevoli per sospettare) che i fondi provengano da attività criminosa o siano comunque collegati ad operazioni, anche tentate, di riciclaggio o finanziamento del terrorismo, le comunicazioni relative ai soggetti designati prescindono da qualsiasi valutazione di sospetto e devono essere fatte, anche quando i fondi detenuti o gestiti siano del tutto leciti. Allo stesso tempo va considerato che la mera presenza di un soggetto nella lista di soggetti designati non può essere considerato di per sé un elemento sufficiente a far nascere l'obbligo di invio di una segnalazione sospetta, dato che quest'ultima deve, per la sua natura, fondarsi su un elemento di valutazione più ampia, che afferisca anche alla provenienza o all'utilizzo dei fondi medesimi. Sostenere, infine, l'esistenza di un correlativo obbligo di segnalazione "automatico" avente ad oggetto i soggetti designati, finirebbe anche per produrre un'inutile e antieconomica duplicazione di comunicazioni, posto che la UIF è destinataria sia delle comunicazioni di avvenuto congelamento, sia delle segnalazioni di operazioni sospette.

La differenza fra i due tipi di comunicazione disciplinati dall'art. 7 riguarda l'ambito oggettivo della comunicazione, il termine entro cui deve essere inviata, nonché i destinatari della comunicazione medesima.

Difatti, mentre per la comunicazione avente ad oggetto l'adozione dei congelamenti è richiesto il rispetto di un tempo massimo di, che decorrono dalla data di inserimento in lista o, se successiva, dalla data di detenzione dei fondi e delle risorse economiche, per la comunicazione di ogni altra informazione relativa ai soggetti designati, il legislatore non prevede il rispetto di un termine specifico, limitandosi a richiedere che la comunicazione sia fatta tempestivamente. La ragione di un termine diverso deve riscontrarsi anche nella differente finalità delle due comunicazioni. Mentre la prima rientra nella ordinaria competenza della UIF a raccogliere i dati di natura finanziaria relativi ai soggetti designati⁸⁴⁶, la seconda deve essere considerata in relazione all'attività di controllo dell'attuazione delle sanzioni finanziarie⁸⁴⁷ e, quindi, alla necessità per la UIF di disporre di un quadro informativo ampio, tale da poter facilitare l'individuazione di fondi e risorse da poter sottoporre a congelamento⁸⁴⁸. Per quanto attiene ai destinatari, va infine osservato che le comunicazioni della specie devono essere fatte, oltre che alla UIF, anche al NSPV della Guardia di Finanza laddove abbiano ad oggetto risorse economiche⁸⁴⁹.

⁸⁴⁵ Recentemente modificato e integrato dal D.lgs. 90/2017 di attuazione della quarta direttiva antiriciclaggio

⁸⁴⁶ Cfr. art. 10, comma 2, del D.lgs. 109/2007

⁸⁴⁷ Cfr. art. 10, comma 1, del D.lgs. 109/2007

⁸⁴⁸ È il caso ad esempio dell'esistenza di conti e depositi intestati a soggetti designati ma estinti prima dell'entrata in vigore dei regolamenti europei, o del tentativo di porre in essere transazioni con soggetti designati: la disponibilità di tali informazioni può essere utile allo scopo di individuare altri fondi e risorse (nel primo caso, verificando la destinazione dei fondi dei rapporti estinti, nel secondo valutando possibili tentativi di aggirare il quadro sanzionatorio esistente).

⁸⁴⁹ Cfr. art. 10, comma 3 del D.lgs. 109/2007

6.3. Le attribuzioni della UIF e delle altre Autorità

La normativa europea in materia di sanzioni finanziarie mirate riserva al Consiglio (o al Consiglio e al Parlamento) l'individuazione dei soggetti designati e le successive modifiche agli elenchi medesimi. Ulteriori competenze sono invece radicate in capo alle Autorità competenti nazionali (NCA) che ogni Stato membro designa in base alla propria autonomia, dandone indicazione, anche a beneficio degli operatori economici e professionali, su un apposito sito internet, indicato in uno degli allegati ai regolamenti europei che prevedono le sanzioni medesime.

Limitando l'esame alle sole previsioni che riguardano i congelamenti di fondi e di risorse economiche, le specifiche competenze in materia di sanzioni finanziarie mirate sono previste dal decreto legislativo n. 109/2007. Tale decreto individua quale Autorità centrale, competente anche per l'attuazione delle misure di congelamento, il Comitato di Sicurezza Finanziaria, assegnando ulteriori specifiche attribuzioni ad alcune Autorità rappresentate nello stesso CSF, quali la UIF, il NSPV e l'Agenzia del Demanio.

Il Comitato di Sicurezza Finanziaria ha anzitutto un compito attuativo delle misure di congelamento disposte a livello europeo o nazionale: prescrive a tal proposito il comma 6 dell'art. 3 del D.lgs. 109/2007 che il CSF adotta ogni atto necessario per la corretta e tempestiva attuazione delle misure di congelamento disposte dalle Nazioni unite, dall'Unione europea e dal Ministro dell'economia e delle finanze ai sensi della vigente normativa⁸⁵⁰. Fra gli ulteriori compiti affidati dalla legge nazionale al CSF rientra quello di proporre l'adozione di misure di congelamento nazionali (art. 4-*bis*), proporre agli organismi internazionali competenti l'inserimento (art. 4-*ter*) o la cancellazione (art. 4-*sexies*) di soggetti da sottoporre a misure di congelamento⁸⁵¹, decidere in merito alle istanze di esenzione dal congelamento nei casi in cui la normativa comunitaria prevede una tale esenzione⁸⁵². Ulteriori attribuzioni del Comitato riguardano l'individuazione di modalità operative alternative per l'attuazione del congelamento sulle risorse economiche (art. 12-*bis*), nonché la previsione di particolari poteri d'indirizzo in merito alle attribuzioni previste in capo all'Agenzia del demanio per la gestione delle medesime risorse economiche congelate (art. 12).

Per quanto riguarda la UIF, l'ordinamento nazionale assegna all'Unità tre specifiche competenze (art. 10). Alla UIF spetta, in primo luogo, il controllo dell'attuazione delle sanzioni finanziarie mirate, il che attribuisce quindi all'Unità un ruolo di supervisione sul rispetto delle norme sui congelamenti. In secondo luogo, alla UIF spetta il compito di raccogliere i dati di natura finanziaria relativi ai soggetti designati, con particolare riguardo ai fondi e alle risorse economiche congelate per le quali è destinataria delle comunicazioni di avvenuto congelamento da parte dei soggetti obbligati. Infine, rientra nelle attribuzioni della UIF anche la circolazione delle liste dei soggetti designati e delle relative modifiche, previa acquisizione dei dati necessari, anche per il tramite del MAECI.

Specifiche attribuzioni sono previste anche in capo al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, titolare di compiti in materia di attuazione delle misure di congelamento aventi a oggetto risorse economiche, sulla base delle indicazioni fornite dal Comitato, nonché l'adempimento degli obblighi informativi nei confronti dei soggetti designati medesimi, con riguardo alle misure di congelamento adottate nei loro confronti e ai divieti di disporre degli stessi.

Infine, per quanto riguarda l'Agenzia del Demanio, il D.lgs. 109/2007 individua l'Agenzia quale Autorità competente ad assicurare la gestione delle risorse economiche congelate. Spetta infatti all'Agenzia la custodia, l'amministrazione e la gestione delle risorse economiche oggetto di congelamento, cui può provvedere direttamente o mediante la nomina di un custode. Nei casi, invece, in cui le risorse siano oggetto di un precedente provvedimento di sequestro o confisca, provvede alla gestione l'Autorità che ha disposto il sequestro o la confisca.

⁸⁵⁰ In mancanza di specifiche norme che stabiliscano la portata e i limiti di tale potere attuativo, la prassi ha finora elaborato pochi casi in cui tale potere possa essere esercitato: vi rientrano ad esempio, l'individuazione delle risorse economiche da sottoporre a vincolo di congelamento in quanto possedute o detenute da soggetti listati, ai fini dell'annotazione dei conseguenti vincoli di indisponibilità nei registri immobiliari o mobiliari. Sul punto cfr. ad esempio la recente pronuncia del Tar Lazio – sezione seconda del 27/6/2022 n. 8669/22: https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=tar_rm&nrg=20220-4902&nomeFile=202208669_20.html&subDir=Provvedimenti.

⁸⁵¹ Alcuni presidi a tutela dei soggetti designati sono stabiliti anche nelle risoluzioni ONU (che prevedono al riguardo la figura dell'Ombudsperson, competente a ricevere e valutare le istanze di cancellazione dalle liste) e nella normativa comunitaria, che prevede un riesame della situazione dei soggetti designati al fine della loro eventuale rimozione dalla lista (cfr. art. 7-*ter* e 7-*quater* del Reg. 881/2002). Analoga procedura è prevista, a livello nazionale dall'art. 4-*sexies* del D.lgs. 109/2007.

⁸⁵² Tali casi riguardano, a titolo esemplificativo, il pagamento di spese necessarie al sostentamento (le c.d. "spese di base" che comprendono generi alimentari, affitti o ipoteche, medicinali e cure mediche, imposte, premi assicurativi e servizi pubblici), al pagamento di onorari ragionevoli e alla prestazione di servizi legali, al pagamento delle spese connesse alla normale gestione o custodia dei fondi e delle risorse congelati, al pagamento di spese straordinarie, ivi comprese quelle relative ad obbligazioni sorte in epoca anteriore all'inserimento in lista.

6.4. Le violazioni e il quadro sanzionatorio

Anche la materia delle sanzioni non è disciplinata dalla normativa comunitaria, ma rimessa all'autonomia degli Stati membri: infatti i regolamenti comunitari si limitano a stabilire la necessità per questi ultimi di introdurre norme sulle sanzioni, incluse, ove opportuno, le sanzioni penali, applicabili alle violazioni delle disposizioni dei regolamenti che introducono sanzioni finanziarie mirate e di adottare tutte le misure necessarie per garantirne l'attuazione. Come per altri tipi di sanzioni, anche quelle relative all'inosservanza degli obblighi di congelamento devono essere efficaci, proporzionate e dissuasive.

Le sanzioni previste dal legislatore per le violazioni alle norme sui congelamenti sono essenzialmente di carattere amministrativo (cfr. al riguardo gli art. 13 e seguenti del D.lgs. 109/2007); ulteriori sanzioni di carattere penale sono invece previste dal D.lgs. 221/2017 e attengono, in particolare, alle operazioni di esportazione di prodotti listati (nonché alla prestazione di servizi di intermediazione o di assistenza tecnica relativa agli stessi prodotti) effettuate in violazione dei divieti previsti dai regolamenti europei, o in difformità alle autorizzazioni concesse. Per tali condotte è prevista la pena della reclusione da due a sei anni oltre alla confisca obbligatoria dei beni, da attuare anche per equivalente⁸⁵³.

Il D.lgs. 109/2007 disciplina e punisce tre categorie di violazioni. La prima è costituita dalle violazioni agli obblighi di congelamento, e quindi riguarda ogni condotta che configuri un atto di disposizione o utilizzo di beni congelati o la messa a disposizione di fondi e risorse a favore di soggetti designati. È altresì punita ogni condotta facilitatoria, e, quindi la partecipazione consapevole e deliberata ad attività aventi l'obiettivo o il risultato, diretto o indiretto, di aggirare le misure di congelamento. Per tali condotte è prevista la sanzione amministrativa da 5.000 a 500.000 Euro.

La seconda fattispecie riguarda gli obblighi dei soggetti tenuti a comunicare alla UIF informazioni relative ai congelamenti adottati e ai soggetti designati: per tali violazioni è invece prevista una sanzione amministrativa da 500 a 25.000 Euro, anche in considerazione della minore gravità della condotta.

Infine, una recente modifica normativa ha introdotto una terza categoria "residuale" che riguarda ogni altra violazione delle disposizioni restrittive previste dai regolamenti europei⁸⁵⁴, nonché le violazioni degli obblighi di notifica o di richiesta di autorizzazione all'Autorità competente. Come per le violazioni ai congelamenti, anche in tal caso la sanzione prevista varia da 5.000 a 500.000 euro.

In tutti e tre i casi è prevista la prevalenza della fattispecie incriminatrice penale, laddove la violazione costituisca reato, per cui in tali casi non si applicherà la sanzione amministrativa bensì quella più grave di tipo penale.

La sanzione colpisce l'autore materiale della violazione e, nel caso in cui costui agisca per conto o nell'interesse di una persona giuridica, sussiste anche la responsabilità solidale di quest'ultima, fatto salvo il diritto di regresso nei confronti dell'autore della violazione. La responsabilità dell'ente continua a sussistere anche quando il responsabile della violazione non è identificabile o non è più perseguibile.

L'art. 13-ter detta numerosi criteri per l'irrogazione delle sanzioni relative al mancato rispetto delle tre categorie di fatti sopra indicati⁸⁵⁵: al riguardo occorre tenere conto di numerose circostanze, quali il valore dell'operazione, la gravità e durata della violazione, il grado di responsabilità della persona fisica o giuridica, il livello di cooperazione con le Autorità competenti e le precedenti violazioni delle disposizioni. Le sanzioni possono essere anche ridotte fino a un terzo o aumentate fino al triplo a seconda della collaborazione prestata nell'accertamento delle violazioni o in caso di violazioni particolarmente gravi, ripetute o sistematiche. È infine prevista la possibilità di pubblicare un estratto del decreto che irroga la sanzione sul sito web del Ministero dell'Economia e delle finanze o su quello dell'autorità di vigilanza di settore in caso di violazioni gravi ripetute o sistematiche ovvero plurime. Tutti i decreti sanzionatori adottati in base al D.lgs. 109/2007 sono assoggettati alla giurisdizione ordinaria, con la competenza esclusiva del Tribunale di Roma.

⁸⁵³ Tali sanzioni di carattere penale attengono non solo ai divieti previsti nel c.d. regolamento dual-use /Reg. UE n. 428/2009), ma anche per le ulteriori fattispecie di divieto stabilite nei regolamenti europei adottati ai sensi dell'art. 215 del TFEU.

⁸⁵⁴ Sebbene il testo del terzo comma dell'art. 13 rimandi, per l'individuazione dei regolamenti in questione, alle definizioni contenute nell'art. 1 del decreto 109, il riferimento ivi contenuto è fatto alla lett. g) delle definizioni (che riguarda la legge antiriciclaggio), anziché alla lett. h) (che riguarda appunto i regolamenti europei adottati ai sensi degli art. 75 e 215 del TFEU. Sebbene il rinvio non sia formalmente corretto, si ritiene che la volontà del legislatore sia chiara nel rimandare alla lett. h) delle definizioni anziché alla precedente lett. g).

⁸⁵⁵ Le sanzioni sono irrogate dal Ministro dell'Economia e delle finanze, sulla base della contestazione effettuate a cura dell'autorità che ha accertato i fatti, secondo le procedure previste dalla L. 689/81.

7. Le sanzioni dell'UE in risposta all'invasione russa dell'Ucraina (C. Greco e M. Soscia)

L'Unione europea ha introdotto le prime sanzioni contro la Federazione russa già nel 2014 a seguito dell'invasione della Crimea. Nel marzo 2015 la UE ha deciso di collegare il regime delle sanzioni economiche in vigore alla piena attuazione degli accordi di Minsk, accordi che la Russia non ha mai pienamente adempiuto, portando così l'Unione a prorogare le restrizioni adottate⁸⁵⁶. Tali misure sono state successivamente riprese e inasprite a partire dal febbraio 2022 in risposta all'invasione dell'Ucraina, che ha portato la UE ad adottare una serie di successivi e articolati “pacchetti sanzionatori” contenenti sanzioni individuali, economiche nonché misure diplomatiche. L'efficacia di tali misure è stata, da ultimo, prorogata fino al 15 marzo 2023. In tale contesto, l'Unione ha, inoltre, applicato restrizioni anche nei confronti della Bielorussia e dell'Iran a causa del loro coinvolgimento, a diverso titolo, nel conflitto in corso.

La disciplina in questione è contenuta principalmente in due Regolamenti del Consiglio: il Reg. (UE) 269/2014 del 17-03-2014, relativo ai c.d. congelamenti di fondi e risorse economiche detenuti dai soggetti ivi listati, e il Reg. (UE) 833/2014 del 31-07-2014, che comprende una molteplice varietà di misure restrittive. Tali provvedimenti, in quanto Regolamenti, sono direttamente applicabili in tutti gli Stati membri senza necessità di una loro trasposizione da parte del legislatore nazionale.

7.1. Il Regolamento (UE) 269/2014 e le misure restrittive individuali

L'art. 2 del Reg. (UE) 269/2014 impone l'adozione di misure di congelamento⁸⁵⁷ nei confronti di una vasta platea di soggetti, persone fisiche e giuridiche, che a vario titolo hanno fornito supporto all'invasione dell'Ucraina. Trattandosi di “sanzioni finanziarie mirate”, tali misure operano di diritto e sono efficaci direttamente dal momento della pubblicazione nella Gazzetta Ufficiale dell'Unione europea del relativo regolamento attuativo. Da questo momento, quindi, decorrono i termini per adempiere agli obblighi dichiarativi previsti dall'art. 7 del D.lgs. 109/2007.

L'elenco dei nominativi è contenuto nell'allegato I che, costantemente riesaminato e sottoposto a rinnovi periodici da parte del Consiglio, è stato progressivamente ampliato dal 2014 e, attualmente, comprende più di 1200 persone fisiche e oltre 120 persone giuridiche.

Fra le entità sanzionate figurano molte delle principali banche russe, circostanza questa che ha comportato un'applicazione peculiare delle misure di congelamento. Come invero precisato dalla Commissione UE nel parere C(2019)5175 del 4 luglio 2019 rilasciato in un caso simile⁸⁵⁸, i fondi di un soggetto non designato che sono depositati o anche solo trasferiti a una banca listata possono considerarsi “posseduti” dalla stessa, benché temporaneamente e, quindi, sottoposti alla misura di congelamento. L'art. 2, invero, non richiede una durata minima per il possesso dei fondi da parte dell'entità listata; ne consegue che i fondi provenienti da un conto detenuto presso una banca listata non devono né essere rifiutati né restituiti all'ordinante, dovendo gli stessi piuttosto rimanere congelati presso una banca di uno Stato membro⁸⁵⁹.

Particolarità del sistema sanzionatorio disciplinato dal Reg. (UE) 269/2014 è l'introduzione di nuovi e ulteriori obblighi (previsti dagli artt. 8 e 9⁸⁶⁰) di comunicazione e misure di verifica sull'esistenza di beni e disponibilità economiche sottoposte a vincoli di congelamento. Tali disposizioni si aggiungono a quanto già previsto dalla disciplina nazionale, i cui obblighi ai sensi dell'art. 7 del D.lgs. 109/2007 vengono ricalcati solo in parte dalle nuove norme europee.

Nello specifico, l'art. 8 introduce un obbligo dichiarativo di carattere generale, imponendo a qualsiasi persona fisica o giuridica di comunicare immediatamente all'autorità della Nazione competente in cui

⁸⁵⁶ Nello specifico, il Consiglio ha inizialmente prorogato le sanzioni economiche fino al 31-07-2016, per poi prorogarle di volta in volta, sulla scorta di una valutazione dell'attuazione degli accordi di Minsk, per ulteriori periodi di sei mesi.

⁸⁵⁷ La misura di cui all'art. 2 del reg. (UE) 269/2014 è stata anche qui declinata nella sua tipica duplice accezione di obbligo di congelamento e correlativo divieto di mettere a disposizione fondi e risorse economiche descritto nei capitoli precedenti.

⁸⁵⁸ Si trattava di una richiesta di interpretazione relativa alla corretta applicazione delle norme contenute nel Reg. (UE) 267/2012 concernente misure restrittive nei confronti dell'Iran.

⁸⁵⁹ Questa circostanza ha portato al congelamento di numerosi bonifici eseguiti da/verso conti incardinati presso le banche russe listate, anche se detenuti da soggetti terzi. Tale applicazione della norma, tuttavia, non impedisce di richiedere all'autorità nazionale competente il successivo scongelamento dei fondi al ricorrere di eventuali deroghe, come ad es. quelle previste dall'art. 6 e seguenti del regolamento.

⁸⁶⁰ Introdotti dal regolamento (UE) 1273/2022 del Consiglio del 21 luglio 2022, che ha modificato il regolamento (UE) 269/2014.

risiedono o sono situati, qualsiasi informazione atta a facilitare il rispetto del Reg. (UE) 269/2014⁸⁶¹ nonché di collaborare con tale autorità per le relative verifiche.

Rispetto agli obblighi previsti a livello domestico dall'art. 7 del D.lgs. 109/2007, l'art. 8, in primo luogo, sembra introdurre una dichiarazione di avvenuto congelamento che, tuttavia, non sostituisce, ma si aggiunge a quella prevista dall'art. 7, comma 1; in particolare, infatti, questo specifico obbligo dichiarativo, per il quale non è disposto un termine specifico, in quanto l'art. 8 prevede che sia effettuato "immediatamente", non elide il termine di 30 giorni imposto dalla normativa nazionale che, quindi, integra la disposizione europea in questione. In secondo luogo, la norma introduce un generale obbligo dichiarativo, simile a quello previsto dall'art. 7, comma 2, del D.lgs. 109/2007, ampliando, tuttavia, il novero dei soggetti tenuti alla presente comunicazione⁸⁶², che qui ricade su qualsiasi persona fisica o giuridica in possesso, a qualsiasi titolo, delle informazioni indicate dall'art. 8. In quest'ottica, al fine di rafforzare l'incisività di questa nuova dichiarazione, il comma 1 dell'art. 8 precisa che l'obbligatorietà della comunicazione non è esclusa dalle norme applicabili in materia di relazioni, riservatezza e segreto professionale, prevalendo dunque su quest'ultime l'obbligo di cui all'art. 8.

L'art. 9, comma 2, del regolamento, invece, introduce un'assoluta novità rispetto al tradizionale sistema delle sanzioni mirate, ponendo in capo agli stessi soggetti designati dall'allegato I del Reg. (UE) 269/2014 l'obbligo di trasmettere all'autorità competente dello Stato membro in cui i fondi e/o le risorse economiche sono situati, le informazioni relative ai fondi o alle risorse economiche loro appartenenti o da loro posseduti nella relativa giurisdizione. Il termine per l'adempimento è stato fissato al 1 settembre 2022 o, se posteriore, entro 6 settimane dalla data dell'inserimento del nominativo nell'elenco.

La portata coercitiva di tale obbligo è rafforzata dalle altre previsioni contenute nell'art. 9, che, in combinato disposto con l'art. 15, prevedono un meccanismo di divieti e sanzioni di eventuali comportamenti elusivi delle misure restrittive in questione. In particolare, mentre il par. 1 dell'art. 9 sancisce il divieto di partecipare, consapevolmente e deliberatamente, ad attività aventi l'obiettivo o il risultato di eludere le misure di congelamento cui all'art. 2, il par. 3 stabilisce che l'inosservanza da parte dei soggetti designati dell'obbligo dichiarativo di cui al par. 2 integra un'ipotesi di partecipazione vietata dal citato par. 1. La disciplina sanzionatoria è contenuta nell'art. 15 del regolamento, il quale impone agli Stati membri, innanzitutto, di stabilire sanzioni, ove opportuno anche di tipo penale applicabili in caso di violazione delle disposizioni del regolamento; in secondo luogo, di prevedere altresì misure appropriate per la confisca dei proventi di tali violazioni.

In Italia il CSF, in qualità di autorità nazionale competente per l'attuazione delle misure di congelamento, con delibera dell'11 agosto 2022, ha designato la UIF alla ricezione e alla raccolta delle informazioni di cui agli artt. 8 e 9 del regolamento (UE) 269/2014, nonché alla definizione di contenuti e formati per eseguire le citate comunicazioni⁸⁶³.

Infine, oltre al congelamento delle loro risorse economiche e finanziarie, alle persone designate è stato imposto un "travel ban" che ne impedisce l'ingresso nel territorio dell'Unione europea⁸⁶⁴.

7.2. Il Regolamento (UE) 833/2014 e le misure restrittive al "sistema paese"

I Regolamenti (UE) 833/2014 e (CE) 765/2006, come modificati dai successivi Regolamenti di esecuzione, introducono una molteplicità di misure restrittive nei confronti della Russia e della Bielorussia, con l'obiettivo di esercitare pressioni sulla leadership politica russa e bielorussa al fine di prevenire ulteriori violenze, repressioni e atti ostili.

Le misure restrittive introdotte dall'Unione europea riguardano l'economia russa, il Governo e la diplomazia di Mosca e di Minsk a trecentosessanta gradi. Sono stati colpiti specifici settori dell'economia quali, in particolare, quello finanziario, dei trasporti, della difesa, dell'energia, della tecnologia e del commercio.

⁸⁶¹ Si tratta in particolare delle "informazioni relative ai conti e agli importi congelati a norma dell'articolo 2 o relative ai fondi e alle risorse economiche nel territorio dell'Unione appartenenti a, posseduti, detenuti o controllati dalle persone fisiche o giuridiche, dalle entità o dagli organismi elencati nell'allegato I del Regolamento che non sono stati ancora trattati come congelati dalle persone fisiche e giuridiche, dalle entità e dagli organismi obbligati a congelarli".

⁸⁶² Gli obblighi dichiarativi previsti a livello nazionale dall'art. 7 del D.lgs. 109/2007, riguardano infatti i soli c.d. soggetti obbligati, quelli cioè identificati come tali ai sensi del decreto legislativo antiriciclaggio (D.lgs. 231/2007).

⁸⁶³ L'Unità, quanto alle informazioni relative ai fondi, verifica che trovino coerente riscontro nelle comunicazioni trasmesse dai soggetti obbligati ai sensi del D.lgs. 109/2007 e relative ai medesimi fondi; le informazioni relative alle risorse economiche, invece, vengono rese disponibili al NSPV della Guardia di Finanza per le verifiche sul congelamento di tali risorse.

⁸⁶⁴ Il divieto è previsto dall'art. 1 della Decisione 2014/145/PESC del Consiglio del 17-03-2014.

Settore finanziario. Per talune banche e società russe è stato ristretto l'accesso al mercato dei capitali primari e secondari dell'Unione europea, riducendo quindi la possibilità per tali entità di ottenere risorse finanziarie dall'Europa. È inoltre entrato in vigore il divieto di fornire banconote denominate in euro a Russia e Bielorussia nonché il divieto di finanziare o effettuare investimenti pubblici in Russia. È stato inoltre previsto il divieto di effettuare operazioni con la Banca centrale russa e la Banca centrale bielorussa ed è stato bloccato l'accesso al sistema SWIFT per alcuni intermediari finanziari.

Settore dei trasporti. Le vie di accesso all'Unione europea sono state fortemente ristrette attraverso l'introduzione del divieto di sorvolare l'UE, con la chiusura dello spazio aereo, per gli aeromobili di proprietà russa o immatricolati in Russia, la chiusura dei porti alle navi russe e il divieto di accesso per i trasportatori su strada russi e bielorussi. È previsto, inoltre, il divieto di esportazione di beni e tecnologia nei settori aeronautico, spaziale e marittimo verso la Russia.

Settore della difesa. È previsto il divieto di esportare e commercializzare con la Russia armi, munizioni, veicoli militari, equipaggiamenti paramilitari e, più in generale, beni e tecnologie il cui uso potrebbe essere in grado di contribuire alle capacità di difesa e sicurezza della Russia.

Settore dell'energia. L'Unione europea ha introdotto il divieto di importazione, salvo limitate eccezioni, di carbone e petrolio dalla Russia e ha previsto un tetto sui prezzi relativo al trasporto marittimo del petrolio russo per i Paesi terzi, oltre al divieto di esportazione di beni e tecnologie nel settore della raffinazione del petrolio, nonché di investimenti nel settore dell'energia in Russia.

Settori della tecnologia e del commercio. Numerosi sono i prodotti e i servizi per i quali è fatto divieto di commercializzare con la Russia. Tra gli altri si annoverano: il divieto all'importazione di oro e altri beni di lusso, prodotti siderurgici, legno, plastica, prodotti ittici; il divieto di prestare servizi di portafoglio, di architettura e ingegneria, di consulenza informatica e giuridica.

Il regolamento prevede ulteriori misure restrittive e sanzionatorie che non si limitano a colpire il sistema economico dei paesi destinatari delle sanzioni, ma puntano a colpirne più direttamente i rispettivi Governi.

Misure diplomatiche prevedono che i vertici periodici che vedono la partecipazione di UE e Russia sono sospesi. La Russia non è, ad esempio, più invitata alle riunioni del G8 – che ora si riunisce nella forma del G7 – e i diplomatici, i funzionari, gli imprenditori e – dal settembre 2022 – tutti i cittadini russi non possono più beneficiare delle disposizioni sulla facilitazione del rilascio dei visti.

Restrizioni ai media hanno determinato la sospensione delle trasmissioni nell'Unione europea degli organi di informazione pubblici russi in quanto sotto il controllo diretto del Governo russo e, da questo, utilizzati come strumenti di propaganda, di manipolazione delle informazioni e di disinformazione sull'invasione dell'Ucraina. Restrizioni alla cooperazione economica, invece, impediscono l'erogazione di prestiti alla Russia da parte della Banca europea per gli Investimenti (BEI) e della Banca europea per la Ricostruzione e lo Sviluppo (BERS).

7.3. I divieti sui depositi e le comunicazioni "DEPRU"

Una delle misure maggiormente innovative nell'ambito delle sanzioni finanziarie è stata introdotta con gli artt. 5-ter e seguenti del regolamento (UE) 833/2014 e gli artt. 1-duovicies e seguenti del regolamento (CE) 765/2006, i quali dispongono il divieto di accettare depositi di cittadini russi o bielorussi o di persone fisiche residenti in Russia o Bielorussia, ovvero di persone giuridiche, entità od organismi stabiliti in Russia o Bielorussia o di persone giuridiche, entità od organismi stabiliti fuori dall'Unione, i cui diritti di proprietà sono riconducibili, direttamente o indirettamente, per oltre il 50% a cittadini russi o persone fisiche residenti in Russia, se il valore dei depositi è superiore a 100.000 euro, per singolo ente creditizio.

Tale restrizione è stata successivamente estesa ad altri servizi; in particolare, nel solo ambito del Reg. (UE) 833/2014, il par. 2 dell'art. 5-ter ha ampliato il divieto, includendo anche i servizi di portafoglio, conti o custodia di cripto-attività. Ai sensi del par. 3 del medesimo articolo, i citati divieti non si applicano, invece, ai cittadini o ai titolari di permesso di soggiorno europeo, di un paese dello Spazio economico europeo o della Svizzera. Pertanto, rientrano nella deroga tutti quei soggetti che posseggano anche la cittadinanza o un permesso di soggiorno europeo, sia esso permanente o temporaneo.

Il citato regolamento prevede delle deroghe al divieto in base alle quali le autorità competenti possono autorizzare l'accettazione dei depositi per importi superiori ai 100.000 euro in casi specifici come, ad esempio, per consentire il pagamento di onorari o rimborsi spese per prestazioni di servizi legali, per scopi ufficiali di missioni diplomatiche, qualora fosse necessario per scambi transfrontalieri non vietati di beni e servizi tra Unione e Russia o Bielorussia, per scopi umanitari, ecc.

Altra novità è rappresentata dall'art. 5-octies del citato regolamento (UE) 833/2014 e dall'art. 1-septuies del citato regolamento (CE) 765/2006, i quali introducono l'obbligo per gli enti creditizi di comunicare alla UIF – autorità delegata alla ricezione di predette comunicazioni dal Comitato di Sicurezza

Finanziaria – informazioni: a) sui depositi di importo superiore a 100.000 euro detenuti da cittadini russi o bielorussi o persone fisiche residenti in Russia o Bielorussia, o da persone giuridiche, entità od organismi stabiliti in Russia o Bielorussia, con periodicità annuale e con saldo di riferimento al 25 febbraio di ogni anno; b) sui depositi di importo superiore a 100.000 euro detenuti da cittadini russi o bielorussi o persone fisiche residenti in Russia o Bielorussia che hanno acquisito la cittadinanza di uno Stato membro od ottenuto diritti di soggiorno in uno Stato membro attraverso un programma di cittadinanza o un programma di soggiorno per investitori, con periodicità mensile e con saldo di riferimento al 27 di ogni mese.

Le due comunicazioni sono alternative tra di loro e, dunque, le informazioni trasmesse ai sensi della lett. b) non devono essere oggetto di comunicazione anche ai sensi della lett. a)⁸⁶⁵. I dati così ottenuti vengono poi condivisi dalla UIF con la Commissione europea.

8. La proliferazione armi di distruzione di massa (D. Bartolozzi)

Il GAFI, con l'adozione delle nuove raccomandazioni nel 2012, oltre ad aver accorpato in un unico testo gli standard in materia di riciclaggio di denaro sporco (le originali 40 raccomandazioni) e quelli in materia di finanziamento del terrorismo (le nove “raccomandazioni speciali”) ha anche esteso il proprio campo d'azione, aggiungendo al proprio mandato il contrasto al finanziamento della proliferazione di armi di distruzione di massa (d'ora in poi indicato come “finanziamento della proliferazione”).

È stata così introdotta una nuova raccomandazione (la settima), che richiede agli stati di implementare senza ritardo le sanzioni finanziarie mirate stabilite nelle risoluzioni del Consiglio di Sicurezza dell'Onu in materia di proliferazione, che prevedono obblighi di congelamento di fondi e i correlativi divieti di mettere fondi a disposizioni dei soggetti designati.

Nel corso del 2020 il tema della proliferazione ha formato oggetto di un'ulteriore modifica delle raccomandazioni GAFI, a seguito di un esplicito invito formulato in tal senso dal G20 nel 2019, che richiedeva proprio al GAFI di rafforzare la sua azione di contrasto in tale materia. Le modifiche introdotte riguardano, in particolare, le prime due raccomandazioni che disciplinano l'adozione di politiche e forme di coordinamento efficaci in materia di prevenzione e contrasto al riciclaggio e finanziamento del terrorismo.

Delle due modifiche, quella relativa alla prima raccomandazione è sicuramente quella di maggiore impatto. Il nuovo testo della raccomandazione richiede infatti ai paesi di identificare, valutare e comprendere il rischio di finanziamento della proliferazione inerente il paese stesso. Tale attività di valutazione, che replica in gran parte quella relativa alla valutazione nazionale del rischio di riciclaggio e di finanziamento del terrorismo, ha tuttavia una portata specifica e un ambito del tutto particolare. Infatti, nell'assenza di una definizione univoca e vincolante di finanziamento della proliferazione⁸⁶⁶, l'ambito della valutazione deve intendersi limitata esclusivamente al rischio di mancata attuazione delle sanzioni finanziarie mirate in materia di proliferazione. Tale valutazione del rischio deve essere effettuata non soltanto dalle Autorità del settore pubblico, ma anche dai soggetti obbligati, allo scopo di individuare le opportune contromisure da prendere, specie in relazione all'allocazione delle risorse necessarie, tenuto conto del concreto livello di rischio identificato.

La modifica della prima raccomandazione, ancorché formalmente in vigore già dal 2020, non è stata ancora resa vincolante per i Paesi membri del GAFI, a causa della difficoltà e del tempo necessario per introdurre e sviluppare le adeguate procedure all'interno dei paesi, oltre che per fornire l'indispensabile supporto, anche al settore privato⁸⁶⁷, per l'adozione delle procedure di valutazione del rischio: è attualmente previsto che la valutazione di tali aspetti prenderà avvio con il nuovo ciclo di *Mutual Evaluation*, che dovrebbe essere avviato appena finito il quarto ciclo di valutazioni.

L'ulteriore modifica adottata dal GAFI nel 2020 riguarda la seconda raccomandazione e concerne l'introduzione del finanziamento della proliferazione (insieme al riciclaggio e al finanziamento del

⁸⁶⁵ Cfr. le FAQ pubblicate sul sito della UIF.

⁸⁶⁶ Va infatti evidenziato che, al di là della previsione di specifici obblighi e divieti, quali i congelamenti di fondi e la previsione di limitazioni alle esportazioni), le convenzioni internazionali e le risoluzioni del Consiglio di Sicurezza dell'ONU non prevedono una criminalizzazione delle condotte di proliferazione, come invece è espressamente previsto per il riciclaggio del denaro sporco e il finanziamento del terrorismo.

⁸⁶⁷ Una guidance in tal senso è stata recentemente approvata e pubblicata dal GAFI: cfr. al riguardo. <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>.

terrorismo) fra gli ambiti nei quali assicurare la presenza di efficaci meccanismi che assicurino la possibilità di cooperare e scambiare informazioni fra autorità competenti, in particolare allo scopo di garantire lo sviluppo e l'adozione di politiche e attività di contrasto a tali tre fenomeni.

Come si è detto, non esiste un nozione univoca di proliferazione⁸⁶⁸ né una convenzione internazionale che impone di criminalizzare il reato di proliferazione⁸⁶⁹. Al riguardo, la fonte principale degli obblighi in materia di contro-proliferazione è contenuta nelle Risoluzioni del Consiglio di Sicurezza dell'ONU, adottate ai sensi del Capitolo VII dello statuto dell'ONU medesima.

Le risoluzioni in argomento, che sono vincolanti per gli Stati membri ancorché non immediatamente efficaci nei confronti dei loro cittadini, prevedono sia un approccio generale, finalizzato a vietare determinate operazioni in capo ai privati, quali il divieto di esportare e finanziarie operazioni in merci che potrebbero contribuire alla proliferazione delle armi di distruzione di massa⁸⁷⁰, sia un approccio specifico, indirizzato a colpire le attività di determinati paesi che sono stati identificati per aver compiuto violazioni agli obblighi imposti dall'ONU⁸⁷¹. Tali misure hanno formato oggetto di tempestivo recepimento da parte dell'Unione europea, mediante l'emanazione di appositi regolamenti, che hanno volta per volta recepito le modifiche stabilite dalle Nazioni Unite, prevedendo, altresì, ulteriori misure adottate in maniera autonoma⁸⁷².

La base normativa valida in tutto il territorio dell'Unione è costituita da due regolamenti: il regolamento n. 1509/2017, relativo a misure restrittive nei confronti della Repubblica popolare democratica di Corea e che abroga il precedente regolamento n. 329/2007, e il regolamento n. 267/2012, concernente misure restrittive nei confronti dell'Iran e che abroga il precedente regolamento n. 961/2010.

Ci si limiterà in questa sede a passare brevemente in rassegna i principali divieti e limitazioni previsti dal regolamento relativo alla Corea del Nord, posto che è quello che contiene i divieti e le limitazioni di maggiore portata, alcuni dei quali si applicavano prima del 2015 anche alla Repubblica islamica dell'Iran. L'attuale testo del regolamento 1509/2017 prevede, oltre a specifiche misure di congelamento e di divieto di messa a disposizione di fondi e risorse economiche nei confronti di determinati individui ed entità, specifiche restrizioni commerciali e finanziarie nei confronti della Corea del Nord.

Tali restrizioni riguardano, in particolare, il divieto di importazione ed esportazione, anche in via indiretta, di determinate categorie di beni, specificate negli allegati al regolamento. Il divieto si estende non solo all'operazione di import-export in sé, ma anche alle connesse attività di intermediazione, commerciale e finanziaria, e riguarda anche le attività accessorie di assistenza tecnica e assistenza finanziaria. Rientrano nell'ambito dei beni e tecnologie sottoposti a divieto non solo quelli suscettibili direttamente di impiego proliferante o militare, ma anche altre tipologie quali l'oro, i beni di lusso e i prodotti petroliferi.

Ulteriori divieti riguardano l'effettuazione di determinate attività di carattere commerciale rese nei confronti o con la partecipazione di cittadini nordcoreani: è ad esempio vietato approvare investimenti o partecipare ad imprese comuni con

⁸⁶⁸ Una possibile definizione può tuttavia essere ricavata dal secondo punto della Risoluzione ONU 1540/2006, che chiede agli Stati membri di vietare “*to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in them as an accomplice, assist or finance them*”. Su tale base il GAFI ha proposto la seguente come possibile “definizione” di finanziamento della proliferazione, non vincolante per gli stati: “*the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligation*”.

⁸⁶⁹ Alcuni stati, tuttavia prevedono delle fattispecie incriminatrici che possono coprire la condotta di proliferazione: per esempio facendo riferimento alle norme sul contrabbando o a quelle che colpiscono le esportazioni di beni dual-use senza le previste autorizzazioni delle competenti autorità.

⁸⁷⁰ Risoluzione ONU 1540/2004.

⁸⁷¹ Si tratta, in particolare, delle Risoluzioni 1718/2006, nei confronti della Repubblica Democratica della Corea del Nord (DPRK) e 2231/2015 nei confronti della Repubblica Islamica dell'Iran. Il contenuto dei divieti imposti nei confronti dell'Iran è stato sensibilmente ridotto dopo la sottoscrizione degli accordi relativi al JCPOA (Joint Comprehensive Plan of Action), pur mantenendosi ancora un numero di misure comprendenti congelamenti di fondi e altre misure, seppure di natura sensibilmente contenuta rispetto alle precedenti risoluzioni ONU (1737/2006 e successive integrazioni e modificazioni).

⁸⁷² È il caso, ad esempio, del regolamento UE 1509/2017 che comprende liste differenti di soggetti designati nei confronti dei quali devono essere adottate misure di congelamento dei fondi: l'allegato XIII, infatti, comprende i nominativi designati dall'ONU, mentre gli allegati XV, XVI e XVII comprendono i nominativi ed entità listati in maniera autonoma dall'Unione.

cittadini o entità nordcoreane, nonché concedere loro in locazione immobili, ad eccezione di quelli destinati ad attività diplomatiche e consolari.

Sanzioni di particolare rilevanza sono quelle relative ai trasferimenti di fondi e alla prestazione di servizi finanziari. Il regolamento, infatti, non solo vieta agli enti creditizi e finanziari europei di continuare o iniziare transazioni con enti finanziari e creditizi aventi sede in Corea del Nord, ma vieta anche l'effettuazione di qualsiasi trasferimento di fondi da e verso la Corea del Nord (art. 21, comma 1 del reg. 1509/2017). A tale regime di divieto sono previste tuttavia alcune eccezioni che riguardano, in particolare, le rimesse personali non superiori ai 5.000 euro, nonché determinate transazioni, fino ad un importo pari o inferiore a 15.000 euro relative a determinate finalità quali l'esecuzione di contratti relativi a prodotti alimentari, le esigenze di rappresentanze diplomatiche o consolari e l'esecuzione di altri contratti non espressamente vietati dal regolamento. Entrambe le soglie possono essere derogate laddove intervenga un'esplicita autorizzazione da parte della competente Autorità nazionale dello Stato membro. Ulteriori divieti sono previsti in relazione alla possibilità di detenere conti presso enti creditizi nordcoreani, o di aprire succursali o uffici di rappresentanza in Corea del Nord, nonché di effettuare operazioni di diverso genere con enti creditizi e finanziari nordcoreani.

Anche l'apertura di conti per le rappresentanze e gli uffici diplomatici e consolari e i loro membri è sottoposta a particolari restrizioni: stabilisce, infatti, l'art. 29 del regolamento che l'apertura di tali rapporti finanziari deve essere autorizzata dalla competente Autorità nazionale su espressa richiesta della rappresentanza o ufficio diplomatico e che ciascuno di essi non può detenere più di un unico rapporto in tutto il territorio nazionale.

Infine, una norma avente una portata del tutto particolare è quella che prevede l'obbligo in capo agli intermediari finanziari di inviare una segnalazione di operazione sospetta se vi sono fondati motivi di sospettare che i fondi possano contribuire a programmi o attività nordcoreani connessi alle armi nucleari, ai missili balistici o ad altre armi di distruzione di massa, nonché di segnalare tempestivamente qualsiasi transazione sospetta, compresi i tentativi di transazioni sospette.

Si tratta di un obbligo del tutto autonomo e differente, per quanto con un contenuto molto simile, rispetto a quello previsto dall'art. 35 del D.lgs. 231/2007. Una delle differenze più evidenti va riscontrata nel destinatario della norma che, in maniera poco comprensibile e sicuramente poco coordinata, nel regolamento europeo è individuata solo negli enti finanziari e creditizi dell'Unione, mentre gli obblighi di segnalazione si applicano, in base alla direttiva antiriciclaggio, anche a una serie di professionisti ed esercenti altre attività.

Una seconda differenza va riscontrata nel presupposto della segnalazione, che il regolamento individua esclusivamente nell'attività con enti creditizi e finanziari appartenenti alla Corea del Nord⁸⁷³, limitando quindi di gran lunga la portata dell'obbligo: infatti, la presenza di numerosi divieti nell'operatività con intermediari finanziari nordcoreani scoraggia o rende estremamente improbabile forme di relazione diretta fra tali intermediari e quelli europei, rendendo più frequente la possibilità di triangolazioni con Paesi terzi, che tuttavia sfuggono al precetto normativo.

Il regolamento specifica, infine, che l'Unità di informazione finanziaria del Paese membro riceve relazioni riguardanti il finanziamento potenziale della proliferazione e ha accesso, direttamente o indirettamente, in maniera tempestiva alle informazioni finanziarie, amministrative e giudiziarie necessarie per assolvere correttamente questo compito, compresa l'analisi delle segnalazioni di transazioni sospette.

Appare pertanto di tutta evidenza come tale disciplina finisca per creare un differente regime di approfondimento delle segnalazioni di "proliferazione": se, infatti, per l'analisi "domestica" la FIU sembra potersi avvalere di tutti i poteri e prerogative attribuite dalla legge nazionale, tuttavia appare esclusa, in modo sorprendente, la possibilità del ricorso allo strumento della cooperazione internazionale, atteso che la stessa non è richiamata dal regolamento e che le norme che regolano gli scambi tra FIU (sia nelle raccomandazioni GAFI, sia negli standard del Gruppo Egmont, sia, infine, nelle regole europee) non prevedono tale fattispecie fra quelle che consentono il ricorso agli scambi fra FIU estere.

⁸⁷³ Rientrano in tale definizione ai sensi del par. 2 dell'art. 21 gli enti finanziari o creditizi con sede nella RPDC; le succursali o controllate di enti finanziari e creditizi con sede nella RPDC; gli enti finanziari e creditizi che non sono domiciliati nella RPDC e che sono controllati da persone, entità o organismi domiciliati nella RPDC.

CAPITOLO 8

Le disposizioni sanzionatorie penali e amministrative

(a cura di V. Tusini Cottafavi)

1. Principi ed evoluzione del quadro sanzionatorio (V. Tusini Cottafavi)

La normativa di prevenzione del riciclaggio e del finanziamento del terrorismo si fonda sulla collaborazione con le autorità competenti di un ampio spettro di operatori economici, che rischiano di venire attratti inconsapevolmente in attività illecite a danno dell'integrità, della stabilità e della reputazione del sistema economico-finanziario.

Si tratta di una specificità della predetta normativa, che si rivolge essenzialmente agli operatori onesti, incoraggiandone la predisposizione di appositi presidi nonché l'invio di flussi informativi verso le Autorità pubbliche a tutela della legalità e del loro stesso interesse a non essere coinvolti in contesti criminali.

Questo incentivo "naturale" all'adempimento degli obblighi di collaborazione è corroborato e reso cogente dalla previsione di un articolato insieme di prescrizioni organizzative e comportamentali e di un correlato sistema di controlli e di sanzioni.

In un contesto fondato sulla collaborazione tra operatori e istituzioni è particolarmente rilevante che la risposta sanzionatoria alle violazioni sia improntata a equilibrio ed equità e sia riconosciuta come tale dai destinatari, in modo da realizzare in modo ottimale gli obiettivi di dissuasione e deterrenza che le sono propri. Le misure, sia sul piano normativo sia su quello applicativo, devono tendere a un elevato grado di chiarezza e proporzionalità, colpire in modo efficace chi si pone in contrasto con il sistema di collaborazione commettendo violazioni gravi di aspetti sostanziali della disciplina e tralasciare, invece, le mancanze meramente formali o prive di reale offensività.

Il vigente quadro normativo – oggetto di importanti riforme nell'ultimo quinquennio in connessione col recepimento delle nuove normative antiriciclaggio europee – punisce le violazioni della disciplina di prevenzione con sanzioni sia penali sia amministrative.

Sul versante penalistico le attuali fattispecie incriminatrici riguardano condotte effettivamente gravi perché realizzate attraverso frode o falsificazione ovvero in violazione di una regola fondamentale della collaborazione attiva, quella del divieto di comunicazione dell'avvenuta segnalazione di operazioni sospette. Sono stati così superati gli eccessi punitivi del sistema previgente, portando a compimento il processo di evoluzione della normativa in materia, che era stata anche oggetto di un intervento di depenalizzazione nel 2016⁸⁷⁴.

Con riguardo al versante amministrativo, la disciplina sanzionatoria è stata profondamente riformata nel 2017 e ulteriormente ritoccata nel 2019, in occasione del recepimento, rispettivamente, della quarta e della quinta direttiva europea⁸⁷⁵.

La riforma ha rappresentato un'occasione importante per superare le notevoli criticità del sistema previgente, che aveva generato dubbi interpretativi e difficoltà applicative principalmente connesse all'individuazione delle persone fisiche responsabili e alla correlazione fra entità della sanzione e importo delle operazioni poste a base delle contestazioni⁸⁷⁶.

⁸⁷⁴ L'apparato penale previgente era invece considerato "caratterizzato da eccessi punitivi per comportamenti non particolarmente gravi e da notevoli lacune" da L. Criscuolo, *L'apparato sanzionatorio: disciplina e problematiche applicative*, in G. Castaldi e C. Conforti (a cura di), *Manuale antiriciclaggio*, cit., p. 301.

⁸⁷⁵ Si fa riferimento al D.lgs. 25 maggio 2017, n. 90, e al D.lgs. 4 ottobre 2019, n. 125, con i quali sono state recepite, rispettivamente, la direttiva (UE) 2015/849 (c.d. quarta direttiva) e la direttiva (UE) 2018/848 (c.d. quinta direttiva). Il D.lgs. 125/2019 ha altresì apportato taluni correttivi al D.lgs. 231/2007 anche in materia sanzionatoria.

⁸⁷⁶ In proposito L. Criscuolo, *L'apparato sanzionatorio: disciplina e problematiche applicative*, cit., p. 306, ha rilevato che "difficoltà applicative sono riscontrabili anche nei casi in cui occorre contestare a più soggetti una parte (magari minima) dell'operatività ovvero nei casi di operazioni

Al fine di risolvere in radice tali criticità si palesava l'esigenza di un cambio profondo di impostazione giuridica che passasse a un sistema di sanzionabilità delle persone giuridiche tenute all'adempimento degli obblighi antiriciclaggio (con rivalsa verso il responsabile effettivo della violazione), e di sanzioni in misura fissa (eventualmente differenziate in relazione alla natura del soggetto obbligato), con minimi e massimi parametrati alla effettiva gravità della violazione e alla tipologia del soggetto obbligato⁸⁷⁷. La citata riforma del 2017 si è mossa lungo queste direttrici, ma il quadro che ne è scaturito non può dirsi abbia centrato appieno gli obiettivi enunciati dalla legge di delega al Governo (Legge 170/2016), di un sistema dotato di misure efficaci, proporzionali, dissuasive e rispettose del principio del *ne bis in idem*.

Seppur con alcune incertezze e ridondanze, i criteri della legge delega⁸⁷⁸ indicavano di: *i)* graduare l'entità e la tipologia delle sanzioni amministrative tenuto conto della natura del soggetto cui è ascrivibile la violazione (persona fisica o giuridica) nonché del settore di attività, delle dimensioni e della complessità organizzativa dei soggetti obbligati e, in funzione di ciò, delle differenze tra enti creditizi e finanziari e altri soggetti obbligati; *ii)* prevedere che, in caso di violazione commessa da una persona giuridica, la sanzione possa essere applicata ai membri dell'organo di gestione o alle altre persone fisiche titolari di poteri di amministrazione, direzione o controllo all'interno dell'ente, ove venga accertata la loro responsabilità; *iii)* stabilire che, in caso di violazioni gravi, ripetute o sistematiche ovvero plurime delle disposizioni in materia di adeguata verifica della clientela, di segnalazione di operazioni sospette, di conservazione dei documenti e di controlli interni, le misure sanzionatorie comprendano sanzioni amministrative pecuniarie (di importo più elevato per le violazioni commesse da intermediari bancari e finanziari⁸⁷⁹) e misure ulteriori rispetto alle predette sanzioni⁸⁸⁰. Le Autorità di vigilanza di settore sono state inoltre chiamate a definire disposizioni attuative con riferimento alle sanzioni da esse irrogate nel nuovo quadro normativo.

La disciplina sanzionatoria emanata in attuazione di tale delega nel 2017⁸⁸¹ ha delineato un sistema molto articolato e complesso per un intreccio di: previsioni riguardanti violazioni gravi, ripetute, sistematiche o plurime e violazioni "base" (ossia prive di dette qualificazioni); disposizioni relative ai soggetti obbligati in generale e disposizioni speciali per i soggetti vigilati; responsabilità delle persone giuridiche, di esponenti aziendali e del personale di talune categorie di soggetti obbligati; competenze sanzionatorie parallele delle Autorità di vigilanza e del Ministero dell'Economia e delle finanze⁸⁸² (cfr. quadro sinottico riportato nelle Tavole n. 1 e n. 2).

molteplici e durature nel tempo. Le sanzioni dirette alle persone fisiche si prestano a essere eluse attraverso artate frammentazioni dei compiti, che possono rendere problematica l'attribuzione della responsabilità delle omissioni". "La parametrizzazione dell'entità delle sanzioni all'importo delle operazioni può comportare la contestazione di sanzioni del tutto sproporzionate rispetto alla capacità patrimoniale dei responsabili (persone fisiche e giuridiche) ovvero l'impossibilità di quantificare le violazioni connesse a operazioni prive di importo (ad esempio, rilascio di garanzie) o alla valutazione complessiva dell'operatività di un soggetto".

⁸⁷⁷ Così L. Criscuolo, *L'apparato sanzionatorio: disciplina e problematiche applicative*, cit., p. 307.

⁸⁷⁸ Art. 15, comma 2, lett. h), della legge 170/2016.

⁸⁷⁹ Sanzioni amministrative pecuniarie comprese tra 30.000 euro e il 10 per cento del fatturato ove applicate alla persona giuridica; sanzioni amministrative pecuniarie comprese tra 10.000 euro e un massimo di 5 milioni di euro ove applicate alle persone fisiche responsabili. Invece, per le violazioni di scarsa offensività e pericolosità commesse da enti creditizi o finanziari prevedere, in alternativa alla sanzione pecuniaria, una dichiarazione pubblica che individua la persona fisica o giuridica responsabile e la natura della violazione e un ordine che impone alla persona giuridica di porre termine al comportamento vietato e di astenersi dal ripeterlo, nonché l'irrogazione di una sanzione pecuniaria maggiorata per la violazione del medesimo ordine.

⁸⁸⁰ Una dichiarazione pubblica che individua la persona fisica o giuridica responsabile e la natura della violazione; un ordine che impone alla persona fisica o giuridica di porre termine al comportamento vietato e di astenersi dal ripeterlo; nel caso in cui l'autore della violazione sia soggetto ad autorizzazione o altro titolo abilitativo, la revoca o, ove possibile, la sospensione dell'autorizzazione ovvero un'altra sanzione disciplinare equivalente da parte dell'autorità di vigilanza di settore o dell'organismo di autoregolamentazione competenti; per le persone fisiche, titolari di poteri di amministrazione, direzione o controllo all'interno della persona giuridica obbligata e ritenute responsabili della violazione ovvero per qualsiasi altra persona fisica ritenuta responsabile della violazione, l'interdizione temporanea dall'esercizio delle funzioni per un tempo non superiore a cinque anni.

⁸⁸¹ D.lgs. 90/2017, che ha modificato il D.lgs. 231/2007.

⁸⁸² È stata altresì prevista una disciplina transitoria per il passaggio dal vecchio al nuovo regime correttamente ispirata al principio del *favor rei*, ma di non agevole applicazione data la complessità dell'articolazione delle nuove fattispecie e del loro raccordo con le precedenti (cfr. art. 69, comma 1). Inoltre, è stato stabilito che il termine per la conclusione del procedimento sanzionatorio è di due anni, decorrenti dalla ricezione della contestazione notificata all'amministrazione procedente. Il termine può essere prorogato di ulteriori sei mesi nel caso di formale richiesta da parte dell'interessato di essere auditato nel corso del procedimento. In ogni caso, il procedimento si considera concluso con l'adozione del decreto che dispone in ordine alla sanzione. Per i procedimenti pendenti alla data di entrata in vigore della riforma, il termine ivi previsto, ove non ancora maturato, è stato prorogato di ulteriori dodici mesi (art. 69, commi 2 e 3), con estinzione del procedimento in caso di mancata adozione del provvedimento sanzionatorio anche entro tale data. Sul tema del *favor rei* cfr. in giurisprudenza Cass. n. 20647/2018, Cass. 24017/2022; Cass. n. 20697/2018 e Cass. n. 24476/2022 nonché per note di commento a quest'ultima pronuncia E.

In questo contesto, il rilievo sanzionatorio attribuito anche alle violazioni diverse da quelle qualificate come “gravi, ripetute o sistematiche ovvero plurime” non appare coerente con l’esigenza di disegnare un apparato sanzionatorio robusto e selettivo, in grado di dare rilievo soltanto alle violazioni che rischiano di incidere sul funzionamento del sistema di prevenzione. Per le omesse segnalazioni di operazioni sospette tale impostazione è ancora più problematica data la complessità che caratterizza la valutazione del sospetto e la necessità di approntare un *enforcement* in grado di produrre effetti conformativi e di deterrenza senza incentivare un anomalo incremento di segnalazioni meramente cautelative.

Sotto altro profilo la previsione che con riguardo agli intermediari bancari e finanziari e alle società fiduciarie contempla la sanzionabilità del “personale” nel caso di omessa segnalazione delle operazioni sospette risulta non allineata agli indirizzi della legge delega volti a segnare un cambio di impostazione in materia passando, con riguardo ai soggetti obbligati persone giuridiche, dalla sanzionabilità dei loro dipendenti a quella delle persone giuridiche in proprio, con l’eventuale aggiunta, al ricorrere di specifici profili di responsabilità, di quella degli esponenti aziendali. D’altro canto, il mantenimento della possibilità di comminare la sanzione anche ai dipendenti è scelta che può porre problemi di equità e proporzionalità, data l’entità elevata delle sanzioni, e di potenziale contrasto col principio di *ne bis in idem*, visto che per lo stesso fatto la persona giuridica potrebbe rispondere sia in proprio sia come responsabile solidale dell’inosservanza di un proprio dipendente.

Infine, la distribuzione delle competenze sanzionatorie tra Autorità di vigilanza e Ministero dell’Economia, a seconda che la violazione sia da riferire a persona giuridica (vigilata) o a persona fisica, pone delicate questioni di coordinamento istituzionale e rischi di sovrapposizione di poteri, di inefficienza delle procedure e incoerenza delle decisioni.

Si tratta di critiche e dubbi rappresentati da più parti nell’ambito del dibattito parlamentare che ha preceduto la citata riforma del 2017⁸⁸³, che sono stati solo in parte risolti con il successivo intervento del 2019⁸⁸⁴.

La funzionalità complessiva del riformato sistema sanzionatorio è stata peraltro assicurata grazie al pronto riorientamento delle attività istituzionali di controllo per adeguarle alle nuove configurazioni delle responsabilità e delle violazioni nonché alle prassi messe a punto dalle diverse Autorità competenti per il coordinamento delle rispettive azioni di accertamento, contestazione e irrogazione delle sanzioni.

In prospettiva va infine considerato che sulla materia sanzionatoria si profila in un prossimo futuro un’ulteriore evoluzione normativa nell’ambito della riforma attuativa del c.d. AML Package, proposto dalla Commissione europea il 20 luglio 2021 per accrescere la convergenza dei sistemi di prevenzione ML/TF degli Stati membri. Il “pacchetto” si compone di tre regolamenti, direttamente applicabili in ciascuno Stato membro, e di una sesta direttiva antiriciclaggio, inerente a profili per i quali è necessario

Fisicaro, *Antiriciclaggio, sanzioni leggere*, in Diritto e Fisco, 22 ottobre 2022.

⁸⁸³ C. Clemente, *Schema di decreto legislativo recante attuazione della direttiva (UE) 2015/849 (A. 389)*, Audizione del Direttore dell’Unità di informazione finanziaria per l’Italia del 27 marzo 2017, presso le Commissioni riunite della Camera dei Deputati, 2^a Giustizia e 6^a Finanze. Si vedano anche: il Parere delle Commissioni riunite II (Giustizia) e VI (Finanze) della Camera dei Deputati, del 4 maggio 2017, sullo Schema di decreto legislativo recante attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell’uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e l’attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006 (n. 389); il Parere delle Commissioni riunite 2^a (Giustizia) e 6^a (Finanze e Tesoro), del 9 maggio 2017, sul medesimo Schema di decreto legislativo. Per le critiche sulla previsione della sanzionabilità del “personale” e la distribuzione delle competenze sanzionatorie si veda anche la Memoria della Banca d’Italia sullo schema di decreto legislativo recante attuazione della direttiva 2015/849/UE (A. 389) del 3 aprile 2017, presentata alle Commissioni riunite della Camera dei Deputati, 2^a Giustizia e 6^a Finanze.

⁸⁸⁴ Col D.lgs. 125/2019 sono stati realizzati specifici interventi correttivi nella materia sanzionatoria in particolare per: i) chiarire l’applicabilità della sanzione per omessa segnalazione di operazioni sospette anche al revisore persona fisica responsabile dell’incarico di revisione; ii) prevedere espressamente la competenza sanzionatoria del MEF in caso di violazione degli obblighi di informazione nei confronti della UIF; iii) stabilire chiaramente che sono sanzionabili le violazioni delle disposizioni emanate dalle Autorità di vigilanza di settore in materia di organizzazione, procedure e controlli interni; iv) attribuire espressamente alla competenza sanzionatoria delle medesime Autorità di vigilanza le violazioni commesse dai titolari di funzioni di amministrazione e controllo di intermediari; v) introdurre nuove disposizioni sanzionatorie rivolte agli operatori che svolgono attività di trattamento del contante vigilati dalla Banca d’Italia.

preservare margini di flessibilità nazionale; tra questi ultimi dovrebbe rientrare anche la materia sanzionatoria⁸⁸⁵. Resta confermata l'impostazione europea di prevedere misure e sanzioni amministrative in caso di gravi violazioni ripetute o sistematiche da parte dei soggetti obbligati e sono specificate le circostanze da prendere in considerazione per determinare il tipo e il livello delle sanzioni o misure amministrative. L'AMLA elaborerà norme tecniche di regolamentazione che definiranno gli indicatori per classificare il livello di gravità delle violazioni e i criteri da prendere in considerazione nel fissare il livello delle sanzioni amministrative o nell'adottare altre misure amministrative. Si offre dunque una nuova occasione di affinamento del quadro sanzionatorio nazionale che è auspicabile il nostro legislatore sappia cogliere appieno in conformità con le indicazioni comunitarie e facendo tesoro dell'esperienza fin qui maturata nell'applicazione dell'ordinamento vigente.

2. Le violazioni antiriciclaggio rilevanti dal punto di vista del diritto penale (L. Criscuolo e A. Cuzzocrea)

Le sanzioni penali attualmente previste dal D.lgs. 231 del 2007 sono frutto di una evoluzione normativa che, passando attraverso un intervento di depenalizzazione realizzato nel 2016, ha trovato il suo punto di arrivo nell'art. 5 del D.lgs. 25 maggio 2017, n. 90, che ha operato un sostanziale riequilibrio tra disposizioni sanzionatorie penali e amministrative in materia di prevenzione del riciclaggio.

Nel ripercorrere tale evoluzione emerge come il quadro normativo in materia abbia storicamente suscitato giudizi critici da parte delle Autorità⁸⁸⁶ per l'eccessivo rigore delle sanzioni previste a fronte di condotte spesso prive di effettiva offensività⁸⁸⁷. È sempre stata chiara l'esigenza di adeguare il sistema sanzionatorio con la previsione di fattispecie penali rispondenti ai principi di determinatezza e tassatività e di sanzioni amministrative efficaci e proporzionate alla reale gravità della violazione⁸⁸⁸.

Del resto, la previsione di sanzioni penali per la violazione delle norme di prevenzione del riciclaggio poteva apparire eccessiva in relazione alla rilevanza delle fattispecie e inefficace sul piano applicativo. Le condotte sanzionate, se dolose,

⁸⁸⁵ Nel considerando (71) della proposta di sesta direttiva si legge: "Attualmente vige negli Stati membri una gamma differenziata di sanzioni e misure amministrative per le violazioni delle vigenti disposizioni fondamentali di natura preventiva, così come un approccio incoerente per indagare e sanzionare le violazioni degli obblighi antiriciclaggio, e non esiste neppure un'intesa comune tra i supervisori su cosa debba costituire una violazione "grave" e poter così distinguere i casi che richiedono una sanzione amministrativa. Tale diversità pregiudica gli sforzi compiuti per contrastare il riciclaggio e il finanziamento del terrorismo e la risposta dell'Unione è frammentaria. È pertanto opportuno stabilire criteri comuni per determinare la risposta di supervisione più adeguata alle violazioni e prevedere una serie di misure amministrative che i supervisori potrebbero imporre quando le violazioni non sono sufficientemente gravi da essere punite con sanzioni amministrative. Al fine di incentivare i soggetti obbligati a rispettare le disposizioni del regolamento [...], è necessario rafforzare la natura dissuasiva delle sanzioni amministrative. Di conseguenza dovrebbe essere aumentato l'importo minimo della sanzione massima che può essere irrogata in caso di gravi violazioni del regolamento [...]. Nel recepimento della presente direttiva, gli Stati membri dovrebbero assicurare che l'imposizione di sanzioni e misure amministrative e di sanzioni penali in conformità con il diritto nazionale non violi il principio del *ne bis in idem*".

⁸⁸⁶ Valutazioni critiche furono espresse dal Governatore della Banca d'Italia dinanzi alla Commissione Antimafia il 14 giugno 2007, in occasione della consultazione sullo schema di decreto legislativo predisposto dal Governo, http://leg15.camera.it/_dati/leg15/lavori/stenbic/24/2007/0614/s020.htm. Il Governatore, in una successiva audizione resa il 22 luglio 2009, tornò a suggerire il riordino della disciplina sanzionatoria osservando che "molte sanzioni penali colpiscono condotte di scarsa potenzialità offensiva ovvero ipotesi di carenza di controllo, che dovrebbero rilevare solo sul piano amministrativo ... Risultano più efficaci sanzioni amministrative pecuniarie piuttosto che misure penali lievi, destinate a rapida prescrizione e che finiscono, in genere, per colpire solo dipendenti sprovvisti di significativi poteri decisionali" https://www.bancaditalia.it/publicazioni/interventi-governatore/integov2009/raghi_220709.pdf. Considerazioni critiche sono state espresse dal Direttore della UIF nell'audizione del 28 giugno 2011 innanzi alla Commissione Antimafia; <https://uif.bancaditalia.it/publicazioni/interventi/documenti/AUDIZIONE-COMMISSIONE-ANTIMAFIA.pdf>.

⁸⁸⁷ Il gruppo di studio sull'auto-riciclaggio costituito presso il Ministero della Giustizia (cfr. https://www.giustizia.it/giustizia/it/mg_1_12_1.wp?facetNode_1=0_15&facetNode_2=4_57&previousPage=mg_1_12&contentId=SPS914213) osservò che le sanzioni penali si erano rivelate di scarsissima applicazione: il reato di violazione degli obblighi di identificazione era individuato in modo generico e non includeva gli altri obblighi di adeguata verifica, per i quali non era prevista alcuna sanzione; inoltre, non erano puniti tutti i casi di omessa o falsa identificazione del titolare effettivo; la sanzione per omessa o tardiva registrazione appariva sproporzionata rispetto alla gravità della violazione e incoerente con la previsione di una sanzione amministrativa per la più grave violazione dell'obbligo di istituire l'archivio unico informatico. La relazione conclusiva dei lavori, nell'evidenziare le criticità del complessivo sistema sanzionatorio, sollecitò una revisione della materia con l'obiettivo, da un lato, di limitare la previsione di sanzioni penali a talune rilevanti violazioni degli obblighi di adeguata verifica e di registrazione connotate da condotte di falsità o frode e, dall'altro, di prevedere adeguate sanzioni amministrative per le altre violazioni degli obblighi oggetto di depenalizzazione.

⁸⁸⁸ Per una sintesi cfr. L. Criscuolo, *L'apparato sanzionatorio: disciplina e problematiche applicative*, in G. Castaldi e G. Conforti (a cura di), *Manuale Antiriciclaggio*, cit., p. 301 e ss.

sarebbero comunque perseguibili penalmente nell'ambito dei reati di falso ovvero a titolo di concorso o favoreggiamento del riciclaggio o dei reati presupposto dello stesso. Inoltre, considerate la natura contravvenzionale di molti reati all'epoca previsti e la tenuità delle pene, eventuali procedimenti giudiziari sarebbero stati quasi certamente destinati a rapida prescrizione⁸⁸⁹. Pressoché unanime era l'auspicio di prevedere poche fattispecie penali determinate e tassative, escludendo la tecnica, opinabile, del rinvio alla violazione di altre norme del decreto che, a loro volta, in taluni casi, rinviavano alle disposizioni secondarie delle Autorità di vigilanza di settore⁸⁹⁰.

Il D.lgs. 15 gennaio 2016, n. 8, nell'attuare un'estesa e non chiara depenalizzazione dei reati minori puniti con la sola pena pecuniaria della multa o dell'ammenda, incideva sulla normativa antiriciclaggio, non espressamente richiamata tra le numerose leggi escluse dall'intervento, trasformando in illecito amministrativo i reati inerenti alle violazioni degli obblighi di identificazione e registrazione di cui al previgente art. 55, commi 1, 4 e 7⁸⁹¹.

Sotto il profilo applicativo, l'intervento di depenalizzazione determinava un difficile esercizio di valutazione, caso per caso, della rilevanza penale ovvero amministrativa di una serie di violazioni. L'incertezza, alimentata dall'assenza di specifiche disposizioni di coordinamento sotto il profilo procedurale, comportava defatiganti scambi di atti e documenti tra Procure e Autorità amministrative ritenute competenti per gli illeciti "degradati", con ripercussioni negative sui tempi per l'avvio di procedimenti sanzionatori amministrativi⁸⁹².

Nel definire i criteri di delega per il recepimento della quarta direttiva antiriciclaggio⁸⁹³, l'art. 15 della legge n. 170 del 2016 prevedeva correttamente, in materia sanzionatoria, il rispetto dei principi di *ne bis in idem* sostanziale⁸⁹⁴ e di effettività, proporzionalità e dissuasività delle sanzioni⁸⁹⁵. La riforma del 2017 ha pertanto limitato il presidio penale, quale *extrema ratio*, a condotte contraddistinte da una effettiva gravità, valorizzando il principio generale di proporzionalità e di "approccio basato sul rischio"⁸⁹⁶. A tal fine, le fattispecie incriminatrici sono state circoscritte alle sole condotte delittuose di grave violazione degli obblighi di adeguata verifica e di conservazione delle informazioni e dei documenti, connotate, sul piano dell'elemento materiale del reato, dall'utilizzo di dati o documenti falsi o di altri mezzi fraudolenti; è stata mantenuta altresì la sanzione penale per la violazione del divieto di comunicazione dell'avvenuta segnalazione. In parallelo, sono state assoggettate a sanzioni amministrative pecuniarie le restanti

⁸⁸⁹ Così G. Castaldi, *Prevenzione del riciclaggio: criticità nelle misure sanzionatorie*, Bancaria, febbraio 2019, pp. 63 e ss.

⁸⁹⁰ Emblematica, al riguardo, era la contravvenzione punita dall'art. 55, comma 1, in forza della quale era punito "*chiunque contravviene alle disposizioni contenute nel Titolo II, Capo I, concernenti l'obbligo di identificazione*". Le disposizioni richiamate andavano dall'art. 15 al 35 e contemplavano una vasta gamma di obblighi di "adeguata verifica della clientela", nozione ben più ampia di quella di semplice "identificazione", richiamata nella norma penale.

⁸⁹¹ Permaneva il presidio penale a fronte di ipotesi eterogenee in materia di adeguata verifica, di condotte omissive o di falso poste in essere dall'esecutore dell'operazione, delle violazioni degli obblighi di comunicazione imposti all'organo di controllo, per l'inosservanza del divieto di comunicazione delle segnalazioni di operazioni sospette e per le ipotesi di indebito utilizzo, alterazione o falsificazione di carte di pagamento.

⁸⁹² Un giudizio critico sulla citata depenalizzazione è stato espresso da F. Di Vizio, *Relazione per la Struttura didattica territoriale di Bologna della Scuola Superiore della Magistratura e per la Scuola Superiore di Studi Giuridici dell'Università di Bologna*, Seminario 5 L'antiriciclaggio, Bologna, 17 giugno 2016.

⁸⁹³ Fino alla emanazione della direttiva (UE) 2015/849 le norme comunitarie in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo non avevano dato risalto agli aspetti sanzionatori. Una maggiore armonizzazione della materia si era resa pertanto necessaria per porre rimedio alle conseguenze negative sia sul piano dell'equità che della parità concorrenziale.

⁸⁹⁴ Il richiamo del principio del *ne bis in idem*, sancito dall'art. 4 del Protocollo 7 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, pone il problema della legittimità dell'eventuale cumulo tra sanzioni amministrative e penali. Sul punto, con particolare riguardo agli orientamenti giurisprudenziali della Corte europea dei Diritti dell'Uomo e della Corte di Giustizia dell'Unione europea, cfr. V. Vallefucio, *Evoluzione del sistema sanzionatorio antiriciclaggio*, in AA.VV., *Le nuove regole antiriciclaggio*, Guide operative Ipsoa 2021, Cap. XV, p. 946 e ss.

⁸⁹⁵ Con riferimento alle sanzioni penali, la legge delega impegnava il Governo a "*limitare la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti, perpetrate attraverso frode o falsificazione, e di violazione del divieto di comunicazione dell'avvenuta segnalazione, prevedendo sanzioni penali adeguate alla gravità della condotta e non eccedenti, nel massimo, tre anni di reclusione e 30.000 euro di multa*".

⁸⁹⁶ Nell'Audizione resa nel marzo 2017 dinanzi alla Camera dei Deputati sullo schema di decreto legislativo di recepimento della quarta direttiva comunitaria, il Direttore della UIF ebbe ancora modo di richiamare l'importanza di un sistema sanzionatorio improntato a equilibrio ed equità, con sanzioni dissuasive, volte a penalizzare adeguatamente chi si pone in una logica non collaborativa, ma evitando di colpire pesantemente comportamenti privi di reale offensività; https://uif.bancaditalia.it/publicazioni/interventi/documenti/Audizione_Clemente_27032017.pdf.

fattispecie di violazioni meramente formali degli obblighi di adeguata verifica e conservazione, prevedendo l'oscillazione dell'entità della sanzione entro un determinato *range* e la relativa graduazione in funzione del grado di responsabilità e della capacità patrimoniale della persona fisica o giuridica autrice della violazione.

Sotto un profilo generale, le nuove fattispecie penali, tipicamente dedicate alla prevenzione del riciclaggio dall'art. 55, constano di tre delitti (commi da 1 a 3, in materia di adeguata verifica e conservazione) e una contravvenzione (comma 4, relativo al divieto di comunicazione e correlato *feedback*)⁸⁹⁷. Le condotte incriminate in tali fattispecie spesso si inquadrano in un disegno criminoso più complesso e articolato, tale da configurare il concorso con altre fattispecie di reato. Ciò, salvo che il fatto costituisca più grave reato (commi 3 e 4⁸⁹⁸).

Quanto all'autore del reato, le nuove norme incriminatrici configurano reati propri, essendo rivolte non più genericamente a "chiunque", ma a soggetti destinatari di specifici obblighi ai sensi della disciplina antiriciclaggio. Ne trae giovamento la chiarezza della fattispecie e la certezza dei comportamenti puniti.

Passando all'esame delle singole fattispecie, vengono in rilievo anzitutto le violazioni degli obblighi di adeguata verifica perpetrate attraverso una condotta commissiva, consistente nella falsificazione degli elementi acquisiti nell'ambito dell'adeguata verifica della clientela cui è tenuto il soggetto obbligato di cui all'art. 3 del D.lgs. 231/2007⁸⁹⁹ ovvero nell'utilizzo di tali dati.

Il comma 1 punisce infatti chi, essendo tenuto a effettuare l'adeguata verifica, dolosamente "*falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione*" ovvero "*utilizza dati e informazioni falsi*".

In assenza di ulteriori specificazioni, deve ritenersi che la falsificazione si riferisca sia al falso materiale che a quello ideologico, per cui è punibile non solo chi ha falsificato materialmente dati veri ma anche chi, senza alterare i dati, riporta dichiarazioni false o mendaci in ordine ai dati stessi.

La condotta di falsificazione o utilizzo di dati falsi, commessa al di fuori dell'adempimento dei predetti obblighi di adeguata verifica, non dovrebbe rientrare nella previsione in commento, che configura un reato proprio, ma potrebbe essere ricompresa in altre condotte di falso, previste dal codice penale.

L'art. 55, comma 2, riguarda la violazione degli obblighi di conservazione dei dati e delle informazioni e punisce chi "*acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei predetti dati e informazioni*".

La norma configura due distinte figure criminose; in entrambe le ipotesi la *ratio* della norma è volta a garantire la genuinità dei dati acquisiti e conservati in vista di eventuali successive indagini finanziarie o giudiziarie.

Nel secondo caso l'elemento soggettivo è costituito da dolo specifico, essendo richiesto il fine di alterare, con mezzi ingannevoli, la corretta conservazione dei dati e delle informazioni (si pensi alla dolosa manomissione di un sistema informatico in modo da cancellare o alterare i dati). Come per la fattispecie precedente si tratta di un reato proprio dei destinatari degli obblighi di conservazione dei dati. Va valutato se in tale novero possano rientrare gli amministratori delle persone giuridiche tenute all'iscrizione nel Registro delle imprese di cui all'art. 2188 c.c., i quali, ai sensi dell'art. 22, comma 3, del decreto antiriciclaggio, sono tenuti ad acquisire e conservare informazioni adeguate, accurate e aggiornate sulla titolarità effettiva dell'impresa. *Idem* per i fiduciari di *trust* espressi, i quali, ai sensi dell'art. 22, comma 5, del citato decreto, sono tenuti ad acquisire e conservare informazioni adeguate, accurate e aggiornate sulla titolarità effettiva del *trust*.

L'art. 55, comma 3, punisce il cliente e l'esecutore, in quanto soggetti obbligati "*a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela*", che forniscano "*dati falsi o informazioni non veritiere*". La *ratio* della norma è la salvaguardia degli obblighi di acquisizione delle informazioni necessarie

⁸⁹⁷ Le prime sono punite con la reclusione da sei mesi a tre anni e con la multa da 10.000 a 30.000 euro; la seconda è punita con l'arresto da sei mesi a un anno e con l'ammenda da 5.000 a 30.000 euro.

⁸⁹⁸ In particolare, laddove operi la clausola di salvezza di cui comma 4, la riconducibilità del divieto di comunicazione alla fattispecie, punita più gravemente, di violazione del segreto d'ufficio (art. 326 c.p.) può consentire l'allungamento dei tempi di prescrizione agevolando la perseguibilità in concreto del reo.

⁸⁹⁹ La norma previgente puniva indiscriminatamente "chiunque", compresi i soggetti che instaurano il rapporto o eseguono la prestazione, mentre la disposizione attuale configura un reato proprio, commesso dal soggetto destinatario degli obblighi di adeguata verifica.

a completare correttamente l'adeguata verifica⁹⁰⁰, quale presupposto indispensabile per la conoscenza del cliente, la conservazione dei relativi dati e la valutazione dell'adeguatezza dell'operatività posta in essere ai fini dell'eventuale segnalazione delle operazioni sospette.

In questo caso il soggetto attivo è il cliente⁹⁰¹, tenuto ai sensi dell'art. 22 a fornire per iscritto, sotto la propria responsabilità, tutte le informazioni necessarie ai fini dell'adeguata verifica⁹⁰², ovvero l'esecutore⁹⁰³ delegato a operare per conto del cliente. La clausola di riserva posta nell'*incipit* esclude il concorso di reati nell'ipotesi in cui il fatto che il soggetto fornisce le informazioni false sia elemento di un reato più grave, quale ad esempio il riciclaggio o il favoreggiamento.

Un reato contravvenzionale⁹⁰⁴ che riveste particolare rilevanza è previsto dal comma 4 a carico di chi *“viola il divieto di comunicazione di cui agli articoli 39, comma 1, e 41, comma 3”*⁹⁰⁵. La norma tutela il segreto riguardante l'avvenuta segnalazione di un'operazione sospetta, l'invio di ulteriori informazioni richieste dalla UIF o l'esistenza anche solo probabile di indagini in materia di riciclaggio o di finanziamento del terrorismo, nonché il flusso di ritorno delle informazioni (dalla UIF ai segnalanti) inerenti alle segnalazioni stesse. Risulta quindi salvaguardata, in via mediata, la tenuta dell'intero sistema di prevenzione, di cui la segnalazione di operazioni sospette costituisce il perno, a salvaguardia della collaborazione attiva e del regolare svolgimento delle analisi finanziarie condotte dalla UIF e delle successive indagini da parte degli Organi inquirenti.

Sul piano oggettivo viene in rilievo la condotta di chi comunica al cliente interessato o a terzi l'avvenuta segnalazione ovvero l'esito della medesima in violazione di specifici divieti normativi. Trattandosi di una contravvenzione, il reato è punito anche a titolo di colpa, perseguendo anche la semplice negligenza e trascuratezza nella gestione della notizia riservata e la sottovalutazione della delicatezza dell'informazione comunicata a soggetti non autorizzati.

Soggetto attivo del reato è qualunque soggetto destinatario dell'obbligo di segnalazione di operazioni sospette nonché i soggetti che siano comunque venuti a conoscenza dell'avvenuta segnalazione. In tale ambito devono ritenersi inclusi non soltanto i soggetti individuabili all'interno dell'organizzazione dei destinatari tenuti all'obbligo segnaletico, ma anche il personale dei soggetti pubblici che, avendo acquisito le informazioni per lo svolgimento delle proprie funzioni istituzionali, le disseminano a soggetti diversi da quelli deputati a riceverle in base al decreto antiriciclaggio.

Recentemente il c.d. “Decreto Milleproroghe 2022”⁹⁰⁶ ha apportato modifiche al decreto antiriciclaggio tese a rafforzare la tutela del segnalante. In particolare, all'art. 38 del D.lgs. 231/2007 è stato inserito il comma 3-bis, in base al quale *“chiunque rivela indebitamente l'identità del segnalante è punito con la reclusione da due a sei anni”* e *“la stessa pena si applica a chi rivela indebitamente notizie riguardanti l'invio della*

⁹⁰⁰ Per la Cassazione, l'impostazione della regolamentazione realizza un'anticipazione della soglia di tutela: le regole imposte a presidio della piena e adeguata conoscenza del cliente vengono dettagliate e rafforzate, sino a prevedere che, nelle ipotesi in cui non si verifichi una completa “rivelazione” tra le parti, il rapporto non debba essere instaurato o debba essere interrotto; cfr. Cass. Pen. Sez. II, sentenza n. 18141 del 30 aprile 2015.

⁹⁰¹ Come individuato dall'art. 1, comma 2, lett. f), del D.lgs. 231/2007.

⁹⁰² La disposizione colma una lacuna del precedente impianto sanzionatorio che non prevedeva una sanzione per l'ipotesi in cui i dati e le informazioni forniti dal cliente fossero consapevolmente falsi.

⁹⁰³ La definizione è contenuta nell'art. 1, comma 2, lett. p), del D.lgs. 231/2007.

⁹⁰⁴ Rispetto al testo previgente, l'ammenda non è alternativa all'arresto; ciò, per ovviare alle criticità in passato connesse all'estinzione dell'illecito per oblazione in caso di ammenda.

⁹⁰⁵ L'art. 39, comma 1, vieta *“ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo”*. L'art. 41, comma 3 estende il divieto al “flusso di ritorno delle informazioni”. Il divieto ammette deroghe con riferimento alle comunicazioni effettuate: alle Autorità di vigilanza di settore in occasione dell'esercizio delle funzioni di cui all'art. 7, comma 2, o alla Guardia di Finanza nell'ambito dei controlli di cui all'art. 9; agli Organi investigativi ai fini degli approfondimenti di competenza ai sensi dell'art. 40; tra gli intermediari bancari e finanziari appartenenti al medesimo gruppo e tra questi e le loro succursali e filiazioni, alle condizioni indicate nell'art. 39, comma 3; tra professionisti che svolgono la propria prestazione professionale in forma associata, in qualità di dipendenti o collaboratori, anche se situati in Paesi terzi, a condizione che essi applichino misure equivalenti a quelle previste dal decreto antiriciclaggio italiano, ai sensi dell'art. 39, comma 4; tra due o più intermediari bancari e finanziari ovvero tra due o più professionisti, nei casi relativi allo stesso cliente o alla stessa operazione, alle condizioni stabilite dall'art. 39, comma 5.

⁹⁰⁶ Cfr. art. 3, comma 1, lett. b), n. 2), del decreto-legge 30 dicembre 2021, n. 228, convertito con modificazioni dalla legge 25 febbraio 2022, n. 15.

segnalazione e delle informazioni trasmesse dalle FIU o il contenuto delle medesime, se le notizie rivelate sono idonee a consentire l'identificazione del segnalante".

La modifica è volta a rafforzare la tutela dei soggetti che effettuano segnalazioni di operazioni sospette, prevedendo: a) che in tutte le fasi del procedimento vengano adottate dall'autorità giudiziaria le misure necessarie ad assicurare la riservatezza sull'identità dei soggetti segnalanti, così come la riservatezza delle informazioni e il contenuto delle stesse inviate dalle FIU; b) il non disvelamento dei dati dei soggetti segnalanti né nel fascicolo del PM, né in quello relativo al dibattimento, ad eccezione della circostanza che tali dati siano indispensabili – previa emissione di decreto motivato – all'accertamento dei reati; c) la violazione dei citati obblighi di riservatezza comporta la sanzione della pena della reclusione da due a sei anni.

I reati fin qui illustrati presentano quale elemento comune l'obiettivo della tutela della corretta osservanza degli obblighi di prevenzione antiriciclaggio. Lo stesso art. 55, nei commi da 5 a 7, si incentra invece su condotte di indebita utilizzazione o falsificazione di strumenti di pagamento elettronici, perseguendo finalità complementari di tutela della tracciabilità dei trasferimenti finanziari.

La disposizione più rilevante era quella originariamente contenuta nel comma 5, che è poi confluita – sulla base del decreto legislativo 1° marzo 2018, n. 21 e a far data dal 6 aprile 2018 – nell'art. 493-ter del Codice penale⁹⁰⁷ per una scelta di politica legislativa in favore della riserva di codice⁹⁰⁸.

Quest'ultima disposizione è stata successivamente modificata dal decreto legislativo 8 novembre 2021, n. 184 (di recepimento della direttiva (UE) 2019/713): si è passati dall'originaria formulazione – che puniva l'indebito utilizzo e la falsificazione, alterazione, possesso, cessione o acquisizione di carte di credito o di pagamento di illecita provenienza – al più generale riferimento all'indebito utilizzo e falsificazione di *“strumenti di pagamento diversi dai contanti”*. Tali strumenti sono stati definiti *“agli effetti della legge penale”* includendo anche i *“mezzi di scambio digitali”* che, a loro volta, comprendono anche la valuta virtuale (art. 1, comma 1, lett. a), c) e d), del D.lgs. 184/2021)⁹⁰⁹.

La giurisprudenza di legittimità ha avuto più volte occasione di pronunciarsi sulla configurabilità del reato nella versione antecedente le modifiche apportate nel 2021, con argomentazioni che appaiono peraltro valide anche con riferimento all'estensione della fattispecie a tutti gli strumenti di pagamento diversi dal contante. È stato specificato che il bene giuridico tutelato non è solo il patrimonio del titolare della carta, ma anche la sicurezza delle transazioni commerciali, che costituisce interesse collettivo indisponibile dal privato⁹¹⁰.

Il reato si articola in due fattispecie. La prima consiste nell'utilizzazione illecita di carte di credito o di altri mezzi di pagamento e risulta imputabile a chiunque indebitamente utilizzi carte di credito o altri documenti equivalenti⁹¹¹ senza esserne titolare, al fine di trarne profitto per sé o per altri.

Il materiale possesso della carta o del documento non è stato considerato presupposto necessario dell'utilizzo, essendo sufficiente l'effettuazione di transazioni non autorizzate dal titolare, previa immissione dei dati di una valida carta di pagamento altrui di cui l'agente non abbia la materiale disponibilità⁹¹². La mancanza di titolarità segnerebbe il perimetro dell'utilizzo indebito della carta, cosicché sarebbe configurabile il reato di indebita utilizzazione nell'ipotesi in cui la carta di credito

⁹⁰⁷ L'articolo punisce *“chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi ... con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi”*.

⁹⁰⁸ La continuità della punibilità della fattispecie è confermata dalla Cass. Pen. Sez. IV, sentenza n. 13492 del 21/01/2020.

⁹⁰⁹ Per un primo commento cfr. F. Ciraolo e E. La Rosa, *Contrasto alle frodi e alle falsificazioni dei mezzi di pagamento diversi dai contanti. Brevi note intorno al d.lgs. 184/21 (con focus sulle valute virtuali)*, marzo 2022, in *diritto bancario.it*.

⁹¹⁰ Cfr. Cass. Pen. Sez. II, sentenza n. 18609 del 16/02/2021.

⁹¹¹ La giurisprudenza nel tipizzare i possibili *“documenti analoghi”* sembrerebbe fare riferimento soprattutto agli strumenti di pagamento elettronici, mentre sarebbero esclusi, in quanto assimilabili piuttosto ai titoli di credito, gli assegni bancari e circolari, gli eurocheques ed i traveller's cheques; cfr. Cass. Pen. Sez. I, n. 5279 del 7 aprile 1999. Si deve trattare, peraltro, di una carta o di un documento idoneo ad assolvere alla propria funzione di strumento di pagamento, non assumendo rilievo l'utilizzo di una carta di credito scaduta e, quindi, inidonea ad assolvere funzioni di credito, di pagamento ovvero di prelievo di contante; cfr. Cass. Pen. Sez. II, sentenza n. 37758 dell'11/10/2005.

⁹¹² Cfr. Cass. Pen. Sez. II, sentenza n. 47725 del 07/11/2014.

nominativa sia usata da chi non ne è titolare (salvo il consenso dell'avente diritto), mentre il reato non sussisterebbe se la carta è al portatore, ove l'agente fosse in buona fede.

Anche l'uso di una carta di credito da parte di un terzo, benché autorizzato dal titolare, è stato ritenuto rilevante ai fini della integrazione del reato in commento posto che solo l'intestatario sarebbe contrattualmente legittimato all'impiego della carta. Di contro, non ricorrerebbero gli estremi dell'uso indebito penalmente rilevante ove il soggetto legittimato si servisse del terzo come mero esecutore di un'operazione che non comporta la sottoscrizione di alcun atto⁹¹³.

Inoltre, la giurisprudenza di legittimità è stata costante nel ritenere che l'indebita utilizzazione a fini di profitto di una carta di credito da parte di chi non ne sia titolare è sufficiente ad integrare il reato *de quo*, indipendentemente dal conseguimento di un profitto per il soggetto agente o dal verificarsi di un danno per il titolare della carta, non essendo necessario ai fini della consumazione del reato che la transazione giunga a buon fine⁹¹⁴. Pertanto, il reato sarebbe consumato anche in caso di utilizzo di un bancomat rubato per effettuare degli acquisti poi non portati a termine a causa del blocco preventivo della carta o dell'intervento della polizia. Sarebbe, invece, configurabile il tentativo con riferimento alla condotta di chi introduca un bancomat di illecita provenienza in uno sportello automatico e, non disponendo del codice di accesso, esegua una serie di combinazioni numeriche, senza riuscirvi.

Con riferimento ai possibili rapporti con altri reati, si è ritenuto che integri il delitto di indebita utilizzazione di carte di credito di cui al previgente art. 55, comma 5 (oggi art. 493-*bis* c.p.), e non quello di frode informatica *ex* art. 640-*ter* c.p., la condotta di colui che, avendo ottenuto, senza realizzare frodi informatiche, i dati relativi ad una carta di debito o di credito, unitamente alla stessa tessera elettronica, la utilizzi indebitamente per effettuare prelievi di denaro⁹¹⁵. È, invece, configurabile il concorso formale fra il delitto di furto della carta di credito e l'indebito utilizzo del medesimo documento *ex* art. 55, comma 5, (ora art. 493-*ter* c.p.) trattandosi di condotte eterogenee aventi anche una diversa collocazione temporale.

La seconda fattispecie consiste nella falsificazione o alterazione di carta di credito o di qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi nonché nel possesso, cessione o acquisizione di tali documenti se di provenienza illecita, o comunque se falsificati o alterati, o di ordini di pagamento prodotti con gli stessi documenti.

La falsificazione consiste nella materiale creazione di una nuova carta "artefatta" solo apparentemente riconducibile all'istituto emittente, ma in realtà priva di qualsiasi collegamento negoziale con quest'ultimo. L'alterazione, invece, presuppone l'esistenza di una carta regolarmente creata dall'emittente e si concretizza nella modificazione artificiosa di alcuni dati rilevanti quali la data di scadenza, il nome del titolare o la banda magnetica.

In secondo luogo, viene in rilievo il fatto di chi si trovi in possesso ovvero ceda o acquisti carte di credito o documenti analoghi se di provenienza illecita o di ordini di pagamento realizzati con i medesimi documenti. Il concetto di possesso va inteso in senso penalistico, come autonoma disponibilità della *res* accompagnata dall'animo di tenere la cosa presso di sé. Tale nozione di possesso costituisce il presupposto delle condotte di acquisizione e di cessione, le quali si sostanziano rispettivamente nel conseguimento e nella alienazione del possesso medesimo⁹¹⁶.

La provenienza illecita, quale ulteriore elemento costitutivo della fattispecie in commento, implica il possesso della carta di credito o di qualsiasi altro documento analogo derivante da un illecito civile o amministrativo o anche penale, ma di natura contravvenzionale; ove, infatti, la condotta acquisitiva della carta o del documento fosse ricollegabile ad un delitto, sarebbe integrato il reato di cui all'art. 648 c.p.⁹¹⁷

Il comma 6 dell'art. 55⁹¹⁸ prevede, infine, l'applicazione della confisca nell'ipotesi di abusiva attività di prestazione di servizi di pagamento⁹¹⁹. Sono confiscabili – non è chiaro se a seguito di sentenza di condanna – gli strumenti che sono serviti a commettere il reato i quali, una volta sottoposti a sequestro ai fini della confisca, sono affidati dall'Autorità giudiziaria agli organi di polizia che ne facciano richiesta.

⁹¹³ Cfr. Cass. Pen. Sez. II, sentenza n. 17453 del 22/02/2019.

⁹¹⁴ Cfr. Cass. Pen. Sez. V, sentenza n. 5692 del 11/12/2018.

⁹¹⁵ Cfr. Cass. Pen. Sez. II, sentenza n. 50395 del 30/10/2019.

⁹¹⁶ Così V. Vallefucio, *Evoluzione del sistema sanzionatorio antiriciclaggio*, in AA.VV., *Le nuove regole antiriciclaggio*, Guide operative Ipsoa 2021, Cap. XV, p. 973 e ss.

⁹¹⁷ Cfr. Cass. Pen. Sez. II, sentenza n. 7658 del 27/01/2015.

⁹¹⁸ Il comma 6 prevede che "Per le violazioni delle disposizioni di cui all'art. 131-*ter* del decreto legislativo 1° settembre 1993, n. 385, è ordinata, nei confronti degli agenti in attività finanziaria che prestano servizi di pagamento attraverso il servizio di rimessa di danaro di cui all'art. 1, co. 1, lett. n), del decreto legislativo 27 gennaio 2010, n. 11, la confisca degli strumenti che sono serviti a commettere il reato". Il successivo comma 7 prevede che "Gli strumenti sequestrati ai fini della confisca di cui al comma 6 nel corso delle operazioni di polizia giudiziaria, sono affidati dall'Autorità giudiziaria agli organi di polizia che ne facciano richiesta".

⁹¹⁹ Nel caso di condanna o di applicazione della pena su richiesta delle parti per i delitti in tema di uso indebito di carte di pagamento, l'applicazione della confisca è ora contenuta direttamente nell'art. 493-*ter*, c.p.

3. Le sanzioni amministrative per violazioni degli obblighi antiriciclaggio (*A. Cuzzocrea e L. La Rocca*)

Le violazioni degli obblighi antiriciclaggio sono sanzionate sulla base di un articolato sistema di fattispecie e competenze disciplinato dal D.lgs. 231/2007, come modificato dal D.lgs. 90/2017 di recepimento della direttiva (UE) 2015/849 (c.d. quarta direttiva); ulteriori correttivi sono stati apportati dal D.lgs. 125/2019 che ha dato attuazione nell'ordinamento nazionale alla direttiva (UE) 2018/843 (c.d. quinta direttiva). Il quadro d'insieme del predetto sistema è riportato nelle Tavole che seguono, con l'individuazione dei soggetti che possono essere chiamati a rispondere, rispettivamente, della violazione dell'obbligo di segnalazione delle operazioni sospette (Tavola n. 1) e degli altri principali obblighi antiriciclaggio (Tavola n. 2); per ciascuna fattispecie sono altresì indicate le sanzioni irrogabili e le Autorità competenti all'esercizio del potere sanzionatorio.

Il sistema sanzionatorio per la violazione dell'obbligo di segnalazione delle operazioni sospette

D.lgs. 231/2007	SOGGETTI RESPONSABILI	SANZIONI IRROGABILI			COMPETENZA
Art. 58, co. 1, 2 e 4	Soggetti obbligati non vigilati	Sanzione base (€ 3.000)	Sanzione da € 30.000 a € 300.000 in caso di violazioni gravi, ripetute, sistematiche ovvero plurime	Sanzione parametrata al vantaggio economico i.importo massimo elevato al doppio del vantaggio se determinato, determinabile e ≥ € 450.000 ii.€ 1 mln se il vantaggio (esiste ma) non sia determinato o determinabile	MEF (art. 65, co. 1)
Art. 58, co. 3 e 4	Personale di intermediari bancari e finanziari e di società fiduciarie non iscritte nella sezione dell'albo 106 TUB, responsabile, in via esclusiva o concorrente, con l'ente				
Art. 62, co. 1	Intermediari bancari e finanziari (responsabili in via esclusiva o concorrente)	Sanzione da € 30.000 a € 5 mln ovvero 10% del fatturato (se disponibile, determinabile e ≥ € 5 mln) in caso di violazioni gravi, ripetute, sistematiche ovvero plurime			BdI/IVASS (Art. 62, co. 7 e art. 65, co. 1)
Art. 62, co. 2	Titolari di funzioni di amministrazione, direzione e controllo degli intermediari bancari e finanziari che, non assolvendo ai propri compiti, abbiano agevolato o reso possibile la violazione o inciso in modo rilevante sull'esposizione al rischio dell'intermediario	Sanzione da € 10.000 a € 5 mln. Se il vantaggio ottenuto è disponibile, determinabile e ≥ € 5 mln, la sanzione è elevata fino al doppio		Interdizione da sei mesi a tre anni (a seconda della gravità della violazione)	MEF (Art. 62, co. 9 e art. 65, co. 1); Raccordo con BdI/IVASS (Art. 62, co. 7 e art. 65, co. 1) limitatamente all'eventuale interdizione
Art. 62, co. 5	Revisori legali vigilati dalla Consob	Sanzione da € 3.000 a € 1 mln in caso di violazioni gravi, ripetute, sistematiche ovvero plurime			MEF (art. 65, co. 1)
	Società di revisione vigilate dalla Consob				Consob (art. 62, co. 8 e 65, co. 1)
	Titolari di funzioni di amministrazione, direzione e controllo della società di revisione (vigilate dalla Consob) che, non assolvendo ai propri compiti, abbiano agevolato o reso possibile la violazione	Sanzione da € 3.000 a € 1 mln	Interdizione da sei mesi a tre anni a seconda della gravità della violazione)		MEF (art. 62, co. 9, e 65, co. 1); Raccordo con Consob (art. 62, co. 8 e 65, co. 1) limitatamente all'eventuale interdizione

Il sistema sanzionatorio per la violazione degli altri principali obblighi antiriciclaggio

D.lgs. 231/2007	SOGGETTI RESPONSABILI	SANZIONI IRROGABILI		COMPETENZA
Art. 56 (violazioni in materia di adeguata verifica e obbligo di astensione) art. 57 (violazioni in materia di conservazione)	Soggetti obbligati non vigilati	Sanzione base (€ 2.000)	Sanzione da € 2.500 a € 50.000 in caso di violazioni gravi, ripetute, sistematiche ovvero plurime	MEF (art. 65 co. 1)
Art. 62, co. 1 e 4 (violazioni in materia di adeguata verifica, conservazione, organizzazione, procedure e controlli interni; omessa istituzione del punto di contatto centrale)	Intermediari bancari e finanziari (responsabili in via esclusiva o concorrente)	Sanzione da € 30.000 a € 5 mln ovvero 10% del fatturato (se disponibile, determinabile e $\geq$ € 5 mln) in caso di violazioni gravi, ripetute, sistematiche ovvero plurime	Per le violazioni caratterizzate da scarsa offensività o pericolosità, in alternativa alla sanzione pecuniaria: <i>i) cease and desist order;</i> <i>ii) public statement</i>	BdI/IVASS (Art. 62, co. 7)
Art. 62, co. 2 e 3 (violazioni in materia di adeguata verifica, conservazione, organizzazione, procedure e controlli interni)	Titolari di funzioni di amministrazione, direzione e controllo degli intermediari bancari e finanziari che, non assolvendo ai propri compiti, abbiano agevolato o reso possibile la violazione o l'inosservanza del <i>cease and desist order</i> o abbiano inciso in modo rilevante sull'esposizione al rischio dell'intermediario	Sanzione da € 10.000 a € 5 mln . Se il vantaggio ottenuto è disponibile, determinabile e $\geq$ € 5 mln, la sanzione è elevata fino al doppio	Interdizione da sei mesi a tre anni (a seconda della gravità della violazione)	BdI/IVASS (Art. 62, co. 7)
Art. 62, co. 5 (violazioni in materia di adeguata verifica, conservazione, organizzazione, procedure e controlli interni)	Revisori legali vigilati dalla Consob	Sanzione da € 3.000 a € 1 mln in caso di violazioni gravi, ripetute, sistematiche ovvero plurime		Consob (art. 62, co. 8)
	Società di revisione vigilati dalla Consob Titolari di funzioni di amministrazione, direzione e controllo della società di revisione (vigilate dalla Consob) che, non assolvendo ai propri compiti, abbiano agevolato o reso possibile la violazione	Sanzione da € 3.000 a € 1 mln	Interdizione da sei mesi a tre anni (a seconda della gravità della violazione)	
Art. 62, co. 7-bis (violazioni in materia di adeguata verifica, conservazione, organizzazione, procedure e controlli interni)	Soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori di cui all'articolo 3, comma 5, lettera f)	Sanzione da € 2.500 a € 350.000	Sanzione fino al triplo del massimo edittale ovvero fino al doppio dell'importo dei profitti se determinato o determinabile, in caso di violazioni gravi, ripetute o sistematiche ovvero plurime	BdI (Art. 62, co. 7bis)

3.1 Le violazioni in materia di adeguata verifica, conservazione e segnalazione di operazioni sospette

Il sistema sanzionatorio antiriciclaggio delineato dopo il recepimento della quarta e della quinta direttiva, diversamente da quello previgente⁹²⁰, distingue le violazioni in materia di adeguata verifica, conservazione e segnalazione di operazioni sospette a seconda che la condotta del soggetto obbligato sia priva di elementi qualificanti (fattispecie c.d. “base”) o sia invece possibile individuarne, alternativamente o cumulativamente, il carattere “grave”, “ripetuto”, “sistematico” ovvero “plurimo” (fattispecie c.d. “qualificate”)⁹²¹.

Ai fini della distinzione tra fattispecie c.d. “base” e “qualificate”, va considerato che il livello di gravità della fattispecie è determinato, ai sensi degli artt. 56, 57 e 58 del D.lgs. 231/2007, considerando: a) l'intensità e il grado dell'elemento soggettivo, anche avuto riguardo all'ascrivibilità della violazione alla carenza, all'incompletezza o alla non adeguata diffusione di prassi operative e procedure di controllo interno; b) il grado di collaborazione dell'incolpato con le Autorità; c) la rilevanza ed evidenza dei motivi del sospetto, anche avuto riguardo al valore dell'operazione e al grado della sua incoerenza rispetto alle caratteristiche del cliente e del relativo rapporto⁹²²; d) la reiterazione e diffusione dei comportamenti, anche in relazione alle dimensioni, alla complessità organizzativa e all'operatività del soggetto obbligato.

Parametri integrativi per la qualificazione delle violazioni concernenti le omesse segnalazioni di operazioni sospette sono inoltre contenuti nelle istruzioni applicative pubblicate dal Ministero dell'Economia e delle finanze dapprima in data 6 luglio 2017 e da ultimo in data 17 giugno 2022⁹²³.

⁹²⁰ Per un *excursus* della normativa sanzionatoria nazionale prima delle modifiche del 2017 e del 2019 si veda G. Castaldi, *Prevenzione del riciclaggio: criticità nelle misure sanzionatorie*, Bancaria, 2019, 2, p. 67-68.

⁹²¹ Secondo G. Castaldi, *Prevenzione del riciclaggio: criticità nelle misure sanzionatorie*, cit., p. 70, “il decreto antiriciclaggio [...] non sfrutta l'opzione, pure offerta dalla direttiva, di limitare le fattispecie sanzionabili alle violazioni gravi, reiterate o sistematiche [...]”. Se, da un lato, questa tradizionale severità colloca il nostro Paese tra quelli eticamente più virtuosi, per altro verso, essa discrimina gli operatori italiani in termini concorrenziali e può generare arbitraggi normativi e conseguenti fenomeni di delocalizzazione non solo in Stati extracomunitari, ma anche verso altri paesi della stessa Unione europea meno rigorosi del nostro [...]”.

⁹²² Tale criterio è richiamato anche negli artt. 56 e 57 del D.lgs. 231/2007 che disciplinano le sanzioni per l'inosservanza degli obblighi di adeguata verifica, astensione e conservazione, anche se a ben vedere può trovare applicazione solo nell'ipotesi in cui la contestazione abbia a oggetto una omessa segnalazione di operazioni sospette.

⁹²³ Tali istruzioni, seppur formalmente indirizzate agli uffici centrali e territoriali del Ministero, contengono linee di indirizzo che assumono rilievo nella fase di avvio del procedimento sanzionatorio da parte delle autorità “verbalizzanti” (come UIF e Guardia di Finanza), nel corso del procedimento che porta all'irrogazione della sanzione e in quello successivo in cui l'Autorità giudiziaria è chiamata a valutarne la legittimità; d'altra parte le medesime istruzioni ministeriali dovrebbero rilevare anche per le Autorità di vigilanza per evitare disomogeneità di applicazione della disciplina nell'ambito delle procedure sanzionatorie di propria competenza. È in particolare stabilito che: “Il carattere ripetuto delle violazioni si desume anzitutto dall'esistenza di ulteriori contestazioni della stessa violazione, almeno una delle quali sia stata riconosciuta sussistente con irrogazione di una sanzione”; “La rilevazione del carattere sistematico delle violazioni presuppone un ambito di osservazione della condotta del soggetto obbligato sufficientemente ampio sia dal punto di vista dell'arco temporale oggetto dell'accertamento, sia quanto all'ambito oggettivo delle violazioni accertate. In particolare, la sistematicità delle violazioni deve ritenersi sussistente quando, nell'ambito di uno o più atti di contestazione e a seguito dell'analisi da parte dell'autorità verbalizzante di un numero sufficientemente elevato di singole operazioni, riconducibili a distinte operatività e/o prestazioni professionali, non necessariamente riferibili al medesimo cliente o alla medesima tipologia di negozio o transazione, distinte dal punto di vista soggettivo e/o oggettivo, si rilevi – per la maggior parte di esse – il comportamento omissivo sanzionato dalla legge”; “il carattere “plurimo” attiene alla singola contestazione elevata. In tale prospettiva, le plurime violazioni: possono afferire anche ad una singola operatività, purché nel suo ambito si registrino più operazioni, distribuite in un apprezzabile arco temporale che, anche singolarmente considerate o per il loro manifestarsi con frequenza e con caratteristiche analoghe nel corso del rapporto continuativo, presentino elementi di sospetto in base ai vigenti parametri normativi. Il carattere plurimo della violazione può invece escludersi ogni qual volta le operazioni sospette non segnalate risultino tra loro strettamente connesse, orientate al conseguimento di uno scopo determinato, specifico e unitario e poste in essere in un limitato arco temporale, ferma restando la rilevanza che tali circostanze possono eventualmente assumere ai fini della valutazione dell'intensità e del grado dell'elemento soggettivo e/o della rilevanza ed evidenza dei motivi del sospetto; possono riguardare anche una singola prestazione professionale, se articolata in più operazioni distinte sul piano oggettivo o economico-giuridico, che danno luogo a più fattispecie autonome, per ciascuna delle quali siano rilevabili i suddetti elementi di sospetto”. La circolare in questione è consultabile sul sito del MEF. In argomento cfr. M. Krogh, *Prime note di commento alla circolare MEF Prot. DT 56499 – 17/06/2022 sulle sanzioni antiriciclaggio*, in AML&Fintech, 3, 2022, p. 15 e ss. Sulla precedente circolare ministeriale del 2017 cfr. G. Castaldi, *Antiriciclaggio: le criticità in materia sanzionatoria rafforzano l'esigenza di un Testo unico*, Bancaria, 2019, 5, p. 49, secondo cui “... il quale il Ministero “preoccupato di garantire una quantificazione uniforme delle sanzioni pecuniarie in presenza di circostanze e condotte equiparabili, stabilisce una classificazione rigida e articolata del «peso» da attribuire alle diverse infrazioni, ricorrendo ad artificiosi rapporti di corrispondenza tra importo delle sanzioni e livelli di responsabilità. Ciò senza considerare che, oltre certi limiti, le valutazioni dei singoli casi non possono essere ricondotte a logiche matematiche, ma rimesse alla prudente ed equilibrata valutazione discrezionale di chi accerta in concreto le infrazioni. La determinazione e la pubblicazione di criteri troppo analitici, inoltre, rischia di innescare un ampio contenzioso, che può trarre spunto da effettivi o presunti scostamenti dalle tassative e minuziose indicazioni

In merito alle violazioni degli obblighi segnaletici occorre richiamare due aspetti: le omesse segnalazioni di operazioni sospette sono sanzionate in via amministrativa salvo che il fatto costituisca reato (art. 58, commi 1 e 2)⁹²⁴; le sanzioni previste per tali omissioni si applicano in luogo di quelle stabilite per le violazioni in materia di adeguata verifica e conservazione quando il soggetto obbligato commette anche in tempi diversi violazioni della specie da cui derivi come conseguenza immediata e diretta l'inosservanza dell'obbligo di segnalazione (art. 58, comma 5, del D.lgs. 231/2007)⁹²⁵.

Ciò posto, sotto il profilo dell'imputabilità delle sanzioni amministrative il legislatore si rivolge ai soggetti tenuti all'osservanza degli obblighi antiriciclaggio, siano essi persone fisiche (ad esempio professionisti) o giuridiche (ad esempio intermediari bancari e finanziari, prestatori di servizi di gioco). Partendo dai soggetti obbligati non sottoposti a vigilanza a fini antiriciclaggio, è prevista una sanzione di importo contenuto, in misura fissa, pari a 2.000 euro in materia di adeguata verifica e conservazione⁹²⁶ e a 3.000 euro per l'omessa segnalazione di operazioni sospette (artt. 56, comma 1, 57, comma 1, e 58, comma 1). Nel caso di violazioni gravi, ripetute o sistematiche ovvero plurime (c.d. violazioni qualificate) la sanzione è più severa: da 2.500 a 50.000 euro per l'inosservanza degli obblighi di adeguata verifica e conservazione (artt. 56, comma 2⁹²⁷, e 57, comma 2) e da 30.000 a 300.000 euro per l'omessa segnalazione di operazioni sospette (art. 58, comma 2)⁹²⁸.

Per le violazioni riferibili ai soggetti obbligati vigilati, in coerenza con il ruolo primario che essi assumono in materia e con la conseguente maggior ampiezza e intensità della disciplina e degli obblighi, viene disegnato un regime sanzionatorio specifico e a più livelli.

In particolare, è stabilito che le predette sanzioni previste per le violazioni segnaletiche (3.000 e 30.000 euro a seconda che si tratti di violazione semplice o qualificata) si applichino anche al "personale"⁹²⁹ degli intermediari bancari e finanziari e delle società fiduciarie diverse da quelle iscritte nell'albo di cui all'art. 106 T.U.B. nonché al responsabile dell'incarico nell'ambito delle società di revisione legale dei conti.

Sono così state mantenute, anche dopo la riforma del 2017 e del 2019, forme di responsabilità a carico di persone fisiche inserite nell'organizzazione del soggetto obbligato e connesse alle modalità di adempimento degli obblighi di segnalazione prescritte dagli artt. 36 e 37 del decreto antiriciclaggio⁹³⁰.

contenute nella normativa interna. Meglio sarebbe stato limitarsi a sensibilizzare gli uffici sulla necessaria coerenza tra motivazione e decisione, ricorrendo a programmi di adeguata formazione del personale e alla circolazione, a fini di coordinamento, delle informazioni sulla casistica esaminata e sulle decisioni assunte".

⁹²⁴ La clausola di riserva "salvo che il fatto costituisca reato" denota la specifica attenzione del legislatore a evitare il rischio di cumulo della sanzione amministrativa con quella penale data la potenziale contiguità dell'omessa segnalazione di operazioni sospette con l'ipotesi di coinvolgimento criminale dell'operatore a titolo di concorso in riciclaggio o nei reati-presupposto.

⁹²⁵ La prevalenza della sanzione per l'omessa segnalazione di operazioni sospette nel caso di violazione degli obblighi di adeguata verifica e conservazione riflette il carattere strumentale di questi ultimi rispetto all'obiettivo finale del legislatore antiriciclaggio di stimolare la collaborazione attiva, confermando la centralità dell'obbligo segnaletico nel quadro della disciplina di prevenzione.

⁹²⁶ Ai sensi dell'art. 67, comma 2, a fronte di violazioni ritenute di minore gravità, la sanzione di cui agli artt. 56, comma 1, e 57, comma 1, può essere ridotta da un terzo a due terzi.

⁹²⁷ Le medesime sanzioni di cui all'art. 56, commi 1 e 2, si applicano ai soggetti obbligati in caso di violazione dell'obbligo di astensione di cui all'art. 42 del D.lgs. 231/2007.

⁹²⁸ Ai sensi dell'art. 58, comma 4, è inoltre stabilito che nel caso in cui le violazioni gravi, ripetute o sistematiche ovvero plurime producono un vantaggio economico, l'importo massimo della sanzione: a) è elevato fino al doppio dell'ammontare del vantaggio medesimo, qualora detto vantaggio sia determinato o determinabile e, comunque, non sia inferiore a 450.000 euro; b) è elevato fino ad un milione di euro, qualora il predetto vantaggio non sia determinato o determinabile.

⁹²⁹ Cfr. art. 1, comma 2, lett. cc), del D.lgs. 231/2007.

⁹³⁰ Una posizione critica sulla configurazione della responsabilità del personale dipendente degli intermediari per omessa segnalazione di operazioni sospette è stata espressa da G. Castaldi, *Antiriciclaggio: le criticità in materia sanzionatoria rafforzano l'esigenza di un Testo unico*, *Bancaria*, 2019, 5, p. 44. L'Autore ha in particolare evidenziato che "il legislatore ha inteso recepire la disposizione della direttiva che impone ai Paesi membri di applicare anche ai «membri dell'organo di gestione o alle altre persone fisiche responsabili» le sanzioni previste per la violazione degli obblighi imposti alle «entità giuridiche». Ebbene, se è pur vero che il richiamo alle «altre persone fisiche responsabili» contenuto nella direttiva non sembrerebbe escludere la punibilità del personale dipendente di ogni ordine e grado direttamente responsabile delle violazioni, l'accostamento ai «membri dell'organo di gestione», che la legge delega traduce nell'espressione «membri dell'organo di gestione o le altre persone fisiche titolari di poteri di amministrazione, direzione o controllo», fa dubitare che tra i destinatari delle sanzioni antiriciclaggio s'intendessero comprendere anche i dipendenti di grado non elevato. L'espressione usata dalla legge delega, infatti, sembra volersi ragionevolmente riferire solo alle posizioni apicali della scala gerarchica aziendale. Questa tesi è rafforzata dalla circostanza che la direttiva, nello stabilire l'entità delle sanzioni pecuniarie applicabili alle persone fisiche, stabilisce che l'importo massimo non sia inferiore a 5 milioni di euro. È vero che si tratta di un importo massimo, ma è più che

Nello specifico, per gli intermediari e altri operatori finanziari è stabilito che il c.d. “primo livello” (responsabile della dipendenza, dell’ufficio, di altro punto operativo, unità organizzativa o struttura dell’intermediario o del soggetto cui compete l’amministrazione e la gestione concreta dei rapporti con la clientela) ha l’obbligo di comunicare, senza ritardo, le operazioni sospette al c.d. “secondo livello” (titolare della competente funzione o legale rappresentante o altro soggetto all’uopo delegato) che esamina le segnalazioni pervenute e, qualora le ritenga fondate alla luce dell’insieme degli elementi a propria disposizione e delle evidenze desumibili dai dati e dalle informazioni conservati, le trasmette alla UIF, prive del nominativo del segnalante⁹³¹. Analogo doppio livello è altresì previsto nelle società di revisione legale con riguardo, da un lato, al responsabile dell’incarico di revisione che partecipa al compimento della prestazione e a cui compete la gestione del rapporto con il cliente e, dall’altro, al titolare della competente funzione, al legale rappresentante o a un suo delegato (art. 37, comma 3, del D.lgs. 231/2007). Ne deriva che la richiamata sanzionabilità del “personale” è riferita per intermediari e revisori all’inadempimento dei descritti obblighi segnaletici da parte del primo e del secondo livello⁹³².

Gli aspetti qualificanti della riformata disciplina sanzionatoria per i soggetti vigilati si rinvencono nell’art. 62 del D.lgs. 231/2007.

Con riferimento agli intermediari bancari e finanziari, vigilati a fini antiriciclaggio dalla Banca d’Italia la sanzione va da un minimo di 30.000 euro a un massimo di 5.000.000 di euro ovvero pari al dieci per cento del fatturato complessivo annuo, quando tale importo percentuale è superiore a 5.000.000 di euro e il fatturato è disponibile e determinabile. È inoltre prevista la sanzionabilità, oltre che per la violazione degli obblighi prescritti dal D.lgs. 231/2007, anche per le disposizioni emanate dalla medesima Autorità di vigilanza in materia di organizzazione, procedure e controlli interni di cui agli artt. 7, 15 e 16 del predetto decreto (art. 62, comma 1).

verosimile che anche la direttiva non intenda coinvolgere i numerosissimi dipendenti che, specie in aziende caratterizzate da dimensioni rilevanti e organizzazione complessa, sono necessariamente destinatari di deleghe per l’esercizio di circoscritti poteri amministrativi, direttivi o di controllo”. [...] “Non sono inoltre da escludere problemi di costituzionalità con riguardo al trattamento discriminatorio riservato ai dipendenti degli intermediari bancari e finanziari titolari di responsabilità non dissimili da quelle dei colleghi dipendenti da imprese operanti in altri settori. Meglio sarebbe stato se – come d’altra parte avviene per le violazioni in materia di adeguata verifica e di conservazione – le sanzioni fossero state previste solo a carico delle entità giuridiche, lasciando a queste ultime il compito di valutare le eventuali responsabilità dei propri dipendenti e, quindi, di assumere nei loro confronti provvedimenti disciplinari, di intraprendere azioni di risarcimento danni ovvero di effettuare denunce all’Autorità giudiziaria”.

⁹³¹ Più in dettaglio, ai sensi dell’art. 36 del decreto antiriciclaggio, il responsabile della dipendenza, dell’ufficio, di altro punto operativo, unità organizzativa o struttura dell’intermediario o del soggetto cui compete l’amministrazione e la gestione concreta dei rapporti con la clientela, ha l’obbligo di comunicare, senza ritardo, le operazioni sospette al titolare della competente funzione o al legale rappresentante o ad altro soggetto all’uopo delegato. Gli intermediari assicurativi – art. 3, comma 2, lett. o) – e gli agenti in attività finanziaria – art. 3, comma 3, lett. c) – trasmettono la segnalazione al titolare della competente funzione, al legale rappresentante o ad altro soggetto all’uopo delegato dell’intermediario mandante o di riferimento. I mediatori di assicurazione o di riassicurazione (qualora non sia individuabile un intermediario di riferimento) e i mediatori creditizi inviano la segnalazione direttamente alla UIF. La comunicazione all’intermediario di riferimento è inoltre prevista da parte dei soggetti convenzionati e agenti di cui all’art. 1, comma 2, lett. nn), mentre i soggetti convenzionati e agenti operanti sul territorio nazionale per conto di istituti aventi sede legale e amministrazione centrale in altro Stato membro, sono tenuti a trasmettere al punto di contatto centrale ogni circostanza e informazione rilevante, ai fini della valutazione, da parte di questi ultimi, in ordine all’inoltro di una segnalazione di operazione sospetta. Il titolare della competente funzione, il legale rappresentante o altro soggetto all’uopo delegato dell’intermediario mandante o di riferimento, o il responsabile del punto di contatto centrale, esamina le segnalazioni pervenute e, qualora le ritenga fondate alla luce dell’insieme degli elementi a propria disposizione e delle evidenze desumibili dai dati e dalle informazioni conservati, le trasmette alla UIF, prive del nominativo del segnalante. Secondo Cass. n. 20647/2018, “in tema di sanzioni per la violazione della normativa antiriciclaggio, ai sensi dell’art. 3 del DL n. 143 del 1991, conv. dalla l. n. 197 del 1991, sostituito dall’art. 1 del D.lgs. 153 del 1997, il potere di valutare le segnalazioni e (in caso di ritenuta fondatezza delle medesime) trasmetterle al questore, spetta soltanto al “titolare dell’attività”, mentre il “responsabile della dipendenza”, cui è attribuito un margine di discrezionalità ridotto, è tenuto a segnalare al suo superiore ogni operazione che lo induca a ritenere che il suo oggetto possa provenire dai reati di cui agli artt. 648-bis e 648-ter c.p.”. In senso conforme cfr. Cass. n. 24209/2022. Secondo Cass. n. 7951/2017 “è esclusa, per il principio di personalità della responsabilità per l’illecito amministrativo, la responsabilità “aziendale” del direttore di filiale, ove questi non abbia direttamente gestito il rapporto con il cliente, ovvero non abbia personalmente comunque rilevato la sussistenza di un’operazione sospetta, né abbia ricevuto la segnalazione”.

⁹³² Un’interpretazione strettamente formale degli artt. 36 e 37 indurrebbe a ritenere che il secondo livello non possa essere considerato responsabile nel caso in cui nessuna segnalazione gli sia pervenuta dal primo livello; nondimeno si tratterebbe di un’interpretazione, da un lato, contraria alle finalità della norma volta a tenere conto di quale elemento dell’organizzazione sia effettivamente in grado di rilevare l’operazione sospetta, dall’altro, paradossale nelle realtà aziendali più complesse, specie degli intermediari bancari e finanziari, dove le procedure e gli strumenti adottati a livello centrale in genere consentono al secondo livello di disporre dei maggiori elementi informativi per l’individuazione dei profili di anomalia e sospetto. In tale direzione le disposizioni della Banca d’Italia in materia di organizzazione, procedure e controlli interni (parte terza, sezione II) sembrano affidare al secondo livello un certo grado di autonomia nella collaborazione attiva. Infatti, in base alle procedure organizzative interne, il responsabile per le segnalazioni di operazioni sospette ha il compito di valutare alla luce di tutti gli elementi disponibili sia le operazioni sospette comunicate dal primo livello (responsabile della dipendenza o di altro punto operativo o unità organizzativa o struttura competente alla gestione concreta dei rapporti con la clientela) sia - e qui sta il punto - quelle di cui sia altrimenti venuto a conoscenza nell’ambito della propria attività.

In caso di violazioni qualificate realizzate con riferimento a obblighi diversi da quello di segnalazione delle operazioni sospette⁹³³, caratterizzate da scarsa offensività o pericolosità⁹³⁴, in alternativa alla sanzione pecuniaria, l'Autorità di vigilanza può: i) ordinare all'intermediario di eliminare le infrazioni e astenersi dal ripeterle, anche indicando le misure da adottare e il termine per attuarle (c.d. *cease and desist order*); ii) qualora l'infrazione contestata sia cessata, applicare la sanzione consistente in una dichiarazione pubblica avente a oggetto la violazione commessa e il soggetto responsabile (c.d. *public statement*)⁹³⁵ art. 62, comma 4).

Inoltre, fermo quanto previsto per la responsabilità dell'intermediario, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 5.000.000 di euro ai soggetti titolari di funzioni di amministrazione, direzione e controllo dell'intermediario che, non assolvendo in tutto o in parte ai compiti direttamente o indirettamente correlati alla funzione o all'incarico, hanno agevolato, facilitato o comunque reso possibili le violazioni da parte dell'intermediario stesso o l'inosservanza del *cease and desist order* ovvero hanno inciso in modo rilevante sull'esposizione dell'intermediario al rischio di riciclaggio o di finanziamento del terrorismo. Qualora il vantaggio ottenuto dall'autore della violazione sia superiore a 5.000.000 di euro, la sanzione è elevata fino al doppio del vantaggio ottenuto, purché di ammontare determinato o determinabile. Tenuto conto della gravità della violazione l'Autorità di vigilanza ha anche il potere di adottare nei confronti del responsabile la sanzione dell'interdizione dallo svolgimento della funzione o dell'incarico di amministrazione, direzione o controllo dell'ente, per un periodo non inferiore a sei mesi e non superiore a tre anni (art. 62, commi 2 e 3).

Lo stesso art. 62, comma 5, prevede la sanzione compresa tra 3.000 e 1.000.000 di euro nei confronti dei revisori legali e delle società di revisione legale con incarichi di revisione su enti di interesse pubblico o su enti sottoposti a regime intermedio nonché nei confronti dei soggetti titolari di funzioni di amministrazione, direzione e controllo della società che, non assolvendo in tutto o in parte ai compiti direttamente o indirettamente correlati alla funzione o all'incarico, hanno agevolato, facilitato o comunque reso possibili le violazioni.

Infine, fermo quanto previsto dagli artt. 56, 57 e 58⁹³⁶, per l'inosservanza delle disposizioni in materia di organizzazione da parte dei soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'art. 134 TULPS, si applica la sanzione da 2.500 euro a 350.000 euro. Nei casi di violazioni qualificate la sanzione può essere aumentata fino al triplo del massimo edittale ovvero fino al doppio dell'importo dei profitti ricavati dalle violazioni accertate, quando tale importo sia determinato o determinabile (art. 62, comma 7-bis).

3.2 Le violazioni degli altri obblighi antiriciclaggio

Il decreto antiriciclaggio prevede ulteriori fattispecie sanzionabili, inerenti a profili specifici del sistema di prevenzione.

⁹³³ Si tratta degli obblighi in materia di adeguata verifica, di conservazione, di organizzazione, procedure e controlli interni.

⁹³⁴ Ai sensi dell'art. 67 del D.lgs. 231/2007 si considera ogni circostanza rilevante e, in particolare, tenuto conto del fatto che il destinatario della sanzione sia una persona fisica o giuridica: a) la gravità e durata della violazione; b) il grado di responsabilità della persona fisica o giuridica; c) la capacità finanziaria della persona fisica o giuridica responsabile; d) l'entità del vantaggio ottenuto o delle perdite evitate per effetto della violazione, nella misura in cui siano determinabili; e) l'entità del pregiudizio cagionato a terzi per effetto della violazione, nella misura in cui sia determinabile; f) il livello di cooperazione con le autorità di cui all'art. 21, comma 2, lett. a) prestato dalla persona fisica o giuridica responsabile; g) l'adozione di adeguate procedure di valutazione e mitigazione del rischio di riciclaggio e di finanziamento del terrorismo, commisurate alla natura dell'attività svolta e alle dimensioni dei soggetti obbligati; h) le precedenti violazioni delle disposizioni di cui al presente decreto.

⁹³⁵ Sono state quindi previste in ambito antiriciclaggio anche misure alternative alla sanzione pecuniaria coerenti con la [Comunicazione](#) del 2010 della Commissione sul potenziamento dei regimi sanzionatori nel settore dei servizi finanziari e già adottate in altri contesti della regolamentazione, ad esempio in materia di vigilanza prudenziale.

⁹³⁶ La salvezza degli artt. 56, 57 e 58 sembra potersi interpretare nel senso di applicare le fattispecie e le sanzioni ivi previste nei confronti dei soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, nel caso di violazioni degli obblighi in materia di adeguata verifica, conservazione e segnalazione di operazioni sospette.

È punita con la sanzione amministrativa pecuniaria da 5.000 a 50.000 euro l'omessa esecuzione del provvedimento di sospensione dell'operazione sospetta, disposto dalla UIF ai sensi dell'art. 6, comma 4, lett. c), del D.lgs. 231/2007 (art. 58, comma 6).

Rilevano, inoltre, le disposizioni sanzionatorie applicabili per la violazione delle limitazioni all'uso del contante e dei titoli al portatore, del divieto di conti o libretti di risparmio in forma anonima o con intestazione fittizia e di prodotti di moneta elettronica anonimi, nonché dell'obbligo di comunicazione al Ministero dell'Economia e delle finanze delle infrazioni in materia di contanti e assegni (art. 63).

Nei confronti dei prestatori di servizi di pagamento e degli istituti di moneta elettronica che omettono l'istituzione del punto di contatto centrale (art. 43, comma 3, del D.lgs. 231/2007) si applica la sanzione da un minimo di 30.000 euro a un massimo di 5.000.000 di euro ovvero pari al dieci per cento del fatturato complessivo annuo, quando tale importo percentuale è superiore a 5.000.000 di euro e il fatturato è disponibile e determinabile (art. 62, comma 1).

Sono invece puniti con una sanzione da 10.000 a 200.000 euro gli intermediari bancari e finanziari che violano il divieto di aprire o mantenere, anche indirettamente, conti di corrispondenza con banche di comodo (art. 62, comma 6).

È punito con una sanzione da 5.000 a 30.000 euro ciascun componente degli organi di controllo presso i soggetti obbligati che, nell'esercizio della funzione, ometta di effettuare le comunicazioni di cui all'art. 46 del D.lgs. 231/2007 inerenti: *i)* alle operazioni potenzialmente sospette di cui siano venuti a conoscenza; *ii)* ai fatti che possono integrare violazioni qualificate delle disposizioni antiriciclaggio⁹³⁷.

Disposizioni sanzionatorie specifiche sono altresì previste per l'inosservanza degli obblighi di trasmissione e informazione nei confronti della UIF (art. 60, che indica sanzioni tra 5.000 e 50.000 euro), a presidio dell'ampio novero di comunicazioni, diverse e ulteriori rispetto alle segnalazioni di operazioni sospette, di cui è destinataria l'Unità ai sensi di legge. Vi rientrano in particolare le segnalazioni antiriciclaggio aggregate di cui all'art. 33, le richieste di dati e informazioni formulate in sede di analisi finanziaria delle segnalazioni di operazioni sospette (art. 40, comma 2) e le comunicazioni oggettive di cui all'art. 47 del D.lgs. 231/2007; si ritiene che rientrino nella fattispecie anche le ipotesi di violazione degli obblighi informativi nei confronti della UIF che il decreto antiriciclaggio pone in capo alle pubbliche amministrazioni⁹³⁸.

La stessa sanzione tra 5.000 e 50.000 euro si applica nei casi di rifiuto di esibire documenti o di fornire notizie ovvero di comunicazione di notizie errate o incomplete in occasione delle ispezioni del MEF di cui all'art. 5, comma 3, del D.lgs. 231/2007 (art. 60, comma 2).

Ulteriori previsioni riguardano le sanzioni applicabili nei confronti dei prestatori di servizi di pagamento e degli istituti di moneta per la violazione degli obblighi di comunicazione all'OAM funzionali all'alimentazione del registro dei soggetti convenzionati e degli agenti, nonché nei confronti di tali soggetti

⁹³⁷ In proposito, si rammenta che nella relazione illustrativa del D.lgs. 90/2017 si legge che l'art. 46 "scioglie i dubbi sollevati all'indomani dell'intervento del decreto legislativo 151 del 2009, con l'introduzione del comma 3-bis, all'interno dell'art. 12. Benché infatti la relazione illustrativa alla predetta novella specificasse chiaramente che essa si attagliava esclusivamente agli organi di controllo dei soggetti obbligati, la collocazione della disposizione all'interno dell'art. 12, riguardante tutti i professionisti, aveva dato adito all'interpretazione per cui l'esenzione ivi prevista fosse da estendere anche ad organi di controllo di soggetti diversi da quelli obbligati. La norma di cui all'art. 46 trova fondamento nell'esigenza di precisare che i singoli componenti degli organi di controllo presso i soggetti obbligati sono tenuti unicamente alle comunicazioni ivi previste, sgombrando il campo dal rischio di una gravosa duplicazione degli adempimenti a cui i componenti degli organi di controllo sarebbero tenuti in quanto composti da soggetti obbligati (ai sensi dell'art. 3, comma 4). Peraltro, poiché anche il soggetto controllato è, a sua volta, tenuto all'adempimento degli obblighi previsti dal decreto (adeguata verifica, conservazione e segnalazione di operazione sospetta) i medesimi obblighi sarebbero inutilmente replicati. Le esigenze di razionalizzazione e semplificazione degli adempimenti non sussistono, di contro, per i professionisti componenti di organi di controllo di soggetti non obbligati. Tali professionisti in forza del loro assoggettamento agli adempimenti prescritti in funzione di prevenzione del riciclaggio e di finanziamento del terrorismo sono obbligati agli adempimenti di cui al Titolo II, Capi I, II e III".

⁹³⁸ Cfr. *Le Pubbliche amministrazioni nel sistema di prevenzione del riciclaggio*, UIF, Quaderni dell'antiriciclaggio – Analisi e studi, settembre 2022, p. 15, nota 11, in cui si afferma che l'art. 40, comma 2, del D.lgs. 231/2007 pone a carico delle pubbliche amministrazioni specifici obblighi di fornire dati e informazioni su richiesta della UIF, il cui inadempimento, in base all'art. 60 dello stesso decreto, comporta l'irrogazione della sanzione amministrativa.

convenzionati e agenti per l'omissione degli adempimenti a loro carico prescritti dalla normativa antiriciclaggio (art. 61).

Il quadro sanzionatorio è infine completato dalle disposizioni rivolte ai distributori ed esercenti nel comparto del gioco per l'inosservanza degli adempimenti posti a loro carico nei confronti degli operatori di gioco che svolgono l'attività su concessione dell'Agenzia delle Dogane e dei Monopoli e che sono, in quanto tali, destinatari degli obblighi antiriciclaggio (art. 64).

4. Le competenze e le procedure sanzionatorie per le violazioni degli obblighi antiriciclaggio *(A.M.A. Carriero e L. La Rocca)*

Il quadro normativo di riferimento in materia di sanzioni antiriciclaggio prevede procedure distinte a seconda della tipologia di violazione e di soggetto obbligato sanzionabile, con il coinvolgimento a vario titolo di più Autorità nelle fasi di accertamento e contestazione delle violazioni nonché di istruttoria e irrogazione delle relative sanzioni amministrative.

In particolare, avendo a mente i poteri attribuiti alle Autorità dal Titolo I, Capo II, del D.lgs. 231/2007, si può anzitutto constatare come il riparto di competenze in materia sanzionatoria risponda a un criterio misto soggettivo e per materia che, in virtù di specifiche eccezioni previste dal legislatore, non sempre collima con le attribuzioni delle Autorità sul piano della normativa secondaria e dei controlli antiriciclaggio⁹³⁹. Ci si soffermerà quindi, dapprima, sulla distinzione delle competenze a seconda che rilevino violazioni commesse da soggetti obbligati vigilati oppure non vigilati; saranno poi approfondite le previsioni particolari che riguardano le violazioni degli obblighi di segnalazione delle operazioni sospette, materia che vede la coesistenza di plurimi livelli di responsabilità corrispondenti a distinte competenze sanzionatorie delle Autorità di vigilanza e del Ministero dell'Economia e delle finanze (MEF). Il medesimo dicastero è competente a sanzionare le omissioni segnaletiche imputabili ai soggetti obbligati non vigilati nonché le ulteriori violazioni di disposizioni del decreto antiriciclaggio non attribuite alla potestà di altre Autorità (art. 65, comma 1, del D.lgs. 231/2007).

Più in dettaglio, le Autorità di vigilanza di settore verificano il rispetto degli obblighi previsti dal decreto antiriciclaggio e dalle relative disposizioni di attuazione da parte dei soggetti vigilati e, in caso di inosservanza, irrogano le relative sanzioni⁹⁴⁰.

Il Nucleo Speciale di Polizia Valutaria delle Guardia di Finanza (NPSV) ha invece una competenza generale di controllo sul rispetto delle disposizioni antiriciclaggio da parte dei soggetti obbligati non vigilati; effettua ulteriori controlli in collaborazione con la UIF qualora questa ne richieda l'intervento a supporto delle proprie funzioni e, previa intesa con le Autorità di vigilanza di settore, può anche eseguire verifiche presso alcune categorie di soggetti vigilati. Il NPSV ha quindi il potere di accertare e contestare, con le modalità e nei termini di cui alla legge 689/1981, ovvero di trasmettere alle Autorità di vigilanza di settore le violazioni degli obblighi riscontrate nell'esercizio dei propri poteri di controllo⁹⁴¹.

La UIF effettua, anche attraverso ispezioni, verifiche al fine di accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione (art. 35 del D.lgs. 231/2007), nonché con riguardo alle prescritte comunicazioni all'Unità e ai casi di omesse comunicazioni sanzionate ai sensi dell'art. 60 del medesimo decreto; in relazione a tali compiti, la UIF ha il

⁹³⁹ In argomento cfr. parere del Consiglio di Stato del 3 agosto 2018, n. 2018, in cui si afferma: "in via generale, nei settori in cui è presente un'Autorità di vigilanza (Banca d'Italia, Consob e l'IVASS a mente delle definizioni date dall'art. 1 comma 2 del decreto) è quest'ultima a effettuare i controlli sui soggetti obbligati e vigilati. Nei settori in cui invece non opera una specifica Autorità di vigilanza, sono le Amministrazioni e gli organismi interessati che hanno la supervisione dei soggetti obbligati, e che siano titolari di poteri di controllo ovvero competenti al rilascio di titoli abilitativi prescritti dalla pertinente normativa di settore, a dover esercitare la vigilanza. [...] La previsione generale è contenuta nell'art. 65 del decreto in commento, il quale prevede che, salva specifica eccezione della quale si dirà oltre, il Ministero dell'Economia e delle finanze che provvede all'irrogazione delle sanzioni per violazione degli obblighi di cui al presente decreto nei confronti dei soggetti obbligati non sottoposti alla vigilanza delle autorità di vigilanza di settore". Per i settori sottoposti a specifica vigilanza dispone invece l'art. 62 cit., il quale attribuisce la competenza sanzionatoria all'Autorità di vigilanza del settore. Le due disposizioni costituiscono il fulcro del sistema sanzionatorio e danno linfa al criterio generale che governa il riparto di competenze tra MEF e Autorità di vigilanza, in forza del quale quest'ultima associa sempre al potere di vigilanza quello sanzionatorio, salvo espresse e specifiche deroghe previste dalla legge, mentre il primo gode di una competenza di carattere residuale per tutti i rimanenti operatori non vigilati da apposite Autorità.

⁹⁴⁰ Cfr. art. 7, comma 1, del D.lgs. 231/2007 (si veda in particolare la lett. e), del citato comma 1).

⁹⁴¹ Cfr. art. 9, comma 2, del D.lgs. 231/2007. Analogo potere è attribuito alla Direzione Investigativa Antimafia ai sensi dell'art. 9, comma 7, del D.lgs. 231/2007.

potere di accertare e contestare la violazione per poi rimettere gli atti al MEF per la fase istruttoria ovvero trasmettere alle Autorità di vigilanza di settore le violazioni degli obblighi di competenza delle predette Autorità, di cui viene a conoscenza nell'esercizio delle proprie funzioni istituzionali⁹⁴².

Tenuto conto del predetto riparto di competenze, le procedure sanzionatorie possono essere distinte, in primo luogo, a seconda che esse si svolgano nei confronti di soggetti obbligati vigilati o non vigilati (si tratta dell'applicazione del richiamato "criterio di riparto soggettivo").

Nei confronti dei soggetti obbligati vigilati si esplica, infatti, la potestà sanzionatoria delle Autorità di vigilanza di settore le quali, sulla base delle verifiche di competenza o delle risultanze dei controlli svolti dalla UIF ovvero dal NSPV o dalla DIA⁹⁴³, provvedono all'accertamento delle violazioni e alla relativa contestazione ai sensi delle disposizioni di settore (art. 65, comma 11)⁹⁴⁴. In questi casi non è ammesso il pagamento della sanzione in misura ridotta, ai sensi dell'ar. 16 della legge 689/1981.

Le medesime Autorità di vigilanza provvedono altresì all'irrogazione delle sanzioni nei confronti dei titolari di funzioni di amministrazione, direzione e controllo dell'ente che, non assolvendo in tutto o in parte ai compiti direttamente o indirettamente correlati alla funzione o all'incarico, hanno agevolato, facilitato o comunque reso possibili le violazioni ovvero che, nel caso degli intermediari bancari e finanziari, hanno agevolato, facilitato o comunque reso possibile l'inosservanza del *cease and desist order* ovvero hanno inciso in modo rilevante sull'esposizione degli stessi al rischio di riciclaggio o di finanziamento del terrorismo⁹⁴⁵.

L'irrogazione delle sanzioni nei confronti dei soggetti obbligati non vigilati avviene invece ad opera del MEF (art. 65, comma 1).

Regole specifiche vigono per le omesse segnalazioni di operazioni sospette, che sono rimesse alla competenza delle Autorità di vigilanza (Banca d'Italia, IVASS e Consob) se riferibili a persone giuridiche vigilate e a quella del MEF se imputabili ai soggetti obbligati non vigilati o a persone fisiche con ruoli specifici presso talune categorie di soggetti obbligati vigilati (si tratta dell'applicazione del sopra richiamato "criterio di riparto per materia").

Con particolare riguardo alla responsabilità delle predette persone fisiche, si richiama quanto descritto nel par. 3 di questo capitolo, in merito alle modalità di adempimento degli obblighi di segnalazione di cui agli artt. 36 e 37 del D.lgs. 231/2007, da parte dei soggetti che svolgono il ruolo di c.d. primo e secondo livello.

Il MEF è competente all'irrogazione delle sanzioni per l'inosservanza dei richiamati obblighi imputabile al personale degli intermediari, ai revisori legali ovvero ai responsabili dell'incarico di revisione legale nel caso di società di revisione, nonché ai titolari di funzioni di amministrazione, direzione e controllo di intermediari bancari e finanziari, società di revisione o di operatori non finanziari di cui all'art. 3, comma 5, lett. f), del D.lgs. 231/2007 (art. 65, comma 1, lett. a) e b), del medesimo decreto). In forza di tale previsione di legge si realizza, quindi, l'intersezione tra i richiamati criteri di riparto "soggettivo" e "per materia", con l'individuazione della competenza sanzionatoria in capo a un'Autorità (il MEF) priva di attribuzioni sul piano della normativa secondaria e dei controlli antiriciclaggio⁹⁴⁶.

⁹⁴² Art. 6, comma 4, lett. f) e g), del D.lgs. 231/2007.

⁹⁴³ Ai sensi dell'art. 9, comma 7, del D.lgs. 231/2007 la DIA [...] trasmette alle Autorità di vigilanza di settore le violazioni degli obblighi di cui al decreto antiriciclaggio riscontrate nell'esercizio delle proprie attribuzioni.

⁹⁴⁴ La Banca d'Italia, la Consob e l'IVASS applicano, in quanto compatibili, le rispettive previsioni di cui all'art. 145 TUB, all'art. 195 TUF, al Titolo XVIII, Capo VII, CAP e le relative disposizioni attuative. Le previsioni di cui all'art. 145 TUB e le relative disposizioni attuative si applicano altresì al procedimento con cui la Banca d'Italia provvede all'irrogazione delle sanzioni nei confronti dei soggetti obbligati vigilati di cui all'art. 3, comma 5, lett. f), del D.lgs. 231/2007.

⁹⁴⁵ In argomento cfr. art. 62, commi 7 e 8, del D.lgs. 231/2007, come modificato dal D.lgs. 125/2019. Prima della modifica del 2019 il Consiglio di Stato, con pronuncia del 18 luglio 2018, per le violazioni commesse dai titolari di funzioni in materie diverse dalle segnalazioni di operazioni sospette, si era espresso nel senso che anche la competenza fosse attribuita alle Autorità di vigilanza di settore.

⁹⁴⁶ Il mancato riconoscimento alle Autorità di vigilanza di una competenza sanzionatoria generale nei confronti degli intermediari bancari e finanziari e dei relativi esponenti è considerato "del tutto ingiustificato" da G. Castaldi, *Antiriciclaggio: le criticità in materia sanzionatoria rafforzano l'esigenza di un Testo unico*, *Bancaria*, 2019, 5, p. 43. Secondo l'Autore, "una tale valutazione, infatti, richiede una specifica professionalità ed è senz'altro agevolata dalla conoscenza approfondita dell'attività dell'intermediario, che la Banca d'Italia e le altre Autorità hanno acquisito nel pluriennale esercizio delle proprie funzioni istituzionali. Senza considerare, poi, le conseguenze negative

Nell'ambito del procedimento sanzionatorio che si svolge nei confronti delle predette persone fisiche, l'ente risponde comunque in solido, ai sensi dell'art. 6 della legge 689/1981, e anche quando l'autore della violazione non è univocamente identificabile ovvero quando lo stesso non è più perseguibile ai sensi della medesima legge (art. 65, comma 10). Nel caso di pagamento della sanzione da parte dell'ente, questi ha diritto di regresso per l'intero nei confronti dell'autore della violazione.

Un'ipotesi di omessa segnalazione di operazioni sospette – in particolare se a carattere grave, ripetuto, sistematico ovvero plurimo – può quindi dare luogo a plurimi addebiti e cumuli dei livelli di responsabilità nei confronti di persone fisiche (personale ed esponenti) ed enti, da accertare nell'ambito di procedure sanzionatorie distinte demandate alla competenza di Autorità diverse (rispettivamente il MEF e l'Autorità di vigilanza di settore). In mancanza di coordinamento e visione unitaria sull'azione sanzionatoria, l'istruttoria condotta da Autorità diverse, oltre a essere accompagnata da garanzie procedurali distinte, potrebbe sfociare in esiti difformi, minando la coerenza della risposta sanzionatoria a fronte del medesimo illecito. Inoltre, l'ente potrebbe in particolare essere chiamato a rispondere per lo stesso fatto sia in proprio, in ragione dell'addebito mosso dall'Autorità di vigilanza, sia in solido nel caso di infrazione contestata al proprio dipendente o titolare di funzioni di amministrazione, direzione e controllo. Si pone quindi il rischio di una duplicazione di responsabilità⁹⁴⁷ che si porrebbe in contrasto con il principio di *ne bis in idem*. Non può d'altra parte escludersi l'eventualità che la stessa condotta materiale venga qualificata diversamente nelle distinte procedure previste dalla normativa.

Al fine di evitare situazioni della specie, è necessario garantire forme di intervento coordinato tra tutte le Autorità coinvolte, basate su scambi informativi, comunicazione delle iniziative assunte e consolidamento di buone prassi, per assicurare l'adozione della procedura di volta in volta più idonea rispetto ai fatti accertati. Risponde a questa finalità il Tavolo Tecnico di Coordinamento in materia di controlli e sanzioni che è stato costituito nei primi mesi del 2021 presso la UIF e a cui partecipano le altre Autorità coinvolte in materia sanzionatoria (MEF, Banca d'Italia, Guardia di Finanza, Ivass e Consob, nonché le altre Autorità e amministrazioni interessate in relazione a specifiche questioni). Il Tavolo rappresenta uno strumento per la condivisione di esperienze e di approcci tra le diverse Autorità coinvolte nel processo di accertamento, al fine di incentivare modalità di valutazione condivise e rendere più efficace il sistema sanzionatorio⁹⁴⁸.

Al MEF sono altresì attribuite le competenze sanzionatorie per le violazioni commesse da soggetti convenzionati e agenti (art. 61), da distributori ed esercenti nel comparto del gioco (art. 64), nonché nei casi di violazioni del Titolo III del decreto antiriciclaggio in materia di limiti all'utilizzo del contante, di titoli al portatore, conti o libretti di risparmio in forma anonima o con intestazione fittizia e di prodotti di moneta elettronica anonima, nonché ogni altra sanzione amministrativa non espressamente attribuita alla potestà sanzionatoria di altra Autorità o organismo⁹⁴⁹.

Al procedimento di competenza del MEF si applicano, in quanto compatibili, le disposizioni di cui alla predetta legge 689/1981.

All'accertamento e alla contestazione delle violazioni provvede l'Autorità (NSPV/DIA, UIF, Autorità di vigilanza) che, nell'esercizio dei propri poteri, rilevi l'inosservanza degli obblighi antiriciclaggio.

Per le violazioni di competenza del MEF si applica l'art. 14, comma 2, della legge 689/1981 e la contestazione della violazione – quando non è immediata – deve essere notificata agli interessati residenti nel territorio della Repubblica entro il termine di novanta giorni e a quelli residenti all'estero entro il termine di trecentosessanta giorni dall'accertamento⁹⁵⁰.

che la suddetta condotta dei vertici aziendali può comportare anche sulla stabilità degli intermediari”.

⁹⁴⁷ G. Castaldi, *Antiriciclaggio: le criticità in materia sanzionatoria rafforzano l'esigenza di un Testo unico*, cit., p. 45, evoca “il contrasto con il principio del *ne bis in idem*, quantomeno perché per lo stesso fatto la persona giuridica potrebbe rispondere sia in proprio sia come responsabile solidale dell'inosservanza del dipendente”.

⁹⁴⁸ In argomento si veda il [Rapporto annuale della UIF per il 2021](#), pp. 64-65.

⁹⁴⁹ Ne deriva che è per esempio demandata al MEF l'irrogazione delle sanzioni in caso di violazioni degli obblighi informativi nei confronti della UIF ai sensi dell'art. 60 del D.lgs. 231/2007.

⁹⁵⁰ Nel caso delle violazioni sanzionate dalle Autorità di vigilanza si applicano i termini previsti dalle discipline di settore, comunque differenziati a seconda che l'incolpato sia residente in Italia oppure all'estero. Per la Banca d'Italia la contestazione avviene mediante apposita notifica, entro novanta o centottanta giorni dall'accertamento, rispettivamente per le procedure avviate ai sensi dell'art. 145 del TU e dell'art. 195 del TUF; in entrambi i casi, il termine è di trecentosessanta giorni per le società o enti aventi la sede legale all'estero e le persone fisiche residenti all'estero (Disposizioni di vigilanza in materia di sanzioni e procedura sanzionatoria amministrativa di cui al

I termini per le contestazioni decorrono dall'accertamento della violazione ed è pertanto essenziale l'individuazione di tale *dies a quo*. La giurisprudenza che si è pronunciata in argomento ha ritenuto che l'attività di accertamento dell'illecito non coincide con il momento in cui viene acquisito il fatto nella sua materialità, ma deve essere intesa come comprensiva del tempo necessario alla sua valutazione; il momento dell'accertamento, per la notifica degli estremi della violazione amministrativa, va individuato nel momento in cui l'Autorità abbia acquisito e valutato tutti i dati indispensabili ai fini della verifica dell'esistenza della violazione segnalata ovvero in quello in cui il tempo decorso non risulti ulteriormente giustificato dalla necessità di tale acquisizione e valutazione. Il compito di individuare, secondo le caratteristiche e la complessità della situazione concreta, il momento in cui ragionevolmente la contestazione avrebbe potuto essere tradotta in accertamento e da cui deve farsi decorrere il termine per la contestazione spetta al giudice del merito, la cui valutazione non è sindacabile nel giudizio di legittimità, ove congruamente motivata⁹⁵¹.

In proposito, le Autorità di vigilanza di settore, nel dare attuazione alle previsioni legislative che attribuiscono alle medesime la potestà sanzionatoria, hanno adottato talune disposizioni che fissano il *dies a quo* in un atto adottato dalle medesime⁹⁵². Si tratta di un approccio condivisibile che attribuisce rilievo con valenza esterna al predetto *dies a quo*, in modo da contenere la durata complessiva degli accertamenti entro limiti di ragionevolezza e garantire certezza e trasparenza all'azione amministrativa, in conformità con quanto previsto dalla legge 241/1990. *De iure condendo* è auspicabile che la materia sia oggetto di intervento normativo per tutte le Autorità coinvolte nelle fasi di accertamento e contestazione delle violazioni.

Per quanto riguarda il procedimento presso il MEF, il contraddittorio con l'interessato si svolge ai sensi della sopra richiamata legge 689/1981 e la decisione è assunta con decreto, udito il parere della Commissione consultiva per le infrazioni valutarie ed antiriciclaggio⁹⁵³.

Il termine per la conclusione del procedimento sanzionatorio è di due anni, decorrenti dalla ricezione della contestazione notificata dall'amministrazione procedente. Tale termine è prorogato di ulteriori sei mesi nel caso di formale richiesta da parte dell'interessato di essere audito nel corso del procedimento. In

[Provvedimento del 18 dicembre 2012 e successive modifiche](#)). Per la Consob l'avvio del procedimento sanzionatorio è disposto a mezzo di lettera di contestazione degli addebiti sottoscritta congiuntamente dal responsabile della Divisione competente e dal Direttore Generale o, su delega di quest'ultimo, dal Vice Direttore Generale. La contestazione degli addebiti è effettuata entro il termine di centottanta giorni, ovvero di trecentosessanta giorni se gli interessati risiedono o hanno la sede all'estero, dall'accertamento compiuto sulla base degli elementi comunque acquisiti e dei fatti emersi a seguito dell'attività di vigilanza svolta dalla Consob e delle successive valutazioni (regolamento sul Procedimento Sanzionatorio della Consob adottato con delibera n. 18750 del 19 dicembre 2013 e successive modifiche). Per l'IVASS l'atto di contestazione è notificato ai soggetti destinatari entro il termine di 120 giorni dall'accertamento dei fatti per i soggetti residenti in Italia, ovvero di 180 giorni per i soggetti residenti all'estero ([Regolamento Ivass n. 39 del 2 agosto 2018 e successive modifiche](#)).

⁹⁵¹ Cfr. Cass. n. 9311/2007, n. 10621/2010, n. 28210/2019, n. 27702/2019, n. 27405/2019, n. 20159/2019, n. 13509/2019 e n. 24476/2022.

⁹⁵² La Banca d'Italia accerta la violazione una volta acquisiti gli elementi necessari a valutare la sussistenza di un'irregolarità sanzionabile. L'accertamento si perfeziona con l'apposizione agli atti del visto del Capo del Dipartimento Vigilanza bancaria e finanziaria o, in caso di sua assenza o impedimento, del Vice Capo Dipartimento. Da tale data, comunicata nella lettera di contestazione, decorrono i termini per la notifica della contestazione delle violazioni agli interessati (si veda il sopra citato [Provvedimento del 18 dicembre 2012 e successive modifiche](#)). L'IVASS avvia la procedura sanzionatoria nei casi in cui accerta la violazione delle norme per le quali è prevista l'irrogazione di sanzioni amministrative, una volta acquisiti gli elementi necessari a valutarne la sussistenza. L'accertamento si perfeziona, nel caso di illeciti emersi nell'ambito di verifiche ispettive nei confronti degli intermediari assicurativi e riassicurativi o degli intermediari assicurativi a titolo accessorio, alla data di sottoscrizione del verbale ispettivo. Nel caso di illeciti emersi nell'ambito di verifiche ispettive nei confronti di soggetti diversi dagli intermediari assicurativi e riassicurativi o dagli intermediari assicurativi a titolo accessorio, l'accertamento si perfeziona alla data di apposizione agli atti del visto del Capo del Servizio Ispettorato. L'accertamento di illeciti emersi nell'ambito di verifiche a distanza si perfeziona nel momento in cui è completata la valutazione degli elementi oggettivi e soggettivi costitutivi della fattispecie suscettibile di dar luogo all'applicazione di una sanzione (si veda il sopra citato [Regolamento Ivass n. 39 del 2 agosto 2018 e successive modifiche](#)).

⁹⁵³ Secondo G. Castaldi, *Antiriciclaggio: le criticità in materia sanzionatoria rafforzano l'esigenza di un Testo unico*, Bancaria, cit., p. 50, con riferimento al preventivo parere (obbligatorio ma non vincolante) della Commissione istituita, all'epoca delle leggi valutarie, dal d.p.r. n. 148/1988 e mantenuta in vita dal d.p.r. 114/2007. "non può non rilevarsi che, considerata la pluriennale esperienza acquisita dai competenti uffici ministeriali, il passaggio appare superfluo e rischia di rallentare inutilmente il procedimento sanzionatorio". D'altra parte, i pareri di massima, per categoria di violazioni, formulati dalla Commissione di cui all'art. 1 del decreto del Presidente della Repubblica 14 maggio 2007, n. 114 sono richiamati nelle istruzioni applicative pubblicate dal Ministero dell'Economia e delle finanze in data 6 luglio 2017, come da ultimo modificate con circolare DT 56499 del 17 giugno 2022, consultabile sul sito del Ministero dell'Economia e delle finanze all'indirizzo https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/normativa/circolare-prot.-DT-56499-del-17-06-2022.pdf.

ogni caso quest'ultimo si considera concluso con l'adozione del decreto che dispone in ordine alla sanzione. Ne consegue che, in caso di decorso del termine senza che sia stato emanato il provvedimento finale, il procedimento sanzionatorio si estingue e non può essere ulteriormente proseguito.

I decreti sanzionatori sono impugnabili dinanzi al giudice ordinario ed è competente in via esclusiva il Tribunale di Roma. Fanno eccezione i decreti sanzionatori riguardanti le violazioni riguardanti soggetti convenzionati e agenti, distributori ed esercenti nel comparto del gioco nonché il Titolo III del decreto antiriciclaggio, per i quali permane la competenza del tribunale del luogo in cui è stata commessa la violazione.

È infine previsto che il MEF e le Autorità di vigilanza di settore si trasmettano reciprocamente gli atti adottati, per consentire a ciascuna Autorità di valutare l'eventuale applicabilità delle sanzioni rimesse alla propria competenza.

In caso di violazioni gravi, ripetute o sistematiche ovvero plurime il MEF informa le competenti amministrazioni interessate e gli organismi di autoregolamentazione di ogni atto idoneo ad intimare ai responsabili di porre termine alle violazioni e di astenersi dal ripeterle. Le medesime violazioni costituiscono presupposto per l'applicazione delle sanzioni disciplinari, ai sensi e per gli effetti dei rispettivi ordinamenti di settore. In tali ipotesi l'interdizione dallo svolgimento della funzione, dell'attività o dell'incarico non può essere inferiore a due mesi e superiore a cinque anni.

Il decreto che irroga le sanzioni nei casi di violazioni qualificate in materia di adeguata verifica della clientela, di conservazione, di segnalazione di operazione sospetta e di controlli interni è pubblicato senza ritardo e per estratto su apposita sezione del sito web del MEF ovvero delle Autorità di vigilanza di settore. La pubblicazione per estratto reca indicazione delle violazioni accertate, delle disposizioni violate, dei soggetti sanzionati, delle sanzioni rispettivamente applicate nonché, nel caso in cui sia adita l'autorità giudiziaria, dell'avvio dell'azione giudiziaria e dell'esito della stessa. Le informazioni pubblicate restano sul sito web per un periodo di cinque anni. Ferma la discrezionalità dell'Autorità procedente in ordine alla valutazione della proporzionalità della misura rispetto alla violazione sanzionata, non si dà luogo alla pubblicazione nel caso in cui essa possa comportare rischi per la stabilità dei mercati finanziari o pregiudicare lo svolgimento di un'indagine in corso. Qualora detti impedimenti abbiano carattere temporaneo, la pubblicazione può essere differita al momento in cui essi siano venuti meno. Infine, le sanzioni amministrative applicate dalle Autorità di vigilanza di settore – ivi comprese quelle pubblicate in forma anonima, nonché le informazioni ricevute dai soggetti interessati sulle azioni da essi avviate avverso i provvedimenti sanzionatori e sull'esito delle stesse – sono comunicate alle Autorità di vigilanza europee (ABE, AEAP e AESFEM) dall'Autorità di vigilanza di settore che ne è membro.

APPENDICE

Gli altri operatori

(a cura di L. Criscuolo)

Premessa (L. Criscuolo)

Una delle linee di fondo nella trentennale evoluzione della normativa antiriciclaggio è la progressiva estensione dei presidi al di fuori del tradizionale ambito bancario e finanziario. Sulla base di impulsi comunitari e di concrete esigenze del contesto nazionale gli obblighi di identificazione (e poi di adeguata verifica), di conservazione e di segnalazione delle operazioni sospette sono stati man mano applicati a nuove categorie di intermediari finanziari, a diverse figure di collaboratori esterni agli intermediari stessi, a operatori non finanziari che svolgono attività ritenute particolarmente suscettibili di utilizzo a fini di riciclaggio e a un'ampia galassia di professionisti impegnati nel settore legale e contabile.

Si è trattato di un processo lungo e farraginoso, che ha incontrato (e, in parte, ancora incontra) difficoltà e resistenze, sia per la scarsa consapevolezza dei rischi di coinvolgimento inconsapevole in ipotesi di riciclaggio da parte di tali soggetti, spesso più attenti ai costi indotti dal rispetto dei presidi, sia per i ritardi palesati dalle Autorità nella definizione di una cornice normativa adeguata alle variegate esigenze della vasta platea di destinatari e nella strutturazione di un sistema di controlli attento alla condivisione dei principi piuttosto che all'applicazione delle sanzioni per eventuali carenze.

In tale contesto sono di seguito velocemente illustrate le specificità regolamentari di alcune categorie di destinatari, partendo dal mondo finanziario per giungere ai professionisti e ad alcune categorie di operatori non finanziari.

1. Imprese e intermediari assicurativi (E. Gatti e D. Blanco)

Nel settore assicurativo la disciplina antiriciclaggio si applica alle imprese di assicurazioni e agli intermediari assicurativi operanti in uno dei rami vita di cui all'art. 2, comma 1 del Codice delle Assicurazioni Private (CAP). In particolare, il D.lgs. 231/2007⁹⁵⁴ include, nel novero dei soggetti obbligati, le imprese di assicurazione con sede legale in Italia, le succursali italiane di imprese con sede in un altro Stato membro dell'UE o in uno Stato terzo, le imprese aventi sede legale e amministrazione centrale in un altro Stato membro stabilite in Italia senza succursale, nonché gli intermediari assicurativi⁹⁵⁵.

Sulla base di quanto previsto dall'art. 7 del D.lgs., l'IVASS ha emanato il regolamento n. 44/2019 che riunisce in un unico testo i preesistenti regolamenti attuativi in tema, rispettivamente, di organizzazione, procedure e controlli (Reg.to ISVAP 41/2012) e di adeguata verifica della clientela (Reg.to IVASS 5/2014). La disciplina è stata completata con il Provvedimento n. 111/2021, che ha: a) aggiornato il Reg.to 44/2019, introducendo una specifica sezione dedicata⁹⁵⁶ ai criteri e alle metodologie per la valutazione dei rischi di riciclaggio da parte delle imprese; b) introdotto le disposizioni sulle procedure di mitigazione del rischio, individuando i requisiti dimensionali e organizzativi in base ai quali le sedi secondarie di imprese estere, gli intermediari assicurativi e le imprese e gli intermediari stabiliti senza succursale – di cui all'art. 3 comma 3 lett. u), del decreto - devono istituire dei presidi organizzativi minimi (funzione antiriciclaggio, funzione di revisione interna e Responsabile delle segnalazioni di operazioni sospette, a seconda dei casi).

⁹⁵⁴ Cfr. art. 3, comma. 2, lett. n), o), t) e u).

⁹⁵⁵ Agenti, broker, banche, intermediari finanziari, società di intermediazione mobiliare, Poste Italiane – Divisione servizi di bancoposta di cui agli artt. 109 comma 2, lett. a), b) e d) e 116 del CAP, indipendentemente dal regime – di stabilimento o di libera prestazione di servizi – con cui concretamente svolgono l'attività sul territorio della Repubblica Italiana.

⁹⁵⁶ Capo II, Sezione VI.

L'ambito di applicazione del Reg.to 44/2019 è stato ampliato dal provvedimento del 2021. Oltre alle sedi secondarie italiane di imprese e di intermediari assicurativi con sede all'estero⁹⁵⁷, le disposizioni si applicano ora anche ai seguenti soggetti: a) l'ultima società controllante italiana, anche nel caso in cui l'IVASS abbia deciso di non esercitare la vigilanza a livello del sottogruppo nazionale; b) le imprese di assicurazione aventi sede legale e amministrazione centrale in un altro Stato membro dell'UE o in un Paese dello SEE, che operano in Italia in regime di libera prestazione di servizi, limitatamente all'esercizio di autovalutazione dei rischi; c) le imprese e gli intermediari assicurativi con sede legale in un altro Stato membro dell'UE o in un Paese dello SEE, stabiliti senza succursale sul territorio della Repubblica italiana.

Con specifico riferimento alle imprese italiane e alle sedi secondarie in Italia di imprese con sede in Paesi terzi, il regolamento integra, per i profili relativi al rischio di riciclaggio, le norme sul sistema di governo societario contenute nel CAP e nelle relative disposizioni attuative. Ai destinatari, infatti, si richiede espressamente di tener conto della portata e della complessità del rischio di riciclaggio anche nella definizione del sistema di governo societario, dei controlli interni e dei flussi informativi. Per le sedi secondarie di imprese comunitarie, invece, è stato introdotto l'obbligo di documentare all'Autorità italiana le analoghe misure adottate dalla sede centrale per la gestione del rischio di riciclaggio delle sedi secondarie.

Con riguardo al ruolo degli organi sociali, le disposizioni chiariscono la ripartizione dei compiti tra organo amministrativo e alta direzione. Per l'organo amministrativo, è stato introdotto l'obbligo di definire una *policy* che individui, in modo specifico e motivato, le scelte rilevanti per l'adempimento nel concreto degli obblighi antiriciclaggio; sull'alta direzione, invece, grava l'obbligo di formalizzare in un documento analitico le scelte operative effettuate sui diversi profili rilevanti individuati dall'organo amministrativo.

Per rafforzare l'indipendenza della funzione antiriciclaggio, il regolamento ha poi previsto il riporto funzionale della stessa all'organo amministrativo e all'organo di controllo, favorendone l'interlocuzione con gli organi societari, nonché il possesso, da parte del responsabile, dei requisiti previsti dal CAP (art. 76) e dal Reg.to 38/2018⁹⁵⁸ per i titolari delle altre funzioni di controllo. Anche quando la funzione è esternalizzata, il titolare designato internamente deve essere in possesso di specifici requisiti individuati dalla citata *policy*, affinché sia in grado di valutare criticamente la prestazione svolta e i risultati raggiunti dal fornitore esterno. La possibilità di ricorrere all'esternalizzazione, anche all'interno del gruppo, è stata subordinata alla ridotta portata e complessità del rischio di riciclaggio e alla circostanza che l'istituzione di una funzione interna non risponda ai criteri di economicità, efficienza e affidabilità. Al riguardo, è precisato che l'esternalizzazione può riguardare anche le sole attività di acquisizione e conservazione di dati, informazioni e documenti, possibilità prima non esplicitata. È stato poi espressamente attribuito alla funzione antiriciclaggio, tra gli altri compiti, quello di curare l'istruttoria per l'esame delle segnalazioni di operazioni sospette (SOS) provenienti dal primo livello valutativo ovvero individuate autonomamente. Infine, è stato specificato che i rischi connessi all'esternalizzazione della funzione AML devono essere inclusi nella politica di gestione dei rischi adottata dall'impresa ai sensi del CAP e del Reg.to 38/2018.

Il Reg.to 44/2019 definisce le modalità di assolvimento degli obblighi di collaborazione attiva per talune categorie di intermediari assicurativi. In particolare, le disposizioni prevedono che i *broker* esteri, se operano in Italia in regime di stabilimento, inviano la SOS direttamente alla UIF qualora non sia possibile individuare un'impresa di riferimento⁹⁵⁹.

Gli intermediari assicurativi esteri stabiliti senza succursale, invece, inviano una segnalazione all'impresa di riferimento anche in relazione alle medesime operazioni già segnalate direttamente alla UIF e danno notizia alla stessa impresa dell'avvenuta SOS sullo stesso cliente, in linea con l'art. 39, comma 4 del decreto antiriciclaggio⁹⁶⁰. Al riguardo, le disposizioni precisano i criteri per individuare, fra le operazioni segnalate autonomamente alla UIF, quelle da segnalare anche all'impresa di riferimento. Le stesse modalità di segnalazione valgono anche per gli intermediari di cui all'art. 109, comma 2, lett. d), del CAP⁹⁶¹ e per quelli che svolgono attività analoga in regime di stabilimento.

Per i gruppi assicurativi, il regolamento aggiorna i contenuti delle precedenti disposizioni. In particolare, per garantire un approccio globale al rischio di riciclaggio, è stato rafforzato il ruolo di direzione, coordinamento e controllo della capogruppo. Innanzitutto, l'ultima società controllante italiana

⁹⁵⁷ Stato membro della UE, paese dello SEE o Stato terzo per le sole imprese assicurative.

⁹⁵⁸ Recante disposizioni in materia di sistema di governo societario.

⁹⁵⁹ Analogamente a quanto previsto dal decreto antiriciclaggio per i broker con sede in Italia (cfr. 36, comma 4).

⁹⁶⁰ In particolare, nei casi relativi allo stesso cliente o alla stessa operazione, che coinvolgono due o più soggetti obbligati, il divieto di comunicazione non impedisce la comunicazione tra i medesimi soggetti, in presenza di determinate condizioni.

⁹⁶¹ Banche, intermediari finanziari dell'elenco speciale di cui all'art. 106 e 114-*septies* del TUB, società di intermediazione mobiliare di cui all'art. 19 del TUF, Poste Italiane - Divisione servizi di bancoposta.

deve adottare una metodologia di gruppo per la valutazione del rischio di riciclaggio, nonché procedure di raccordo con le altre società del gruppo in materia di adeguata verifica e di SOS. Inoltre, con riguardo all'articolazione della procedura di segnalazione delle operazioni sospette all'interno del gruppo, il regolamento chiarisce che il modello "accentrato", basato sulla presenza di un delegato SOS di gruppo, trova applicazione alle sole controllate con sede in Italia di gruppi assicurativi italiani.

In merito agli obblighi di conservazione previsti per gli intermediari assicurativi, che in precedenza potevano essere affidati alle imprese produttrici, il regolamento stabilisce ora, in linea con il principio di proporzionalità, la generale possibilità di esternalizzare a soggetti terzi l'attività di conservazione di dati, informazioni e documenti, in presenza di determinati requisiti⁹⁶²; coerentemente, istituisce l'obbligo per le imprese di assumere il ruolo di *outsourcer* se richiesto dall'intermediario.

Con riferimento agli obblighi di adeguata verifica, le disposizioni introducono il principio della valutazione unitaria del rischio di riciclaggio associato ad un medesimo cliente. In particolare, i destinatari devono tener conto di tutti i contratti assicurativi, indipendentemente dal regime di distribuzione (regime di stabilimento oppure libera prestazione di servizi). Ad esempio, le imprese italiane applicano il principio di valutazione unitaria in relazione a clienti comuni con le altre società estere del gruppo che distribuiscono in Italia contratti assicurativi in LPS; le sedi secondarie italiane (di imprese con sede nello SEE) applicano la valutazione unitaria in relazione ai clienti che hanno sottoscritto contratti assicurativi con la sede secondaria e anche con la sede centrale in regime di libera prestazione.

La valutazione del rischio di un cliente dovrà considerare i fattori di rischio relativi al titolare effettivo dello stesso, al beneficiario nonché all'eventuale titolare effettivo di quest'ultimo. Le disposizioni confermano l'obbligo di identificare il titolare effettivo anche nei casi in cui il decreto non fornisce indicazioni (ad es.: società di persone; associazioni non riconosciute). Inoltre è stato precisato che l'obbligo di individuare il titolare effettivo riguarda anche il beneficiario della polizza (se diverso da persona fisica). Infine, il regolamento definisce una dettagliata procedura per lo svolgimento dell'adeguata verifica a distanza.

Con riferimento all'adeguata verifica semplificata, come noto, il decreto antiriciclaggio ha eliminato le ipotesi di basso rischio definite *ex ante*. Conseguentemente le imprese, sulla base dei fattori previsti dal medesimo decreto, definiscono nella propria *policy* specifici rapporti continuativi e operazioni a basso rischio, per i quali è possibile applicare misure semplificate. In tale quadro, le disposizioni attuative riguardano perlopiù la calibrazione dei controlli in corso di rapporto; nella fase di identificazione del cliente, le disposizioni consentono di differire l'effettiva acquisizione della copia del documento identificativo. In merito all'adeguata verifica rafforzata, il regolamento individua invece gli ulteriori fattori di rischio elevato - rispetto a quelli già definiti dalla normativa primaria - che i destinatari devono considerare; disciplina poi le diverse modalità di adempimento delle misure di AV rafforzata, anche in presenza di fattispecie particolari (es. PEP).

Il Reg.to 44/2019 definisce le modalità di conduzione dell'autovalutazione del rischio da parte delle imprese, tramite l'identificazione del rischio intrinseco, la misurazione dell'efficacia dei presidi di controllo e la stima del conseguente rischio residuo; sono previste semplificazioni per le imprese che commercializzano esclusivamente prodotti standardizzati a basso rischio e per le imprese stabilite senza succursale. Sono invece esclusi dall'obbligo di autovalutazione gli intermediari; fanno eccezione le banche iscritte quali intermediari ai sensi dell'art. 109, comma 2, lett. d), del CAP, che sono tenute a predisporre una apposita sezione per la distribuzione di prodotti assicurativi, nell'ambito del documento di autovalutazione richiesto dalle disposizioni attuative della Banca d'Italia.

È stato anche previsto, sempre per le imprese, l'invio annuale all'Ivass di un insieme strutturato di dati e informazioni di carattere qualitativo e quantitativo, riguardanti diversi ambiti, quali ad esempio l'autovalutazione ovvero la rete distributiva. Per le imprese con sede in un altro Stato membro dell'UE o in un Paese dello SEE, l'obbligo di trasmissione annuale riguarda invece solo l'attività svolta in Italia, nel ramo vita, in regime di libera prestazione dei servizi ed è limitato alle informazioni sugli intermediari.

Il Provvedimento 111/2021, oltre alle citate modifiche del Reg.to 44/2019, ha disciplinato le procedure di mitigazione del rischio previste dall'art. 16 del decreto antiriciclaggio, che si applicano alle sedi secondarie di imprese con sede legale in un altro Stato membro o in un Stato Terzo, agli intermediari assicurativi nonché alle imprese e gli intermediari stabiliti senza succursale. Quest'ultima categoria - non definita dal decreto antiriciclaggio - è individuata sulla base di parametri relativi alle modalità di distribuzione dei prodotti assicurativi e ai premi raccolti⁹⁶³.

⁹⁶² In particolare, l'esternalizzazione dovrà essere regolata da uno specifico accordo (cfr. art. 28 Reg.to 44/2019).

⁹⁶³ Per le imprese i requisiti, che devono valere congiuntamente, sono: a) operare sul territorio italiano in LPS nei rami vita; b) distribuire

In particolare, il provvedimento individua i casi in cui le citate sedi secondarie possono non istituire la funzione antiriciclaggio, attribuendone i compiti all'omologa funzione della sede centrale oppure a un rappresentante generale purché privo di deleghe che ne pregiudichino l'autonomia⁹⁶⁴.

Il Provvedimento definisce poi i requisiti dimensionali e organizzativi⁹⁶⁵ in base a cui gli agenti e i *broker*⁹⁶⁶ devono istituire presidi organizzativi in precedenza non previsti, quali la funzione antiriciclaggio e la funzione di revisione interna per le verifiche sul rispetto degli obblighi antiriciclaggio.

Alle imprese stabilite senza succursale il Provvedimento richiede l'istituzione del Responsabile delle SOS, tenuto a valutare e segnalare alla UIF le operazioni sospette in relazione alle polizze distribuite sul territorio italiano. Tale incarico può essere affidato anche al responsabile SOS di un'altra entità del gruppo oppure al responsabile SOS di un altro intermediario che opera in Italia per conto dell'impresa stabilita senza succursale⁹⁶⁷. Agli intermediari assicurativi stabiliti senza succursale, invece, è richiesto di trasmettere le segnalazioni di operazioni sospette al responsabile per le segnalazioni sospette dell'impresa di riferimento o, qualora quest'ultima non sia individuabile, direttamente alla UIF. Infine, il provvedimento individua quali disposizioni, tra quelle contenute nel capo II⁹⁶⁸ del Reg.to 44/2019, sono applicabili agli intermediari assicurativi, tenuto conto dei requisiti dimensionali e organizzativi degli stessi⁹⁶⁹.

2. Società fiduciarie (A. Cuzzocrea)

La legge 23 novembre 1939, n. 1966 definisce società fiduciarie “*quelle che, comunque denominate, si propongono, sotto forma di impresa, di assumere l'amministrazione dei beni per conto di terzi, l'organizzazione e la revisione contabile di aziende e la rappresentanza dei portatori di azioni e di obbligazioni*” (art. 1)⁹⁷⁰. Le operazioni di amministrazione di beni assumono forme svariate includendo, senza pretesa di esaustività, l'amministrazione di beni immobili e mobili (titoli, valori, polizze assicurative, partecipazioni societarie⁹⁷¹, patrimoni, crediti, finanziamenti, ecc.) per conto di terzi, con o senza l'intestazione fiduciaria degli stessi, e l'interposizione nell'esercizio dei diritti eventualmente ad essi connessi nonché la rappresentanza (dei diritti patrimoniali e personali) di azionisti e obbligazionisti⁹⁷².

L'attività fiduciaria riveste particolare interesse sotto il profilo antiriciclaggio in quanto consente, attraverso l'istituto del negozio fiduciario⁹⁷³, di realizzare una separazione tra la titolarità effettiva dei beni, che resta in capo al fiduciante, e l'amministrazione o gestione degli stessi, che viene trasferita alla società

sul territorio italiano prodotti assicurativi attraverso una rete di intermediari assicurativi previsti dal CAP; c) conseguire premi lordi contabilizzati (comunicati all'IVASS dalla sede centrale dell'impresa stessa) superiori a 5 milioni di euro. Per gli intermediari assicurativi stabiliti senza succursale, il requisito è la distribuzione sul territorio italiano di prodotti assicurativi in regime di LPS tramite intermediari assicurativi di cui all'art. 109, comma 2, lett. e), del CAP.

⁹⁶⁴ Cfr. art. 5, comma 1, del Provv.to n. 111/2021.

⁹⁶⁵ Cfr. art. 5, comma 2, del Provv.to n. 111/2021.

⁹⁶⁶ Con sede in Italia ovvero in altro Stato dell'UE o Paese dello SEE, che distribuiscono in Italia prodotto vita in regime di stabilimento.

⁹⁶⁷ Cfr. art. 7, comma 2 del Provv.to n. 111/2021.

⁹⁶⁸ Sezioni da I a IV.

⁹⁶⁹ Ad esempio, le norme relative ai compiti dell'organo amministrativo, dell'alta direzione, dell'organo di controllo (ove esistente) trovano applicazione con alcune semplificazioni.

⁹⁷⁰ La legge 1939/1966 (Disciplina delle società fiduciarie e di revisione) è stata attuata con il regolamento R.D. 22 aprile 1940, n. 531. Detta legge, insieme al DM Industria 16 gennaio 1995, rappresenta ancora oggi la cornice fondamentale della materia. Per una disamina delle fonti normative in materia di società fiduciarie v. M. Sepe, *Le società fiduciarie nel diritto dell'economia*, in *Rivista Trimestrale di Diritto Dell'economia*, Roma, n. 4/2016, pp. 338-360.

⁹⁷¹ Uno dei settori in cui si riscontra con maggiore frequenza il fenomeno dell'intestazione fiduciaria è quello societario. I motivi per cui si ricorre all'intestazione di pacchetti di quote o di azioni a società fiduciarie sono riconducibili, principalmente, alla riservatezza che viene garantita dall'intestazione fiduciaria nei confronti dei creditori, dei concorrenti e, persino, dei soci cui occultare l'esercizio di attività in concorrenza.

⁹⁷² Vi rientrano incarichi di custodia dei suddetti beni, amministrazione di piani azionari e stock option, trustee ai sensi dell'art. 7 della convenzione relativa alla legge sui trusts adottata a l'Aja il 1° luglio 1985, ratificata con Legge 16 ottobre 1989, n. 364, e altri servizi specialistici quali escrow agreement e patti di famiglia.

⁹⁷³ Il negozio fiduciario è un istituto di origini antiche, radicate nel diritto romano, caratterizzato dalla scissione tra proprietà e legittimazione all'esercizio di diritti su beni destinati a uno scopo definito e concordato tra le parti. L'istituto della c.d. fiducia romanistica prevede il trasferimento al fiduciario della proprietà dei beni conferiti dal fiduciante, svolgendo un effetto reale rilevante per i terzi, ma limitato nei rapporti interni dal pactum fiduciae, avente natura obbligatoria. Al contrario, la c.d. fiducia germanistica, tipica del diritto tedesco, non trasferisce la proprietà ma solo la legittimazione all'esercizio del diritto. Per una disamina storica dell'istituto fiduciario, cfr. G. Diurni, *Voce: Fiducia e negozio fiduciario (storia)*, in *Digesto, IV edizione*, a cura di Sacco, Torino, 2002.

fiduciaria. Pur in assenza di una tipizzazione legislativa del contratto fiduciario nell'ordinamento italiano⁹⁷⁴, tale istituto è ampiamente riconosciuto dalla dottrina e dalla giurisprudenza⁹⁷⁵, che ritengono allo stesso applicabili le disposizioni sul contratto di mandato. Viene richiamato, in particolare, lo schema del mandato senza rappresentanza, che legittima la società fiduciaria ad amministrare e gestire in nome proprio beni altrui, su istruzioni del fiduciante⁹⁷⁶.

Attualmente, la forma ed i contenuti del mandato fiduciario sono espressamente disciplinati dall'art. 5, comma 10, n. 1, del DM 16 gennaio 1995, in base al quale si applicano le disposizioni sul mandato di cui agli artt. da 1703 al 1730 del codice civile, con la possibilità per il fiduciante di modificare in ogni momento i poteri conferiti e di revocarli, nonché di impartire istruzioni per il relativo esercizio, con comunicazione scritta; il mandato fiduciario deve necessariamente prevedere, *inter alia*, l'elencazione dei singoli beni e diritti intestati, l'individuazione analitica dei poteri attribuiti alla società e l'indicazione delle aziende di credito presso le quali vengano depositate le somme e i valori mobiliari dei fiducianti⁹⁷⁷. Le singole operazioni debbono sempre essere precedute da apposite istruzioni conferite dal fiduciante, dal momento che la fiduciaria non ha alcuna facoltà di compiere, *sua sponte*, atti dispositivi del patrimonio fiduciario.

Per queste caratteristiche di separazione tra proprietà effettiva e potere gestorio, l'attività fiduciaria ha sempre formato oggetto di attenzione da parte delle Autorità e Istituzioni, anche internazionali, competenti in materia antiriciclaggio.

Il GAFI ha da tempo posto in luce il possibile utilizzo dei veicoli fiduciari per finalità di riciclaggio, raccomandando di rafforzare gli standard applicabili a tali istituti, specie con riferimento all'acquisizione e conservazione di informazioni complete e aggiornate sulla c.d. "*beneficial ownership*"⁹⁷⁸. La direttiva (UE) 2015/849 (quarta direttiva antiriciclaggio), come modificata dalla direttiva (UE) 2018/843 (quinta direttiva antiriciclaggio) contiene un espresso riferimento agli istituti fiduciari e detta nuove misure volte a conferire maggiore chiarezza e accessibilità alle informazioni sui titolari effettivi di società, enti e *trust*⁹⁷⁹.

Nell'ordinamento italiano, il decreto antiriciclaggio conferma tra i soggetti destinatari della normativa antiriciclaggio le società fiduciarie disciplinate dalla legge n. 1966/1939 che svolgono attività di custodia e amministrazione di valori mobiliari, distinguendo:

i) all'art. 3, comma 2, lett. s), le società fiduciarie iscritte nell'albo *ex* art. 106 del decreto legislativo 1° settembre 1993, n. 385 (TUB). Queste sono collocate fra gli "intermediari bancari e finanziari", essendo fiduciarie di grandi dimensioni, prevalentemente di emanazione bancaria o finanziaria, e sono sottoposte alla vigilanza della Banca d'Italia, al solo fine di assicurare il rispetto delle disposizioni antiriciclaggio. Prima della riforma introdotta dal D.lgs. 90/2017, la collocazione di tali società nell'art. 11, comma 1, del decreto antiriciclaggio le esonerava dall'obbligo di comunicare il titolare effettivo quando erano clienti di altri intermediari (c.d. fiduciarie di "primo livello");

ii) all'art. 3, comma 3, lett. a), le società fiduciarie non iscritte nel citato albo *ex* art. 106 TUB. Queste sono incluse tra gli "altri operatori finanziari" e sono soggette al Ministero dello Sviluppo economico

⁹⁷⁴ La legge 22 giugno 2016, n.112 ha introdotto disposizioni relative al contratto di affidamento fiduciario, istituto alternativo al trust con il quale la fiduciaria assume in amministrazione beni destinati in favore di persone con grave disabilità prive del sostegno familiare (funzione di "asset protection").

⁹⁷⁵ Cfr. per tutti, in dottrina, Santoro Passarelli, *Dottrine generali del diritto civile*, 2012, p. 179; Bianca, *Diritto Civile*, 3, *Il contratto*, 1992, p. 672 ss., Gazzoni, *Manuale di diritto privato*, 2013, p.919. In giurisprudenza, cfr. Cass. 28.05.1997, n. 10031, la quale ha precisato che le società fiduciarie non possono disporre, né utilizzare nel proprio interesse i beni loro affidati, e Cass. 27.08.2012, n. 12654 che ha individuato nel negozio fiduciario l'accordo tra due soggetti, con cui il primo trasferisce al secondo una situazione giuridica soggettiva per il conseguimento di uno scopo ulteriore.

⁹⁷⁶ Cfr. Cass. Sez. Unite, sentenza 27 aprile 2022, n. 13143, secondo cui "le attività tipiche prese in considerazione dalla l. n. 1966 del 1939, sono, in pratica, tutte sussumibili nel concetto di amministrazione di elementi patrimoniali altrui, mediante contratti che legittimano le società a operare in nome proprio sui capitali affidati secondo lo schema del mandato senza rappresentanza".

⁹⁷⁷ Ai sensi dell'art. 14, comma 4, del citato DM 16 gennaio 1995, la società deve depositare le disponibilità liquide dei fiducianti presso enti creditizi in conti rubricati come di amministrazione fiduciaria.

⁹⁷⁸ Cfr. in particolare Raccomandazione 25 sulla "Trasparenza e titolare effettivo di negozi giuridici di natura fiduciaria", in base alla quale "i Paesi devono adottare misure atte ad impedire l'utilizzo di negozi giuridici di natura fiduciaria per finalità di contrasto del riciclaggio di denaro e/o finanziamento del terrorismo".

⁹⁷⁹ Cfr. considerando 26 della direttiva UE 843/2018.

(MISE), che rientra tra le Amministrazioni interessate di cui all'art. 1, comma 2, lett. a), del decreto antiriciclaggio ed esercita la "sorveglianza"⁹⁸⁰ su tali società in base alla normativa di settore. Dette società erano collocate nel comma 2 dell'art. 11 del decreto *ante* novella e, pertanto, tenute alla *disclosure* del titolare effettivo nei rapporti con altri intermediari (c.d. fiduciarie di "secondo livello")⁹⁸¹.

Caratteristica peculiare delle società fiduciarie è che le stesse, di norma, operano in nome proprio per conto di terzi, senza svelare il nome del fiduciante, laddove non ostino specifici obblighi di legge. Il vincolo di segretezza che connota l'attività di amministrazione fiduciaria recede, ad esempio, di fronte agli obblighi di *Customer due diligence* imposti dalla normativa antiriciclaggio, che impongono di risalire, nella procedura di adeguata verifica del cliente, al "titolare effettivo"⁹⁸² delle transazioni.

Tutte le società fiduciarie, a prescindere dall'iscrizione o meno all'albo *ex* art. 106 TUB, sono tenute agli obblighi previsti dal decreto antiriciclaggio in materia di: procedure di mitigazione del rischio (art. 16), adeguata verifica della clientela (art. 17 e ss.)⁹⁸³, conservazione dei dati e delle informazioni (art. 31 e ss.), trasmissione dei dati aggregati (art. 33) e segnalazione di operazioni sospette (artt. 35 e 36), nonché comunicazione delle misure di congelamento in materia di contrasto al finanziamento del terrorismo (artt. 5 e 7 del D.lgs. 22 giugno 2007, n. 109).

Con riferimento agli obblighi di invio dei dati aggregati e di segnalazione di operazioni sospette si applicano altresì il provvedimento del 25 agosto 2020 e il provvedimento del 4 maggio 2011. A quest'ultimo riguardo, ai sensi dell'art. 6, comma 4, lett. e), del decreto antiriciclaggio la UIF, al fine di agevolare l'individuazione delle operazioni sospette, emana e aggiorna periodicamente, previa presentazione al Comitato di sicurezza finanziaria, indicatori di anomalia, pubblicati nella Gazzetta Ufficiale della Repubblica italiana e in apposita sezione del proprio sito istituzionale

Solamente alle fiduciarie iscritte, tuttavia, si applicano altresì le disposizioni secondarie emanate dalla Banca d'Italia in materia di organizzazione, procedure e controlli interni (provvedimento del 26 marzo 2019)⁹⁸⁴, adeguata verifica della clientela

⁹⁸⁰ I poteri di sorveglianza sono posti a presidio della tutela del mercato e degli investitori: l'omesso, o non puntuale, esercizio di tali poteri può dar luogo a responsabilità risarcitoria da fatto illecito in capo al Ministero dello Sviluppo economico. Si segnala, tra le molte, la decisione di Cass. Civ., sez. III, 27 marzo 2009, n. 7531 (con nota di C. Scognamiglio, *Responsabilità della P.A. per violazione di obblighi di vigilanza e di informazione sull'attività delle società fiduciarie*, in Nuova Giur. Civ. Comm., 2009, p. 1151), con cui la Suprema Corte ha sancito che "la disciplina normativa in materia di autorizzazione all'esercizio e controllo dell'attività delle società fiduciarie, interpretata alla luce degli artt. 41, 47 e 97 Cost. è posta anche a tutela degli interessi dei privati, che abbiano affidato i propri risparmi alla società fiduciaria". Si richiama anche Cass. Sez. Unite, sentenza 27 aprile 2022, n. 13143, cit.

⁹⁸¹ La distinzione tra fiduciarie "106" e "non 106" consente di ritenere superata la tradizionale bipartizione tra fiduciarie "statiche" e "dinamiche", che si basava sulle caratteristiche dell'attività svolta: l'amministrazione conservativa era tipica delle fiduciarie "statiche", prevalentemente di matrice professionale, disciplinate dalla legge n. 1966/1939, mentre l'attività di straordinaria amministrazione, finalizzata alla valorizzazione e all'incremento del patrimonio, caratterizzava le fiduciarie "dinamiche", già disciplinate dall'art. 60, comma 4, del D.lgs. 415 del 1996. In tema di società fiduciarie "statiche" si veda G. Artale, L. Criscuolo e P. Panico, *Le attività, i soggetti, i collaboratori esterni*, in E. Galanti (a cura di), *Diritto delle banche e degli intermediari finanziari*, Trattato di diritto dell'economia, Vol. V, Padova, 2008, pp. 324-327. I due corpi normativi relativi alle fiduciarie statiche e dinamiche erano richiamati dall'art. 199 del D.lgs. 58/1998 (TUF) che stabiliva, al comma 1, che "fino alla riforma organica della disciplina delle società fiduciarie e di revisione, conservano vigore le disposizioni previste dalla l. 23 novembre 1939, n. 1966, e dall'art. 60, comma 4, del D.lgs. 415 del 1996". L'auspicata revisione organica della disciplina delle società fiduciarie non è stata tuttavia compiutamente realizzata, in quanto ancora oggi manca un regime uniforme applicabile a tutte le fiduciarie. Infatti, a seguito delle modifiche apportate al citato art. 199 TUF dal comma 8 dell'art. 9 del D.lgs. 13 agosto 2010, n. 141 le società fiduciarie di cui alla L. 1966/1939, che sono controllate da una banca o da un intermediario finanziario o hanno adottato la forma di società per azioni ed hanno capitale versato di ammontare non inferiore al doppio di quello richiesto dall'art. 2327 c.c. (100.000 euro), sono autorizzate e iscritte, come detto, in una sezione separata del citato albo previsto dall'art. 106 TUB.

⁹⁸² I criteri di individuazione del titolare effettivo sono disciplinati all'art. 20 del decreto antiriciclaggio. Per una disamina in tema di individuazione della titolarità effettiva, cfr. G. Castaldi, *Antiriciclaggio. Individuazione della titolarità effettiva: un percorso a ostacoli*, in *Bancaria*, n. 2-2022.

⁹⁸³ Se poi solo alle fiduciarie iscritte nell'art. 106 TUB è consentito rilasciare l'attestazione utilizzabile da terzi per l'assolvimento dell'adeguata verifica, pur in assenza del cliente (cfr. art. 26 e ss. del decreto antiriciclaggio), va sottolineato che quando sono le fiduciarie a ricevere detta attestazione rilasciata da altro intermediario, ciò non le esime, a prescindere da quale categoria appartengano, dallo svolgere una propria valutazione del rischio di riciclaggio o di finanziamento del terrorismo, né le libera dalle responsabilità connesse agli obblighi di adeguata verifica.

⁹⁸⁴ La sezione III del provvedimento in materia di organizzazione, procedure e controlli interni richiama alcuni presidi per le società fiduciarie iscritte nella sezione separata dell'albo di cui all'art. 106 del TUB che sono, peraltro, già previsti dall'art. 13 del DM 16 gennaio 1995 applicabile a tutte le fiduciarie. Si fa in particolare riferimento all'attenzione che deve essere posta alle operazioni condotte e concluse autonomamente dal fiduciante, senza l'intervento o il preventivo assenso della società fiduciaria (c.d. operazioni "franco valuta"), anche nel caso in cui queste operazioni vengano perfezionate attraverso il sistema bancario. Le società, in sede di stipula del contratto fiduciario, concordano per iscritto con il cliente modalità atte a ottenere la tempestiva comunicazione di tali operazioni, nonché

e profilatura del rischio (provvedimento del 30 luglio 2019)⁹⁸⁵, conservazione dei dati e delle informazioni (provvedimento del 24 marzo 2020). Allo stato, invece, le fiduciarie non iscritte all'albo *ex art.* 106 TUB, non essendo sottoposte alla vigilanza della Banca d'Italia, non sono destinatarie delle disposizioni secondarie emanate dalla stessa.

Anche il regime dei controlli presenta delle diversità per le due categorie di fiduciarie. Infatti, solo le fiduciarie “106” possono essere sottoposte a controlli (e sanzioni⁹⁸⁶) da parte della Banca d'Italia⁹⁸⁷, fermo restando per tutte le fiduciarie il potere ispettivo del Nucleo speciale di polizia valutaria della Guardia di Finanza (d'intesa con la Banca d'Italia, per le “106”⁹⁸⁸) e della UIF⁹⁸⁹ con riferimento agli obblighi di segnalazione di operazioni sospette e agli altri obblighi di comunicazione di informazioni nelle materie di propria competenza.

Dalla sintetica ricognizione che precede emerge che la distinzione tra fiduciarie iscritte e non iscritte all'albo *ex art.* 106 TUB determina degli effetti meritevoli di essere approfonditi onde evitare distorsioni sul piano applicativo.

È di tutta evidenza che la disciplina secondaria dettata dalla Banca d'Italia per gli intermediari bancari e finanziari (incluse le fiduciarie “106”) è sostanzialmente applicabile, in via analogica, anche alle fiduciarie “non 106”. Per tale ragione, in assenza di un'Autorità di supervisione antiriciclaggio e di regole specifiche per le c.d. fiduciarie “MISE”, un ruolo di supplenza (peraltro non istituzionale) sembra essere svolto dall'Assofiduciaria, pur non essendo assimilabile a un “organismo di autoregolamentazione” di cui all'art. 11 del decreto antiriciclaggio. In tale ambito, ha elaborato per le fiduciarie “MISE” dei “codici di autodisciplina” contenenti regole analoghe a quelle dettate dall'Organo di vigilanza per le fiduciarie “106”; inoltre, ha promosso iniziative di *audit* volontaria che consentono a tutte le proprie associate di verificare in autonomia, attraverso appositi piani di *audit* messi in atto da consulenti terzi, il proprio livello di *compliance* agli obblighi antiriciclaggio⁹⁹⁰.

La neutralità sostanziale della differente qualificazione *ex lege* delle due tipologie di società fiduciarie si coglie maggiormente quando le fiduciarie sono clienti di altri soggetti obbligati (es. banche o professionisti). Venuto meno il regime di esenzione previsto dagli artt. 25 e ss. (obblighi semplificati) del decreto antiriciclaggio *ante* riforma, che esonerava le c.d. fiduciarie di primo livello dall'obbligo di comunicare il titolare effettivo, mentre lo imponeva alle fiduciarie “MISE”, nel quadro vigente tutte le fiduciarie sono tenute a comunicare a un altro soggetto destinatario degli obblighi antiriciclaggio il nominativo del titolare effettivo di un mandato fiduciario, quando le stesse fiduciarie aprono un rapporto continuativo in nome proprio e per conto del cliente/fiduciante.

In base al decreto, infatti, i soggetti obbligati possono adottare misure semplificate di adeguata verifica in presenza di un basso rischio di riciclaggio, ma non è più prevista una completa esenzione di alcune categorie di clienti od operazioni dagli obblighi di adeguata verifica. Anzi, nel caso in cui il cliente sia una “società partecipata da fiduciari”, ciò rappresenta un fattore di rischio elevato, secondo quanto previsto sia dal decreto antiriciclaggio che dalle relative disposizioni attuative⁹⁹¹. Tuttavia, ai sensi delle medesime disposizioni, per le società fiduciarie “106” la vigilanza della Banca d'Italia costituisce uno strumento di mitigazione del rischio, che può determinare l'applicazione di misure ordinarie di adeguata verifica.

misure idonee ad assicurarne la valutazione da parte delle società fiduciarie e la necessaria trasparenza informativa ai fini del rispetto della normativa antiriciclaggio.

⁹⁸⁵ La sezione II del provvedimento in materia di adeguata verifica della clientela, relativa ai criteri generali per la valutazione del rischio, indica alle società fiduciarie di cui all'art. 106 di tenere conto, ai fini della definizione del profilo di rischio del cliente, delle caratteristiche della società in cui acquisiscono fiduciariamente una partecipazione (es., la sede, il settore operativo, l'eventuale sottoposizione a procedure concorsuali). Idem, in caso di intestazione fiduciaria di polizze assicurative, rileva ogni informazione utile sui beneficiari delle stesse. È evidente che tali disposizioni sono sostanzialmente applicabili anche alle fiduciarie non “106”.

⁹⁸⁶ Ai sensi dell'art. 62 del D.lgs. 231/2007.

⁹⁸⁷ Ai sensi dell'art. 7, comma 2, del D.lgs. 231/2007.

⁹⁸⁸ Ai sensi dell'art. 9, comma 2, lett. c), del D.lgs. 231/2007.

⁹⁸⁹ Ai sensi dell'art. 6, comma 4, lett. f), e comma 5, lett. a), del D.lgs. 231/2007.

⁹⁹⁰ Cfr. <https://www.assofiduciaria.org/antiriciclaggionews>.

⁹⁹¹ Ai sensi dell'art. 24, comma 2, lett. a), n. 4 del D.lgs. 231/2007. Inoltre, l'allegato 2 al provvedimento della Banca d'Italia del 30 luglio 2019 richiama, tra i fattori di rischio alto, i trust, le società fiduciarie, le fondazioni e ulteriori soggetti giuridici che possono essere strutturati in maniera tale da beneficiare dell'anonimato e permettere rapporti con banche di comodo o con società aventi azionisti fiduciari, nonché le società che hanno emesso azioni al portatore o siano partecipate da fiduciari (c.d. *nominee shareholder*). Si richiama anche l'art. 42, comma 2, il quale prevede il divieto di instaurare il rapporto continuativo e porre fine al rapporto continuativo già in essere di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio o entità giuridiche aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo né verificare l'identità.

Un aspetto particolarmente delicato per tutte le società fiduciarie attiene agli obblighi di comunicazione del titolare effettivo al Registro delle imprese di cui all'art. 2188 del codice civile, delle persone giuridiche private, dei *trust* e degli istituti e soggetti giuridici affini⁹⁹², stabiliti o residenti sul territorio della Repubblica italiana, al quale possono accedere, fra gli altri, le Autorità competenti e i soggetti obbligati in base alla normativa antiriciclaggio. In tale contesto, in funzione dissuasiva e a tutela del principio di riservatezza, opportuna sarebbe stata la previsione di un'apposita norma sanzionatoria per eventuali abusi nella diffusione e utilizzo delle informazioni sulla titolarità effettiva di cui all'art. 21.

Al fine di tutelare la trasparenza delle entità giuridiche e degli istituti affini ai *trust* e considerata la varietà di tali istituti giuridici utilizzati nell'UE, l'art. 31, par. 10, della quarta direttiva antiriciclaggio stabilisce che gli Stati membri debbano individuare gli istituti giuridici che hanno un assetto o funzioni affini a quelli dei *trust* e notificare tali istituti alla Commissione, per la successiva pubblicazione in Gazzetta ufficiale europea. Con riferimento all'ordinamento italiano, sono stati notificati alla Commissione gli istituti del mandato fiduciario e del vincolo di destinazione⁹⁹³.

Una interpretazione ampia del mandato fiduciario, volta a includere in tale istituto qualunque negozio di amministrazione fiduciaria⁹⁹⁴, appare coerente con le finalità di trasparenza della titolarità effettiva perseguite dall'ordinamento antiriciclaggio, ma andrebbe attentamente valutata anche alla luce della disciplina adottata dagli altri paesi dell'Unione, onde evitare possibili effetti distorsivi della concorrenza tra i vari ordinamenti.

3. Revisori legali e società di revisione legale (C. Di Biase)

I revisori legali e le società di revisione legale sono soggetti obbligati appartenenti alla categoria dei professionisti⁹⁹⁵. In linea con le previsioni della disciplina generale della revisione legale⁹⁹⁶, il D.lgs. 231/2007 ha distinto i Revisori con incarichi di revisione legale su enti di interesse pubblico o su enti sottoposti a regime intermedio (di seguito "Revisori EIP") dai Revisori privi di tali incarichi, assoggettando i primi alla supervisione ai fini antiriciclaggio della Consob e i secondi a quella del MEI⁹⁹⁷.

Il rischio principale al quale i Revisori sono esposti nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo è quello di non valorizzare, nell'ambito del considerevole patrimonio informativo acquisito nello svolgimento degli incarichi professionali, elementi di potenziale anomalia o sospetto rilevanti ai fini della disciplina di settore.

In ragione delle caratteristiche dell'attività, che tipicamente si sostanzia nella revisione contabile, ma che può avere ad oggetto molteplici ulteriori incarichi (ad es. *due diligence*, pareri di congruità, consulenze ecc.), gli obblighi di adeguata verifica dei Revisori presentano significative peculiarità rispetto agli omologhi adempimenti applicabili agli altri destinatari della disciplina antiriciclaggio.

Sotto il profilo dell'ambito di applicazione, gli obblighi di adeguata verifica dei Revisori sono limitati agli incarichi professionali svolti per conto dei clienti, non risultando strutturalmente applicabile a detti soggetti obbligati il riferimento alle operazioni occasionali disposte dalla clientela che comportino trasmissione o movimentazione di mezzi di pagamento.

Inoltre, prima di eseguire le attività di identificazione del cliente, i Revisori devono porsi la questione preliminare di individuare chi sia il soggetto qualificabile come cliente in relazione allo specifico incarico professionale ricevuto, in quanto può non esservi coincidenza tra il soggetto che conferisce l'incarico e quello nei cui confronti deve essere svolta l'attività professionale del Revisore.

⁹⁹² Ai sensi dell'art. 22, comma 5-*bis*, si considerano istituti giuridici affini al *trust* gli enti e gli istituti che, per assetto e funzioni, determinano effetti giuridici (di separazione patrimoniale) equivalenti a quelli dei *trust* espressi, anche avuto riguardo alla destinazione dei beni ad uno scopo ed al controllo da parte di un soggetto diverso dal proprietario, nell'interesse di uno o più beneficiari o per il perseguimento di uno specifico fine.

⁹⁹³ Il vincolo di destinazione di cui all'art. 2645-*ter* c.c. determina un effetto di segregazione patrimoniale per tutto il tempo in cui i beni sono destinati e vincolati allo scopo meritevole di tutela.

⁹⁹⁴ Si pensi ad esempio all'attività di amministrazione fiduciaria svolta in funzione di asset protection, a tutela dei beni familiari o di situazioni di disabilità, ovvero a fini di escrow, in cui a nome della fiduciaria vengono costituiti in pegno o deposito valori a garanzia di operazioni finanziarie e non, in attesa del realizzarsi di condizioni di efficacia della transazione stipulata tra le parti.

⁹⁹⁵ Cfr. art. 3, comma 4, lett. d) ed e), del D.lgs. 231/2007.

⁹⁹⁶ Cfr. D.lgs. 39/2010.

⁹⁹⁷ Cfr. art. 1, comma 2, lett. a) e c), del D.lgs. 231/2007.

Al fine di orientare i Revisori EIP nell'individuazione del cliente in caso di dissociazione tra soggetto conferente l'incarico ed entità nei cui confronti devono essere svolte le verifiche, il regolamento Consob adottato con la Delibera 20570 del 4 settembre 2018 (di seguito anche "regolamento Consob") ha definito come "cliente" ai fini di detto regolamento il soggetto al quale i Revisori rendono una prestazione professionale in seguito al conferimento di un incarico, ovvero l'entità – persona fisica o giuridica – nel cui interesse è resa la prestazione⁹⁹⁸.

Ad esempio, in caso di incarichi conferiti dal collegio sindacale *ex art. 2403-bis c.c.*, la prestazione professionale è svolta nell'interesse della società che forma oggetto delle attività di controllo del Revisore e non anche dei componenti degli organi sociali conferenti⁹⁹⁹. Del pari, in caso di incarichi di *acquisition due diligence*, il cliente nel cui interesse viene eseguita la prestazione professionale sarà individuato nell'aspirante acquirente, mentre in caso di *vendor due diligence* il cliente sarà identificabile, a seconda dei casi, nella società in vendita o nei singoli azionisti che intendono cedere la propria partecipazione.

Occorre tuttavia evidenziare che, a prescindere dall'individuazione del soggetto cliente ai fini dell'adeguata verifica della clientela, permane l'obbligo dei Revisori di segnalare eventuali operazioni sospette relative al patrimonio informativo acquisito nell'ambito dello svolgimento dell'attività professionale.

Altro tratto caratteristico dell'adeguata verifica dei Revisori è individuabile nella circostanza che questi ultimi, contrariamente ad altri soggetti abilitati, non sono tenuti all'identificazione dell'"esecutore" (soggetto delegato ad *operare* in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di *operare* in nome e per conto del cliente). Tale esclusione è conseguente alla considerazione delle peculiarità dell'attività svolta dai Revisori, i quali danno attuazione all'incarico ricevuto dal cliente eseguendo l'attività professionale richiesta, rispetto alla quale non residua alcun margine per *operare* né al cliente né ad eventuali rappresentanti dello stesso¹⁰⁰⁰.

Un'ulteriore peculiarità degli adempimenti di adeguata verifica dei Revisori riguarda l'acquisizione delle informazioni sullo scopo e sulla natura della prestazione professionale oggetto dell'incarico, in quanto di norma tali informazioni risultano immediatamente desumibili dalla tipologia di incarico affidato e non richiedono pertanto lo svolgimento di particolari attività di verifica da parte del Revisore.

Meritano di essere segnalate le specificità del processo di *on-boarding* dei clienti dei Revisori - in particolare in caso di incarichi di revisione legale - ai fini delle previsioni della normativa primaria che disciplinano la tempistica degli obblighi di identificazione e verifica dell'identità del titolare effettivo. Infatti, tra la proposta di incarico professionale inviata dal Revisore all'entità giuridica potenziale cliente e l'eventuale accettazione da parte di quest'ultima (dopo l'avvenuta approvazione da parte dell'organo assembleare) può decorrere un lasso temporale non breve e di norma solo all'atto dell'accettazione, che segna il momento in cui il contratto professionale si perfeziona, il cliente fornisce le informazioni circa la titolarità effettiva.

Ciò considerato, e dato che ai sensi dell'art. 18, comma 2, del D.lgs. 231/2007 l'identificazione e la verifica dell'identità del titolare effettivo devono essere effettuate *prima* del conferimento dell'incarico per lo svolgimento di una prestazione professionale, tali adempimenti, già eseguiti in fase di emissione della proposta, dovranno essere ripetuti dal Revisore quando il cliente, unitamente all'accettazione della proposta d'incarico professionale, fornirà anche le informazioni relative all'identità del titolare effettivo. In tale fase infatti, soprattutto in caso di clienti con assetti partecipativi complessi, poco trasparenti, o con entità giuridiche estere, potrebbero essere individuati titolari effettivi che non erano noti al Revisore, o comunque differenti da quelli rilevati all'atto dell'emissione della proposta professionale.

Da tale circostanza consegue altresì che qualora le informazioni sulla titolarità effettiva ottenute all'atto del perfezionamento del contratto professionale introducano variazioni del *set* informativo disponibile al Revisore in fase di emissione della proposta, il Revisore dovrà effettuare ulteriori controlli ai fini della corretta determinazione del profilo di rischio del cliente (ad es. la verifica dello *status* di PEP o di eventuali notizie pregiudizievoli dei titolari effettivi indicati dal cliente)¹⁰⁰¹.

⁹⁹⁸ Cfr. art. 3, comma 2, lett. a), del regolamento Consob.

⁹⁹⁹ In virtù del principio di immedesimazione organica, il collegio sindacale agisce infatti nell'interesse della società oggetto delle operazioni di controllo.

¹⁰⁰⁰ Resta tuttavia fermo l'obbligo da parte del Revisore di verificare l'identità e l'effettiva esistenza del potere di rappresentanza di chi conferisce l'incarico in nome e per conto del cliente.

¹⁰⁰¹ Potrebbero infatti venire in rilievo fattori di rischio di riciclaggio o di finanziamento del terrorismo non noti all'atto dell'emissione della proposta (o anche, in ipotesi, comportamenti reticenti del cliente con riguardo alla titolarità effettiva), che devono essere rilevati e valutati dal Revisore al fine di determinare il profilo di rischio del cliente e declinare in ragione di tale rischio i controlli da adottare ai fini

Anche l'attività di controllo costante assume connotazione specifica per i Revisori. Avendo a riferimento gli incarichi di revisione contabile, il controllo costante si sostanzia soprattutto nello svolgimento delle verifiche e dei controlli previsti dai Principi di revisione e nell'esame dei dati e delle informazioni (contabili ed extracontabili) acquisiti nell'esecuzione della prestazione professionale, che devono essere analizzati anche nell'ottica di individuare elementi di anomalia o di sospetto di riciclaggio o di finanziamento del terrorismo.

Il livello di pervasività dell'attività di controllo costante deve essere modulato, come per gli altri soggetti obbligati, sulla base del livello di rischio attribuito al cliente e in tale contesto il regolamento Consob richiede ai Revisori EIP di prendere in considerazione anche gli elementi riscontrabili nello svolgimento dell'attività professionale, quali eventuali incompletezze, irregolarità o manipolazioni della documentazione contabile, ovvero il rifiuto o la riluttanza a concedere accesso alle registrazioni contabili¹⁰⁰².

Data la pluralità dei fattori di rischio della clientela che vengono in rilievo ai fini della profilatura del rischio, le medesime disposizioni di attuazione richiedono ai Revisori EIP, al fine di limitare la discrezionalità degli addetti e assicurare omogeneità nei comportamenti, di adottare sistemi di classificazione che si avvalgano, per quanto possibile, di procedure informatiche e di algoritmi predefiniti, in grado di assegnare in automatico la classe di rischio¹⁰⁰³.

Con riferimento ai Revisori EIP, il regolamento Consob prevede inoltre una disciplina specifica degli obblighi di adeguata verifica rafforzata da attuare nei confronti dei clienti ad elevato rischio. Nelle predette disposizioni di attuazione sono stati infatti individuati, in relazione alle attività svolte dai Revisori, i fattori di elevato rischio di riciclaggio e di finanziamento del terrorismo rilevanti ai fini dell'applicazione delle misure rafforzate, corredati, ove opportuno, da esempi esplicativi¹⁰⁰⁴.

In caso di clienti ad alto rischio, è stato altresì previsto l'obbligo del *partner* responsabile dell'incarico professionale di: a) comunicare tale circostanza al responsabile della funzione antiriciclaggio e, ove presente, alla funzione di *risk management* al fine di decidere se accettare/continuare l'incarico; b) stabilire, con il contributo del responsabile della funzione antiriciclaggio, le specifiche misure di rafforzata verifica da applicare al cliente, anche in base alla tipologia di attività professionale prestata; c) formalizzare le misure pianificate e conservare evidenza scritta dell'applicazione delle stesse e dei relativi esiti¹⁰⁰⁵.

Quanto all'oggetto, nel caso degli incarichi di revisione le verifiche rafforzate si sostanziano soprattutto nell'esecuzione di analisi e verifiche contabili più approfondite, estese e/o frequenti nel corso dello svolgimento della prestazione professionale, coerenti con i fattori di rischio del cliente e volte a rilevare eventuali elementi di sospetto di riciclaggio o di finanziamento del terrorismo.

In tale contesto, la previsione di obblighi di formalizzazione delle misure rafforzate programmate e attuate con riferimento ai singoli incarichi ad elevato rischio è funzionale all'esigenza di estendere strumenti di pianificazione e rendicontazione tipici dell'attività di revisione anche alle verifiche rafforzate da eseguire a fini di antiriciclaggio, con conseguente necessaria adozione di strumenti operativi (ad es. modulistica *ad hoc*, funzionalità informatiche, *form* esemplificativi) e disposizioni procedurali interne volte a declinare in concreto gli adempimenti dei *partner*.

In un apposito documento di pianificazione devono infatti essere formalizzate le misure contabili e non contabili programmate, specificando cadenza e orizzonte temporale delle verifiche e indicando chiaramente le voci di bilancio impattate dai fattori di rischio del cliente e le soglie di significatività e i criteri di campionamento conseguentemente adottati a livello di singola voce di bilancio e/o classe di operazioni. Detto documento deve altresì tenere traccia del coinvolgimento e del contributo della funzione antiriciclaggio alla pianificazione preventiva delle misure rafforzate e deve essere storicizzato e conservato nel fascicolo antiriciclaggio. Le misure rafforzate attuate e i relativi esiti devono poi essere formalizzati, per essere documentabili *ex post*, mediante evidenze dettagliate distinte dalle carte di lavoro relative allo svolgimento delle ordinarie procedure di revisione.

antiriciclaggio nello svolgimento della prestazione professionale.

¹⁰⁰² Cfr. art. 20, comma 3, del regolamento Consob.

¹⁰⁰³ Cfr. art. 21, comma 2, del regolamento Consob. Occorre in questa sede sottolineare che il rischio di riciclaggio e finanziamento del terrorismo del cliente deve essere definito dai Revisori EIP in modo del tutto autonomo rispetto al c.d. rischio generale "di revisione", ovvero dal rischio che il Revisore possa inconsapevolmente non tener conto, nell'espressione dell'opinione sul bilancio, di errori significativi o di frodi che ne inficiano la veridicità. Al riguardo si rinvia alle specifiche previsioni di cui all'art. 15, commi 2 e 3, del regolamento Consob.

¹⁰⁰⁴ Cfr. art. 31, comma 2, e Allegato 2 al regolamento Consob.

¹⁰⁰⁵ Cfr. art. 15, comma 3, e 31 del regolamento Consob.

Passando alle disposizioni in tema di conservazione in archivi informatizzati dei dati relativi ai clienti, il regolamento Consob ha previsto per i Revisori EIP, in ragione della già rilevata assenza di operazioni, solo l'obbligo di registrazione dei dati e delle informazioni sui rapporti continuativi originati dagli incarichi professionali ricevuti: data di instaurazione e di cessazione del rapporto, dati identificativi del cliente e del titolare effettivo, informazioni sullo scopo e la natura della prestazione professionale, settore di attività economica e profilo di rischio del cliente¹⁰⁰⁶. Le modalità di registrazione devono essere idonee a prevenire perdite dei dati e ad assicurare l'ordine cronologico delle registrazioni e la tracciabilità, in caso di rettifiche, delle scritture di modifica e delle registrazioni antecedenti alla modifica. Ciò al fine di disporre di un *database* affidabile di pronta consultazione circa i clienti (e i relativi titolari effettivi) per i quali è stata svolta l'attività professionale e in relazione ai quali, quindi, possono risultare evidenze rilevanti ai fini della prevenzione del riciclaggio e del finanziamento del terrorismo.

Infine, le peculiarità operative dei Revisori si manifestano anche sotto il profilo degli obblighi di segnalazione delle operazioni sospette. Un ruolo cruciale è infatti attribuito in tale ambito al *partner* responsabile dell'incarico di revisione, “*che partecipa al compimento della prestazione e al quale compete la gestione del rapporto con il cliente*” e che pertanto è individuato quale soggetto obbligato a segnalare al legale rappresentante o a un suo delegato (di seguito “responsabile SOS”) le operazioni potenzialmente sospette¹⁰⁰⁷.

Proprio in ragione della partecipazione all'esecuzione dell'attività professionale, il *partner* responsabile dell'incarico è innanzitutto responsabile di identificare, all'interno del patrimonio informativo acquisito nel corso di svolgimento della prestazione, eventuali elementi di anomalia di potenziale rilevanza ai fini dell'obbligo di segnalazione di operazioni sospette¹⁰⁰⁸.

Occorre in proposito sottolineare che la valenza per i Revisori di eventuali procedure automatizzate di *screening* automatico ai fini della *detection* di operazioni anomale non è paragonabile a quella che detti sistemi assumono per gli intermediari bancari e finanziari. Negli incarichi di revisione, infatti, l'identificazione di eventuali elementi di sospetto discende di norma dall'analisi di un complesso di informazioni acquisite progressivamente nel corso della prestazione professionale e sulle quali il *team* di lavoro conduce articolati approfondimenti in relazioni ai Principi di revisione. Gli elementi di anomalia o di sospetto possono essere connessi a rilievi di carattere contabile o anche a fatti e/o operazioni che non danno luogo a rilievi sotto il profilo contabile (ad es. operazioni straordinarie, cambi di *management*, rapporti di finanziamento infragruppo).

In tale contesto, l'estrema variabilità dei possibili scenari esaminati dai Revisori rende non facile stabilire soglie predefinite o *alert* standardizzati rispetto a possibili situazioni e schemi comportamentali anomali, a maggior ragione ove si consideri che di norma durante lo svolgimento dell'incarico il patrimonio informativo acquisito e le evidenze relative alle attività di verifica sono accessibili solo al *partner* e al *team* di lavoro¹⁰⁰⁹.

Per le stesse ragioni, è remota la possibilità per il responsabile SOS di venire a conoscenza di elementi di sospetto in assenza di segnalazioni dirette da parte dei *partner* responsabili degli incarichi.

Da ultimo, proprio con riguardo alla figura del responsabile SOS, merita menzione la circostanza che presso i Revisori, data la loro natura di professionisti, il ruolo di responsabile SOS può essere affidato a *partner* che sono anche responsabili dello svolgimento di incarichi professionali. Al fine di preservare l'autonomia di giudizio del responsabile SOS nella valutazione degli elementi di potenziale sospetto, il regolamento Consob richiede che le disposizioni procedurali interne dei Revisori EIP definiscano specifici presidi da adottare a tutela dell'indipendenza del responsabile SOS con

¹⁰⁰⁶ Cfr. art. 33 del regolamento Consob.

¹⁰⁰⁷ Cfr. art. 37, comma 3, del D.lgs. 231/2007.

¹⁰⁰⁸ Tale principio è stato espressamente previsto per i Revisori EIP dall'art. 15, comma 4. Al fine di agevolare l'adempimento degli obblighi di collaborazione attiva, la Banca d'Italia ha adottato con Delibera n. 61 del 30 gennaio 2013 il “Provvedimento recante gli indicatori di anomalia per le società di revisione e revisori legali con incarichi di revisione su enti di interesse pubblico”, contenente una serie di indicatori di anomalia specifici per i Revisori EIP.

¹⁰⁰⁹ Il coinvolgimento di una pluralità di soggetti che a vario titolo contribuiscono allo svolgimento dell'attività professionale rende peraltro necessaria l'adozione di stringenti procedure volte a garantire la necessaria formalizzazione e riservatezza dei processi funzionali alla segnalazione delle operazioni sospette.

riferimento alla clientela dallo stesso seguita¹⁰¹⁰. Detti presidi si pongono sullo stesso piano di quelli che, in base al medesimo regolamento Consob, devono essere definiti e adottati dai Revisori EIP per il caso che il responsabile della funzione antiriciclaggio svolga attività professionale diretta nei confronti di clienti¹⁰¹¹.

4. Collaboratori esterni, soggetti convenzionati e agenti (C. Oriolo)

Per “collaboratori esterni” deve intendersi una rete di soggetti, non equiparabili ai dipendenti o a coloro che sono stabilmente incardinati nell’organizzazione dell’intermediario, di cui quest’ultimo si avvale nell’esercizio della propria attività, in virtù di apposita convenzione, mandato o contratto, e che, a seconda della qualificazione giuridica, sono abilitati a eseguire compiti meramente esecutivi ovvero a promuovere e concludere contratti in nome e per conto dell’intermediario stesso¹⁰¹².

La disciplina antiriciclaggio annovera tra i soggetti tenuti all’adempimento degli obblighi AML anche alcune categorie di collaboratori esterni degli intermediari bancari e finanziari. In particolare, rientrano tra i *soggetti obbligati* gli agenti assicurativi e i broker¹⁰¹³, i consulenti finanziari e le società di consulenza finanziaria¹⁰¹⁴, i mediatori creditizi¹⁰¹⁵ e gli agenti in attività finanziaria¹⁰¹⁶. Sono ritenuti soggetti obbligati anche le succursali insediate nel territorio italiano di mediatori o agenti in attività finanziaria, aventi sede legale e amministrazione centrale in uno Stato estero¹⁰¹⁷.

Le suddette categorie di collaboratori esterni sono tenute all’adempimento di tutti gli obblighi AML. In tema di adeguata verifica della clientela, il decreto AML prevede che nella prestazione di servizi di pagamento e nell’emissione e distribuzione di moneta elettronica effettuate tramite agenti in attività finanziaria, l’intermediario di riferimento è tenuto ad osservare gli obblighi di adeguata verifica della clientela anche per le operazioni occasionali di importo inferiore a 15.000 euro¹⁰¹⁸. Per i clienti il cui contatto è avvenuto attraverso l’intervento di mediatori creditizi o agenti in attività finanziaria, l’intermediario può procedere all’identificazione acquisendo da tali soggetti obbligati le informazioni necessarie, anche senza la presenza contestuale del cliente¹⁰¹⁹.

Con riferimento alla collaborazione attiva, gli agenti assicurativi, i broker e gli agenti in attività finanziaria adempiono all’obbligo di segnalazione trasmettendola al titolare della competente funzione, legale rappresentante o altro soggetto all’uopo delegato dell’intermediario mandante o di riferimento. I mediatori creditizi e i broker, qualora non sia individuabile un intermediario di riferimento, inviano la segnalazione direttamente alla UIF¹⁰²⁰.

¹⁰¹⁰ Cfr. art. 14, comma 7, del regolamento Consob.

¹⁰¹¹ Cfr. art. 10, comma 8, del regolamento Consob.

¹⁰¹² Mentre le banche sono in grado di operare anche tramite propri dipendenti grazie all’articolazione delle proprie succursali, per gli istituti di moneta elettronica e gli istituti di pagamento, caratterizzati in genere da strutture aziendali particolarmente leggere, il ricorso all’utilizzo di collaboratori esterni costituisce un *modus operandi* pressoché obbligato. Cfr. G. Castaldi, *Servizi di pagamento e moneta elettronica: la disciplina antiriciclaggio dei collaboratori esterni*, in Riv. Trim. Dir. Econ., 2019, pp. 180 ss.

¹⁰¹³ Gli agenti assicurativi operano in nome o per conto di imprese assicurative, mentre i broker agiscono su incarico del cliente e senza poteri di rappresentanza. Il riferimento è agli intermediari assicurativi di cui all’art. 109, comma 2, lett. a) e b), del CAP, che operano nei rami vita.

¹⁰¹⁴ I consulenti finanziari e le società di consulenza finanziaria sono abilitati a prestare consulenza in materia di investimenti, relativamente a valori mobiliari e a quote di organismi di investimento collettivo, senza detenere fondi o titoli appartenenti ai clienti. Caratteristica essenziale di tali tipologie di consulenti è la loro indipendenza (cfr. artt. 18-*bis* e 18-*ter* del TUF); i consulenti sono iscritti nell’albo tenuto dall’Organismo dei Consulenti Finanziari (OCF), il quale espleta la propria attività sotto la vigilanza della Consob.

¹⁰¹⁵ Il mediatore creditizio è il soggetto che “*mette in relazione, anche attraverso attività di consulenza, banche o intermediari finanziari con la potenziale clientela per la concessione di finanziamenti sotto qualsiasi forma*” e “*svolge la propria attività senza essere legato ad alcuna delle parti da rapporti che ne possano compromettere l’indipendenza*” (cfr. art. 128-sexies del TUB). Per i mediatori creditizi è prevista l’adozione della forma giuridica di società di capitali, al fine di garantire un’organizzazione più complessa e strutturata sotto il profilo dei controlli.

¹⁰¹⁶ L’agente in attività finanziaria è il soggetto “*che promuove e conclude contratti relativi alla concessione di finanziamenti sotto qualsiasi forma o alla prestazione di servizi di pagamento, su mandato diretto di intermediari finanziari, istituti di pagamento o istituti di moneta elettronica*” (Cfr. art. 128-quater, commi 2 e 6, del TUB.).

¹⁰¹⁷ Cfr. art. 3, comma 7, del D.lgs. 231/2007.

¹⁰¹⁸ Cfr. art. 17, comma 6, del D.lgs. 231/2007.

¹⁰¹⁹ Cfr. art. 27, comma 4, del D.lgs. 231/2007.

¹⁰²⁰ Cfr. art. 36, commi 3 e 4, del D.lgs. 231/2007.

Per effetto delle nuove regole in materia di “passaporto europeo”, in vigore dal 1° febbraio 2022¹⁰²¹, gli agenti in attività finanziaria e i mediatori creditizi italiani possono operare su tutto il territorio dell’Unione, in regime di libera prestazione di servizi (LPS) o con succursale, con riferimento ai contratti di credito immobiliare ai consumatori¹⁰²², previa comunicazione all’OAM, che a sua volta informerà l’Autorità competente dell’altro Stato membro. Dall’altro lato, gli agenti e i mediatori abilitati in un altro Stato membro possono svolgere le stesse attività nel territorio della Repubblica dopo che l’Autorità competente dello Stato membro di origine ne abbia dato comunicazione all’OAM¹⁰²³. I soggetti autorizzati in altro Stato membro per i quali viene fornita tale comunicazione sono iscritti in un apposito elenco tenuto dall’OAM, operativo dal 1° febbraio 2022.

Con riferimento alla disciplina antiriciclaggio, al momento, la normativa primaria non prevede nulla in relazione ai mediatori creditizi e agli agenti in attività finanziaria comunitari abilitati ad operare in Italia in regime di libera prestazione dei servizi. Sembra, pertanto, riproporsi una problematica analoga con quanto emerso in passato in relazione all’attività svolta da prestatori di servizi di pagamento (IP) e istituti emittenti moneta elettronica (IMEL) comunitari in LPS ovvero attraverso forme di insediamento diverso dalla succursale.

Il decreto AML richiama ulteriori categorie di collaboratori esterni che, a differenza di quelle descritte in precedenza, non sono incluse nel novero dei soggetti obbligati di cui all’art. 3 del D.lgs. 231/2007. In particolare, si tratta di *collaboratori del soggetto obbligato* che possono procedere alla sola identificazione del cliente e del titolare effettivo, in presenza del medesimo cliente ovvero dell’esecutore, acquisendo i dati identificativi forniti dal cliente e copia in formato cartaceo o elettronico di un documento d’identità in corso di validità o altro documento di riconoscimento equipollente¹⁰²⁴ ovvero di *collaboratori esterni legati all’intermediario da apposita convenzione* che, allo stesso modo, possono effettuare la sola identificazione della clientela per conto dell’intermediario di riferimento, qualora operino in nome e per conto di quest’ultimo nel proporre alla clientela la sottoscrizione di contratti, riconducibili alla loro attività istituzionale, relativi al credito al consumo ovvero al leasing, al factoring, al microcredito, al credito agrario e peschereccio¹⁰²⁵.

Un’altra tipologia di collaboratori esterni non inclusa tra i soggetti obbligati di cui all’art. 3 del D.lgs. 231/2007 è quella dei soggetti convenzionati e agenti di cui all’art. 1, comma 2, lett. nn), del D.lgs. 231/2007, introdotta dal D.lgs. 90 del 2017¹⁰²⁶. Si tratta degli operatori diversi dagli agenti in attività finanziaria di cui IP e IMEL italiani e comunitari¹⁰²⁷ si avvalgono per l’esercizio della propria attività sul territorio italiano. Gli intermediari comunitari stabiliti in Italia senza succursale, che si avvalgono di soggetti convenzionati e agenti, sono tenuti a designare un punto di contatto centrale attraverso cui adempiere agli obblighi antiriciclaggio¹⁰²⁸.

¹⁰²¹ L’art. 23 della Legge europea 2019-2020 (L. 23 dicembre 2021, n. 238), nel completare l’attuazione della direttiva 2014/17/UE sui contratti di credito ai consumatori relativi a beni immobili - recepitamente parzialmente nel nostro ordinamento con il D.lgs. 72 del 2016 che ha inserito il Capo I-bis nel TUB, dedicato al credito immobiliare ai consumatori - integra nella normativa nazionale le regole in materia di “passaporto europeo” per gli agenti in attività finanziaria e i mediatori creditizi.

¹⁰²² Per consumatore si intende “la persona fisica che agisce per scopi estranei all’attività imprenditoriale, commerciale, artigianale o professionale eventualmente svolta”. Per contratto di credito si intende “un contratto di credito con cui un finanziatore concede o si impegna a concedere a un consumatore un credito sotto forma di dilazione di pagamento, di prestito o di altra facilitazione finanziaria, quando il credito è garantito da un’ipoteca sul diritto di proprietà o su altro diritto reale avente a oggetto beni immobili residenziali o è finalizzato all’acquisto o alla conservazione del diritto di proprietà su un terreno o su un immobile edificato o progettato”. Cfr. art. 120-*quinquies*, comma 1, lett. b) e c), del TUB, inserito dal D.lgs. 72 del 2016.

¹⁰²³ Al medesimo Organismo sono attribuiti poteri atti a verificare il rispetto delle disposizioni applicabili agli agenti in attività finanziaria e ai mediatori creditizi che svolgono la loro attività in Italia, anche senza succursali, da esercitare nelle forme e modalità stabilite con decreto del MEF, sentita la Banca d’Italia.

¹⁰²⁴ Cfr. art. 19, comma 1, lett. a), del D.lgs. 231/2007.

¹⁰²⁵ Cfr. art. 27, comma 5, del D.lgs. 231/2007 e le Disposizioni di vigilanza in tema di adeguata verifica della clientela.

¹⁰²⁶ Il medesimo decreto del 2017 ha introdotto all’art. 128-*quater* del TUB i commi 7 e 7-bis, dando atto dell’esistenza di questa nuova tipologia di collaboratori esterni anche nel TUB.

¹⁰²⁷ La prestazione di servizi di pagamento è riservata alle banche, agli IMEL e agli IP (cfr. art. 114-*sexies*, comma 1, del TUB). L’emissione di moneta elettronica è riservata alle banche e agli IMEL (cfr. art. 114-bis, comma 1, del TUB). Le banche e gli IMEL possono avvalersi di soggetti convenzionati che agiscano in loro nome per la distribuzione e il rimborso della moneta elettronica (art. 114-bis, comma 1, del TUB).

¹⁰²⁸ Cfr. art. 43, comma 3, del D.lgs. 231/2007. La mancata istituzione del punto di contatto è sanzionata ai sensi dell’art. 62, comma 1 del D.lgs. 231/2007. I prestatori di servizi di pagamento e gli IMEL comunitari sono tenuti a comunicare all’OAM gli estremi identificativi del punto di contatto per il tramite del quale operano sul territorio nazionale. Quest’ultimo, a sua volta, è tenuto a comunicare

Al riguardo, occorre precisare che il D.lgs. 231/2007 aveva ricompreso gli agenti di pagamento comunitari operanti in Italia tra i destinatari degli obblighi già per effetto del D.lgs. 141/2010¹⁰²⁹. Peraltro, il secondo correttivo al citato decreto del 2010, in merito alle modalità di adempimento di tali obblighi e sulla scorta degli orientamenti maturati a livello europeo, aveva già previsto l'istituzione di un punto di contatto da parte di IP e IMEL comunitari operanti in Italia attraverso una pluralità di agenti¹⁰³⁰. Ciò al fine di superare i rischi di arbitraggi normativi e comportamenti elusivi nonché di rimediare alla frammentazione della rete distributiva dell'operatore estero, accentrando presso il punto di contatto la trasmissione alla UIF di tutte le segnalazioni di operazioni sospette rilevate dagli agenti in Italia¹⁰³¹. La trasmissione delle segnalazioni alla sola FIU del paese d'origine - in conformità del criterio di territorialità previsto dalla terza direttiva antiriciclaggio - ancorché l'operazione fosse posta in essere all'estero in regime di LPS, non consentiva alla FIU del paese nel quale l'attività potenzialmente illecita veniva posta in essere di ricevere le informazioni necessarie per attivare tempestivamente i propri approfondimenti¹⁰³².

Pertanto, la quarta direttiva AML, in linea con quanto già previsto dalla normativa nazionale, che, tra l'altro, detta una disciplina più stringente rispetto a quella comunitaria, (i) ha ampliato l'elenco dei soggetti obbligati, includendo gli intermediari europei non insediati sul territorio nazionale, operanti in Italia per il tramite di reti di agenti e soggetti convenzionati, al fine di contenere i rischi di infiltrazione criminale nel settore dei money transfer e di comparti che adottano modelli simili per la distribuzione di prodotti e servizi; (ii) nel caso degli IP e degli IMEL che operano in LPS attraverso una rete di agenti ha previsto l'istituzione di un "punto di contatto" per l'applicazione degli obblighi antiriciclaggio e per l'effettuazione di segnalazioni di operazioni sospette nei confronti della FIU del paese ospitante. Il punto di contatto centrale rappresenta, pertanto, l'intermediario in Italia ed è l'interlocutore unico delle Autorità¹⁰³³.

Per i soggetti convenzionati e agenti, al pari degli altri collaboratori esterni non inclusi tra i soggetti obbligati *ex art.* 3 del D.lgs. 231/2007, rimane ferma la responsabilità dell'intermediario di riferimento o succursale o punto di contatto centrale nell'assolvimento degli obblighi AML.

Il decreto antiriciclaggio detta una disciplina specifica per i soggetti convenzionati e agenti¹⁰³⁴. In particolare, nell'adempimento degli obblighi di adeguata verifica della clientela, i soggetti convenzionati e agenti acquisiscono i dati identificativi del cliente, dell'esecutore e del titolare effettivo e li comunicano, entro 20 giorni dall'effettuazione dell'operazione, all'intermediario di riferimento ovvero al punto di contatto centrale, ferma restando la responsabilità di questi ultimi nell'assolvimento del relativo obbligo. In caso di operazioni occasionali attinenti al servizio di rimessa di denaro¹⁰³⁵, la comunicazione è inviata

all'Organismo l'avvio della propria operatività e ogni variazione ad essa attinente. L'omessa comunicazione è sanzionata ai sensi dell'art. 61, comma 2, del D.lgs. 231/2007. L'art. 43, comma 4, ha attribuito alla Banca d'Italia il potere di adottare disposizioni su requisiti, procedure, sistemi di controllo e funzioni del punto di contatto centrale. Tali disposizioni sono confluite nel Provvedimento della Banca d'Italia in tema di organizzazione, procedure e controlli interni, il quale prevede tra l'altro che l'intermediario che opera in Italia anche attraverso una succursale designa quest'ultima come punto di contatto centrale in relazione all'attività da esso svolta sul territorio nazionale per il tramite di soggetti convenzionati e agenti (cfr. in particolare la Parte VI del richiamato Provvedimento).

¹⁰²⁹ L'art. 11, comma 3, lett. d), del D.lgs. 231/2007, come modificato dal D.lgs. 141/2010, includeva tra i destinatari degli obblighi AML gli agenti indicati nell'art. 128-*quater*, commi 6 (ossia gli agenti che prestano esclusivamente i servizi di pagamento) e 7 del TUB (ossia gli agenti che prestano servizi di pagamento per conto di IMEL o IP comunitari).

¹⁰³⁰ L'art. 42, comma 3, del D.lgs. 231/2007, come modificato dal D.lgs. 141/2010, prevedeva che "la segnalazione è inviata alla UIF dagli agenti di cui all'art. 128-*quater*, comma 7, del TUB direttamente ovvero per il tramite del punto di contatto centrale, insediato in Italia dall'istituto di moneta elettronica o istituto di pagamento comunitario. La costituzione del punto di contatto è obbligatoria in caso di pluralità di agenti".

¹⁰³¹ Cfr. Rapporto annuale della UIF per il 2012, p. 17. In particolare, per effetto delle Direttive 2007/64/CE (Payment Services Directive, c.d. PSD) e 2009/110/CE (c.d. direttiva IMEL 2), nel mercato italiano hanno iniziato ad operare, accanto agli IP nazionali, gli IP comunitari, tramite insediamento di succursali, avvalendosi di agenti o in regime di LPS. In tale quadro, molti soggetti che in passato operavano in Italia come intermediari finanziari per conto dei circuiti internazionali di money transfer si sono trasformati in IP comunitari, costituiti in base alla normativa vigente nello stato estero di stabilimento. Tali istituti, pertanto, operavano in Italia attraverso agenti censiti dalle Autorità del paese d'origine o in regime di LPS. Al riguardo, il GAFI aveva raccomandato che nei servizi di pagamento concernenti il trasferimento di fondi la segnalazione di operazioni sospette doveva essere trasmessa sia alla FIU del paese dell'ordinante che del beneficiario. Inoltre, la Corte di Giustizia dell'Unione europea ha riconosciuto, nella Decisione C-212/11 del 25 aprile 2013 sul caso "Jyske Bank", la legittimità di disposizioni nazionali che rendevano obbligatoria la segnalazione diretta alla FIU locale di operazioni sospette realizzate da intermediari stabiliti all'estero. Cfr. Rapporto annuale della UIF per il 2014, p. 89.

¹⁰³² Cfr. Rapporto annuale della UIF per il 2013, p. 40.

¹⁰³³ Cfr. Rapporto annuale della UIF per il 2017, p. 17.

¹⁰³⁴ Cfr. Capo V del Titolo II (artt. 43, 44 e 45).

¹⁰³⁵ L'attività prestata dai soggetti convenzionati e agenti nel servizio di rimessa di denaro è considerata ad alto rischio AML rilevante ai fini dell'applicazione delle misure di adeguata verifica rafforzata (cfr. allegato 2 delle Disposizioni di vigilanza in tema di adeguata verifica della clientela).

prima della relativa esecuzione, quale che sia l'importo dell'operazione. I soggetti convenzionati e agenti conservano, per un periodo di 12 mesi, i dati acquisiti¹⁰³⁶.

Gli intermediari di riferimento o punto di contatto centrale sono tenuti ad adottare procedure e sistemi di controllo idonei a mitigare e gestire i rischi di riciclaggio e finanziamento del terrorismo cui sono esposti i soggetti convenzionati e agenti¹⁰³⁷.

Inoltre, è stato istituito presso l'OAM il Registro dei soggetti convenzionati e agenti. Il Ministero dell'Economia e delle finanze, con decreto, ha stabilito le modalità tecniche di alimentazione e consultazione del registro e della relativa sottosezione ad accesso riservato, ai sensi dell'art. 45, comma 3, del decreto antiriciclaggio¹⁰³⁸.

Ogni sei mesi i prestatori di servizi di pagamento, gli IMEL e le rispettive succursali, direttamente ovvero per il tramite del punto di contatto centrale, devono comunicare all'OAM i dati relativi ai soggetti convenzionati e agenti di cui si avvalgono per l'annotazione nell'apposito registro. È prevista anche un'apposita sottosezione contenente l'avvenuta cessazione del rapporto di convenzionamento o del mandato per motivi non commerciali, comunicata dall'intermediario di riferimento o succursale o punto di contatto centrale, entro 30 giorni dall'estinzione del rapporto¹⁰³⁹.

L'art. 61 del decreto antiriciclaggio detta una disciplina sanzionatoria specifica per le eventuali violazioni degli obblighi previsti per i soggetti convenzionati e agenti¹⁰⁴⁰.

Con riferimento alla collaborazione attiva, i soggetti convenzionati e agenti sono tenuti a comunicare all'intermediario di riferimento ovvero al punto di contatto centrale ogni circostanza e informazione rilevante, ai fini della valutazione, in ordine all'inoltro di una segnalazione di operazione sospetta¹⁰⁴¹, con le modalità e nel rispetto dei tempi previsti nell'atto di convenzionamento o nel mandato.

Come già detto per gli agenti in attività finanziaria, l'intermediario di riferimento, qualora nella prestazione di servizi di pagamento e nell'emissione e distribuzione di moneta elettronica si avvalga di soggetti convenzionati e agenti, è tenuto ad osservare gli obblighi di adeguata verifica della clientela anche per le operazioni occasionali di importo inferiore a 15.000 euro.

Le Disposizioni di vigilanza del 26 marzo 2019 in tema di organizzazione, procedure e controlli interni prevedono che per i servizi offerti attraverso reti di agenti in attività finanziaria, consulenti finanziari, soggetti convenzionati e agenti o altri soggetti legati all'intermediario da vincoli contrattuali, quest'ultimo adotta le precauzioni necessarie ad assicurare il rispetto delle disposizioni in materia di contrasto al riciclaggio da parte della rete distributiva¹⁰⁴².

Si richiama infine l'attenzione sui *"Punti operativi abilitati all'incasso ai sensi dell'art. 12, comma 2, del D.lgs. 141/2010"* menzionati, insieme agli agenti e ai soggetti convenzionati, nelle *"Disposizioni di vigilanza*

¹⁰³⁶ Cfr. art. 44, comma 1, lett. a) e b), del D.lgs. 231/2007. Le modalità di conservazione devono essere indicate espressamente nell'atto di convenzionamento o nel mandato e devono essere tali da garantirne l'accessibilità completa e tempestiva da parte delle autorità competenti, nonché l'integrità e la non alterabilità, successivamente alla loro acquisizione.

¹⁰³⁷ L'intermediario di riferimento o punto di contatto centrale dovrà (i) individuare standard e pratiche di riferimento in materia di gestione del rischio AML/CFT, adeguata verifica della clientela, conservazione e segnalazione di operazioni sospette - verificandone la corretta osservanza - nonché i requisiti reputazionali che gli stessi devono possedere e mantenere nel corso del rapporto di convenzionamento o del mandato, estinguendolo in caso di infrazioni o del venir meno dei requisiti; (ii) predisporre programmi di formazione idonei ad orientare i soggetti convenzionati e gli agenti nel riconoscimento di operatività potenzialmente anomale.

¹⁰³⁸ Il decreto ministeriale è stato pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 208 del 6.9.2022.

¹⁰³⁹ L'accesso alla sottosezione è consentito alla Guardia di Finanza, Banca d'Italia e UIF per l'esercizio delle rispettive competenze in materia di vigilanza e di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo e ai prestatori dei servizi di pagamento, IMEL, succursali e i punti di contatto centrale, al fine di valutare la reputazione e legalità dei soggetti operanti in questo specifico settore di mercato. La mancata comunicazione all'OAM dei dati relativi ai soggetti convenzionati e agenti o dell'avvenuta estinzione del rapporto comporta l'applicazione della sanzione pecuniaria di 4.500 euro, triplicata in caso di violazioni gravi, ripetute o sistematiche ovvero plurime. Per la contestazione della violazione, l'irrogazione e riscossione della relativa sanzione, è competente il medesimo Organismo. Cfr. art. 61, comma 2, del D.lgs. 231/2007.

¹⁰⁴⁰ In particolare, la Guardia di Finanza esercita il controllo sull'osservanza degli obblighi previsti dal decreto AML da parte dei soggetti convenzionati e degli agenti. La competenza sanzionatoria spetta al MEF; il decreto che irroga la sanzione è comunicato all'OAM per l'annotazione nella sottosezione del registro.

¹⁰⁴¹ Il responsabile del punto di contatto centrale è anche responsabile delle segnalazioni di operazioni sospette (cfr. art. 36, commi 5 e 6, e art. 44, comma 1, lett. c), del D.lgs. 231/2007).

¹⁰⁴² In particolare, l'intermediario indica regole di condotta a fini AML nell'ambito dei contratti di collaborazione, monitorandone il rispetto, fornisce strumenti e procedure per l'esecuzione delle operazioni e dei relativi adempimenti AML, appronta programmi di formazione, effettua verifiche periodiche presso i punti operativi, interviene a supporto della rete distributiva nell'adempimento degli obblighi di verifica rafforzata della clientela.

per gli istituti di pagamento e gli istituti di moneta elettronica” del 23 luglio 2019, tra i collaboratori di cui gli intermediari autorizzati alla prestazione di servizi di pagamento possono avvalersi per l’incasso materiale di fondi senza esercizio di alcun potere dispositivo¹⁰⁴³. Al riguardo, sembrerebbe che l’ambito di operatività della categoria in questione, pur esentata dagli adempimenti antiriciclaggio, non coincida con le ipotesi di esenzione dagli obblighi antiriciclaggio previste dall’art. 44, comma 3, del D.lgs. 231/2007¹⁰⁴⁴.

5. Professionisti (S. Pace)

Il D.lgs. 20 febbraio 2004, n. 56, di recepimento della seconda direttiva antiriciclaggio, ha ampliato il novero dei destinatari degli obblighi antiriciclaggio, includendovi anche i professionisti, indipendentemente dalla forma giuridica mediante la quale essi svolgono la propria attività (professionista individuale, studio associato ovvero società di professionisti).

L’estensione degli obblighi di collaborazione è stata giustificata dalla necessità di prevedere una più incisiva azione di contrasto che coinvolgesse anche soggetti che, pur non svolgendo propriamente attività di tipo finanziario, potessero ugualmente essere esposti, consapevolmente o meno, a rischi di infiltrazione e/o favoreggiamento della criminalità economica. Il progressivo e crescente livello di collaborazione attiva è essenziale per la circostanza che tali segnalanti godono di una visuale sull’operatività dei loro clienti diversa da quella degli intermediari finanziari, in grado di far emergere anomalie spesso complementari alle movimentazioni di denaro.

Le categorie di professionisti obbligati sono elencate nell’art. 3, comma 4, del D.lgs. 231/2007 che, con riferimento ai notai e agli avvocati delinea un ambito di applicazione della normativa antiriciclaggio più limitato. In particolare, tali soggetti sono destinatari degli obblighi solo quando realizzano in prima persona “qualsiasi operazione finanziaria o immobiliare” (atti di rappresentanza) ovvero quando “assistono” i clienti nella predisposizione o nella realizzazione di alcune operazioni determinate *ex ante* (atti di assistenza)¹⁰⁴⁵.

I professionisti devono adempiere agli obblighi di adeguata verifica della clientela sia in occasione dell’instaurazione di un rapporto continuativo o del conferimento dell’incarico per l’esecuzione di una prestazione professionale, sia in occasione dell’esecuzione di un’operazione occasionale, disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che venga posta in essere un’unica operazione o che vengano effettuate più operazioni, che appaiono collegate per realizzare un’operazione frazionata¹⁰⁴⁶.

¹⁰⁴³ L’art. 12 del decreto - nel dettare disposizioni attuative dell’art. 128-*quater* del TUB - prevede, al comma 2, che “Per l’esercizio dell’attività di incasso di fondi su incarico di soggetti autorizzati alla prestazione di servizi di pagamento non è necessaria l’iscrizione nell’elenco degli agenti in attività finanziaria, a condizione che detta attività sia svolta sulla base di un contratto di esternalizzazione, che ne predetermini le modalità di svolgimento, abbia carattere meramente materiale e in nessun caso sia accompagnata da poteri discretivi”.

¹⁰⁴⁴ La disposizione richiamata elenca alcune fattispecie ritenute prive di rischio (pagamenti di “tributi o sanzioni in favore di pubbliche amministrazioni” o “la fruizione di beni e servizi di pubblica utilità” nonché il “servizio di pagamento di bollettini prestampati e trattati automaticamente, senza possibilità di alterazioni manuali”) per le quali i soggetti incaricati sono esentati dagli adempimenti antiriciclaggio. La categoria di collaboratori prevista dall’art. 12, invece, sembra riguardare l’adempimento di mere attività esecutive, senza poteri di rappresentanza per la stipulazione dei contratti. In questa fattispecie potrebbero ricondursi le ipotesi di stipulazione a distanza di accordi contrattuali effettuata, ad esempio, con l’ausilio di programmi informatici e terminali che, sia pure azionati dal collaboratore, annullano la distanza fisica, impegnando direttamente gli intermediari che prestano servizi di pagamento o emettono moneta elettronica. Cfr. G. Castaldi, *Servizi di pagamento e moneta elettronica: la disciplina antiriciclaggio dei collaboratori esterni*, cit.

¹⁰⁴⁵ L’elenco delle diverse tipologie di operazioni è molto ampio e consente di includere una molteplicità di transazioni, soprattutto in materia di trasferimento di beni immobili e di attività economiche (trasferimento a qualsiasi titolo di diritti reali su beni immobili o attività economiche; gestione di denaro, strumenti finanziari o altri beni; apertura o gestione di conti bancari, libretti di deposito e conti di titoli; organizzazione degli apporti necessari alla costituzione, alla gestione o all’amministrazione di società; costituzione, gestione o amministrazione di società, enti, trust o soggetti giuridici analoghi).

¹⁰⁴⁶ Cfr. art. 17 del D.lgs. 231/2007.

Gli obblighi di adeguata verifica sono esclusi per le attività di mera redazione e trasmissione, ovvero di sola trasmissione delle dichiarazioni derivanti da obblighi fiscali¹⁰⁴⁷ e dagli adempimenti in materia di amministrazione del personale di cui all'art. 2, comma 1, della legge 11 gennaio 1979, n. 12¹⁰⁴⁸.

I professionisti devono eseguire l'identificazione e la verifica dell'identità del cliente, dell'esecutore e del titolare effettivo, contestualmente al conferimento dell'incarico. In presenza di un basso rischio, la verifica dell'identità può essere effettuata anche in un momento successivo, se necessario ai fini della gestione ordinaria delle attività oggetto del rapporto¹⁰⁴⁹.

Fermi gli obblighi di identificazione e solo fino al momento del conferimento dell'incarico, i professionisti sono esonerati dall'obbligo di verifica dell'identità del cliente e del titolare effettivo limitatamente ai casi di esame della posizione giuridica del loro cliente o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'Autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di negoziazione assistita da uno o più avvocati ai sensi di legge.

Nell'adempimento dell'obbligo di adeguata verifica il professionista deve inoltre acquisire e valutare le informazioni sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale ed eseguire un controllo costante del rapporto con il cliente, attraverso l'analisi delle operazioni effettuate e delle attività svolte o individuate durante il rapporto, in modo da verificare che esse siano coerenti con la conoscenza che ha del cliente e del suo profilo di rischio, anche riguardo, se necessario, all'origine dei fondi¹⁰⁵⁰. Il completamento della verifica deve avvenire al più presto e comunque entro trenta giorni dall'instaurazione del rapporto o dal conferimento dell'incarico¹⁰⁵¹.

L'art. 42, comma 2, del D.lgs. 231/2007 impone, inoltre, di non dare inizio o proseguire e di porre fine alla prestazione professionale nel caso in cui siano parte, direttamente o indirettamente, società fiduciarie, *trust*, società anonime o controllate attraverso azioni al portatore con sede in Paesi terzi ad alto rischio. L'obbligo sussiste anche nei confronti di entità giuridiche ulteriori aventi sede in tali paesi, nel caso in cui non sia possibile identificarne il titolare effettivo né verificarne l'identità. L'obbligo non opera tuttavia nei casi in cui l'attività svolta abbia ad oggetto l'esame della posizione giuridica del cliente, ovvero l'espletamento dei compiti di difesa o rappresentanza del cliente in un procedimento giudiziario o in relazione a tale procedimento, compresa la consulenza sull'eventualità di intentarlo o evitarlo o nelle ipotesi in cui l'operazione debba essere necessariamente eseguita in quanto sussiste un obbligo di legge di ricevere l'atto (ad es. notai). In tali ipotesi, dopo aver ricevuto l'atto, il professionista è comunque tenuto ad informarne subito la UIF.

Una delle principali novità del riformato D.lgs. 231/2007 è stata l'abolizione dell'obbligo di istituzione dei registri, tanto cartacei quanto elettronici, nei quali i professionisti dovevano registrare,

¹⁰⁴⁷ Ad es. dichiarazioni redditi, IVA, successione, ecc., registrazione di contratti, redazione/invio di Mod. F23 e F24, redazione/invio di fatture elettroniche per conto dei clienti e adempimenti simili o connessi.

¹⁰⁴⁸ La norma primaria non contempla ulteriori ipotesi di esonero dalla adeguata verifica ma le regole tecniche del CNN e del CNDCEC individuano una serie di prestazioni a rischio di riciclaggio e di finanziamento al terrorismo "non significativo" per le quali sono previste delle regole di condotta semplificate.

¹⁰⁴⁹ Ai sensi dell'art. 22, comma 1, del D.lgs. 231/2007 "i clienti forniscono per iscritto, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire ai soggetti obbligati di adempiere agli obblighi di adeguata verifica". Tale disposizione può assumere particolare rilevanza laddove, ad esempio, si riscontrino delle criticità nella corretta individuazione e identificazione del titolare effettivo.

¹⁰⁵⁰ Sulla base dei risultati del controllo, il professionista potrà: mantenere il livello di controllo costante del cliente; aggiornare il fascicolo (cartaceo/informatico) del cliente con acquisizione di ulteriore documentazione; modificare il profilo di rischio e la periodicità del controllo; modificare il tipo di obbligo di adeguata verifica attribuito al cliente (semplificato, rafforzato, ordinario). Al riguardo, il CNN ha proposto di istituire un archivio informatico centralizzato ("datawarehouse") contenente i dati del Notariato, pertinenti allo svolgimento delle attività di analisi e valutazione del rischio in materia di antiriciclaggio e all'adempimento dei correlati obblighi in ambito notarile (dati repertoriali e/o copie di atti). Con tale strumento informatico centralizzato, ispirato ad analoga esperienza spagnola, si vorrebbe garantire una maggiore uniformità di comportamenti nell'ambito della categoria notarile e rafforzare i rapporti di collaborazione con le competenti Autorità antiriciclaggio.

¹⁰⁵¹ I dati e le informazioni utili sono acquisiti man mano che viene istruita la prestazione professionale ed è questo il motivo per cui è espressamente previsto, quale momento finale per completare l'acquisizione, il termine di trenta giorni dall'ultimazione della prestazione. In tal senso si esprime la regola tecnica n. 8 approvata dal CNN che, sulla base delle caratteristiche tipologiche della prestazione notarile e tenuto conto che l'incarico non sempre è conferito da tutte le parti dell'atto congiuntamente e nello stesso momento, conclude che è considerata tempestiva l'acquisizione dei dati e delle informazioni relativi all'adeguata verifica del cliente nei trenta giorni dall'esecuzione della prestazione professionale ovvero dalla chiusura del rapporto continuativo o della prestazione professionale.

entro trenta giorni dall'accettazione dell'incarico professionale, dall'eventuale conoscenza di ulteriori informazioni rispetto a quelle precedentemente fornite ovvero dal termine della prestazione professionale, i dati identificativi del cliente e gli ulteriori elementi necessari per rispettare la normativa antiriciclaggio. Negli artt. 31 e 32 del D.lgs. 231/2007 non si fa quindi più riferimento a obblighi di "registrazione" bensì di "conservazione" dei documenti, dei dati e delle informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o finanziamento al terrorismo. Per tutti i clienti dello studio, i professionisti devono pertanto creare, all'atto del conferimento dell'incarico, il fascicolo antiriciclaggio, all'interno del quale conservare copia dei documenti acquisiti in occasione dell'adeguata verifica della clientela e l'originale ovvero copia avente efficacia probatoria ai sensi della normativa vigente, delle scritture e registrazioni inerenti le operazioni¹⁰⁵².

La documentazione conservata deve permettere, quanto meno, di ricostruire univocamente: la data di instaurazione del rapporto continuativo o del conferimento dell'incarico; i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione; la consultazione, ove effettuata, dei registri di cui all'art. 21 del D.lgs. 231/2007 (sezioni speciali del Registro Imprese); la data, l'importo e la causale dell'operazione; i mezzi di pagamento utilizzati. I documenti, i dati e le informazioni acquisiti devono essere conservati per un periodo di dieci anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale¹⁰⁵³.

L'art. 34, comma 2, del D.lgs. 231/2007 detta una norma specifica per i notai, stabilendo che il fascicolo del cliente, conforme a quanto prescritto agli artt. 31 e 32 del decreto, e la custodia dei documenti, delle attestazioni e degli atti presso il notaio, nonché la tenuta dei repertori notarili costituiscono idonea modalità di conservazione¹⁰⁵⁴.

In presenza di elementi di sospetto, i professionisti sono obbligati a inviare senza ritardo alla UIF una segnalazione di operazione sospetta. Fino al momento in cui non hanno adempiuto a tale obbligo, non compiono l'operazione, salvi i casi in cui la medesima debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto (es. notai) ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In queste ipotesi, dopo aver ricevuto l'atto o eseguito l'operazione, ne informano immediatamente la UIF.

Per valutare la sussistenza di un'operazione sospetta, i professionisti si avvalgono degli indicatori di anomalia¹⁰⁵⁵. In particolare, si distinguono indicatori connessi al cliente, alle modalità di esecuzione delle prestazioni professionali, alle modalità di pagamento dell'operazione, alla costituzione e alla amministrazione di imprese, società, *trust* ed enti analoghi, a operazioni aventi a oggetto beni immobili o mobili registrati e a operazioni contabili e finanziarie.

Ulteriore strumento di supporto, nella rilevazione di operazioni sospette, è rappresentato dagli schemi rappresentativi di comportamenti anomali sul piano economico e finanziario elaborati e diffusi dalla UIF, avvalendosi delle informazioni raccolte nello svolgimento delle proprie attività. Tra gli schemi finora pubblicati, rilevano soprattutto quelli relativi a operatività connessa con illeciti fiscali¹⁰⁵⁶, con l'anomalo utilizzo di *trust*, con il rischio di frodi nell'attività di *factoring*, con le frodi nell'attività di *leasing*, con l'abuso di finanziamenti pubblici e con operatività riconducibili all'usura e imprese in crisi.

L'art. 35, comma 5, del D.lgs. 231/2007 prevede che *"l'obbligo di segnalazione di operazioni sospette non si applica ai professionisti in relazione alle informazioni che essi ricevono da un loro cliente o ottengono riguardo allo stesso, nel corso dell'esame della posizione giuridica o dell'espletamento dei compiti di difesa o di rappresentanza del medesimo in un procedimento innanzi a un'autorità giudiziaria o in relazione a tale procedimento, anche tramite una convenzione di*

¹⁰⁵² Ad esempio, il fascicolo del cliente contiene: copia dei documenti identificativi; visura camerale; documentazione acquisita per l'individuazione del titolare effettivo; dichiarazione del cliente; scheda di valutazione del rischio; copia del mandato professionale; ogni altro documento o annotazione che il professionista ritenga opportuno conservare ai fini della normativa antiriciclaggio.

¹⁰⁵³ Le modalità di conservazione dei dati e delle informazioni devono essere conformi ai principi elencati nell'art. 32 del D.lgs. 231/2007 (accessibilità completa e tempestiva da parte delle autorità; tempestiva acquisizione, da parte del soggetto obbligato, con indicazione della relativa data; integrità e non alterabilità; trasparenza, completezza e chiarezza; mantenimento della storicità).

¹⁰⁵⁴ Per le attività che non sono annotate nel repertorio, quali ad esempio le attività di mera consulenza o l'attività svolta per l'esecuzione di un incarico che viene poi revocato, occorre conservare il fascicolo del cliente.

¹⁰⁵⁵ Al momento, quelli emanati, su proposta della UIF, con decreto del Ministro della Giustizia del 16 aprile 2010, sentiti gli ordini professionali, dopo essere stati sottoposti al Comitato di sicurezza finanziaria.

¹⁰⁵⁶ In particolare, lo schema sulla cessione di crediti fiscali fittizi e altri indebiti utilizzi (Schema D) si riferisce prevalentemente all'attività dei professionisti.

negoziiazione assistita da uno o più avvocati ai sensi di legge, compresa la consulenza sull'eventualità di intentarlo o evitarlo, ove tali informazioni siano ricevute o ottenute prima, durante o dopo il procedimento stesso".

La norma disciplina una specifica esimente dall'obbligo segnaletico ("legal privilege"), finalizzata alla tutela del diritto di difesa e del giusto processo¹⁰⁵⁷. L'ambito di applicazione di tale esenzione ha generato numerose criticità applicative, in particolare per gli avvocati, con riguardo soprattutto ai temi del segreto professionale e del dovere di lealtà nei confronti del cliente¹⁰⁵⁸.

Mentre la seconda parte della disposizione riferisce chiaramente l'esonero a tutte quelle informazioni apprese dal professionista nell'ambito del rapporto prodromico ovvero direttamente attinente al patrocinio, non altrettanto chiara risulta la prima parte ("esame della posizione giuridica del cliente") che, in quanto ambito distinto, non concerne il contenzioso né la fase che precede immediatamente qualsivoglia procedimento giudiziario. L'espressione adottata dal legislatore ha, infatti, dato luogo a dubbi sulla esatta portata della esenzione e, in particolare, sul se l'attività di consulenza debba ritenersi esente comunque dagli obblighi di segnalazione ovvero solo se e in quanto connessa con un procedimento giudiziario.

Ne sono derivati più orientamenti tesi a differenziare, ai fini dell'esenzione, la consulenza legale (o consulenza "statica") che implicherebbe l'esame della posizione giuridica del cliente, dalla consulenza d'affari *tout court* (o consulenza "dinamica") sottoposta all'obbligo di segnalazione: ne conseguirebbe una distinzione tra professionista "togato" (che svolge attività giudiziale e di assistenza in materia di contenzioso legale) e professionista "consulente" (es. avvocato di affari che presta una consulenza priva di alcuna connessione diretta con profili di rischio di causa e di assistenza continuativa nell'ambito di operazioni complesse e di transazioni talvolta fondamentali per l'attività commerciale del cliente).

Con riferimento all'obbligo di segnalazione di operazioni sospette, la sfera della professionalità legale potrebbe quindi essere suddivisa in tre distinte aree: 1) una zona sensibile che riguarda l'aiuto giuridico negli affari (operazioni immobiliari, finanziarie e societarie) che non hanno alcuna prospettiva giudiziaria (consulenza "dinamica" per la quale sussiste l'obbligo di segnalazione); 2) una sfera corrispondente a tutta l'area della prestazione che abbia come riferimento funzionale la prospettiva di un giudizio, anche se solo per evitarlo (attività contenziosa e pre-contenziosa per la quale opera la predetta esenzione); 3) un'altra area che non è attività di difesa, ma nemmeno attività di affari (di cui non condivide la natura di operazione), e consiste nell'esame della posizione statica del cliente (consulenza "statica", consulenza e assistenza stragiudiziale): in questa ipotesi intermedia sarebbe necessario verificare, ai fini dell'obbligo segnaletico, se la valutazione effettuata dal professionista ha lo scopo principale di realizzare un'operazione commerciale o finanziaria subordinata alle istruzioni del cliente (in tal caso il professionista è equiparabile a un agente di affari che svolge sostanzialmente un'attività non giuridica ed è obbligato a segnalare).

A parte la complessità di tali distinzioni, il Legislatore sembra comunque specificare che l'esenzione debba riguardare informazioni che *"siano ricevute o ottenute prima, durante e dopo il procedimento stesso"*. Attenendosi a un'interpretazione letterale si può quindi affermare che tale esenzione si applichi per quelle informazioni ricevute nel corso dell'esame della posizione giuridica del cliente, ma con utilizzo comunque collegato con l'attività tipicamente giudiziale: ciò proprio perché si è inteso separare tale attività rispetto a quella della consulenza d'affari, per la quale vige sia l'obbligo di adeguata verifica che di segnalazione.

Ulteriore ipotesi di esonero dall'obbligo segnaletico riguarda la "procedura di negoziazione assistita da un avvocato"¹⁰⁵⁹. Fermi restando gli obblighi di adeguata verifica, il Legislatore ha ritenuto prevalente, anche in tal caso, la tutela del segreto professionale qualora le informazioni per le quali c'è un obbligo di segnalazione vengano fornite all'avvocato dal proprio cliente.

¹⁰⁵⁷ Cfr. considerando n. 9 della direttiva UE 2015/849 (quarta direttiva antiriciclaggio) per cui i professionisti legali sono soggetti alla normativa antiriciclaggio "quando partecipano ad operazioni di natura finanziaria o societaria, ivi incluso quando prestano consulenza tributaria, settore in cui l'attività dei professionisti corre un elevato rischio di essere utilizzata impropriamente per operazioni di riciclaggio di proventi di attività criminose o operazioni di finanziamento del terrorismo. Tuttavia, dovrebbe sussistere l'esenzione da qualsiasi obbligo di comunicare le informazioni ottenute prima, durante o dopo procedimenti giudiziari o nel corso dell'esame della posizione giuridica di un cliente. Di conseguenza, la consulenza legale dovrebbe rimanere soggetta al vincolo del segreto professionale tranne qualora il professionista legale partecipi alle attività di riciclaggio o di finanziamento del terrorismo, la consulenza sia fornita a scopo di riciclaggio o di finanziamento del terrorismo ovvero il professionista legale sia a conoscenza del fatto che il cliente richiede la consulenza a scopo di riciclaggio o di finanziamento del terrorismo".

¹⁰⁵⁸ Ai sensi dell'art. 35, comma 4, del D.lgs. 231/2007, le segnalazioni inoltrate ai sensi e per gli effetti della legge non costituiscono violazioni del segreto professionale e se poste in essere in buona fede e per le finalità ivi previste non comportano responsabilità di alcun tipo.

¹⁰⁵⁹ Ipotesi introdotta a seguito della modifica apportata al D.lgs. 231/2007 dall'art. 10 del DL 132/2014 conv. nella L. 162/2014. Si tratta di un accordo mediante il quale le parti convengono di cooperare in buona fede e con lealtà per risolvere in via amichevole la controversia (purché questa non abbia ad oggetto diritti indisponibili), tramite l'assistenza di avvocati. Tale procedura si distingue da quella di mediazione, in quanto non è previsto il ricorso ad un soggetto terzo al fine di dirimere la lite insorta tra le parti.

Ai fini della più rigorosa tutela della riservatezza del segnalante, il D.lgs. 231/2007 prevede che le segnalazioni dei professionisti, oltre ad essere trasmesse direttamente all'UIF, possano, in alternativa, essere indirizzate agli organismi di autoregolamentazione per il successivo inoltro alla UIF, secondo le specifiche e con le modalità e garanzie di tutela della riservatezza dell'identità del segnalante, individuate con apposito decreto del MEF, di concerto con il Ministro della Giustizia e sentito il Garante per la protezione dei dati personali¹⁰⁶⁰.

Con Decreti MEF del 27 febbraio 2009 e del 4 maggio 2012 sono stati individuati, come organismi di categoria autorizzati a ricevere le segnalazioni di operazioni sospette dai propri iscritti, dapprima, il Consiglio Nazionale del Notariato (CNN) e il Consiglio Nazionale dell'Ordine dei Consulenti del Lavoro (CNOCDL) e, successivamente, il Consiglio Nazionale dell'Ordine dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC). Con protocolli d'intesa tra l'Unità di informazione finanziaria (UIF) e i predetti organismi sono state individuate specifiche modalità di trasmissione delle informazioni relative alle segnalazioni di operazione sospette tra gli stessi soggetti¹⁰⁶¹.

L'organismo di autoregolamentazione riceve dal professionista iscritto la segnalazione di operazione sospetta¹⁰⁶² e provvede, senza ritardo, a trasmetterla in via telematica, nel testo integrale alla UIF priva del nominativo del segnalante¹⁰⁶³.

La trasmissione delle segnalazioni, le richieste di approfondimenti e gli scambi di informazioni tra la UIF, gli Organi investigativi, le Autorità di vigilanza e gli organismi di autoregolamentazione, avvengono per via telematica, con modalità idonee a garantire la tutela della riservatezza dell'identità del segnalante, la riferibilità della trasmissione dei dati ai soli soggetti interessati, nonché l'integrità delle informazioni trasmesse.

L'art. 39 del D.lgs. 231/2007, nel disciplinare il divieto di comunicazioni inerenti le segnalazioni di operazioni sospette, prevede comunque che lo stesso non impedisce la comunicazione tra professionisti che svolgono la propria prestazione professionale in forma associata, in qualità di dipendenti o collaboratori, anche se situati in Paesi terzi, a condizione che questi applichino misure equivalenti a quelle previste dal medesimo decreto. Nei casi relativi allo stesso cliente o alla stessa operazione, che coinvolgano due o più professionisti, il divieto non impedisce inoltre la comunicazione tra i professionisti in questione, a condizione che appartengano ad uno Stato membro o siano situati in un Paese terzo che impone obblighi equivalenti a quelli previsti dal D.lgs. 231/2007. La medesima norma precisa, infine, che il tentativo del professionista di dissuadere il cliente dal porre in atto un'attività illegale non costituisce violazione del divieto di comunicazione.

6. Operatori del settore del gioco (*A. Cassetta e L. Baron*)

Il progressivo allargamento degli operatori appartenenti al settore del gioco è dovuto alla crescente percezione del rischio a esso connesso a seguito della sua notevole espansione collegata all'utilizzo di nuove e sempre più sofisticate tecnologie. L'analisi nazionale del rischio aggiornata nel 2018 sottolinea come "il comparto del gioco, sia illegale che legale, risulta di altissimo interesse per la criminalità organizzata, per la quale ha storicamente costituito un'importante forma di sovvenzione"¹⁰⁶⁴.

¹⁰⁶⁰ Cfr. gli artt. 11, comma 4, e 37, commi 1 e 2, del D.lgs. 231/2007.

¹⁰⁶¹ I protocolli di intesa, con relativi allegati tecnici (che disciplinano le forme tecniche di trasmissione telematica delle segnalazioni), sono stati rispettivamente siglati con la UIF dal CNOCDL in data 22 maggio 2009, dal CNN in data 3 giugno 2009 (con aggiornamento nel dicembre 2012) e, infine, dal CNDCEC in data 23 dicembre 2016. Il CNF non ha ad oggi deciso di esercitare la facoltà di operare come organismo di autoregolamentazione abilitato a ricevere le segnalazioni dai propri iscritti, così che gli avvocati procedono direttamente all'invio delle segnalazioni alla UIF.

¹⁰⁶² Il fatto che la segnalazione ricevuta, per espressa previsione di legge, debba essere trasmessa alla UIF integralmente e prontamente, consente di escludere qualsiasi potere di valutazione o di filtro dell'organismo in relazione alla fondatezza del sospetto che ha indotto il professionista alla segnalazione, in conformità a quanto previsto dalla normativa comunitaria (cfr. art. 34 della direttiva UE 2015/849).

¹⁰⁶³ Le segnalazioni pervengono alla UIF, tramite scambi informativi tra le due caselle di posta elettronica certificata (PEC), attivate rispettivamente presso la UIF e presso l'organismo, secondo un meccanismo di cifratura asimmetrica in grado di assicurare l'anonimato del segnalante e la riservatezza del contenuto informativo della segnalazione nei confronti del destinatario. Nel dettaglio, il professionista compila la segnalazione e invia il relativo file cifrato al rispettivo organismo, utilizzando un software che consente di criptare i dati del segnalante e della segnalazione. L'organismo provvede a caricare il file contenente la segnalazione nella piattaforma predisposta dalla UIF, ottenendo da quest'ultima una ricevuta di accettazione o scarto, in formato pdf, contenente il protocollo rilasciato dalla UIF e l'identificativo univoco della segnalazione. Tale ricevuta, che viene inoltrata automaticamente dal sistema di messaggistica della procedura a una casella di posta elettronica all'uopo predisposta dall'organismo, consente al software di associare all'identificativo univoco della segnalazione il protocollo comunicato dalla UIF, al quale si farà riferimento per le eventuali comunicazioni successive (es. integrazioni o seguiti).

¹⁰⁶⁴ Per l'impatto delle misure in questione sull'attività della UIF, si veda la Comunicazione del 27 marzo 2020, con la quale sono state dettate misure temporanee e avvertenze per mitigare l'impatto sui soggetti tenuti alla trasmissione di dati e informazioni nei confronti della UIF.

L'inserimento del settore del gioco tra i destinatari della normativa antiriciclaggio è stato graduale. Il primo ampliamento è avvenuto con il D.lgs. 56/2004 (di recepimento della seconda direttiva antiriciclaggio), che includeva le case da gioco. Con l'emanazione del D.lgs. 231 del 2007 sono stati aggiunti i soggetti che offrono, attraverso la rete Internet e altre reti telematiche o di telecomunicazione, giochi, scommesse o concorsi pronostici con vincite di denaro. Tuttavia, il mancato riferimento al possesso della concessione rilasciata dall'Agenzia delle dogane e dei monopoli (ADM), pur estendendo potenzialmente l'applicazione della norma a tutti i prestatori di gioco online, di fatto aveva reso pressoché impossibile definire compiutamente il perimetro dei soggetti sottoposti all'obbligo.

La riforma del 2017 ha definito con maggior chiarezza non solo i destinatari degli obblighi, ma anche la loro applicazione da parte dei soggetti che popolano la filiera del comparto, tenendo conto delle criticità emerse in passato. La cornice normativa in vigore individua tre macro-categorie di soggetti: a) gli operatori di gioco online, che offrono, attraverso la rete internet e altre reti telematiche o di telecomunicazione, giochi, con vincite in denaro, su concessione dell'Agenzia delle dogane e dei monopoli; b) gli operatori di gioco su rete fisica, che offrono, anche attraverso distributori ed esercenti a qualsiasi titolo contrattualizzati, giochi, con vincite in denaro, su concessione dall'Agenzia delle dogane e dei monopoli; c) i soggetti che gestiscono case da gioco, in presenza delle autorizzazioni concesse dalle leggi in vigore e del requisito di cui all'art. 5, comma 3, del decreto-legge 30 dicembre 1997, n. 457, convertito, con modificazioni, dalla legge 27 febbraio 1998, n. 30.

L'assoggettamento agli obblighi esula da un criterio territoriale e si applica invece al possesso della concessione pubblica. Peraltro soggetti esteri che offrono i loro servizi in Italia attraverso un sito internet sono automaticamente sottoposti al *framework* antiriciclaggio italiano. Lo sviluppo di attività "a distanza" costituisce per il legislatore un aspetto sfidante da risolvere: nel caso dei giochi¹⁰⁶⁵ si è scelto di far prevalere un criterio che privilegia il paese di residenza del titolare del conto gioco in base alla presunzione che le informazioni siano più utili per la FIU del paese di residenza di quest'ultimo.

Anche se molti operatori esteri titolari di concessione hanno comunque scelto di creare una società italiana, alcuni concessionari non hanno nessun legame "fisico" con l'Italia, pur adeguandosi al rispetto della normativa domestica e inviando SOS all'Unità di Informazione Finanziaria.

Per una compiuta definizione del perimetro di applicazione della norma, tuttavia, non è sufficiente considerare la definizione dei soggetti obbligati, in quanto non tutti i giochi sono sottoposti ai presidi antiriciclaggio. Occorre quindi riferirsi all'"attività di gioco"¹⁰⁶⁶ definita quale *"attività svolta, su concessione dell'Agenzia dogane e monopoli dai prestatori di servizi di gioco, ad esclusione dei giochi numerici a quota fissa e a totalizzatore, delle lotterie ad estrazione istantanea e differita e dei concorsi pronostici su base sportiva ed ippica"*.

Nel caso di questi giochi, infatti, si è ritenuto che la presenza di un'estrazione – istantanea o differita che sia – è già sottoposta a rigide forme di controllo ed è inoltre del tutto disancorata da qualunque abilità del giocatore o da eventi nella sua anche minima disponibilità. Si esclude, pertanto, che possa esserci un effettivo rischio di riciclaggio associato alla realizzazione di tali giochi. Il settore del *gambling* è popolato da numerosi attori con ruoli e funzioni specifiche che devono essere coinvolti e responsabilizzati, tenendo conto delle rispettive caratteristiche, per garantire un efficace sistema antiriciclaggio.

Il Concessionario, definito come colui che offre il gioco online per conto dello Stato, è il soggetto giuridico titolare della Concessione ottenuta a seguito di una procedura di selezione a mezzo gara pubblica indetta dall'ADM e che è autorizzato alla raccolta per giochi pubblici a distanza o anche attraverso una rete fisica di punti di raccolta.

Il concessionario non ha contatti diretti con i giocatori, in quanto - nell'ambito della filiera - dà ai gestori (o distributori) il mandato per la distribuzione, l'installazione e la gestione delle attività di raccolta del gioco. Si tratta di imprese private proprietarie degli apparecchi per l'attività di gioco affidati agli esercenti. Il gestore, su incarico del Concessionario, effettua le attività consistenti nella messa a disposizione degli apparecchi di gioco e nelle azioni necessarie al funzionamento degli stessi presso gli esercizi con modalità conformi alle prescrizioni normative in materia.

Gli esercenti sono i titolari dei punti fisici in cui viene svolta l'attività di gioco. Ad essi spetta l'onere di fornire gli spazi necessari e tutto quanto necessario per consentire il regolare svolgimento delle attività di gioco, in cambio di un corrispettivo. Nel caso dei videotermini, l'esercente stipula un contratto con il gestore che fornisce l'apparecchio.

¹⁰⁶⁵ Le modalità di applicazione della normativa sull'offerta tramite siti internet non è uniforme nei diversi settori. Per esempio, per i money transfer la disposizione di rimesse online è sottoposta alle regole del paese di insediamento dell'intermediario, indipendentemente dal luogo di residenza del *sender*. Il recente decreto sulle valute virtuali, invece, sembra seguire le modalità scelte per il settore del gioco.

¹⁰⁶⁶ Cfr. art. 1, comma 3, lett. a), del D.lgs. 231/2007 e successive modifiche.

Le sale sono gestite da uno o più “preposti di sala”, soggetti autorizzati dal Questore e designati dal titolare della licenza. Il preposto costituisce l'interfaccia amministrativa verso le autorità di ispezione e controllo, in quanto è il responsabile diretto della conduzione della sala e di ciò che avviene al suo interno nell'orario di apertura. Nel caso delle norme antiriciclaggio è corresponsabile, unitamente al titolare di licenza, della loro applicazione. L'incarico di preposto decade automaticamente al decadere della titolarità della licenza. Le sue funzioni non sono delegabili. Il preposto di sala: può essere affiancato da un altro soggetto, il cui nominativo dovrà essere indicato nella licenza stessa, e non può abbandonare la sala; ha il controllo e la sorveglianza della sala nonché la responsabilità del corretto funzionamento degli impianti; deve garantire presenza ed assistenza sulle operazioni in sala; controlla l'età degli avventori, il controllo del rispetto della privacy di gioco, il corretto funzionamento della piattaforma di gioco, il corretto funzionamento e collegamento degli apparecchi, la corretta tenuta dei titoli autorizzatori.

Alcuni Concessionari si avvalgono di intermediari per la gestione del rapporto con gli esercenti che hanno i requisiti per gestire sale VLT: sono i cosiddetti mandatari VLT. Un singolo mandatario può fungere da intermediario per sale riconducibili a gestori diversi, creando dei legami “invisibili”, in quanto la sua figura non emerge né dagli archivi camerali né dai registri dell'ADM. La gestione delle VLT, inoltre, prevede anche la figura del terzo incaricato del riversamento dell'importo residuo (IRIR).

Le VLT sono gestite da piattaforme alle quali affluiscono tutti i dati. Le piattaforme non rientrano tra i soggetti obbligati, ma si configurano come una sorta di società di servizi e non sono considerati interlocutori diretti della UIF e dell'ADM, rendendo più complicata l'acquisizione di informazioni di tipo massivo per l'analisi della corretta gestione di sale e punti fisici. L'inserimento delle piattaforme tra i soggetti obbligati, oltre a rendere disponibili dati di possibile interesse per gli approfondimenti, consentirebbe di avere contezza di ulteriori fenomeni ad alto rischio (es. scollegamento delle macchinette VLT dalla rete telematica dell'ADM).

Il comparto gioco è soggetto ai presidi che caratterizzano l'apparato antiriciclaggio (adeguata verifica, conservazione, invio di operazioni sospette) con alcune specificità che, se da un lato tengono conto delle peculiarità del comparto, dall'altro introducono elementi di novità che potrebbero fornire lo spunto per aggiornare anche le norme applicabili ad altri settori. I presidi antiriciclaggio riguardano sia il gioco fisico che il gioco online e si applicano sia ai concessionari che ai gestori dei punti fisici, i quali, se da un lato sono direttamente responsabili dell'applicazione di alcuni presidi, dall'altro devono essere sottoposti a verifica da parte del concessionario in quanto soggetti contrattualizzati.

Il decreto antiriciclaggio prevede espressamente all'art.17, comma1, lett. c) che i soggetti obbligati del settore procedono all'adeguata verifica del cliente quando questo compie un'operazione di gioco, definita come *“un'operazione atta a consentire, attraverso i canali autorizzati, la partecipazione a uno dei giochi del portafoglio dell'Agenzia delle dogane e dei monopoli, a fronte del corrispettivo di una posta di gioco in denaro”*¹⁰⁶⁷. I successivi artt. 52 e 53 calano tali obblighi nella specificità delle attività e dell'organizzazione del comparto.

Nel caso del gioco online, possibile soltanto a seguito dell'apertura di un conto gioco¹⁰⁶⁸, sono richiesti al momento della creazione del conto l'identificazione, la verifica dei dati forniti e la valutazione del profilo di rischio del cliente da parte del concessionario.

Il profilo del giocatore deve tenere conto delle informazioni a esso relative (quali l'attività economica svolta, l'area geografica di residenza o il profilo reddituale) e dell'operatività effettuata attraverso un monitoraggio eseguito nel continuo di elementi (quali la modalità di ricarica, i rapporti vendite/prelievi, la coerenza tra le ricariche e il profilo reddituale). La regolamentazione del settore da parte dell'ADM prevede che un giocatore possa aprire, versare e iniziare a giocare online anche senza aver inviato la copia del documento di identità. È tuttavia vietato il prelevamento dei fondi. Se il documento non è inviato dopo 30 giorni dall'apertura del conto, il Concessionario provvede a bloccare il conto che deve essere definitivamente chiuso trascorsi ulteriori 60 giorni senza l'invio del documento. La disciplina impone come unico vincolo che il denaro venga restituito con modalità tracciate.

L'art. 53, comma 2, prevede che l'alimentazione del conto avvenga attraverso modalità che permettano la piena tracciabilità dei flussi finanziari. La possibilità di utilizzare carte prepagate anonime e le difficoltà connesse con il trasferimento delle informazioni sui numeri e titolari delle carte di pagamento rendono tuttavia molto difficile avere una piena conoscenza della provenienza dei fondi.

¹⁰⁶⁷ Per la definizione si veda l'art.1, comma 3, lett. h).

¹⁰⁶⁸ Conto intestato al cliente aperto attraverso un concessionario di gioco autorizzato, sul quale sono registrate le operazioni di gioco effettuate su canale a distanza nonché le attività di ricarica e i prelievi. Le attività di gioco alle quali si può accedere tramite un conto di gioco sono più ampie rispetto a quelle accessibili da rete fisica.

Nel caso del gioco fisico, l'obbligo di adeguata verifica ricade sull'esercente, che lo adempie attraverso il "preposto di sala". Per garantire uniformità tra gli esercenti, il Concessionario deve fornire le procedure per il corretto svolgimento dell'adeguata verifica.

Sono previsti obblighi diversi a seconda che si tratti di *betting* oppure di gioco su VLT: nel primo caso la soglia è 2 mila euro, nel secondo 500 euro. L'esistenza di queste soglie unitamente all'espansione del settore del gioco implica che per notevoli i flussi di denaro è impossibile seguire le tracce, individuare l'origine o scoprire i destinatari. Per questo motivo, nonostante gli sforzi fatti, i titoli di gioco possono prestarsi a essere utilizzati in modo improprio per occultare il trasferimento del possesso dei fondi.

Sul Concessionario gravano, inoltre, gli obblighi di conservazione delle informazioni raccolte in sede di apertura del conto gioco e di esecuzione delle operazioni sopra le soglie previste.

Nel caso del gioco fisico, le informazioni raccolte dagli esercenti devono essere trasmesse al Concessionario entro 10 giorni dall'effettuazione dell'operazione. Gli esercenti sono tenuti comunque a conservare le informazioni in proprio per 2 anni. In questo caso, quindi, la normativa del comparto gioco si differenzia da quanto previsto per altri settori (si pensi ai soggetti convenzionati) in cui il trasferimento delle informazioni al soggetto obbligato costituisce l'unico adempimento previsto. Un'ulteriore particolarità delle norme applicabili al settore gioco prevede la conservazione dell'indirizzo IP dello strumento utilizzato per disporre le operazioni di gioco. L'indirizzo IP è l'informazione che consente di sapere se il titolare di un rapporto sta utilizzando strumenti differenti (pc, cellulare, tablet) per l'accesso ed è ampiamente sfruttata da tutti i soggetti che richiedono la creazione di un *account*. Al momento, tuttavia, ne è richiesta la conservazione soltanto ai concessionari di gioco. Si tratta, quindi, di una previsione innovativa relativa a informazioni facilmente disponibili che potrebbe essere estesa a tutte le operatività finanziarie effettuate telematicamente.

Poiché l'Agenzia dei Monopoli non è considerata dal decreto antiriciclaggio un'Autorità di Vigilanza, non sono state emanate regole che disciplinano in modo specifico la conservazione delle informazioni.

Completa il quadro normativo l'obbligo di segnalazione di operazioni sospette alla UIF. I Concessionari devono dotarsi di procedure interne con cui monitorare l'operatività dei propri clienti e individuare tempestivamente comportamenti sospetti da sottoporre a valutazione. L'individuazione di un'operazione sospetta, infatti, prescinde dal superamento di soglie di importo e deve basarsi su una valutazione complessiva, che tenga conto sia delle caratteristiche oggettive dell'operazione sia del profilo soggettivo del cliente, nonché di ogni altra informazione raccolta e rilevante per l'approfondimento del caso in esame.

Il compito degli operatori è agevolato dagli indicatori di anomalia¹⁰⁶⁹ e da due schemi rappresentativi di comportamenti anomali relativi a operatività connesse con il settore dei giochi e delle scommesse diffusi dalla UIF con la collaborazione della GdF e dell'ADM nel 2012¹⁰⁷⁰.

Tra le anomalie soggettive rilevano eventuali incoerenze riscontrate in sede di adeguata verifica, nonché la presenza di alert quali, per esempio, il coinvolgimento in procedimenti penali. Sotto il profilo oggettivo sono richiamate, tra l'altro, le operatività sovradimensionate rispetto al profilo economico del cliente e le attività di gioco particolarmente concentrate presso un medesimo giocatore od operatore di gioco. Rimane, tuttavia, in capo ai soggetti obbligati la responsabilità di valutare ogni condotta anche se non rispondente a quelle elencate nei suddetti documenti, in quanto l'evoluzione continua di strumenti e prassi impedisce la previsione di una lista esaustiva di tutti i comportamenti forieri di elementi di sospetto¹⁰⁷¹.

¹⁰⁶⁹ Al momento ci si riferisce a quelli emanati con decreto del Ministero dell'Interno, su proposta della UIF, il 17 febbraio 2011 e modificati con il DM 27 aprile 2012.

¹⁰⁷⁰ Le indicazioni fornite sono distinte per tipologia di destinatario degli obblighi antiriciclaggio. Il primo schema si applica ai soggetti obbligati che si trovano a operare con operatori di gioco e fornisce un elenco, non esaustivo, di profili da valutare. Il secondo schema è invece rivolto agli stessi operatori del comparto e descrive possibili anomalie sia per il gioco fisico che per quello online.

¹⁰⁷¹ Tra le principali criticità emerse vengono messe in evidenza ricorrenti relazioni tra i responsabili dei punti operativi e le attività transitate presso i medesimi. In relazione al gioco presso sale VLT, le anomalie riguardano la riscossione di ticket vincenti d'importo ricorrente, frequentemente emessi a pochi minuti di distanza l'uno dall'altro, o concentrazioni di vincite realizzate con apparecchi VLT presso una stessa sala in capo a pochi nominativi ripetuti (specie di origine straniera) e con reiterato ricorso al contante per l'incasso. Sovente si riscontrano operazioni di gioco-scommessa di importo al limite della soglia di identificazione. Tra le anomalie maggiormente ricorrenti figura la reiterazione dell'operatività su più sale (anche in province diverse da quella di residenza del giocatore) o siti web, ripetute aperture e chiusure di conti da parte dei medesimi soggetti, l'utilizzo di conti di addebito intestati a terzi soggetti (anche implicati in indagini su scommesse irregolari). Nel gioco a distanza, accanto alle ipotesi consolidate di ricariche di conti di gioco con carte rubate o clonate, e alle pratiche collusive (ad es. chip dumping, best hand), sono stati anche riscontrati molteplici casi di utilizzo di conti di gioco come depositi extra-bancari (anche associati a temporanea autoesclusione del titolare). Il conto gioco, infatti, non rientra tra i rapporti che devono essere dichiarati all'Anagrafe dei rapporti e, quindi, possono costituire un modo per sottrarre disponibilità a eventuali accertamenti fiscali o sequestri.

7. Operatori in valute virtuali (L. La Rocca)

Il D.lgs. 231/2007 include tra i destinatari degli obblighi di prevenzione del riciclaggio e del finanziamento del terrorismo i prestatori di servizi relativi all'utilizzo di valuta virtuale¹⁰⁷² e i prestatori di servizi di portafoglio digitale (art. 3, comma 5, lett. i) e *i-bis*), del D.lgs. 231/2007).

Tali categorie sono state incluse nel novero dei predetti destinatari in esito a due distinte riforme realizzate con i decreti legislativi 25 maggio 2017, n. 90, e 4 ottobre 2019, n. 125, rispettivamente, di recepimento della quarta e della quinta direttiva europea. In occasione di entrambi gli interventi legislativi, è stata delineata una disciplina di prevenzione più ampia di quella prevista a livello europeo¹⁰⁷³, al fine di tenere conto, da un lato, dei rischi connessi all'utilizzo delle valute virtuali e, dall'altro, delle Raccomandazioni formulate dal GAFI nel 2018¹⁰⁷⁴.

La Commissione europea ha in particolare evidenziato l'esposizione significativa delle "monete virtuali" ai rischi di riciclaggio e finanziamento del terrorismo¹⁰⁷⁵. Inoltre, nel tempo, molteplici Autorità hanno sottolineato che, in assenza di un quadro regolamentare di riferimento, l'operatività in valute virtuali appare rischiosa per la scarsa disponibilità di informazioni in merito alle modalità di determinazione dei prezzi, la volatilità del valore a esse attribuito, la complessità delle tecnologie sottostanti, l'assenza di tutele legali e contrattuali, di obblighi informativi nonché di regole a salvaguardia delle somme impiegate. Si sono altresì verificate perdite a causa di malfunzionamenti, attacchi informatici, smarrimento delle credenziali di

¹⁰⁷² Ai fini del presente scritto si utilizzerà principalmente la locuzione "valuta virtuale" in quanto contenuta nel vigente D.lgs. 231/2007; le ulteriori denominazioni in uso quali virtual asset, crypto-asset, cryptocurrency, crypto-assets o cripto-attività sono comunque da intendersi come sinonimi.

¹⁰⁷³ La quarta direttiva non ha introdotto presidi antiriciclaggio inerenti alle valute virtuali; ha soltanto riconosciuto che le nuove tecnologie offrono alle imprese e alla clientela soluzioni efficaci sotto il profilo dei tempi e dei costi e, nel contempo, che le autorità competenti e i soggetti obbligati devono essere proattivi nel contrastare nuovi e innovativi metodi di riciclaggio (cfr. considerando (19) della direttiva (UE) 2015/849); le nuove tecnologie non sono state tuttavia individuate né si è fatto cenno allo sviluppo e alla diffusione delle valute virtuali. Successivamente, nell'Action Plan del febbraio 2016, per rafforzare la lotta contro il finanziamento del terrorismo, la Commissione europea ha osservato che *"i nuovi strumenti finanziari come le valute virtuali creano nuove sfide in termini di lotta contro questi finanziamenti"*; *"esiste il rischio che le organizzazioni terroristiche sfruttino i trasferimenti di valute virtuali per dissimulare movimenti finanziari: le operazioni effettuate con le valute virtuali, in effetti, pur venendo registrate, non sono oggetto di un meccanismo di segnalazione equivalente a quello predisposto nel sistema bancario tradizionale per individuare le attività sospette"*. Sul presupposto che le valute virtuali non erano ancora regolamentate a livello di Unione europea, come primo passo, la Commissione ha dichiarato di voler proporre l'assoggettamento degli scambi anonimi di valuta sotto il controllo delle autorità competenti, estendendo il campo d'applicazione della direttiva antiriciclaggio alle piattaforme di scambio di valute virtuali, nonché di assoggettare i medesimi scambi a controllo nel quadro delle legislazioni nazionali in materia di lotta contro il riciclaggio del denaro e il finanziamento del terrorismo. La Commissione ha inoltre rilevato che, applicando alle piattaforme di scambio di valute virtuali le regole in materia di autorizzazione e vigilanza della direttiva sui servizi di pagamento, si favorirebbe un migliore controllo e una migliore conoscenza del mercato. Un'ulteriore riflessione è stata prospettata dalla Commissione in merito all'opportunità di estendere i presidi anche ai "fornitori di portafogli" di valute virtuali. Le dichiarazioni contenute nell'Action Plan hanno condotto alla direttiva (UE) 2018/843. Quest'ultima ha ampliato il novero dei destinatari degli obblighi di prevenzione includendovi fra l'altro: i) i prestatori di servizi di cambio tra valute virtuali e valute aventi corso forzoso (che l'Italia aveva incluso tra i soggetti obbligati già con il D.lgs. 90/2017) e ii) i prestatori di servizi di portafoglio digitale. Tali soggetti dovranno essere registrati negli Stati membri (cfr. art. 47 della quarta direttiva, come modificato dalla quinta). L'obiettivo è coprire tutti i possibili utilizzi di valute virtuali, non solo quello più frequente come mezzo di pagamento, ma anche il loro uso come mezzo di scambio, di investimento, prodotti di riserva di valore o per il gioco online (cfr. considerando 10 della quinta direttiva). Viene riconosciuto che *"l'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate"* (cfr. considerando 9 della quinta direttiva).

¹⁰⁷⁴ Nell'ottobre 2018 il GAFI ha introdotto specifiche definizioni di Virtual Asset (rappresentazione digitale di valore che può essere scambiata digitalmente, o trasferita, e può essere utilizzata per effettuare pagamenti o investimenti; non sono incluse le rappresentazioni digitali di valuta legale, di titoli o di altri asset finanziari già altrimenti disciplinate dalle stesse Raccomandazioni) e *Virtual Asset Service Providers*, individuati a fini antiriciclaggio in ragione della tipologia di attività svolta: a) conversione tra Virtual Asset e valute legali; b) conversione tra Virtual Asset; c) trasferimento di Virtual Asset; d) custodia e/o amministrazione di Virtual Asset o di strumenti che ne consentono il controllo; e) partecipazione e fornitura di servizi finanziari relativi all'offerta e/o alla vendita di Virtual Asset. Ai sensi della "Raccomandazione n. 15", come modificata dal GAFI nel 2018, i VASP devono essere sottoposti alle normative nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo e devono essere soggetti a regimi di licenza o registrazione, nonché a controlli di compliance.

¹⁰⁷⁵ Si veda p. 5 della [Relazione sulla valutazione sovranazionale dei rischi](#) condotta dalla Commissione europea nel 2017. Le valute virtuali sono state inoltre menzionate anche nella [seconda Relazione della Commissione sulla valutazione sovranazionale dei rischi](#) del luglio 2019, in particolare con riguardo alla circostanza che il crescente ricorso a tali strumenti pone rischi più elevati e alla possibilità che presentino caratteristiche di anonimato simili al contante (pp. 4 e 8 della citata Relazione).

accesso ai portafogli elettronici, attività fraudolente¹⁰⁷⁶. Tali rischi assumono maggiore rilevanza in relazione al diffondersi di forme di offerta attraverso il canale digitale, che facilitano l'acquisto di cripto-attività da parte di una platea molto ampia e indefinita di soggetti. Spesso non è agevole associare le transazioni ai relativi disponenti e beneficiari, se ne registra l'utilizzo nel c.d. *dark web* e la possibilità di utilizzo distorto a fini criminali¹⁰⁷⁷.

Nell'ambito della materia antiriciclaggio le valute virtuali sono state anzitutto definite: si tratta di rappresentazioni digitali di valore, non emesse né garantite da una banca centrale o da un'Autorità pubblica, non necessariamente collegate a una valuta avente corso legale, utilizzate come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferite, archiviate e negoziate elettronicamente¹⁰⁷⁸.

Sono stati inoltre definiti gli operatori rilevanti in valute virtuali, distinguendoli in due categorie: 1) i prestatori di servizi relativi all'utilizzo di valuta virtuale ovvero ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute; 2) i prestatori di servizi di portafoglio digitali: ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali¹⁰⁷⁹.

¹⁰⁷⁶ Ne sono un esempio le notizie di stampa sull'indagine condotta dalla Procura di Firenze per una ipotesi di frode informatica da milioni di euro relativa alla società Bitgrail (https://corrierefiorentino.corriere.it/firenze/notizie/cronaca/22_maggio_23/criptovalute-maxi-frode-120-milioni-euro-processo-l-amministratore-piattaforma-ae6f9c9c-daba-11ec-af96-bd4936e4fc64.shtml).

¹⁰⁷⁷ Con riguardo alle posizioni assunte nel tempo dalle Autorità sovranazionali cfr., *ex multis*, l'Opinion dell'EBA del luglio del 2014, con la quale si è raccomandato al legislatore europeo di considerare la possibilità di includere i c.d. virtual currency exchanges tra i destinatari degli obblighi di prevenzione. Questa raccomandazione veniva formulata ad appena un mese di distanza dalla pubblicazione del primo FATF Report, Virtual Currencies Key Definitions and Potential AML/CFT Risks, volto a comprendere le caratteristiche delle valute virtuali, le modalità di funzionamento e i rischi specifici che le stesse pongono dal punto di vista antiriciclaggio. Inoltre, come rilevato nella Comunicazione della UIF del 28 maggio 2019, caratteristiche e rischi delle valute virtuali, nonché possibili profili evolutivi della regolamentazione sono stati richiamati, tra l'altro, negli esiti del [meeting dei leader del G20 del 21-22 luglio 2018](#); nell'avvertenza delle Autorità europee di vigilanza del febbraio 2018; nei successivi report del 9 gennaio 2019 della European Banking Authority - EBA e della European Securities and Markets Authority - ESMA. Più di recente le Autorità di vigilanza europee hanno ricordato i rischi connessi con i crypto-assets, rispettivamente, nel 2021 e nel 2022. Tra le iniziative assunte a livello nazionale si rinvia alle pubblicazioni di: Banca d'Italia, Avvertenza sull'uso delle cosiddette valute virtuali del 30 gennaio 2015, Comunicazione del 30 gennaio 2015 – valute virtuali, Provvedimenti di carattere generale delle autorità creditizie, Bollettino di Vigilanza n. 1, gennaio 2015 e Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee del 19 marzo 2018; UIF, Comunicazione del 30 gennaio 2015 e Comunicazione del 28 maggio 2019; Consob, ESMA, EBA ed EIOPA avvertono i consumatori circa i rischi delle criptovalute; approfondimento sulle criptovalute a fini di educazione finanziaria; documento del 19 marzo 2019 per l'avvio di un dibattito nazionale sul tema delle offerte iniziali e degli scambi di cripto-attività. Nell'aprile 2021 Consob e Banca d'Italia hanno pubblicato un comunicato congiunto contro i rischi insiti nelle cripto-attività. Nel giugno 2022 la Banca d'Italia ha pubblicato una Comunicazione in materia di tecnologie decentralizzate (cosiddette distributed ledger technologies, DLT) nella finanza e cripto-attività, al fine di richiamare l'attenzione degli intermediari vigilati, dei soggetti sorvegliati e di quelli che operano a vario titolo negli ecosistemi decentralizzati, anche come utenti, sia sulle opportunità sia sui rischi connessi con l'uso di tali tecnologie e con l'operatività in cripto-attività, evidenziando alcuni profili rilevanti per il loro presidio.

¹⁰⁷⁸ Art. 1, comma 2, lett. qq), del D.lgs. 231/2007, come introdotto dal D.lgs. 90/2017 e successivamente modificato dal D.lgs. 125/2019. Non si tratta dell'unica definizione oggi presente nell'ordinamento nazionale. La valuta virtuale è definita, per esempio, anche nel D.lgs. 184/2021, di recepimento della direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. In tale ambito, la tutela penale è estesa all'indebito utilizzo e falsificazione di ogni strumento di pagamento diverso dai contanti (art. 493-ter c.p.); è definito il "mezzo di scambio digitale" ed è inclusa anche la valuta virtuale ovvero "una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente". Ampiamente dibattuta è in dottrina e in giurisprudenza la natura giuridica delle valute virtuali. In argomento, sia vedano, anche per più ampi riferimenti dottrinali e giurisprudenziali, *ex multis*, N. VARDI, *Bit by Bit: Assessing the Legal Nature of Virtual Currencies*, in G. Gimigliano (a cura di), *Bitcoin and Mobile Payments. Constructing a European Union Framework*, London, 2016; M. Mancini, *Valute virtuali e Bitcoin*, in *Analisi giuridica dell'economia*, 2015, 1; G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologia in cerca di un problema*, in *Diritto dell'Informazione e dell'Informatica* (II), 2015, 3; M. Passaretta, *Bitcoin: il leading case italiano*, in *Banca Borsa e Titoli di Credito*, 2017, 4; F. Di Vizio, *Lo statuto penale delle valute virtuali: le discipline e i controlli*, in *dis CRIMEN*, Giugno 2019; *Ibidem*, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, in *dis CRIMEN*, Dicembre 2019.

¹⁰⁷⁹ Art. 1, comma 2, lett. ff) e ff-bis), del D.lgs. 231/2007, a seguito delle riforme di cui al D.lgs. 90/2017 e al D.lgs. 125/2019.

Tanto i prestatori di servizi relativi all'utilizzo di valuta virtuale quanto i prestatori di servizi di portafoglio digitale sono assoggettati a un meccanismo di controllo e censimento: è prevista la loro iscrizione obbligatoria nella sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli agenti e dei mediatori - OAM¹⁰⁸⁰; ai medesimi prestatori di servizi si applicano le disposizioni inerenti all'attività dei cambiavalute di cui all'art. 17-*bis* del decreto legislativo 13 agosto 2010, n. 141¹⁰⁸¹ e ciò significa che la ricorrenza dei requisiti previsti per questi ultimi è obbligatoria ai fini della iscrizione degli operatori in valute virtuali nella sezione speciale del registro¹⁰⁸².

L'OAM riceve le informazioni inerenti alle negoziazioni effettuate dai prestatori di servizi relativi all'utilizzo di valuta virtuale, i quali a loro volta conservano i dati registrati per dieci anni. In caso di violazione dell'obbligo di trasmissione delle informazioni l'Organismo dispone la sospensione dal registro, per un periodo non inferiore a tre mesi e non superiore a un anno¹⁰⁸³.

L'esercizio dell'attività in assenza dei requisiti prescritti dalla legge non è penalmente rilevante ed è punito soltanto con una sanzione amministrativa di importo che può considerarsi irrisorio (da 2.065 euro a 10.329 euro)¹⁰⁸⁴. L'Organismo ha infine il potere di disporre la cancellazione dalla sezione in casi specifici (perdita dei requisiti prescritti, violazione ripetuta degli obblighi segnaletici, protratta inattività o cessazione della stessa)¹⁰⁸⁵.

Ai fini della implementazione della sezione speciale del registro, il decreto del Ministro dell'Economia e delle finanze (MEF) del 13 febbraio 2022 riepiloga i requisiti che gli operatori devono possedere per svolgere legalmente in Italia le attività in valute virtuali rilevanti a fini antiriciclaggio¹⁰⁸⁶. A tale iscrizione devono provvedere anche gli operatori esteri che prestano i servizi nel territorio della Repubblica a distanza, secondo modalità telematiche, eventualmente ricorrendo a offerte in lingua italiana mediante siti web o applicazioni informatiche¹⁰⁸⁷. Ciascun operatore in valute virtuali comunica all'OAM i dati identificativi dei clienti nonché dati sintetici relativi all'operatività complessiva, secondo quanto stabilito nell'art. 5 e nell'allegato 1 del sopra citato decreto. È stabilito che l'OAM collabori con le Autorità coinvolte nella prevenzione e nel contrasto del riciclaggio e del finanziamento del terrorismo e che fornisca, su richiesta, ogni informazione e documentazione detenuta in forza della gestione del registro al MEF, alle Autorità di vigilanza, alla UIF, alla Direzione Investigativa Antimafia, al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza e alla Direzione Nazionale Antimafia e Antiterrorismo. Sono previste, infine, forme di cooperazione con le forze di polizia e l'intervento di queste ultime per contrastare l'esercizio abusivo di attività nel territorio della Repubblica.

I prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale sono c.d. "operatori non finanziari" (art. 3, comma 5); non sono vigilati da una specifica Autorità di settore a fini antiriciclaggio e sono sottoposti alle verifiche AML/CFT, anche ispettive, della Guardia di Finanza nonché, limitatamente alle segnalazioni di operazioni sospette, della UIF.

Gli operatori in valute virtuali sono obbligati, inoltre, alla valutazione del rischio di riciclaggio e di finanziamento del terrorismo cui sono esposti nell'esercizio dell'attività, all'adeguata verifica della clientela, alla conservazione dei dati e delle informazioni e alle segnalazioni di operazioni sospette¹⁰⁸⁸.

¹⁰⁸⁰ La collocazione della sezione nell'ambito del sopra citato registro sembra suggerire che il legislatore abbia inteso accostare gli operatori in valute virtuali alla figura dei cambiavalute, probabilmente sul presupposto che la conversione di valuta virtuale da ovvero in valuta legale sia un momento qualificante della loro attività.

¹⁰⁸¹ Art. 8, comma 1, del D.lgs. 90/2017.

¹⁰⁸² Se si tratta di persona fisica: cittadinanza italiana o di uno stato dell'Unione europea ovvero di stato diverso secondo le disposizioni dell'art. 2 del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, e domicilio nel territorio della Repubblica (art. 17-*bis*, comma 2, lett. a), del D.lgs. 141/2010); se si tratta di soggetti diversi da una persona fisica: sede legale e amministrativa o, per i soggetti comunitari, stabile organizzazione nel territorio della Repubblica (art. 17-*bis*, comma 2, lett. b), del D.lgs. 141/2010).

¹⁰⁸³ Art. 17-*bis*, comma 3, del D.lgs. 141/2010.

¹⁰⁸⁴ Art. 17-*bis*, comma 6, del D.lgs. 141/2010. Eventuali ulteriori profili di abusivismo connessi all'operatività in valute virtuali sono stati oggetto di approfondimento in F. Di Vizio, *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà di nuovi intermediari*, in dis CRIMEN, aprile 2022.

¹⁰⁸⁵ Art. 17-*bis*, comma 7, del D.lgs. 141/2010.

¹⁰⁸⁶ Il decreto ministeriale è stato pubblicato nella Gazzetta Ufficiale del 17 febbraio 2022 e costituisce attuazione dell'art. 17-*bis* del D.lgs. 141/2010, come modificato dal D.lgs. 90/2017 e dal D.lgs. 125/2019.

¹⁰⁸⁷ La sezione speciale del registro è consultabile alla pagina https://www.organismo-am.it/elenchi-registri/operatori_valute_virtuali/.

¹⁰⁸⁸ Per dettagliati riferimenti sugli obblighi in questione si rinvia ai relativi contenuti del presente volume.

Il decreto antiriciclaggio non contiene disposizioni specifiche applicabili ai medesimi prestatori di servizi (come invece accade per gli operatori del comparto del gioco).

L'applicazione delle regole generali in materia di adeguata verifica fa sì che gli operatori in valute virtuali adempiano a tale obbligo nei casi di cui all'art. 17 del D.lgs. 231/2007; laddove si tratta di operazioni occasionali – così sono in genere qualificati, ad esempio, gli acquisti o le vendite di valute virtuali che si perfezionano presso dispositivi automatici (c.d. ATM) – assume quindi rilievo la soglia di 15.000 euro, che rischia probabilmente di essere non del tutto appropriata tenuto conto dell'esigenza, da un lato, di realizzare il presidio rigoroso dei rischi anche in relazione a operazioni di valore inferiore e, dall'altro, di chiarire le modalità concrete di applicazione della regola rispetto a transazioni il cui valore è soggetto a repentine oscillazioni a causa della intrinseca volatilità delle valute virtuali.

Per quanto concerne le disposizioni in materia di conservazione dei dati e delle informazioni, trovano applicazione gli artt. 31 e seguenti del D.lgs. 231/2007 e andrebbe valutata l'opportunità di introdurre disposizioni integrative – in analogia a quanto stabilito per i prestatori di servizi di gioco – volte a tenere conto della tecnologia sottostante all'utilizzo di valute virtuali e dell'esigenza di indicare puntualmente parametri identificativi delle operazioni della specie, per esempio con riguardo ai codici unici distintivi delle stesse e all'indicazione degli indirizzi IP e degli altri elementi identificativi delle connessioni telematiche nel corso delle quali esse sono eseguite.

Ai fini delle segnalazioni di operazioni sospette, la normativa primaria non contiene previsioni specifiche inerenti alle modalità di segnalazione da parte degli operatori in valute virtuali (come invece prevede per altri soggetti obbligati come gli intermediari, altri operatori finanziari e i professionisti) e si applicano le istruzioni contenute nel Provvedimento per le Segnalazioni di Operazioni Sospette emanato dalla UIF il 4 maggio 2011. Nel 2019 l'Unità ha inoltre pubblicato indicazioni integrative per la compilazione delle segnalazioni riconducibili all'utilizzo di valute virtuali e, in particolare, per la migliore rappresentazione dei sospetti e per la trasmissione di più complete informazioni utili all'attività di analisi finanziaria¹⁰⁸⁹. Sono stati inoltre resi disponibili esempi pratici di compilazione delle segnalazioni in alcune casistiche ricorrenti concernenti valute virtuali, con l'indicazione di causali specifiche per le tipologie di operazioni individuate¹⁰⁹⁰. Al fine di agevolare l'individuazione delle operatività sospette, la UIF ha pubblicato due distinte Comunicazioni, rispettivamente, nel gennaio del 2015 e nel maggio del 2019, con le quali ha richiamato l'attenzione su specifici profili comportamentali a rischio¹⁰⁹¹. Possono utilmente essere presi in considerazione anche i *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* pubblicati dal GAFI nel settembre 2020¹⁰⁹².

La disciplina antiriciclaggio degli operatori in valute virtuali sarà d'altra parte oggetto di nuovi interventi normativi. È infatti in via di definizione il negoziato sul c.d. *AML Package*, proposto dalla Commissione europea nel luglio del 2021, che accentuerà la convergenza delle discipline dei singoli Stati membri attraverso regolamenti di diretta applicazione e il consolidamento di un *rulebook* europeo completato da disposizioni secondarie. In tale ambito, si prevede che: tutti i prestatori di servizi in cripto-attività, sostanzialmente oggi già presi in considerazione dalla disciplina AML/CFT italiana, rientreranno tra i soggetti obbligati, in linea con gli standard del GAFI; l'obbligo di trasmettere i dati informativi relativi all'ordinante e al beneficiario, al fine di garantirne la tracciabilità e l'individuazione di eventuali transazioni sospette (già in vigore per quelli in valuta legale) sarà esteso anche ai trasferimenti in cripto-attività.

A questi lavori di riforma si affiancano quelli sulle proposte della Commissione europea del settembre 2020, sulla digitalizzazione del settore finanziario e, in particolare, la proposta di regolamento *Markets in Crypto-assets* (c.d. MiCA), finalizzata a introdurre una disciplina europea uniforme in materia di valute virtuali. Tale proposta non tratta profili AML/CFT sebbene la nuova “*legislazione dovrebbe contribuire all'obiettivo riguardante la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo*”¹⁰⁹³.

¹⁰⁸⁹ Il Provvedimento della UIF del 4 maggio 2011 e le richiamate indicazioni integrative sono disponibili sul sito internet della UIF, rispettivamente, all'indirizzo <https://uif.bancaditalia.it/normativa/norm-antiricic/provv-2011-05-04/index.html> e https://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/Indicazioni_SOS_VV_2019.pdf.

¹⁰⁹⁰ Si fa riferimento al par. 8 dei c.d. “casi d'uso” disponibili sul sito internet della UIF all'indirizzo https://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/casi_d_uso.pdf.

¹⁰⁹¹ Entrambe le Comunicazioni sono consultabili sul sito internet della UIF.

¹⁰⁹² Gli indicatori di anomalia pubblicati dal GAFI sono consultabili alla pagina <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf>.

¹⁰⁹³ Cfr. considerando (8) della proposta MiCA consultabile alla pagina <https://data.consilium.europa.eu/doc/document/ST-11053-2020-INIT/en/pdf>. È prevista l'introduzione di norme uniformi per quanto riguarda: i) gli obblighi di trasparenza e informativa per

8. Operatori in oro (A. Cuzzocrea)

Nell'ambito della filiera degli operatori in oro rilevanti per la normativa di prevenzione del riciclaggio e del finanziamento del terrorismo, occorre distinguere due categorie di soggetti destinatari di distinte discipline dettate in materia: *i)* gli operatori professionali in oro di cui alla legge n. 7 del 17 gennaio 2000¹⁰⁹⁴ (di seguito anche OPO), individuati fra i soggetti destinatari del D.lgs. 21 novembre 2007, n. 231 e successive modifiche e integrazioni (di seguito anche decreto antiriciclaggio), che li annovera fra gli altri operatori non finanziari di cui all'art. 3, comma 5, lett. d); *ii)* gli operatori compro oro disciplinati dal D.lgs. 25 maggio 2017, n. 92 (di seguito anche OCO).

Vi è poi una categoria “ibrida” di soggetti che presentano le caratteristiche di entrambe le figure, ai quali devono ritenersi applicabili le disposizioni contenute nei plessi normativi sopra indicati. Inoltre, tutti gli operatori in oro sono dotati di licenza di pubblica sicurezza ai sensi degli artt. 127 e 128 del Testo unico delle leggi di pubblica sicurezza di cui al Regio decreto 18 giugno 1931, n. 773 (TULPS).

Prima della riforma del decreto antiriciclaggio introdotta dal D.lgs. 25 maggio 2017, n. 90, i soggetti che commerciavano in oro, sia in via professionale sia come compro oro, erano obbligati solamente alla segnalazione delle operazioni sospette, ai sensi dell'abrogato art. 10 del previgente decreto antiriciclaggio. Il legislatore del 2017 ha operato una netta cesura tra le due categorie di operatori in oro, assoggettando gli OPO a tutti gli obblighi antiriciclaggio e alle disposizioni in materia di controlli e sanzioni previste dal D.lgs. 231/2007 per i soggetti obbligati non vigilati, mentre per gli OCO è stata introdotta una specifica normativa, contenuta nel D.lgs. 92/2017.

L'elaborazione di una disciplina per l'attività di compro oro è stata prevista da uno specifico criterio della legge di delegazione europea per il 2015¹⁰⁹⁵, teso a regolare un settore ritenuto particolarmente sensibile a fenomeni di infiltrazione criminale non soltanto per l'elevato utilizzo di denaro contante, ma anche per la mancanza di adeguati presidi antiriciclaggio¹⁰⁹⁶.

L'art. 1, lett. n), del D.lgs. 92 del 2017 definisce operatore compro oro il “*soggetto, anche diverso dall'operatore professionale in oro di cui alla legge 17 gennaio 2000, n. 7, che esercita l'attività di compro oro*”. La successiva lett. o) della stessa disposizione definisce l’“*operazione di compro oro*” come l'attività commerciale consistente nella “*compravendita all'ingrosso o al dettaglio ovvero la permuta di oggetti preziosi usati*”. I compro oro, quindi, vengono identificati con l'ampia categoria dei commercianti di oggetti preziosi usati¹⁰⁹⁷, senza che

l'emissione e l'ammissione alla negoziazione di cripto-attività; ii) l'autorizzazione e la vigilanza dei fornitori di servizi per le cripto-attività, degli emittenti di c.d. asset referenced tokens e degli emittenti di c.d. e-money tokens; iii) la gestione, l'organizzazione e la governance degli emittenti di attività, degli emittenti di token di moneta elettronica e dei fornitori di servizi per le cripto-attività; iv) le disposizioni a tutela dei consumatori per quanto riguarda l'emissione, la negoziazione, lo scambio e la custodia delle cripto-attività; v) le misure volte a prevenire gli abusi di mercato. Sono in particolare individuate regole per l'emissione e l'offerta di crypto-assets ed è stabilito un regime autorizzativo e di vigilanza per gli emittenti di asset referenced tokens ed e-money tokens. L'EBA assumerebbe poteri di supervisione su questi ultimi in caso di token considerati significativi. L'ESMA è indicata come autorità incaricata di tenere il Register of crypto-asset service providers.

¹⁰⁹⁴ Si tratta di operatori autorizzati all'esercizio in via professionale del commercio di oro, per conto proprio o per conto di terzi, ai sensi dell'art. 1, comma 3, della legge n. 7/2000. In particolare, tale disposizione prevede che l'esercizio in via professionale del commercio di oro può essere svolto da banche e da operatori in oro autorizzati dalla Banca d'Italia ai sensi dell'art. 71 del D.lgs. 231/2007), in possesso dei seguenti requisiti: a) forma giuridica di società per azioni, o di società in accomandita per azioni, o di società a responsabilità limitata, o di società cooperativa, aventi in ogni caso capitale sociale interamente versato non inferiore a quello minimo previsto per le società per azioni; b) oggetto sociale che comporti il commercio di oro; c) possesso, da parte dei partecipanti al capitale, degli amministratori e dei dipendenti investiti di funzioni di direzione tecnica e commerciale, dei requisiti di onorabilità previsti dagli artt. 108, 109 e 161, comma 2, del testo unico delle leggi in materia bancaria e creditizia, emanato con decreto legislativo 1° settembre 1993, n. 385 (TUB).

¹⁰⁹⁵ Cfr. art. 15, comma 2, lett. l), della legge 12 agosto 2016, n. 170.

¹⁰⁹⁶ La prima analisi nazionale del rischio condotta nel 2014 aveva suggerito l'opportunità di un intervento normativo per disciplinare il settore e accrescere la consapevolezza del ruolo che gli operatori in oro svolgono nel mercato, specie in periodi di congiuntura economica negativa. Era stato in particolare posto in luce che “la crisi economica ha portato, tra l'altro, ad una crescente diffusione di compro-oro, categoria di operatori eterogenea attualmente tenuta al solo obbligo di segnalazione di operazioni sospette. Diverse attività investigative ne confermano tanto l'elevato rischio specifico quanto le elevate vulnerabilità e suggeriscono l'opportunità di una intensificazione dei presidi ...In particolare per i compro-oro è necessario intervenire normativamente per regolare il settore e per aumentare la consapevolezza del ruolo che svolgono sul mercato, anche prevedendo delle linee guida”.

¹⁰⁹⁷ La Corte costituzionale, con sentenza n. 121 del 1963 ha considerato come “usato” l'oggetto prezioso che, quale che siano la sua caratteristica fisica e il suo valore economico, sia stato rimesso in circolazione dopo che era pervenuto nelle mani di un privato a causa di un negozio, lecito o illecito, o di un rinvenimento o di un'attività criminosa.

rilevino la dimensione dell'esercizio professionale, la denominazione, né la circostanza che il commercio di preziosi usati sia prevalente o accessorio ad altre attività.

Il D.lgs. 92 si applica, pertanto, a tutti i soggetti che comunque esercitano il commercio di oro usato, compresi gli operatori professionali in oro, relativamente all'attività di compravendita o permuta dei preziosi usati. Si tratta di una disciplina improntata ai medesimi principi di trasparenza e tracciabilità su cui poggia il decreto antiriciclaggio, dal quale tuttavia si discosta prevedendo un regime semplificato, che considera la natura essenzialmente commerciale dell'attività di compro oro.

In sostanza, nei confronti degli operatori esercenti la compravendita di oro usato si prevede l'iscrizione in un apposito registro tenuto dall'Organismo degli agenti in attività finanziaria e dei mediatori creditizi (OAM)¹⁰⁹⁸ e l'applicazione di obblighi modulati in relazione alle peculiarità di tale categoria di soggetti e presidiati da specifiche sanzioni.

L'iscrizione nel registro dell'OAM è presupposto indispensabile per l'esercizio dell'attività di compro oro, essendo obbligatoria per qualsiasi operatore commerciale che, a prescindere dalla sua denominazione o svolgimento in via secondaria rispetto ad altre attività, eserciti la compravendita ovvero la permuta di oggetti preziosi usati¹⁰⁹⁹. Pertanto, all'obbligo d'iscrizione sono tenute anche le gioiellerie, nella misura in cui intendano compiere operazioni aventi ad oggetto la compravendita ovvero la permuta di oggetti preziosi usati. L'iscrizione è subordinata al possesso della licenza per l'attività in materia di oggetti preziosi di cui all'art. 127 del TULPS. Inoltre, il mancato versamento del contributo per l'iscrizione al registro è causa ostativa all'iscrizione.

Agli operatori compro oro gli obblighi antiriciclaggio si applicano con un regime peculiare. L'art. 4 del D.lgs. 92/2017 prevede, al posto dell'adeguata verifica del cliente, obblighi di identificazione, da effettuarsi prima del compimento della operazione secondo le modalità di cui agli artt. 18, comma 1, lett. a) e 19 comma 1, lett. a), del decreto antiriciclaggio. Una disposizione peculiare è contenuta nel comma 2 dell'art. 4, in base al quale le operazioni di importo pari o superiore a 500 euro sono effettuate unicamente attraverso l'utilizzo di mezzi di pagamento, diversi dal denaro contante, che garantiscano la tracciabilità dell'operazione e la sua univoca riconducibilità al disponente. In dette ipotesi, l'utilizzo di tali strumenti è obbligatorio, indipendentemente dal fatto che l'acquisto o la vendita dell'oggetto prezioso usato siano effettuati con un'unica operazione o con più operazioni frazionate¹¹⁰⁰.

In tema di tracciabilità, l'art. 5 stabilisce a carico degli operatori compro oro l'obbligo di utilizzare un conto corrente bancario o postale dedicato in via esclusiva alle transazioni finanziarie di compro oro e di predisporre, per ogni operazione, una scheda numerata progressivamente contenente tutti i dati necessari atti ad identificare il contraente, il mezzo di pagamento utilizzato e le caratteristiche del bene prezioso oggetto della transazione. È previsto il rilascio di una ricevuta al cliente per le operazioni effettuate.

Gli operatori adempiono agli obblighi di conservazione con modalità semplificate, idonee a garantire, comunque, l'accessibilità completa e tempestiva ai dati da parte delle Autorità competenti.

Il D.lgs. 92/2017 conferma gli obblighi di segnalazione di operazioni sospette già previsti a carico degli operatori in oro (professionali e non) dal previgente decreto antiriciclaggio. Fino all'entrata in vigore della riforma, peraltro, l'assolvimento degli obblighi di collaborazione attiva ha risentito della mancanza di disposizioni sull'identificazione e sulla conservazione dei dati, necessarie per consentire l'intercettazione di anomalie suscettibili di segnalazione. Tale vuoto normativo era stato in parte colmato

¹⁰⁹⁸ L'iscrizione al registro dell'OAM sarebbe auspicabile anche per gli OPO, per i quali è tuttora previsto l'elenco di cui all'art. 1, comma 3, della legge n. 7/2000, tenuto dalla Banca d'Italia a mero scopo di censimento, posto che l'Organo di vigilanza non ha competenze in materia di regolamentazione e supervisione nei confronti di tali operatori.

¹⁰⁹⁹ Per l'iscrizione nel registro, gli interessati inviano in formato elettronico all'OAM apposita istanza contenente i dati necessari alla identificazione del soggetto, come quelli anagrafici, quelli relativi al rappresentante legale e all'indirizzo della sede operativa. L'Organismo, effettuati i controlli, dispone l'iscrizione nel registro ed assegna un codice identificativo unico. Ogni variazione dei suddetti dati va comunicata all'OAM. Ai medesimi obblighi sono assoggettati gli operatori professionali in oro che intendano svolgere anche l'attività di compro oro; in tali casi, la comunicazione all'OAM va integrata con il codice operatore attribuito dalla Banca d'Italia. Con decreto del Ministro dell'Economia e delle finanze del 14 maggio 2018, emanato ai sensi dell'art. 3, comma 4, del d.lgs. 92/2017, sono state stabilite le modalità operative di invio dei dati e, in generale, di alimentazione del registro degli operatori compro oro.

¹¹⁰⁰ Ai sensi dell'art. 1, comma 1, lett. p) l'operazione frazionata è *“un'operazione unitaria sotto il profilo del valore economico, di importo pari o superiore ai limiti stabiliti dal presente decreto, posta in essere attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi ed in un circoscritto periodo di tempo fissato in sette giorni, ferma restando la sussistenza dell'operazione frazionata quando ricorrano elementi per ritenerla tale”*.

dal decreto del Ministero dell'Interno emanato il 17 febbraio 2011, su proposta della UIF, recante indicatori di anomalia volti ad agevolare la segnalazione di operazioni sospette da parte degli operatori non finanziari¹¹⁰¹; il provvedimento contiene, fra l'altro, specifici indicatori per gli operatori che commerciano oro e indicazioni sulla procedura segnaletica.

Il decreto precisa che l'obbligo di segnalazione delle operazioni sospette deve essere adempiuto secondo le disposizioni contenute nell'art. 35 del decreto antiriciclaggio; si applicano, in quanto compatibili, le disposizioni del Titolo II, Capo III, del decreto stesso. Per rendere più chiari gli adempimenti segnaletici posti a carico degli operatori compro oro, la UIF può adottare istruzioni ed emanare indicatori e schemi di anomalia, ai sensi dell'art. 6, comma 4, lett. d) ed e), del decreto antiriciclaggio.

Sul piano dell'*enforcement* il decreto prevede, oltre alla pena per il reato di abusivo esercizio dell'attività di compro oro¹¹⁰², sanzioni amministrative per l'inosservanza degli obblighi prescritti¹¹⁰³, delineando un sistema di controlli e un procedimento sanzionatorio posti in capo, rispettivamente, alla Guardia di Finanza e al Ministero dell'Economia e delle finanze¹¹⁰⁴. La prima è dotata anche del potere di richiedere al Ministero l'adozione di misure interdittive, a fronte di violazioni gravi o ripetute.

Il sistema prefigurato presenta margini di miglioramento, atteso che gli operatori compro oro, pur avendo ricevuto una disciplina di settore, continuano a non avere un'Autorità di riferimento per la produzione della regolamentazione secondaria e per lo svolgimento dei controlli. Non può sottacersi, infine, il mancato raggiungimento dell'obiettivo, previsto dalla legge di delega, di definire una normativa "organica" per il settore oro. Il decreto richiama, infatti, la legge n. 7 del 2000 e la normativa antiriciclaggio rivolte agli operatori professionali in oro, senza procedere a una revisione tesa a uniformare il regime degli obblighi e dei controlli applicabile a entrambe le categorie di operatori in oro.

9. Società di recupero crediti (C. Carrella e A. Greco)

Il D.lgs. 231/2007, nella formulazione aggiornata dal D.lgs. 90/2017 (art. 3, comma 5, lett. h), ha confermato la presenza, tra i soggetti obbligati della normativa antiriciclaggio degli operatori che svolgono attività di recupero stragiudiziale dei crediti per conto di terzi, in presenza della licenza di cui all'art. 115 TULPS, fuori dall'ipotesi di cui all'art 128-*quaterdecies* TUB¹¹⁰⁵.

Generalmente tali operatori, la cui attività è sottoposta al rilascio di licenza da parte delle articolazioni territoriali (Questure) del Ministero dell'Interno, pongono in essere tutte le attività propedeutiche al recupero del credito, in via diretta (contatto con il cliente o con il suo legale per rimodulare importi e tempistiche di pagamento) o per il tramite della collaborazione di professionisti del settore legale (es. azioni esecutive, iscrizioni a procedure concorsuali, etc.), sulla base di appositi contratti di mandato stipulati con il creditore.

¹¹⁰¹ A titolo esemplificativo, sono indici di anomalia in materia di oro: la richiesta di acquisto o vendita di beni di valore in contanti per importi molto rilevanti; l'acquisto o vendita di beni di valore ad un prezzo incoerente rispetto al profilo economico-finanziario del cliente; l'acquisto di beni per importi molto elevati da parte di una società che presenta un capitale sociale ridotto; l'acquisto o vendita di beni di valore senza disporre di adeguate informazioni sulle caratteristiche e sul valore degli stessi; l'acquisto o vendita di uno o più beni di valore in un ristretto arco di tempo, soprattutto se per importi complessivamente molto differenti; frequenti operazioni di acquisto o vendita di beni di valore in nome o a favore di terzi, quando i rapporti non appaiono giustificati.

¹¹⁰² Ai sensi dell'art. 8, chiunque svolge l'attività di compro oro, in assenza dell'iscrizione al registro degli operatori compro oro è punito con la reclusione da sei mesi a quattro anni e con la multa da 2.000 euro a 10.000 euro.

¹¹⁰³ Con specifico riferimento alla violazione dell'obbligo di segnalazione di operazioni sospette, l'art. 10 prevede, al comma 3, che *"agli operatori compro oro che omettono di effettuare la segnalazione di operazione sospetta ovvero la effettuano tardivamente, si applica la sanzione amministrativa pecuniaria da 5.000 euro a 50.000 euro"*. Nei casi di violazioni gravi o ripetute o sistematiche ovvero plurime, la predetta sanzione amministrativa pecuniaria è raddoppiata nel minimo e nel massimo edittali. Per le violazioni ritenute di minore gravità, la sanzione amministrativa pecuniaria può essere ridotta fino a un terzo.

¹¹⁰⁴ Al procedimento sanzionatorio si applica la legge 21 novembre 1981, n. 689.

¹¹⁰⁵ Si tratta di una categoria che era già stata inclusa tra i destinatari degli obblighi antiriciclaggio con il D.lgs. 374/1999, il quale all'art. 4, comma 1, richiamava *"gli obblighi di identificazione e di registrazione previsti nell'articolo 13, commi 1, 2, 3 e 4, del decreto-legge 15 dicembre 1979, n. 625, convertito, con modificazioni, dalla legge 6 febbraio 1980, n. 15, come sostituito dall'articolo 2 della legge n. 197/1991, e gli obblighi di segnalazione previsti dall'articolo 3, commi 1 e 2, della legge n. 197/1991"* e ne sanciva l'obbligatorietà anche per le attività di cui all'art. 1, comma 1, lett. a), del medesimo decreto.

Se inizialmente il *focus* degli operatori era incentrato principalmente su crediti di natura non finanziaria (es. utenze da *utilities*), nel corso del tempo la crescita dello stock di *non performing loans* (NPL) del settore bancario e le numerose operazioni di cartolarizzazione di tali *asset* hanno rappresentato un'importante opportunità di *business* per le società del settore. Nell'ambito delle operazioni di cartolarizzazione di crediti, infatti, è prassi che il *master servicer* – intermediario finanziario vigilato – assegni ad una o più società di recupero crediti il ruolo di *special servicer*, ovvero l'incarico di porre in essere tutte le attività necessarie al recupero dei crediti cartolarizzati, da cui poi dipenderà anche il rendimento delle *notes* emesse dal veicolo di cartolarizzazione.

I modelli di *business* del settore, inoltre, hanno subito un'evoluzione sostanziale a seguito del decreto del Ministero dell'Economia e delle finanze (MEF) n. 53 del 2 aprile 2015; tale provvedimento, infatti, all'art. 2, comma 2, lett. b), ha sancito che – a determinate condizioni¹¹⁰⁶ – l'acquisto a titolo definitivo di crediti effettuato dalle società titolari di licenza ex art. 115 TULPS non costituisce attività di concessione di finanziamenti. Pertanto, questa forma di acquisto dei crediti non è da considerarsi un'attività finanziaria riservata e chi la pone in essere non deve essere iscritto all'albo di cui all'art. 106 TUB. Ne è conseguito, quindi, che alcuni intermediari finanziari vigilati, specializzati nell'attività, hanno optato per la cancellazione dal rispettivo albo e la trasformazione in società di recupero crediti ex art. 115 TULPS, anche in ragione di una possibile riduzione degli oneri di compliance. Questi, invece di partecipare alle operazioni di cartolarizzazione, hanno intrapreso l'acquisto diretto dal sistema finanziario dei crediti *non performing* e modificato il proprio *business model*, non più basato sulla percezione di *fees*, ma sul differenziale tra prezzo di acquisto – solitamente inferiore al valore nominale del credito – e l'importo incassato al termine delle attività di recupero.

Tenuto conto del quadro descritto, è verosimile che la scelta legislativa di ricomprendere le società di recupero crediti tra i soggetti obbligati della normativa antiriciclaggio risponda all'esigenza di istituire un presidio che ostacoli il riciclaggio di somme di origine illecita; appare infatti evidente il potenziale vantaggio, in particolare da parte delle organizzazioni criminali più strutturate e dotate di adeguati capitali, di acquisire vari tipi di *asset* (immobili, aziende, etc.) a prezzi vantaggiosi rispetto a quelli di mercato.

Al maggior coinvolgimento di tali operatori nella lotta al riciclaggio, non ha fatto seguito un'adeguata produzione di normativa secondaria, che aiutasse gli operatori a calare gli obblighi antiriciclaggio previsti dalla normativa primaria nel loro specifico settore di attività.

L'unico provvedimento di normativa secondaria di settore è il decreto del Ministero dell'Interno del 17/02/2011, con il quale, su proposta della UIF, sono stati emanati gli indicatori di anomalia per l'individuazione delle operazioni sospette destinati agli operatori non finanziari e, tra questi, anche alle società di recupero crediti.

In assenza di una normativa antiriciclaggio specifica, un ruolo preminente ha assunto le iniziative di autoregolamentazione assunte da associazioni di categoria del settore¹¹⁰⁷.

Un esempio è rappresentato dall'interazione intercorsa tra le predette associazioni e il MEF che, nel 2008, ha portato a chiarire la nozione di cliente per gli operatori in questione. Attraverso il parere ministeriale, infatti, si è appurato che, ai fini della normativa antiriciclaggio, il cliente delle società di recupero crediti è identificato sia nel creditore, ovvero colui che conferisce il mandato alla società, sia nel debitore-escusso e/o il terzo soggetto che eventualmente esegua il pagamento per suo conto. Peraltro, le linee guida dell'associazione di categoria stabiliscono che l'adeguata verifica venga effettuata quando la società di recupero crediti instaura un rapporto continuativo, circostanza che certamente si realizza in caso di conferimento di un incarico da parte di un committente. Le relazioni che intercorrono tra la società di recupero crediti e il debitore (e/o l'eventuale terzo pagatore) vengono ricondotte alla categoria delle operazioni occasionali, per le quali l'adeguata verifica è prevista per le transazioni di importo pari o superiore a 15.000 euro; inoltre, viene chiarito che *“in questo caso il presupposto oggettivo si configura se l'impresa di recupero ha un ruolo nella trasmissione o movimentazione dei mezzi di pagamento: il pagamento effettuato dal cliente a mezzo bonifico sui conti corrente della committente non integra il presupposto oggettivo in parola”*.

Ne deriva, quindi, che le società di recupero crediti sarebbero tenute ad adempiere agli obblighi di adeguata verifica soltanto nei seguenti casi: incasso diretto sui propri conti, indipendentemente dallo strumento, delle somme pagate dai debitori (e/o da terzi pagatori) e successiva trasmissione dei fondi al mandante; ricezione delle somme pagate dal debitore (e/o da terzi pagatori) attraverso strumenti diversi dai bonifici, ad esempio tramite assegni bancari/circolari intestati al mandante, e successivo trasferimento fisico dei titoli a quest'ultimo.

L'implementazione di tale approccio, evidentemente volto a limitare le responsabilità giuridiche degli operatori e a ridurre gli oneri operativi, sembra porsi in contrasto con la ratio della normativa primaria e va a depotenziare

¹¹⁰⁶ In particolare, le condizioni previste sono: 1) i crediti sono acquistati a fini di recupero e sono ceduti da: a) banche o altri intermediari finanziari sottoposti alla vigilanza della Banca d'Italia, i quali li hanno classificati in sofferenza, ovvero b) soggetti diversi da quelli indicati al punto i), purché si tratti di crediti vantati nei confronti di debitori che versano in stato di insolvenza, anche non accertato giudizialmente, o in situazioni sostanzialmente equiparabili, secondo quanto accertato dai competenti organi sociali; non rileva, a tal fine, l'esistenza di garanzie reali o personali; 2) i finanziamenti ricevuti da terzi dalla società acquirente non superano l'ammontare complessivo del patrimonio netto; 3) il recupero dei crediti acquistati avviene senza la stipula di nuovi contratti di finanziamento con i debitori ceduti, la novazione di quelli in essere, la modifica delle condizioni contrattuali; non rilevano a tali fini l'estinzione anticipata e la posticipazione dei termini di pagamento.

¹¹⁰⁷ Cfr: Guida all'Antiriciclaggio di UNIREC – Unione Nazionale Imprese a Tutela del Credito.

significativamente i presidi antiriciclaggio, specie nell'ipotesi in cui il mandante (creditore) non sia un soggetto obbligato, come nel caso di una *large corporate* di matrice industriale.

Inoltre, il portato della predetta auto-regolamentazione sui presidi antiriciclaggio risulterebbe limitato nel caso in cui il mandante sia un soggetto a sua volta destinatario degli obblighi antiriciclaggio, ad esempio un *master servicer* di un'operazione di cartolarizzazione. L'impatto dal punto di vista della riduzione degli obblighi operativi, in tali casi, potrebbe essere solo di natura formale: infatti, la società di recupero crediti, essendo l'unico soggetto che entra in relazione con il cliente (debitore/terzo pagatore), sarà verosimilmente tenuta, sulla base di specifici obblighi contrattuali, a effettuare una serie di attività (es. somministrazione del questionario di adeguata verifica al cliente, rilevazione di comportamenti anomali, etc.) propedeutiche al perfezionamento degli obblighi antiriciclaggio da parte del *master servicer* e indipendenti dallo strumento di pagamento utilizzato dal cliente.

Ulteriori criticità riguardanti l'applicazione dell'adeguata verifica si riscontrano anche nei rapporti che le società di recupero crediti intrattengono con professionisti (avvocati o studi legali) che curano tutte le attività di carattere legale necessarie al recupero della posizione creditizia (decreto ingiuntivo, pignoramento, iscrizione allo stato passivo di procedure concorsuali etc.).

A tal riguardo, la normativa primaria qualifica i professionisti legali come soggetti obbligati solo nel corso dello svolgimento delle operazioni tassativamente elencate dall'art. 3 comma 4 lett. c) D.lgs. 231/2007, fra le quali non è riportata l'attività di recupero crediti. Nello stesso senso, le Regole Tecniche approvate dal Consiglio Nazionale Forense il 20 settembre 2019, sebbene non escludano esplicitamente dall'applicazione degli obblighi AML l'attività di recupero crediti, contengono una clausola di chiusura stante la quale è esclusa "ogni altra operazione, atto o negozio non espressamente riconducibile all'elencazione tassativa di cui all'art. 3, comma 4, lett. c), del decreto"¹¹⁰⁸. Ne deriva, quindi, che per tali professionisti l'adempimento degli obblighi di adeguata verifica per gli incarichi della specie non sembrerebbe derivare dalla normativa primaria, ma sarebbe rimesso alle specifiche clausole contenute negli accordi contrattuali sottoscritti con la società di recupero crediti mandante.

Sotto il profilo antiriciclaggio risultano altrettanto critici i rapporti che le società di recupero crediti intrattengono con i professionisti che ricoprono incarichi nell'ambito di procedure concorsuali e con quelle di esecuzione immobiliare. In tale contesto, gli ordini professionali hanno espresso una sensibilità diversa, anche legata alla diversa formulazione della normativa primaria.

Infatti, l'art. 3 comma 4 lett. a), del D.lgs. 231/2007 include tra i soggetti obbligati "i soggetti iscritti nell'albo dei dottori commercialisti", senza ulteriori distinzioni relative al tipo di attività svolta, di talché tali professionisti sono tenuti all'adempimento degli obblighi AML anche nell'ambito delle sopramenzionate procedure. In materia, le linee guida pubblicate dal CNDEC¹¹⁰⁹ classificano tali attività a "rischio non significativo", in ragione del controllo costante dell'Autorità Giudiziaria cui sono sottoposte. Sono fatte salve le "particolari situazioni", nelle quali cioè è opportuno rafforzare i presidi antiriciclaggio in considerazione di eventuali più marcati elementi di sospetto.

Al contrario, i professionisti legali sono chiamati all'adempimento degli obblighi antiriciclaggio solo in presenza delle attività tassativamente elencate dall'art. 3, comma 4, lett. c), del medesimo decreto, elencazione nella quale non sono contenute le attività compiute nell'ambito di procedure concorsuali e di esecuzione immobiliare¹¹¹⁰. Pertanto, qualora la società di recupero crediti incassi somme di denaro rivenienti da procedure esecutive, la stessa si troverà di fronte a situazioni diverse a seconda del tipo di professionista incaricato dal Tribunale.

L'attività svolta dalle società di recupero crediti, inoltre, comporta delle specificità anche nell'applicazione degli obblighi di conservazione previsti dalla normativa primaria. Nella prassi, gli operatori del settore intrattengono relazioni contrattuali, circoscritte nel tempo, anche contemporaneamente con una pluralità di mandanti. Alla scadenza del mandato, tuttavia, può generarsi una contrapposizione di interessi tra la mandante - titolare dei dati sensibili sulle pratiche gestite - e la società di recupero crediti, che ha comunque l'obbligo di conservare tali dati per 10 anni a fini antiriciclaggio, in particolare per facilitare le verifiche da parte delle Autorità competenti. Ne deriva la necessità di prevedere apposite disposizioni contrattuali che permettano agli operatori del settore di

¹¹⁰⁸ Tale conclusione è peraltro avallata dalle precedenti linee guida del CNF del 14 luglio 2017, le quali, richiamando il Provvedimento UIC del 24 febbraio 2006 per i professionisti, rappresentano che l'attività professionale di recupero crediti è esclusa dall'applicazione degli obblighi antiriciclaggio.

¹¹⁰⁹ Linee Guida CNDEC del 20 maggio 2019.

¹¹¹⁰ Esclusione confermata dalle sopramenzionate regole tecniche del 20 settembre 2019.

continuare ad avere accesso a tali dati, specie nei casi in cui il sistema di conservazione utilizzato sia di esclusiva proprietà della mandante.

Le considerazioni sopra effettuate, ovviamente, si ripercuotono anche sulla collaborazione attiva delle società di recupero crediti. I limiti che gli operatori incontrano in sede di adeguata verifica (vuoi per la loro auto-regolamentazione, vuoi per le specificità della loro attività) impattano naturalmente anche sulla capacità di intercettare di operazioni sospette. Va infatti considerato che i principali indicatori di anomalia, enucleati come detto dal decreto del Ministero dell'Interno del 2011, riguardano principalmente il profilo soggettivo del debitore e/o del terzo pagatore e l'origine dei fondi utilizzati per il pagamento del debito. Ne deriva che l'efficacia della collaborazione attiva in questo settore non può che basarsi su un costante e regolamentato flusso informativo lungo tutta la catena dei soggetti coinvolti, realizzabile soltanto attraverso adeguati accordi contrattuali conclusi con il *master servicer* da un lato e con i vari collaboratori professionali dall'altro.

10. Operatori non finanziari gestori del contante (C. Ciccolo e F. D'Urzo)

Dall'introduzione della moneta unica nel 2002, obiettivo dell'Eurosistema, oltre a quello di garantire un'offerta di banconote regolare ed efficiente, è assicurare l'integrità e il buono stato delle banconote in circolazione. Il perseguimento di tale finalità è rimesso a livello nazionale, oltre che alle singole Banche Centrali, ai c.d. gestori del contante, soggetti che partecipano alla gestione e alla distribuzione al pubblico delle banconote. Nella realtà italiana i gestori del contante, cui oggi fa capo circa l'80% dell'attività di ricircolo delle banconote, sono le banche, Poste Italiane e gli operatori non finanziari¹¹¹¹ iscritti in un elenco tenuto dalla Banca d'Italia¹¹¹² e da quest'ultima vigilati a fini antiriciclaggio¹¹¹³.

Gli operatori non finanziari gestori del contante costituiscono un sottoinsieme della macro-categoria degli soggetti che esercitano l'attività di custodia e trasporto di denaro contante in presenza della licenza di cui all'art 134 TULPS¹¹¹⁴, soggetti obbligati al rispetto della normativa antiriciclaggio a partire dal 2007 per un'espressa scelta operata dal Legislatore italiano, pur non essendo contemplati tra i destinatari degli obblighi dalla direttiva UE/2015/849 (quarta direttiva)¹¹¹⁵.

In Italia l'attività degli operatori consiste in concreto nel ritirare quotidianamente per conto degli intermediari, che abbiano esternalizzato il trattamento del contante, le banconote incassate dai punti vendita della grande distribuzione organizzata (GDO) e quelle introitate dalle proprie filiali, al fine di sottoporle alle verifiche di autenticità e idoneità preordinate alla loro reimmersione in circolazione. Nella prospettiva dell'antiriciclaggio, l'attività di *cash management*, svolta nel territorio per il settore bancario, consente a tali soggetti di disporre di un patrimonio informativo qualificato in termini di conoscenza e movimentazione dei flussi di denaro contante.

Il mercato italiano si caratterizza per la presenza di numerosi operatori non finanziari gestori del contante, molti dei quali di dimensioni estremamente ridotte e con assetti organizzativi semplificati, anche in considerazione della circostanza che non è richiesta una specifica forma giuridica e, pertanto, l'attività può essere svolta anche in forma di società a responsabilità limitata o di società di persone. Ciò costituisce un *unicum* nel panorama europeo, nel quale operano, invece, poche società di grandi dimensioni, generalmente multinazionali.

Il D.lgs. 90/2017, nel riscrivere interamente il D.lgs. 231/2007, ha attribuito alla Banca d'Italia la qualifica di Autorità di vigilanza di settore nei confronti degli operatori non finanziari gestori del contante, limitatamente al trattamento delle banconote in euro; sono stati quindi conferiti poteri normativi, di controllo e sanzionatori, meglio precisati con il D.lgs. 125/2019. Tali poteri si sono affiancati a quelli di

¹¹¹¹ Ai sensi dell'art. 6 del regolamento CE n. 1338/2001, possono essere gestori del contante anche gli istituti di pagamento, gli istituti di moneta elettronica e gli altri operatori economici, quali i commercianti e i casinò, che partecipano a titolo accessorio alla gestione e alla distribuzione al pubblico di banconote.

¹¹¹² Art. 8, comma 2-*bis*, del DL n. 350/2001.

¹¹¹³ Artt. 1, comma 2, lett. c) e 7, del D.lgs. 231/2007.

¹¹¹⁴ Art. 1, comma 5, lett. f), del D.lgs. 231/2007.

¹¹¹⁵ Anche nella bozza di regolamento contenuta nel c.d. "AML Package" le società di trasporto contante non figurano tra i soggetti obbligati.

derivazione comunitaria in materia di trattamento delle banconote già esercitati nei confronti di tutti i gestori del contante.

Nel complesso, le disposizioni applicabili agli operatori non contengono particolari elementi di specificità rispetto a quelle riferibili agli altri soggetti obbligati vigilati dalle rispettive Autorità di settore. Meritano alcune riflessioni l'art. 9, in materia di poteri della Guardia di Finanza e l'art. 62, in materia di sanzioni. L'art. 9, comma 1, attribuisce al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza poteri di controllo su tutti i soggetti obbligati non vigilati dalle Autorità di settore, tra i quali sono da ricomprendere anche i soggetti in possesso della licenza di cui all'art. 134 T.U.L.P.S. per le attività di trasporto e custodia di contante. Sui medesimi soggetti la Banca d'Italia ha competenza esclusiva con riguardo all'attività di trattamento delle banconote, in quanto Autorità di vigilanza di settore. Viene pertanto a definirsi un riparto di competenze tra le due Istituzioni "*ratione materiae*", reso ancora più articolato poiché il comma 2 dello stesso art. 9 prevede che il Nucleo possa eseguire, previa intesa con le Autorità di vigilanza di settore, controlli su alcuni soggetti vigilati tra i quali rientrano, per l'attività di trattamento delle banconote, i predetti operatori¹¹¹⁶.

L'assetto di controlli delineato dalla normativa postula una costante esigenza di coordinamento tra le due Autorità, anche nell'ottica di evitare eccessivi aggravii per gli operatori, tra l'altro soggetti anche ai controlli del Ministero dell'Interno per l'osservanza delle disposizioni di Pubblica Sicurezza¹¹¹⁷. In tale prospettiva, nel nuovo Protocollo di intesa, sottoscritto tra la Banca d'Italia e la Guardia di Finanza al fine di rafforzare su un piano generale i rapporti di collaborazione tra le due Istituzioni, sono state inserite disposizioni specifiche relative ai gestori del contante, sia con riferimento alla materia dell'antiriciclaggio che a quella del trattamento delle banconote¹¹¹⁸.

In materia di sanzioni, nell'art. 62, che detta disposizioni specifiche per i soggetti obbligati vigilati, è presente uno specifico comma (7-*bis*) dedicato agli operatori non finanziari gestori del contante. L'impianto sanzionatorio, nella sostanza allineato a quello previsto per gli intermediari bancari e finanziari, presenta tuttavia alcune particolarità.

Sul piano dell'applicabilità delle sanzioni, diversamente da quanto previsto per gli intermediari, la potestà sanzionatoria della Banca d'Italia non è necessariamente subordinata alla sussistenza di violazioni gravi, ripetute, sistematiche o plurime (c.d. qualificate). Anche sotto il profilo della determinazione delle sanzioni irrogabili sono presenti alcune differenze. Mentre per gli intermediari bancari e finanziari l'art. 62 definisce gli stessi importi minimi e massimi per tutte le violazioni delle disposizioni previste dal decreto e delle disposizioni di attuazione, per gli operatori non finanziari gestori del contante esiste un doppio binario: per le violazioni in materia di adeguata verifica, conservazione dei dati e segnalazione di operazioni sospette, si applicano i minimi e i massimi previsti dagli artt. 56, 57 e 58 (peraltro diversi tra loro); per l'inosservanza delle disposizioni emanate dalla Banca d'Italia in materia di organizzazione, procedure e controlli interni, il comma 7-*bis* prevede minimi e massimi specifici, aumentabili in caso di violazioni qualificate.

Infine, il quadro sanzionatorio previsto per gli operatori non finanziari gestori del contante si caratterizza complessivamente per una minore afflittività rispetto a quello delineato per gli intermediari, in ragione delle caratteristiche dimensionali e operative di tali soggetti. Ciò in quanto gli importi sono significativamente più contenuti, non sono previste le sanzioni accessorie del *cease and desist order* e della dichiarazione pubblica avente a oggetto la violazione commessa e il soggetto responsabile e, con riferimento alla responsabilità delle persone fisiche, è prevista la sanzionabilità a cura del Ministero dell'Economia e delle finanze solo per l'omessa segnalazione di operazioni sospette.

Nonostante l'impianto sanzionatorio presenti delle tipicità rispetto a quello delineato per gli intermediari, i due sistemi risultano pienamente allineati sotto il profilo procedimentale. Per espressa previsione dell'art. 65, comma 11, infatti, ai procedimenti per le sanzioni nei confronti degli operatori non finanziari gestori del contante, si applicano le disposizioni dell'art. 145 del Testo Unico Bancario.

Ai sensi dell'art. 7, comma 1, lett. a), del D.lgs. 231/2001, le Autorità di vigilanza di settore adottano nei confronti dei soggetti rispettivamente vigilati disposizioni in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela. A tal proposito la Banca d'Italia, quale Autorità di vigilanza nei confronti degli operatori non finanziari gestori del contante limitatamente all'attività di trattamento delle banconote in euro, ha emanato, rispettivamente, il Provvedimento del 23 aprile 2019 e il Provvedimento del 4 febbraio 2020. Le disposizioni, pertanto, non trovano applicazione ai settori del trasporto e della custodia del contante, attività tipicamente svolte dagli operatori insieme al trattamento, in quanto non rientranti nelle attribuzioni della Banca d'Italia.

¹¹¹⁶ Art. 9, comma 2, lett. h), del D.lgs. 231/2007.

¹¹¹⁷ In proposito, nel 2021 è stato sottoscritto un accordo per disciplinare l'interscambio informativo tra la Banca d'Italia e il Ministero dell'Interno.

¹¹¹⁸ Ai sensi dell'art. 8, comma 7, del decreto-legge n. 350 del 2001, la Banca d'Italia può avvalersi della Guardia di Finanza per gli accertamenti in materia di trattamento delle banconote.

I Provvedimenti, ispirati ai principi di proporzionalità e approccio basato sul rischio, si pongono in linea di continuità con le analoghe disposizioni dettate dalla Banca d'Italia per gli intermediari bancari e finanziari, salve alcune peculiarità legate, anche in questo caso, alle caratteristiche dimensionali e operative dei destinatari.

Le disposizioni contenute nel Provvedimento del 23 aprile 2019 presentano carattere di assoluta novità per gli operatori i quali, pur essendo soggetti obbligati sin dal 2007, non erano tenuti fino ad allora a dotarsi di un assetto organizzativo finalizzato a prevenire il rischio di coinvolgimento in fatti di riciclaggio.

Con riferimento al *management* aziendale, in relazione alle contenute dimensioni aziendali, gli operatori non sono tenuti a istituire un organo di supervisione strategica, le cui attribuzioni sono confluite tra i compiti dell'organo di gestione¹¹¹⁹. Inoltre, considerato che tra gli operatori figurano, oltre a società per azioni, anche società a responsabilità limitata e società di persone, nell'assetto organizzativo antiriciclaggio non è obbligatoriamente presente l'organo di controllo; in tal caso, non vi sarà una specifica struttura aziendale con il compito di vigilare sul rispetto della normativa primaria e secondaria in materia antiriciclaggio. Nel caso in cui, invece, sia presente l'organo di controllo, è stato consentito allo stesso di avvalersi per l'espletamento delle proprie funzioni dell'organismo di vigilanza di cui al D.lgs. 231/2001¹¹²⁰, organo che vigila sulla responsabilità degli enti nell'ambito dell'attività di prevenzione del rischio dei reati che la società potrebbe commettere in relazione al tipo di attività svolta.

Analogamente a quanto disposto per gli intermediari bancari e finanziari, nella struttura organizzativa antiriciclaggio degli operatori, è prevista l'istituzione della Funzione antiriciclaggio, fulcro della *compliance* normativa in materia AML, e del Responsabile per la segnalazione di operazioni sospette.

Nel Provvedimento è altresì disciplinata la figura del Responsabile per le segnalazioni periodiche antiriciclaggio, in quanto la Banca d'Italia si è avvalsa della facoltà prevista dall'art. 7, comma 2, lett. b), del D.lgs. 231/2007 di richiedere agli operatori l'invio di segnalazioni rilevanti per finalità di prevenzione del riciclaggio. Tale soggetto ha il compito di vigilare sulla correttezza dei dati trasmessi, che hanno a oggetto essenzialmente informazioni sui flussi di banconote ritirate e somministrate presso dipendenze bancarie (anche con riferimento ai *cash dispenser*), sulle sale conta, nonché sui punti serviti della grande distribuzione organizzata.

Opzioni di semplificazione sono previste per gli operatori di minori dimensioni e complessità operativa, ossia quelli che trattano annualmente un numero di banconote inferiore a cento milioni e, al contempo, operano con un numero di sale conta inferiore a quattro. Tali soggetti possono conferire l'incarico di Responsabile della funzione antiriciclaggio e di Responsabile delle segnalazioni periodiche a un componente dell'organo di gestione, purché privo di deleghe operative. Nelle imprese individuali, l'incarico di Responsabile delle segnalazioni periodiche può essere ricoperto anche dal titolare dell'impresa. Inoltre, tali operatori possono non istituire la Funzione di revisione interna ed è consentito loro di effettuare la valutazione della propria esposizione al rischio e l'esame del regolamento antiriciclaggio con periodicità biennale, anziché annuale.

Le disposizioni in materia di adeguata verifica della clientela dettate dal Provvedimento del 4 febbraio 2020 ricalcano nella sostanza le analoghe disposizioni per gli intermediari bancari e finanziari, ma sono calibrate sull'attività intrinsecamente *cash intensive* di trattamento del contante. Di rilievo è la previsione di specifici fattori di rischio, legati ad anomalie che possono verificarsi nella gestione del contante, che gli operatori possono valutare ai fini dell'applicazione delle misure rafforzate di adeguata verifica. Si tratta di operazioni caratterizzate dalla presenza di una quantità ingiustificata di banconote di taglio apicale fra quelle oggetto del trattamento e di banconote introdotte in Italia dall'estero dal cliente per un importo complessivo pari o superiore a 10.000 euro.

Elemento di assoluta novità, legato allo schema operativo maggiormente utilizzato dagli operatori, è la previsione del c.d. "soggetto servito", figura non contemplata per la sua peculiarità dal decreto antiriciclaggio, a cui sono dedicate disposizioni specifiche finalizzate a dare maggiore efficacia al complesso dei presidi antiriciclaggio¹¹²¹. In concreto, tipicamente gli operatori stipulano con la banca (cliente) un contratto per il trattamento del contante, che prevede che le operazioni di ritiro e consegna delle banconote siano effettuate presso un soggetto terzo (soggetto servito), di norma la grande distribuzione organizzata, cliente della banca.

Sulla base di tale schema, ai sensi delle disposizioni di legge, la banca è tenuta a eseguire l'adeguata verifica nei confronti del proprio cliente (la GDO), ivi incluso il controllo costante sull'operatività dello

¹¹¹⁹ Art. 15, comma 1, del Provvedimento della Banca d'Italia del 23 aprile 2019.

¹¹²⁰ Art. 16, comma 2, del Provvedimento della Banca d'Italia del 23 aprile 2019.

¹¹²¹ Parte prima, par. 4 e Parte seconda, par. 7.

stesso; gli operatori, a loro volta, sono tenuti ad adempiere gli obblighi di adeguata verifica nei confronti del loro cliente (la banca) e ad acquisire attraverso quest'ultimo un *set* minimo di informazioni sul soggetto servito¹¹²². Tali informazioni sono essenziali ai fini del monitoraggio del soggetto servito e per il corretto assolvimento degli obblighi di segnalazione di operazioni sospette da parte degli operatori. Ciò in quanto questi ultimi, eseguendo materialmente il ritiro e la consegna delle banconote, sono correntemente in possesso di informazioni di dettaglio sull'operatività del soggetto servito, non direttamente e immediatamente note alla banca, utili per cogliere tempestivamente eventuali profili di anomalia (ad esempio, un improvviso incremento di banconote di taglio apicale).

Le informazioni possono inoltre consentire agli operatori di rilevare incoerenze o illogicità nella profilatura della banca cliente, determinandone la modifica del livello di rischio. In alcuni casi, la condivisione delle informazioni con la banca può inoltre portare quest'ultima ad attivare misure rafforzate di adeguata verifica nei confronti della GDO sua cliente¹¹²³.

11. Case d'asta e antiquari (C. Oriolo)

Il settore dell'arte è generalmente considerato uno dei veicoli idonei a riciclare proventi illeciti o per finanziare il terrorismo per una molteplicità di ragioni quali, la presenza di beni di elevato valore, il carattere internazionale del mercato, l'uso frequente di intermediari e rappresentanti o di strutture *offshore* che facilitano l'anonimato, la facilità di accesso al mercato (anche online), l'elevata soggettività e volatilità del prezzo delle opere d'arte. Quest'ultima peculiarità, infatti, può giustificare oscillazioni di prezzi anche elevate e repentine e si presta ad essere strumentalizzata da chi nasconde dietro l'acquisto di un'opera d'arte finalità criminali di "ripulitura" di proventi illeciti. Da non sottovalutare poi la "cultura della discrezione", in un settore dove, di solito, l'acquirente e il venditore sono sconosciuti l'uno all'altro.

Inoltre, si tratta di un settore per molti aspetti ancora non regolamentato e, proprio per questo, vulnerabile nonché caratterizzato sia dalla presenza di numerosi operatori di piccole dimensioni sia da un volume significativo di transazioni private connotate da spiccata riservatezza e dal possibile ricorso al contante, tipicamente idoneo a favorire anonimato e scarsa tracciabilità. Le opere d'arte, inoltre, sono qualificabili come beni rifugio, non soggetti a svalutazione col passare del tempo, che potrebbero essere utilizzati come mezzo di pagamento non tracciato o per occultare capitali di provenienza illecita.

Consapevole di tali rischi, il legislatore nazionale¹¹²⁴, anticipando quello europeo, ha esteso a questo mercato l'applicazione degli obblighi di identificazione e registrazione¹¹²⁵.

Il D.lgs. 56/2004¹¹²⁶ ha imposto in capo ai soggetti che esercitano il commercio di cose antiche¹¹²⁷, alle case d'asta e gallerie d'arte¹¹²⁸, l'adempimento degli obblighi di identificazione della clientela, conservazione dei dati e segnalazione delle operazioni sospette. Successivamente, il D.lgs. 231/2007, di recepimento della terza direttiva, confermava l'obbligo di collaborazione attiva in capo ai medesimi operatori, ma escludeva gli obblighi di identificazione e registrazione¹¹²⁹. Con la quarta direttiva sono stati ripristinati tutti gli obblighi AML in capo agli operatori del settore e con la quinta direttiva è stata ampliata e precisata più nel dettaglio la platea dei destinatari degli obblighi normativi. Ovviamente, queste

¹¹²² Si tratta dei dati identificativi, della prevalente attività e dell'area geografica di residenza/sede del soggetto servito.

¹¹²³ Le disposizioni di vigilanza per gli intermediari in materia di adeguata verifica rafforzata prevedono che – al fine di valutare la coerenza della complessiva movimentazione effettuata sul rapporto con l'attività svolta dal cliente e con il fatturato aziendale – le banche verificano che la società di trasporto valori "sia in grado di fornire, a richiesta, i dati identificativi sui soggetti presso i quali il contante è stato ritirato o consegnato, nonché sulla località di ritiro o di consegna delle somme, sull'importo delle somme ritirate o consegnate e sul taglio delle banconote" (Provvedimento del 30 luglio 2019, Parte Quarta).

¹¹²⁴ D.lgs. 25 settembre 1999, n. 374.

¹¹²⁵ Cfr. art. 1, comma 1, lett. e), f), h) e art. 4, comma 2, del D.lgs. 25 settembre 1999, n. 374.

¹¹²⁶ Cfr. art. 2, comma 1, lett. q), del decreto richiamato.

¹¹²⁷ Tenuti alla dichiarazione preventiva di cui all'art. 126 del TULPS.

¹¹²⁸ In possesso della licenza di cui all'art. 115 del TULPS.

¹¹²⁹ Cfr. art. 10, comma 2, del decreto richiamato.

oscillazioni regolamentari in una fase di prima applicazione non hanno giovato alla effettiva comprensione degli obblighi e alla applicazione omogenea ed efficace degli stessi.

In particolare, sono stati inseriti nel novero dei soggetti obbligati, come “operatori non finanziari”, tutti coloro che esercitano attività di commercio di cose antiche, il commercio di opere d’arte o che agiscono in qualità di intermediari nel commercio delle medesime opere, anche quando tale attività è effettuata da gallerie d’arte o case d’asta, che conservano o commerciano opere d’arte ovvero che agiscono da intermediari nel commercio delle stesse, qualora tale attività sia effettuata all’interno di porti franchi. È stato poi specificato che tali soggetti sono tenuti ad adempiere agli obblighi antiriciclaggio qualora il valore dell’operazione, anche se frazionata, o di operazioni collegate sia pari o superiore a 10.000 euro¹¹³⁰.

Gli operatori che ricadono nelle anzidette categorie devono svolgere un’adeguata verifica della clientela, fermo restando l’obbligo di astensione di cui all’art. 42 del decreto AML; adempiere all’obbligo di conservazione dei dati e della documentazione acquisita per un periodo di 10 anni; segnalare le operazioni sospette di riciclaggio o finanziamento del terrorismo alla UIF, osservando il divieto di comunicazione di cui all’art. 39, comma 1, del decreto e adottando tutte le misure idonee ad assicurare la riservatezza dell’identità del segnalante; svolgere un’autovalutazione dei rischi cui sono esposti; adottare procedure operative proporzionate ai propri rischi, alla natura dell’attività svolta e alle proprie dimensioni, volte a mitigare e gestire i relativi rischi; implementare corsi di formazione interni AML/CFT.

I medesimi operatori devono, ovviamente, aver riguardo anche a quanto previsto dal Titolo III del decreto AML in tema di limitazioni all’uso del contante, divieto di utilizzo di conti o libretti di risparmio in forma anonima o con intestazione fittizia e di prodotti di moneta elettronica anonimi, con il relativo obbligo di comunicazione al MEF. Adeguarsi ai predetti obblighi può evitare il coinvolgimento in attività di riciclaggio o finanziamento del terrorismo con evidenti ripercussioni di natura reputazionale, oltre che sanzionatorie. La categoria in esame risente, tuttavia, della mancanza di disposizioni secondarie in materia e di un’Autorità di vigilanza appositamente designata incaricata della regolamentazione AML/CFT dei partecipanti al mercato dell’arte.

Le compravendite *online* di arte da un lato, e la criptoarte o “NFT artwork”¹¹³¹ dall’altro, sono fenomeni ormai in larga diffusione. L’accelerazione della digitalizzazione dell’offerta di beni artistico-culturali è uno dei risvolti positivi della pandemia, poiché fino al periodo pre-Covid le piattaforme digitali erano state implementate soltanto da una quota limitata di operatori di medie-grandi dimensioni. Le piattaforme virtuali, da un lato, hanno favorito una crescita dei livelli di trasparenza e consapevolezza del mercato dell’arte, dato l’improvviso aumento nella disponibilità di informazioni sui prezzi delle opere; dall’altro, si sono rivelate solo parzialmente in grado di sostenere il mercato, data l’impossibilità di prendere parte fisicamente ai principali appuntamenti dedicati all’arte e ai beni da collezione¹¹³².

In merito agli NFT, questi presentano vulnerabilità specifiche rispetto al mercato dell’arte tradizionale, come la facilità nel trasferimento di proprietà che può avvenire istantaneamente, senza confini geografici e senza sostenere eventuali costi di spedizione o conservazione, necessari per la compravendita di un oggetto fisico. Ai fini del perfezionamento della cessione, anche nell’ottica del trasferimento della proprietà del NFT e dei relativi rischi, deve considerarsi valido il momento in cui il NFT viene trasferito all’interno del portafoglio digitale indicato dall’acquirente¹¹³³. Peraltro, per gli NFT non dovrebbe presentarsi il problema del certificato di autenticità, vale a dire quel documento che attesta che un’opera proviene da un determinato autore.

Il tema delle autentiche, infatti, è uno degli aspetti più delicati del mercato dell’arte: in assenza di regole precise, generalmente, alla morte dell’artista, l’autenticazione delle sue opere è rimessa ai suoi discendenti, i quali, però, possono avere interesse a riconoscere come autentiche opere che in realtà non lo sono o a negare la paternità di opere autentiche, al solo fine di far crescere il valore di mercato di quelle esistenti e che sono in loro possesso; inoltre, anche per gli esperti, non sempre è

¹¹³⁰ Cfr. art. 3, comma 5, lett. b) e c), del D.lgs. 231/2007.

¹¹³¹ Ossia token digitali che rappresentano un’opera d’arte digitale.

¹¹³² Il numero delle aste realizzate nel corso del 2020 grazie alle vendite online ha conosciuto un incremento del 204,8%. L’online si è confermato efficace prevalentemente per la compravendita di lotti di basso-medio valore, mentre risulta ancora limitante nella vendita di lotti di valore medio-alto. Cfr. *Il mercato dell’arte e dei beni da collezione, Speciale Lo stato dell’arte ai tempi del Covid-19*, Report 2021, Deloitte Private, p. 5-6.

¹¹³³ Successivamente, il detentore diventa responsabile dell’adozione di misure ragionevoli per proteggere il wallet, ovvero ogni altro dispositivo di storage impiegato per conservare il token, compresa la custodia delle chiavi private o altre credenziali necessarie per accedere a tali meccanismi di archiviazione. Cfr. F. Antonacchio, *Criptoarte. Mercato dei NFT, tecnologia, regole, rischi*, p. 81-82.

possibile affermare con assoluta certezza che l'opera sia frutto del lavoro di un determinato artista, quindi il rischio di autentiche che vengono smentite nel corso del tempo è concreto¹¹³⁴.

Concludendo, si evidenzia che la rilevanza e la consapevolezza dei rischi di riciclaggio e finanziamento del terrorismo associati al commercio di arte e antichità hanno portato il GAFI ad avviare, nel giugno 2021, un progetto volto alla rilevazione di tali rischi, nonché delle vulnerabilità e delle minacce del settore¹¹³⁵.

¹¹³⁴ Cfr. D. Micco, M. Franca Filho e G. Magri, *Circolazione, cessione, riciclaggio - Alcuni profili giuridici dell'arte e del suo mercato*, in Quaderni del Dipartimento di Giurisprudenza dell'università di Torino 18/2020, p. 38.

¹¹³⁵ Cfr. Report del FATF-GAFI, *Money laundering and terrorist financing associated with arts, antiquities and other cultural objects*, pubblicato il 25 luglio 2022. L'analisi ha evidenziato diversi approcci nella regolamentazione AML/CFT del settore da parte delle giurisdizioni partecipanti. Tali differenze rappresentano potenziali opportunità per i criminali e aumentano il rischio di arbitraggi normativi. È stata osservata anche una mancanza di consapevolezza dei rischi AML/CFT da parte degli operatori del settore. Il mercato dell'arte è stato segnalato come veicolo di riciclaggio di fondi principalmente attraverso investimenti in opere d'arte per occultare proventi derivanti prevalentemente da corruzione, appropriazione indebita, traffico di droga e frode. La contraffazione dell'arte, l'uso di documenti, certificati e fatture falsi rappresentano alcune delle principali minacce nel settore. In particolare, dalle indagini sono emersi casi di coinvolgimento di soggetti indagati, società offshore, soggetti terzi, organizzazioni non profit, attori senza esperienza nel mondo dell'arte che effettuano acquisti o vendite di alto valore, notevole utilizzo di contante, origine sconosciuta dei fondi utilizzati o delle opere, irregolarità delle fatture relative alle operazioni, mancata dichiarazione all'amministrazione doganale delle opere acquistate, presenza di soggetti noti per essere coinvolti nel traffico di antichità o per aver commesso reati finanziari, incongruenza tra la finalità delle società coinvolte e la natura degli acquisti effettuati o tra la documentazione di provenienza delle opere e la loro reale provenienza, flussi da e/o verso Paesi a regime fiscale privilegiato, legami tra venditori e acquirenti, ricorso ai servizi di Art Finance per occultare proventi illeciti. Sono state identificate anche diverse frodi e truffe tra cui: aste fittizie in cui il riciclatore mette in vendita opere d'arte acquistate da un complice con denaro "sporco"; vendita e acquisto simulati di opere d'arte tramite gallerie d'arte; utilizzo di opere d'arte contraffatte come garanzie per ottenere prestiti bancari. Dall'analisi è emerso altresì che in alcune giurisdizioni sono state adottate specifiche linee guida per rafforzare la comprensione del rischio AML/CFT del settore e chiarire la portata degli obblighi di legge, in altre è presente un'autorità di vigilanza ad hoc.