Gennaio 2018

IV Direttiva Antiriciclaggio e approccio basato sul rischio

Avv. Sabrina Galmarini e Dott. Claudio Saba, La Scala Studio legale

Premessa

La minaccia del riciclaggio e del finanziamento del terrorismo muta costantemente in ragione della continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali: occorre, pertanto, trovare soluzioni che consentano al sistema di prevenzione e contrasto di rispondere in maniera puntuale ai nuovi fenomeni.

Lo strumento sul quale il sistema punta è l'istituzionalizzazione e il raffinamento del ricorso al c.d. "**approccio basato sul rischio**", che costituisce un aspetto cardine della c.d. IV Direttiva Antiriciclaggio e, quindi, del novellato D.Lgs. 231/2007.

La IV Direttiva prevede, infatti, nei suoi considerando che «*Dovrebbe essere adottato un **approccio olistico** basato sul rischio. [*Questo,*] non costituisce un'opzione indebitamente permissiva per gli Stati membri e per i soggetti obbligati: implica processi decisionali basati sull'evidenza fattuale, al fine di individuare in maniera più efficace i rischi di riciclaggio e di finanziamento del terrorismo che gravano sull'Unione e su coloro che vi operano*». «***Sostenere l'approccio basato sul rischio è una necessità** […] per individuare, comprende e mitigare i rischi*» (considerando 22, 23 della IV Direttiva).

I nuovi approcci normativi

Con l'introduzione della IV Direttiva, il ***Risk Based Approach*** viene condotto, su tre livelli distinti, in maniera sistematica e con il coinvolgimento di soggetti diversi.

- ***Risk Assessment* a livello europeo (art. 6 IV Direttiva)**

  È richiesto alla Commissione europea di:

  - individuare le minacce transfrontaliere con potenziali impatti sui mercati nazionali;
  - elaborare una relazione che identifica, analizza e valuta tali rischi, aggiornarla ogni due anni e metterla a disposizione degli Stati membri;

- formulare raccomandazioni agli Stati membri riguardo alle misure idonee ad affrontare i rischi.

- ***Risk Assessment* a livello nazionale (art. 7 IV Direttiva)**

  È richiesto agli Stati membri di:

  - identificare, valutare, comprendere e mitigare i rischi di riciclaggio e finanziamento del terrorismo;
  - designare un'Autorità, ovvero istituire in meccanismo, al fine di coordinare il *risk assessment*;
  - svolgere periodicamente il *risk assessment*;
  - utilizzare le risultanze del *risk assessment* europeo per la conduzione delle analisi;
  - mettere tempestivamente a disposizione dei soggetti obbligati le informazioni maggiormente rilevanti per il proprio *risk assessment*.

- ***Risk Assessment* a livello dei soggetti obbligati (art. 8 IV Direttiva)**

  È richiesto ai soggetti obbligati di:

  - svolgere il *risk assessment* interno, adottare misure volte a individuare, valutare e mitigare il rischio di riciclaggio e di finanziamento del terrorismo;
  - documentare, aggiornare e mettere a disposizione delle autorità competenti le valutazioni del rischio.

La IV Direttiva è stata recepita dal legislatore italiano con il D.lgs. 90/2017, il quale ha disciplinato l'approccio basato sul rischio agli artt. 14, 15 e 16.

Il novellato D.lgs. 231/2007 prevede, infatti, che:

- il Comitato di Sicurezza Finanziaria ("CSF") sia l'autorità diretta a identificare, analizzare e valutare il rischio nazionale di riciclaggio e finanziamento del terrorismo;
- le autorità di vigilanza di settore e gli organismi di autoregolamentazione individuano i requisiti dimensionali e organizzativi in base ai quali i soggetti obbligati, rispettivamente vigilati e controllati, adottano specifici presidi, controlli e procedure per la valutazione e gestione del rischio di riciclaggio e finanziamento del terrorismo;

- i soggetti obbligati dovranno documentare, aggiornare e mettere a disposizione delle autorità competenti e degli organismi di autoregolamentazione il *risk assessment* effettuato.

Si tratta di un **sistema in continua evoluzione che si autoalimenta**. Infatti, la valutazione del rischio effettuata dai soggetti obbligati (art. 15) è documentata e aggiornata periodicamente per poi essere messa a disposizione delle Autorità individuate dall'art. 21, comma 2, lettera *a*) (MEF, UIF, DIA, NSPV, Autorità di vigilanza di settore) e degli organismi di autoregolamentazione. Le Autorità, le Amministrazioni e gli organismi di autoregolamentazione forniscono al CSF i dati e le statistiche sulla dimensione e importanza dei vari settori (art. 14, comma 3), che poi verranno utilizzati dal CSF per elaborare la relazione ogni anno. L'analisi di quest'ultimo viene poi comunicata alla Commissione Europea.

Si è, dunque, abbandonato definitivamente un sistema di regole basato sulla casistica precostituita, adottando un **modello flessibile** per valutare le concrete situazioni. Si tratta, cioè, di un passaggio da un approccio *Rule based* ad uno *Risk based*. Conseguentemente, **spetterà ai soggetti obbligati valutare in quali situazioni regolare la frequenza e l'intensità degli adempimenti**, sulla base di un approccio basato sul rischio.

Nell'individuazione del rischio i soggetti obbligati possono fare affidamento anche sui rischi identificati dal GAFI, dalla Commissione europea e dagli Stati membri, nonché da altre Autorità o organismi. A tal proposito, le Raccomandazioni GAFI dispongono che i Paesi debbano identificare, valutare e comprendere i rischi ai fini del riciclaggio e del finanziamento del terrorismo e adottare misure e dedicare risorse per far sì che tali rischi siano effettivamente mitigati. Qualora, i singoli Paesi individuino maggiori rischi, devono garantire che i rispettivi regimi di contrasto al riciclaggio e al finanziamento del terrorismo vi facciano fronte in maniera adeguata. Di contro, qualora individuino rischi minori, i Paesi possono decidere di autorizzare, a determinate condizioni, misure semplificate. In tal senso si rinvia alla Raccomandazione A.1.

Questi rischi sono stati individuati dal Comitato di Sicurezza Finanziaria nella "*Analisi nazionale dei rischi di riciclaggio e finanziamento del terrorismo*" del 2014 e dalla Commissione europea il 26 giugno 2017, nella "*Relazione sulla valutazione dei rischi di riciclaggio e finanziamento del terrorismo che incidono sul mercato interno e sono connessi ad attività transfrontaliere"*.

Non solo, alcune fasi del processo di identificazione del rischio sono state individuate dal Comitato congiunto delle tre autorità di vigilanza europee (EBA, EIOPA, ESMA), il quale, nel mese di novembre 2016, una volta conclusa la fase di consultazione, ha pubblicato il documento recante "*Orientamenti congiunti sulle caratteristiche di un approccio alla vigilanza basata sul rischio nel settore delal prevenzione e del contrasto del riciclaggio e della lotta al finanziamento del terrorismo, e sulle disposizione da adottare ai fini delal vigilanza basata sul rischio*" ("**Orientamenti sulla vigilanza**

basata sul rischio"). Dal documento risulta come l'approccio basato sul rischio sia un **processo ciclico**, nel quale:

- la **fase 1** consiste nella identificazione di criteri di rischio, nell'ambio dei quali le autorità ottengono informazioni, a livello nazionale e sovranazionale, sulle minacce esistenti;
- la **fase 2** consiste nel *risk assessment*, con cui le autorità utilizzano le informazioni al fine di ricalibrare il rischio con le specifiche caratteristiche di ogni singolo soggetto sottoposto a vigilanza;
- la **fase 3** consiste nel responso del *risk assessment*: vengono, cioè, determinati gli obiettivi, il livello di approfondimento, la durata e la frequenza delle attività ispettive;
- la **fase 4** consiste nel monitorare e revisionare la fase 3, al fine di adeguare il contenuto a quanto rilevato.

Ancora, nel giugno del 2017 il Comitato di Basilea ha pubblicato le Linee Guida concernenti "*Sound management of risks related to money laundering and financing of terrorism*", che hanno lo scopo di aiutare le banche nella declinazione pratica del principio in esame. Il documento, richiede alle banche di valutare e conoscere i rischi, dotarsi di un adeguato sistema di "*governance*" e dotarsi di tre linee di difesa.

- **La prima linea di difesa** è rappresentata dalle politiche e le procedure. Esse devono essere chiare e comunicate a tutto il personale. Devono, altresì, contenere una chiara descrizione degli adempimenti che il personale dovrebbe effettuare.
- **La seconda linea di difesa** è rappresentata dalla figura responsabile. Essa dovrebbe monitorare l'adempimento degli obblighi richiesti alla banca in materia di contrasto al riciclaggio e finanziamento del terrorismo. Il responsabile dovrebbe, altresì, avere un rapporto diretto con il "*senior management*".
- **La terza linea di difesa** è rappresentata dall'***internal audit***. Essa gioca un importante ruolo al fine di una valutazione indipendente della gestione e controllo dei rischi. Le banche dovrebbero stabilire politiche e procedure per condurre l'*audit*, inerenti (i) l'adeguatezza alle politiche e procedure di contrasto al riciclaggio e finanziamento del terrorismo nell'affrontare i rischi identificati, (ii) l'efficacia del personale bancario nell'attuazione delle politiche e delle procedure della banca, (iii) l'efficacia dei sistemi di *compliance* e *quality control* , inclusi i criteri per gli allarmi automatici, e (iv) l'efficacia della formazione proposta dalla banca nei confronti del personale.

Tali indicazioni serviranno al soggetto obbligato nella **declinazione pratica** dell'approccio basato sul rischio. Infatti, il *risk based approach* non è solo un principio

di portata generale, ma deve accompagnare il soggetto obbligato nella **concreta** gestione dei rischi.

In particolare, l'approccio basato sul rischio, al fine di essere efficace, consta di due processi:

- **approccio basato sul rischio "strutturale"**, concernente il *risk assessment* proprio di ogni soggetto obbligato, al fine di valutare i rischi cui è esposto e il conseguente adeguamento delle politiche e procedure interne;
- **approccio basato sul rischio "esterno"**, che accompagna il soggetto obbligato nel **concreto** adempimento degli obblighi.

L'approccio basato sul rischio strutturale

L'applicazione del principio in esame prevede che i soggetti obbligati effettuino il "*risk assessment* interno", al fine di valutare i rischi cui sono esposti nell'esercizio della propria attività e adeguare le politiche e procedure ai rischi in astratto individuati.

L'approccio basato sul rischio strutturale si divide in tre fasi. In particolare, i soggetti obbligati:

- **identificano** i rischi (cc.dd. "**inerenti**") attuali e potenziali cui sono esposti in base alla natura e all'estensione dell'attività svolta;
- analizzano l'adeguatezza dell'assetto organizzativo e dei presidi rispetto ai rischi precedentemente identificati, al fine di individuare eventuali **vulnerabilità**;
- determinano il livello di **adeguatezza** delle procedure e implementano le stesse per renderle idonee a mitigare i rischi.

A questo riguardo, nell'attesa di ulteriori provvedimenti attuativi da parte delle autorità competenti, possono essere considerate come "linee guida" sul processo di valutazione del *risk assessment* la Comunicazioni effettuata da Banca d'Italia nell'ottobre del 2015 e la Lettera al Mercato dell'IVASS del 5 giugno 2017 (successivamente aggiornata il 25 luglio 2017), con cui le autorità hanno richiesto ai soggetti vigilati di condurre una "autovalutazione" dei rischi.

In particolare, l'identificazione e la valutazione del rischio inerente viene effettuata per ciascuna delle principali linee di *business* in cui opera il soggetto obbligato (si fa riferimento, a titolo esemplificativo, per le banche al *retail banking*, *corporate* o *investment banking*, ai servizi di investimento, all'attività della controparte, etc.). Ai fini della valutazione vanno presi in considerazione alcuni elementi, tra cui:

- la **natura**, la scala dimensionale, la differenziazione e la complessità dei settori di *business* in cui opera il soggetto obbligato;

- il **volume** e l'**ammontare** delle transazioni, considerata l'operatività tipica del soggetto obbligato;
- il **mercato di riferimento** per prodotti e servizi erogati;
- i **canali distributivi**, distinguendo tra i diversi soggetti cui si fa affidamento per assolvere gli obblighi di adeguata verifica; in tale contesto rileva anche l'utilizzo di modalità di adeguata verifica a distanza;
- il **numero** di clienti classificati nelle fasce a rischio più elevate (ad esempio, numero di: PEPs, esteri o nazionali, compresi familiari e/o soggetti che mantengono stretti legami; titolari di cariche pubbliche locali; società fiduciarie o *trust*; contraenti che hanno stipulato con conto altrui un contratto c.d. "collettivo" di assicurazione);
- la presenza di **succursali** o **filiazioni** situate in Paesi terzi che non impongono obblighi equivalenti;
- il **Paese estero di origine** o di operatività dei clienti o delle controparti esteri, con riguardo a giurisdizioni ad alto rischio ovvero non cooperative nello scambio di informazioni;
- gli elementi significativi risultanti dalle relazioni e dall'ulteriore documentazione rilevante proveniente dalle **funzioni di controllo interno**;
- le risultanze delle verifiche – ispettive e a distanza – condotte dalle **Autorità di controllo**.

In considerazione di questi indici, ciascun soggetto obbligato definisce un proprio indicatore attraverso il quale misurare il livello di rischio intrinseco, da esprimersi con un giudizio in una scala di valori (così, ad esempio i valori possono essere: rischio basso, medio-basso, medio-alto, alto).

L'attribuzione del livello di rischio inerente viene accompagnata dalla descrizione degli elementi di autovalutazione considerati, delle analisi poste in essere e delle motivazioni che hanno determinato le scelte effettuate.

Ai fini della valutazione, viene fatto rifermento anche ad informazioni provenienti da fonti esterne.

A seguito dell'analisi condotta, i soggetti obbligati si attribuiranno un "**rischio basso**" se, ad esempio, i clienti a rischio elevato sono molto limitati; sono assenti i clienti i cui titolari effettivi sono domiciliati in Paesi terzi che non impongo obblighi equivalenti; il monitoraggio dei canali distributivi è pienamente affidabile; e le minacce e i rischi di coinvolgimento di riciclaggio e di finanziamento del terrorismo legati all'utilizzo delle specifiche linee di *business* non sono significativi.

Di contro, il livello di rischio attribuito sarà "**medio-basso**" se i clienti a rischio più elevato sono a un livello limitato o medio; sono presenti ma non in numero significativo i clienti i cui titolari effettivi sono domiciliati in Paesi terzi che non impongono obblighi equivalenti; il monitoraggio dei canali distributivi è sufficientemente affidabile; e le minacce e i rischi di coinvolgimento in attività di riciclaggio e di finanziamento del terrorismo legati all'utilizzo di specifiche linee di *business* sono limitati.

Una volta determinata la categoria di rischio strutturale, il passo logicamente successivo è quello di valutare se le politiche e le procedure interne siano in grado di far fronte ai rischi identificati. Ciascun soggetto obbligato è chiamato a definire un proprio indicatore per misurare il **livello di vulnerabilità** del sistema di presidi. Anche in questo caso, la vulnerabilità dovrà essere ricondotta in una scala di valori (a titolo esemplificativo, vulnerabilità: non significativa, poco, abbastanza o molto significativa).

L'attribuzione del livello di vulnerabilità così misurata è accompagnata da una sintetica illustrazione dei presidi in essere e dalla descrizione dei punti di debolezza eventualmente individuati, con l'esplicitazione delle motivazioni che hanno determinato il punteggio attribuito.

In questo senso il livello di vulnerabilità sarà "**abbastanza significativo**" se i presidi sono limitatamente efficaci per impedire il coinvolgimento del soggetto obbligato nel riciclaggio e finanziamento del terrorismo; il soggetto obbligato ha un livello di consapevolezza non del tutto adeguato del rischio intrinseco di riciclaggio e finanziamento del terrorismo (sulla base delle evidenze, azioni intraprese, formazione, risorse stanziate); il soggetto obbligato è dotato di un assetto organizzativo con numerose carenze, non sufficientemente idoneo a individuare e contrastare i rischi.

Di contro, il livello di vulnerabilità sarà "**molto significativo**" se i presidi in essere sono inefficaci per impedire il coinvolgimento del soggetto obbligato nel riciclaggio e finanziamento del terrorismo; se il soggetto obbligato ha un livello di consapevolezza inadeguato al rischio; il soggetto obbligato è dotato di un assetto organizzativo con carenze molto numerose, non idoneo a individuare e contrastare i rischi.

Il processo di *risk assessment* però non può certamente concludersi qua: una volta determinati il livello di rischio e il livello di vulnerabilità, il soggetto obbligato individua il metodo per correggere o adeguare le politiche e le procedure interne per mitigare i rischi.

A tal fine, efficaci politiche e procedure devono comprendere:

- la gestione dei rischi, l'adeguata verifica della clientela, la segnalazione di operazioni sospette, la conservazione dei dati e delle informazioni, i controlli interni, la funzione antiriciclaggio (e la nomina del relativo responsabile) e i controlli sui dipendenti;

- una funzione di revisione indipendente, sulla base del principio di proporzionalità e in relazione alla natura e dimensioni dei soggetti obbligati, per la verifica delle politiche e procedure di cui sopra.

L'approccio basato sul rischio esterno

L'approccio basato sul rischio non è solo una valutazione astratta dei rischi cui il soggetto obbligato è esposto nell'esercizio della propria attività, ma è un principio che si riflette anche sull'adempimento concreto degli obblighi previsti dalla normativa.

In particolare, si pensi agli obblighi di adeguata verifica. Nell'individuazione dei rischi, i soggetti obbligati devono adottare, ai sensi dell'art. 17, comma 3 D.lgs. 231/2007, misure **proporzionate** all'entità dei rischi, tenendo conto di criteri generali con riferimento al cliente e all'operazione/rapporto continuativo/prestazione professionale. I criteri possono essere così sintetizzati:

- **natura giuridica del cliente**. I soggetti obbligati devono valutare il profilo soggettivo del cliente: persona fisica, società, ente, associazione, etc. Occorre prestare particolare attenzione, ad esempio, alle cariche politiche-istituzionali, alle funzioni svolte nell'ambito della Pubblica Amministrazione soprattutto se connesse con la gestione ed erogazione di fondi pubblici. Occorre valutare, altresì, eventuali legami operativi, economici, societari con entità residenti in Paesi considerati dal GAFI come ad alto rischio e/o non cooperanti, ovvero con lacune strategiche nei loro sistemi di contrasto al riciclaggio e finanziamento del terrorismo;

- **prevalente attività svolta**. Occorre valutare l'attività svolta dal cliente e, in particolare, valutare se si tratta di attività esposte al rischio di infiltrazioni criminali (ad esempio, appalti, sanità, raccolta e smaltimento rifiuti, energie rinnovabili, giochi). Occorre, altresì, valutare la ragionevolezza e la coerenza della prestazione richiesta al soggetto obbligato rispetto all'attività normalmente svolta dal cliente, alla sua situazione finanziaria e alle finalità dichiarate;

- **comportamento**. Assume rilievo la ritrosia del cliente a fornire le informazioni, nonché l'incompletezza e l'erroneità dei dati in occasione della sua identificazione, dell'individuazione del titolare effettivo, della natura e dello scopo della prestazione;

- **area geografica**. Occorre valutare la logicità e la coerenza della prestazione professionale anche in relazione al luogo in cui si svolgono le attività del cliente o della controparte. Sono rilevanti le eventuali informazioni inerenti domiciliazioni di comodo del cliente o della sua controparte ovvero concernenti l'operatività in un territorio da ritenersi a rischio, ad esempio, in ragione di fattori quali il livello elevato di infiltrazione criminale, di economia sommersa o di degrado economico-istituzionale;

- **tipologia dell'operazione**. Occorre prestare particolare attenzione nel caso di ricezione di operazioni relative a schemi negoziali che possano agevolare l'opacità delle relazioni finanziarie o economiche esistenti tra il cliente e le sue controparti. Si fa riferimento, ad esempio, a fattispecie quali atti istitutivi di *trust* in cui alcune parti contraenti siano domiciliate o abbiano sede in aree geografiche a rischio. Rileva, altresì, la potenziale strumentalità dell'operazione al perseguimento di fini illeciti (ad esempio, modalità o mezzi di pagamento utilizzati, specie se verso Stati extracomunitari diversi dai Paesi terzi che sono soggetti ad obblighi contro il contrasto al riciclaggio e finanziamento del terrorismo);

- **modalità di svolgimento dell'operazione**. Si tratta di valutare eventuali clausole contrattuali ovvero collegamenti negoziali che possano ostacolare l'esatta individuazione dei profili soggettivi e oggettivi della transazione finanziaria. Rileva altresì, l'ipotesi in cui l'operatività è ingiustificatamente complessa o attuata con l'impiego di contanti e/o risorse provenienti senza ragionevoli motivi da soggetti terzi;

- **ammontare**. Occorre prestare attenzione alle operazioni di ammontare significativo, soprattutto se non coerenti con il profilo economico-patrimoniale del cliente;

- **frequenza delle operazioni e durata**. La frequenza di determinate operazioni può essere indice di rischio se rapportato ad ulteriori elementi: si pensi al disoccupato o al pensionato che, in un breve periodo, acquista più immobili o aziende commerciali.

Non solo, un altro documento imprescindibile, cui i singoli soggetti obbligati devono tener conto per l'approccio basato sul rischio "esterno", riguarda le "**Linee Guida sui Fattori di Rischio**", emanate dal Comitato congiunto delle tre autorità di vigilanza europee (EBA, EIOPA, ESMA) nel mese di giugno 2017, una volta conclusa la fase di consultazione.

Esse illustrano, in una logica di *risk based approach*, i fattori di rischio che dovrebbero essere presi in considerazione – dai destinatari che operano nel settore bancario e finanziario nonché dalle autorità di vigilanza di settore nell'esercizio delle proprie funzioni di controlli – nello svolgimento dell'**adeguata verifica semplificata e rafforzata**. A titolo esemplificativo, si fa riferimento ai fattori di rischio relativi all'attività professionale del cliente, alla reputazione del cliente, al suo comportamento o ai suoi rapporti d'affari. Ancora, si fa riferimento al valore o al prezzo del prodotto o servizio offerto, alla complessità dell'operazione, all'utilizzo di intermediari per porre in essere l'operazione, e così via.

Sulla base di questi fattori, i soggetti obbligati dovranno assegnare un livello di rischio a ciascun cliente e modellare la frequenza e l'intensità dei controlli sulla base di tale

valutazione. A titolo esemplificativo, il livello di rischio può essere suddiviso in: rischio basso, medio e alto. Maggiore sarà il rischio per tipo di cliente, maggiore sarà la frequenza e l'intensità dei controlli.

Sotto questa prospettiva, al cliente verrà attribuito un rischio alto se si tratta di un soggetto protetto da schermo fiduciario, operante nel settore della raccolta e smaltimento rifiuti, avente sede in un Paese ad alto rischio e operate con un ingente flusso di contanti.