Luglio 2017

IV Direttiva antiriciclaggio: la condivisione delle informazioni all'interno dei gruppi

Francesco Di Carlo e Matteo Catenacci, Craca Di Carlo Guffanti Pisapia Tatozzi & Associati

1. Premessa

Come noto, il 4 luglio è entrato in vigore il D.lgs. 25 maggio 2017, n. 90 ([1]), emanato lo scorso 25 maggio, con cui è stata data attuazione in Italia alla c.d. "IV Direttiva antiriciclaggio" ([2]) e che ha ampiamente modificato il D.lgs. 21 novembre 2007, n. 231.

Una norma potenzialmente innovativa contenuta nel nuovo *framework* normativo comunitario è l'art. 45, par. 1, della IV Direttiva, ai sensi del quale i soggetti appartenenti ad un gruppo hanno l'obbligo di attuare politiche e procedure a livello di succursali e filiazioni controllate a maggioranza situate negli Stati membri e in Paesi terzi, tra cui politiche in materia di protezione dei dati e politiche e procedure per la condivisione delle informazioni all'interno del gruppo a fini antiriciclaggio e di contrasto al finanziamento del terrorismo (AML/CFT).

Come si dirà meglio nel prosieguo, la violazione dell'obbligo di cui al richiamato art. 45, par. 1, è autonomamente sanzionata.

Quale premessa di ordine generale, la disposizione in esame costituisce una novità nell'ambito della legislazione comunitaria in materia: infatti, nella c.d. "III Direttiva antiriciclaggio" ([3]) non vi era alcuna previsione analoga che imponesse (o comunque prevedesse) l'obbligo per società appartenenti ad un gruppo di dotarsi di politiche e

([1]) G.U., Serie Generale n. 140, 19.6.2017.
([2]) Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione (G.U.U.E., 5.6.2015, L 141/73).
([3]) Direttiva 2005/60/CE del Parlamento europeo e del Consiglio, del 26 ottobre 2005, relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (G.U.U.E., 25.11.2005, L 309/15).

procedure per la condivisione delle informazioni (ed eventualmente dei nominativi) sui relativi clienti.

Il presente lavoro propone una valutazione della nuova norma, che rafforza il principio basato sull'approccio globale al rischio e ne garantisce la coerenza con gli standard stabiliti nelle raccomandazioni internazionali adottate dal GAFI, muovendo da un'analisi comparativa con la precedente legislazione in materia.

2. La III Direttiva e la disciplina attuativa italiana

La III Direttiva conteneva – all'art. 34, par. 1 – disposizioni relative all'adozione di idonee ed appropriate politiche e procedure in materia di obblighi di adeguata verifica della clientela, segnalazione di casi sospetti, conservazione dei documenti, controllo interno, valutazione e gestione del rischio, garanzia dell'osservanza delle pertinenti disposizioni e di comunicazione per prevenire e impedire la realizzazione di operazioni connesse con il riciclaggio e il finanziamento del terrorismo.

Come detto, la normativa comunitaria non prevedeva, invece, un obbligo per i gruppi di dotarsi di vere e proprie politiche e procedure di condivisione interna delle informazioni.

La disciplina primaria e secondaria italiana di recepimento della III Direttiva ha previsto talune norme specifiche relative ai gruppi societari, volte essenzialmente a garantire un approccio comune tra le società appartenenti ad un medesimo gruppo rispetto agli adempimenti in materia di AML/CFT nonché – con specifico riguardo alla segnalazione di operazioni considerate sospette – a condividere informazioni attinenti alle informazioni stesse.

In particolare:

– da un lato, l'art. 46, co. 4, del "vecchio" D.lgs. 231/2007 (*ante* D.lgs. 90/2017) ([4]) prevedeva la facoltà (ma non l'obbligo) per gli intermediari appartenenti allo stesso gruppo di condividere i dati della clientela oggetto di segnalazioni di operazioni sospette (SOS), e ciò in deroga al più generale divieto di comunicazione previsto dall'art. 45 e dallo stesso art. 46 (*"il divieto di cui al comma 1 non impedisce la comunicazione tra gli intermediari finanziari appartenenti al medesimo gruppo, anche se situati in Paesi terzi, a condizione che applichino misure equivalenti a quelle previste dalla direttiva"*);

– dall'altro lato, il *"Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'art. 7, comma 2, del decreto legislativo 21 novembre 2007, n. 231"* del 10 marzo 2011 della Banca

([4]) Ora confluito nell'art. 39, co. 3, con gli opportuni adeguamenti di cui si darà conto.

d'Italia, per il settore bancario e finanziario, e il Regolamento n. 41 del 15 maggio 2012 dell'IVASS ([5]), per il settore assicurativo, adottati ai sensi dell'art. 7, co. 2, del D.lgs. 231/2007 ([6]), dove si prevede che i gruppi (bancari, finanziari ed assicurativi) sviluppino un approccio globale al rischio AML/CFT.

Le suddette previsioni – che, per quanto su piani distinti ([7]), rispondono alla medesima esigenza di prevenzione del rischio AML/CFT nei gruppi – hanno dovuto necessariamente coordinarsi con la normativa in materia di tutela della riservatezza e della *privacy* della clientela applicabile alle singole componenti del gruppo (c.d. bilanciamento d'interessi).

(a) Comunicazione infra-gruppo di dati relativi a SOS

In termini generali, ai sensi dell'art. 46, co. 1, del "vecchio" D.lgs. 231/2007, le informazioni relative alle SOS, ivi inclusi i dati relativi al soggetto interessato dalla segnalazione, non potevano essere comunicate al di fuori dei casi specificamente previsti dalla legge. L'inosservanza del divieto comportava sanzioni penali, *ex* art. 55, co. 8, del medesimo D.lgs. ([8]).

Tuttavia, il richiamato art. 46, co. 4, prevedeva la facoltà di condividere infra-gruppo i dati personali dei clienti relativamente alle SOS effettuate.

Quindi, fermo restando che – come sopra accennato – la normativa non prevedeva un generale obbligo di condivisione endo-gruppo dei dati relativi ai clienti, una società appartenente ad un determinato gruppo societario, dopo aver effettuato una SOS (e non, invece, a seguito della semplice assunzione di informazioni relative ai clienti nell'ambito dell'adeguata verifica della clientela e/o nell'ambito degli obblighi di registrazione), poteva comunicare ad altre società del gruppo la "avvenuta segnalazione".

([5]) IVASS, *"Regolamento concernente disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi a fini di riciclaggio e di finanziamento del terrorismo, ai sensi dell'articolo 7, comma 2, del decreto legislativo 21 novembre 2007, n. 231"*.

([6]) I provvedimenti regolamentari indicati rientrano nell'ambito di applicazione dell'art. 9, co. 1, del D.lgs. 90/2017, secondo il quale *"le disposizioni emanate dalle autorità di vigilanza di settore, ai sensi di norme abrogate o sostituite per effetto del presente decreto, continuano a trovare applicazione fino al 31 marzo 2018"*.

([7]) Mentre il Provvedimento della Banca d'Italia e il Regolamento n. 41 prevedono l'obbligo di adottare *ex ante* un assetto organizzativo/procedurale tale da gestire il rischio riciclaggio a livello di gruppo, l'art. 46, co. 4, prevedeva un vero e proprio scambio informativo infra-gruppo *ex post*.

([8]) Salvo che il fatto costituisca più grave reato, la violazione dei divieti di comunicazione di cui agli artt. 46, co. 1, e 48, co. 4, veniva punita con l'arresto da sei mesi a un anno o con l'ammenda da 5.000 a 50.000 euro.

Con riguardo alla condivisione di informazioni in tale ipotesi, si ritiene utile effettuare alcune considerazioni:

– quanto alla *ratio* della previsione, la stessa appariva finalizzata alla condivisione a livello di gruppo delle SOS effettuate, in quanto trattasi di informazioni rilevanti ai fini della conoscenza di clienti con i quali più società di uno stesso gruppo – anche inconsapevolmente – avrebbero potuto intrattenere rapporti rilevanti ai fini AML/CFT. Tale condivisione avrebbe potuto divenire di fatto necessaria al fine di consentire un approccio coordinato e congiunto a livello di gruppo nel contrasto al riciclaggio ed al finanziamento del terrorismo nonché funzionale alla gestione del rischio che operazioni per fini illeciti fossero poste in essere dalla clientela per il tramite dell'intermediario (e, quindi, dei rischi reputazionali e/o sanzionatori derivanti dalla mancata individuazione – e quindi segnalazione – di operazioni sospette);

– le società del gruppo dovevano istituire regole a presidio del rischio che la condivisione interna delle informazioni relative a SOS effettuate – per quanto consentita dal già più volte ricordato art. 46, co. 4 – violasse il divieto di dare comunicazione dell'avvenuta SOS fuori dai casi espressamente consentiti (primo tra tutti, il divieto di comunicare al soggetto interessato o a terzi l'avvenuta SOS). Al riguardo, si evidenzia che nel Provvedimento del 10 marzo 2011 (non si rinviene norma analoga nel Regolamento IVASS n. 41), la Banca d'Italia ha stabilito che *"il responsabile delle segnalazioni di operazioni sospette può consentire che i nominativi dei clienti oggetto di segnalazione di operazione sospetta siano consultabili - anche attraverso l'utilizzo di idonee basi informative – dai responsabili delle diverse strutture operative aziendali, stante la particolare pregnanza che tale informazione può rivestire in sede di apertura di nuovi rapporti contrattuali ovvero di valutazione dell'operatività della clientela già in essere"*. Dalla previsione è da subito emerso in modo evidente che, anche nell'ambito della stessa società che avesse effettuato SOS venivano posti dei limiti alla condivisione delle informazioni relative alle avvenute segnalazioni da parte del responsabile delle segnalazioni: quest'ultimo "poteva" infatti consentire che i nominativi dei clienti oggetto di SOS fossero consultabili dai soli "responsabili" delle diverse strutture operative aziendali (e non da chiunque all'interno della società), allo scopo di valutare l'operatività dei clienti in relazione ai rapporti esistenti ed all'apertura di nuovi rapporti. Quindi, a maggior ragione in caso di condivisione nell'ambito del gruppo, avrebbero dovuto necessariamente essere create regole che vietassero l'accesso a tali informazioni a chiunque ([9]);

– in ogni caso, la condivisione con società di Paesi terzi appartenenti al medesimo gruppo era subordinata alla condizione che tali Paesi applicassero "*misure*

([9]) Ad esempio, una condivisione delle segnalazioni effettuate strutturata in modo tale che l'accesso fosse limitato ai responsabili delle funzioni antiriciclaggio o di funzioni di controllo delle società del gruppo.

equivalenti a quelle previste dalla direttiva", con riguardo al divieto di comunicazione delle SOS effettuate e che, quindi, fosse garantita la "protezione" dell'informazione condivisa con altre società del gruppo.

Sotto il profilo *privacy*, sulle condizioni di liceità di tale comunicazione si era favorevolmente espresso il Garante per la protezione dei dati personali in data 10 settembre 2009 ([10]), il quale aveva ritenuto che ricorressero gli estremi per dare attuazione al c.d. "bilanciamento degli interessi" ([11]) disciplinato dall'art. 24, co. 1, lettera g), del D.lgs. 30 giugno 2003, n. 196 (il "Codice privacy") e, conseguentemente, che potevano formare oggetto di comunicazione i dati personali concernenti le segnalazioni previste dalla disciplina in materia antiriciclaggio, in presenza delle condizioni previste dall'art. 46, co. 4, senza che a tal fine fosse quindi necessario acquisire il consenso dell'interessato.

Sul punto, peraltro già la III Direttiva – nel considerando 33 – aveva precisato che *"la comunicazione di informazioni di cui all'articolo 28 dovrebbe essere in conformità con le norme sul trasferimento dei dati personali a paesi terzi di cui alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Inoltre, l'articolo 28 non può interferire con la legislazione nazionale sulla protezione dei dati personali e sul segreto professionale"*.

Maggiore era l'attenzione al rispetto della normativa in materia di *privacy* con riguardo alla possibilità che le informazioni relative a SOS fossero condivise tra intermediari non appartenenti al medesimo gruppo. Con riguardo a tale ipotesi, l'art. 46, co. 6, richiamava espressamente le disposizioni in materia di *privacy* al cui rispetto era subordinata la condivisione delle informazioni; la norma disponeva, infatti, che *"in casi relativi allo stesso cliente o alle stesse operazioni che coinvolgano due o più intermediari finanziari … il divieto di cui al comma 1 non impedisce la comunicazione tra gli intermediari …, a condizione che siano situati in un Paese terzo che impone obblighi equivalenti a quelli previsti dal presente decreto, fermo restando quanto stabilito dagli articoli 42, 43 e 44 del Codice in materia di protezione dei dati personali. Le informazioni scambiate possono essere utilizzate esclusivamente ai fini di*

([10]) *Misure relative alle comunicazioni fra intermediari finanziari appartenenti al medesimo gruppo in materia di antiriciclaggio* - 10 settembre 2009 (G.U. n. 267, 16.11.2009). Il quesito, di portata generale, posto all'attenzione del Garante, riguardava il coordinamento tra la normativa di protezione dei dati personali e la disciplina di settore in materia di antiriciclaggio (in ordine alla quale il Garante si era già espresso con parere del 25 luglio 2007, doc. web. n. 1431012).

([11]) Che, a parere del Garante, *"consente di non ritenere prevalenti … i diritti degli interessati rispetto al legittimo interesse del titolare del trattamento e del terzo destinatario dei dati (nel caso di specie, altro intermediario finanziario appartenente al medesimo gruppo) alla comunicazione e al conseguente trattamento dei dati personali oggetto della segnalazione. Tale comunicazione potrà essere effettuata … per perseguire le sole finalità connesse all'applicazione della disciplina antiriciclaggio da parte dei soli incaricati (operanti nell'ambito dei diversi intermediari finanziari) deputati ad assolvere compiti relativi all'adempimento delle misure poste a contrasto del riciclaggio di denaro"*.

prevenzione del riciclaggio o del finanziamento del terrorismo". In aggiunta alla cautela stabilita anche dell'art. 46, co. 4, secondo cui la comunicazione poteva avvenire *"a condizione che* [nei Paesi terzi si] *applichino misure equivalenti"* a quelle previste nel D.lgs. 231/2007 in relazione al divieto di comunicazione delle SOS effettuate ed alle deroghe a tale divieto, il co. 6 disponeva che dovesse essere altresì salvaguardata la conformità alle norme sul trasferimento dei dati contenute negli artt. 42 (trasferimenti all'interno della UE), 43 (trasferimenti consentiti in Paesi terzi) e 44 (altri trasferimenti consentiti) del Codice privacy.

(b) Approccio globale al rischio

Come accennato sopra, a prescindere dalla possibilità (e non obbligo) di scambio delle informazioni inerenti ai clienti oggetto di SOS, sulla base della normativa citata i gruppi avevano (e hanno) anche l'obbligo di sviluppare un approccio globale al rischio riciclaggio.

La tutela degli interessi dei gruppi, la loro sana e prudente gestione e stabilità patrimoniale nonché l'adozione di presidi atti ad evitare l'assunzione – anche inconsapevole – del rischio di coinvolgimento diretto in fatti di riciclaggio e/o finanziamento del terrorismo, erano (e restano) obiettivi primari della legislazione comunitaria in materia.

A tale fine, è ormai notorio che i conglomerati finanziari internazionali di rilevanti dimensioni adottino programmaticamente *"un approccio globale al rischio di riciclaggio, con fissazione di standard generali in materia di identificazione e conoscenza della clientela"*, tramite *policy*, processi e procedure sviluppate in modo consolidato e attuate coerentemente sia in Italia che all'estero, come peraltro espressamente richiesto nella richiamata normativa regolamentare. Un approccio di tal genere si basa su alcuni semplici principi:

- omogeneità, in sede di adozione di criteri e sistemi di profilatura del rischio;
- integrazione, mediante la creazione di database contenenti un set standard di informazioni sui clienti (come meglio si dirà nel seguito);
- *governance* e controllo, attraverso il consolidamento di report analitici anche a beneficio degli organi aziendali e delle Autorità ([12]).

È proprio l'esigenza di omogeneità alla base della citata disciplina Banca d'Italia del marzo 2011 in tema di presidi antiriciclaggio nelle strutture di gruppo, laddove l'Autorità ha prescritto che *"particolare attenzione richiede l'articolazione della funzione* [antiriciclaggio] *nei gruppi bancari con operatività cross-border. Come previsto dalle linee guida in materia elaborate a livello internazionale, i gruppi sono*

([12]) Cfr. op. citata, p. 47.

tenuti a sviluppare un approccio globale al rischio di riciclaggio, con fissazione di standard generali in materia di identificazione e conoscenza della clientela", rimettendo agli intermediari l'onere di *"individuare le soluzioni organizzative più idonee per assicurare il rispetto di tutte le disposizioni applicabili in relazione ai diversi ambiti di operatività e, nel contempo, assicurare che la gestione dei rischi in discorso tenga conto di tutti gli elementi di valutazione e di misurazione in possesso delle singole componenti"*. Medesime considerazioni merita il Regolamento n. 41, laddove l'IVASS ha prescritto che *"i gruppi assicurativi con operatività cross-border sviluppano un approccio globale al rischio di riciclaggio e di finanziamento del terrorismo, con fissazione di standard generali in materia di identificazione e conoscenza della clientela"* e che *"le decisioni strategiche a livello di gruppo assicurativo in materia di gestione del rischio di riciclaggio e di finanziamento del terrorismo sono rimesse alla capogruppo che le assume coinvolgendo, nei modi ritenuti più opportuni, gli organi aziendali delle imprese Controllate"*.

Anche in considerazione del fatto che l'inosservanza delle disposizioni regolamentari prevedeva la comminazione di una sanzione amministrativa pecuniaria, ai sensi dell'art. 56 del "vecchio" D.lgs. 231/2007 ([13]), è necessario comprendere meglio la portata pratica del concetto di "approccio globale al rischio" e, per quanto rileva ai fini del presente scritto, se ciò equivalga o meno ad un obbligo di scambio *tout court* dei dati della clientela infra-gruppo, a prescindere dall'avvenuta segnalazione di operazioni sospette.

A tale riguardo, la Banca d'Italia, nelle FAQ sull'applicazione della normativa antiriciclaggio, nel regime della III Direttiva, a fronte del quesito *"In caso di gruppi, il profilo di rischio di un cliente va condiviso anche con le eventuali controllate estere"* si è limitata ad affermare che *"fermo il rispetto degli specifici adempimenti prescritti dall'ordinamento del paese ospitante, le procedure in essere presso le succursali e le filiazioni estere devono essere in linea con gli standard del gruppo e tali da assicurare la condivisione delle informazioni a livello consolidato"*, senza tuttavia chiarirne la portata pratica; la posizione dell'Autorità è peraltro stata ribadita anche pubblicamente, ma sempre a livello di principio ([14]).

([13]) Sanzione amministrativa pecuniaria da 10.000 a 200.000 euro.

([14]) Si segnala, al riguardo, uno stralcio dell'intervento del dott. Luigi Mariani, Sostituito del Capo dell'Ispettorato Vigilanza della Banca d'Italia, al 10° incontro sulla *compliance* – Corruzione, crimini finanziari e reati informatici, conseguenze economiche e reputazionali, tenutosi il 25 giugno 2014: *"Negli intermediari organizzati in strutture di gruppo, va reso effettivo l'utilizzo di un approccio unitario alla gestione del rischio antiriciclaggio; in non pochi casi si è riscontrato che le informazioni disponibili presso alcune componenti del gruppo non sono accessibili alle altre entità del conglomerato, vanificando le sinergie informative potenzialmente fruibili tramite una gestione consolidata del rischio e la valutazione integrata della clientela. La globalità dell'approccio è ormai un'esigenza ineludibile nei gruppi bancari con operatività cross border, specie per garantire l'unicità dei criteri in materia di identificazione e conoscenza della clientela. È necessario che le procedure utilizzate da succursali e filiazioni estere, anche extracomunitarie, siano in linea con le regole generali del gruppo, tali da*

Pertanto, è necessario valutare se i riferimenti elaborati a livello internazionale possano essere d'ausilio in tal senso: ci si riferisce alle *"Guidelines – Sound management of risks related to money laundering and financing of terrorism"* elaborate nell'ottobre 2004 dal Comitato di Basilea per la Vigilanza Bancaria, successivamente confluite nel più ampio documento del febbraio 2016, ma anche alle raccomandazioni elaborate nel febbraio 2012 dal GAFI_FATF (*"International standards on combating money laundering and the financing of terrorism & proliferation – The FATF Recommendations"*), da ultimo aggiornate a ottobre 2016.

Con riguardo a queste ultime, il GAFI-FATF si è limitato a disporre, nella raccomandazione 18, che: *"i gruppi finanziari devono implementare programmi di contrasto del riciclaggio e del finanziamento del terrorismo a livello di gruppo, ivi incluse politiche e procedure di condivisione delle informazioni all'interno del gruppo a scopo di contrasto del riciclaggio di denaro e del finanziamento del terrorismo"*, senza tuttavia fornire particolari indicazioni sull'applicazione del principio.

Anche le linee guida elaborate dal Comitato di Basilea hanno fornito indicazioni laconiche e focalizzate su un determinato ambito, ma comunque utili da considerare:

– da un lato, è stato ribadito come le *policy* e le procedure debbano essere sviluppate e coordinate *"on a group-wide basis"* ([15]);

– dall'altro lato, è stato precisato che tali *policy* e procedure devono permettere lo scambio informativo infra-gruppo (*"information-sharing"*) con riguardo alla clientela ad alto rischio e a quella oggetto di operatività "sospetta" ([16]).

Pertanto, il Comitato di Basilea ha confermato l'approccio di gruppo al rischio in parola ed evidenziato l'esigenza di garantire lo scambio informativo con riguardo alla clientela a più elevato rischio e a quella segnalata come sospetta. Il Comitato ha stabilito, quindi, l'obbiettivo e, con esso, una soglia minima di condivisione, fermo restando la "possibilità" di una condivisione maggiormente estesa nell'ambito dei gruppi, purché nel rispetto della normativa sulla tutela della *privacy* ([17]).

3. La IV Direttiva

Come già accennato, i principi sopra riassunti sono stati di fatto trasposti nella IV Direttiva, laddove si prevede un rafforzamento dell'approccio consolidato stabilendo

---

assicurare la condivisione delle informazioni a livello consolidato. È noto comunque il vincolo rappresentato dalla circostanza che in taluni casi la condivisione di tutte le informazioni sulla clientela di gruppo può confliggere con le legislazioni presenti nei vari Paesi a tutela della privacy dei cittadini, impedendo la circolarità delle informazioni sulla clientela tra entità giuridiche distinte, anche laddove appartenenti al medesimo gruppo".

([15]) Cfr. Linee guida 64 e 71.

([16]) Cfr. Linee guida 72, 77 e 79.

([17]) Cfr. Linea guida 78.

all'art. 45, par. 1, che *"i soggetti appartenenti ad un gruppo attuino politiche e procedure a livello di gruppo, tra cui politiche in materia di protezione dei dati e politiche e procedure per la condivisione delle informazioni all'interno del gruppo ai fini AML/CFT"*, e ciò con riguardo alle *"informazioni relative al sospetto che i fondi provengano da attività criminose o siano collegati al finanziamento del terrorismo"* (art. 45, par. 8). Come già sopra accennato, si passa quindi dalla facoltà di condivisione all'obbligo di attuare politiche e procedure per la condivisione delle informazioni all'interno del gruppo.

La *ratio* di tale norma è da rinvenirsi nei lavori preparatori a livello comunitario ([18]), laddove la Commissione europea:

- ha preso atto delle difficoltà da parte degli operatori di adempiere agli oneri previsti dalla legislazione in materia di AML/CFT e, al tempo stesso, di garantire un elevato livello di protezione dei dati personali della clientela ([19]);

- a fronte delle possibili alternative da adottare, ha riconosciuto una forte preferenza da parte degli operatori per l'introduzione di disposizioni in materia di *privacy* maggiormente dettagliate a fini AML/CFT ([20]);

([18]) Cfr. documento pubblicato dalla Commissione europea in data 5 febbraio 2013: *"Commission staff working document - Impact assessment - Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds"* (SWD/2013/021 final), p. 96 e ss.

([19]) Così la Commissione: *"Private stakeholders point to a number of practical difficulties as regards their ability to comply with AML requirements while at the same time adhering to rules aimed at ensuring a high level of protection of personal data. These difficulties include sharing of information within the group or between FIUs, screening on the basis of non-EU sanctions lists, consent of the data subject, record keeping, and legal uncertainties with regard to processing of AML/CFT related data within entities. The recently proposed EU Regulation and Directive on data protection are aimed at strengthening and clarifying data protection rules and might need to be clarified in the revised AML/CFT legal framework. In its Opinion 14/2011, the Article 29 data protection working party called for more detailed consideration of data protection issues in the AML legislation, in particular as regards retention of personal data. One particular issue is the requirement, reinforced by the new FATF standard, to implement at a group level AML/CFT programmes, including policies and procedures for sharing information within the group. Within the EU, institutions experience in practice some restrictions from local data protection authorities to the sharing of data (e.g. restrictions to information sharing on STRs, to information flows to the auditors of the Head Office). Data sharing with third countries whose data protection regimes are not considered adequate may raise other difficulties"*.

([20]) Così la Commissione: *"Many stakeholders complained that national data protection rules impacted effective intragroup transfer of information – this was one of the most important factors generating administrative burdens and reducing the effectiveness of AML procedures. The business sector also warned about three further issues:*

• under the current data protection regime, there are serious restrictions on disclosure and transfer of personal data to third country public authorities;

• there are difficulties with respect to data retention periods;

- alla luce di quanto sopra, al fine di assicurare un elevato livello di protezione dei dati personali ed assicurare, nel contempo, l'adeguamento agli obblighi in materia di AML/CFT, ha proposto di introdurre nuove regole comunitarie in materia di AML/CFT al fine di un maggiore coordinamento con la protezione dei dati personali, al fine di eliminare l'incertezza legale nell'operatività quotidiana *cross-border* dei gruppi (*"in view of the need to ensure a high level of data protection whilst at the same time ensuring proper compliance with AML rules, it appears appropriate to ensure an adequate legal basis for data processing in specific AML legislation"*) ([21]).

Il "cambio di passo" è confermato anche dalle sanzioni previste con riguardo alla violazione dell'obbligo di attuare politiche e procedure per la condivisione di informazioni ai fini AML/CFT: l'art. 59 della IV Direttiva antiriciclaggio pone l'obbligo per gli Stati Membri di assicurare che le sanzioni a fronte delle violazioni gravi, reiterate, sistematiche, o che presentano una combinazione di tali caratteristiche, commesse dai soggetti obbligati, degli obblighi, *inter alia*, di cui all'art. 45, comprendano almeno quanto segue:

a) dichiarazione pubblica che identifica la persona fisica o giuridica e la natura della violazione;

b) ordine che impone alla persona fisica o giuridica responsabile di porre termine al comportamento in questione e di astenersi dal ripeterlo;

c) ove un soggetto obbligato sia soggetto ad autorizzazione, revoca o sospensione dell'autorizzazione;

d) interdizione temporanea dall'esercizio di funzioni dirigenziali per le persone con compiti dirigenziali in un soggetto obbligato ritenute responsabili della violazione, o per qualsiasi altra persona fisica ritenuta responsabile della violazione;

• *under the proposal for a data protection Regulation, it is not clear how the empowerment to introduce restrictions of data protection principles will be interpreted.*
There was unanimous recognition of the need to address these issues by ensuring effectiveness in monitoring and reporting in ways which would not breach data protection principles. Diverging opinions were however expressed on the right way forward. Support for the idea of introducing more detailed data protection provisions for AML/CFT purposes was particularly strong from business".

([21]) In tale contesto, la Commissione ha espresso la preferenza per l'opzione che prevedeva di introdurre nuove regole a livello comunitario per chiarire l'interazione tra normative AML/CFT e *privacy*, in quanto tale opzione *"would help reduce legal uncertainties to which businesses are confronted in their day-to-day operations and notably facilitate cross-border group compliance of AML/CFT programmes, which would be in line with the new international standards. New provisions might clarify how long data can be held by obliged entities, the circumstances under which data can be transferred to third countries, and ensure that data collected for AML/CFT purposes cannot be processed for commercial purposes".*

e) sanzioni amministrative pecuniarie massime pari almeno al doppio dell'importo dei profitti ricavati grazie alla violazione, quando tale importo può essere determinato, o pari almeno a 1 milione di euro ([22]).

Fermo restando che, secondo l'art. 59, par. 4, gli Stati Membri possono conferire alle autorità competenti la facoltà di imporre ulteriori tipi di sanzioni amministrative in aggiunta a quanto previsto alle lettere da a) a d), o di imporre sanzioni amministrative pecuniarie di importo superiore a quanto previsto alla lettera e), le sanzioni espressamente previste di per sé esprimono la rilevanza attribuita – tra l'altro – all'esigenza di condivisione delle informazioni a livello di gruppo. Si richiama, in particolare, l'attenzione sulla dichiarazione pubblica, rimedio utilizzato nel nuovo sistema sanzionatorio in relazione alle violazioni di maggior rilevanza, nonché alla revoca dell'autorizzazione.

4. La nuova disciplina italiana

Preliminarmente, si noti che la prescrizione dell'art. 45 della IV Direttiva antiriciclaggio non è stata direttamente recepita nel D.lgs. 231/2007 da parte del D.lgs. 90/2017: infatti, non si ritrova, nella normativa primaria, una disposizione che preveda l'obbligo per i soggetti obbligati appartenenti ad un gruppo di dotarsi di politiche e procedure per lo scambio di informazioni a fini AML/CFT.

Tuttavia, l'art. 7, co. 1, lett. a), del nuovo D.lgs. 231/07 (*post* D.lgs. 90/2017) – ricalcando la disposizione del previgente art. 7, co. 2 – dispone che le Autorità di vigilanza di settore adottino nei confronti dei soggetti rispettivamente vigilati, disposizioni di attuazione del D.lgs. in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela.

Pertanto, sarà compito delle Autorità di vigilanza di settore dettare le disposizioni attuative per l'implementazione delle politiche e procedure di gruppo per lo scambio di informazioni, e ciò con le tempistiche previste dall'art. 9 del D.lgs. 90/2017 (31 marzo 2018). Alla luce della appena citata disciplina transitoria, parrebbe che, in mancanza delle disposizioni attuative ex art. 7, co. 1, lett. a) e, quindi, verosimilmente fino al 31 marzo 2018, non vi sia l'obbligo per i gruppi di dotarsi di politiche e procedure di scambio informativo ex art. 45 della IV Direttiva antiriciclaggio.

([22]) Ai sensi dell'art. 59, par. 3, se il soggetto obbligato interessato è un ente creditizio o un istituto finanziario, si possono applicare anche le seguenti sanzioni:

a) nel caso di entità giuridiche, sanzioni amministrative pecuniarie massime pari almeno a 5 milioni di euro o al 10% del fatturato complessivo annuo in base agli ultimi bilanci disponibili approvati dall'organo di gestione;
b) nel caso di persone fisiche, sanzioni amministrative pecuniarie massime pari almeno a 5 milioni di euro o, negli Stati membri la cui moneta non è l'euro, il valore corrispondente nella valuta nazionale alla data del 25 giugno 2015.

Al riguardo, l'art. 39, co. 1, del nuovo D.lgs. 231/2007, invece, riprende il testo dell'art. 46, co. 1, del precedente D.lgs. 231/2007, vietando ai soggetti tenuti alla SOS 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. Tale divieto non impedisce, tuttavia, la comunicazione tra gli intermediari bancari e finanziari ovvero tra tali intermediari e le loro succursali e filiazioni controllate a maggioranza e situate in Paesi terzi, *"a condizione"* che le medesime succursali e filiazioni si conformino a politiche e procedure di gruppo, ivi comprese quelle relative alla condivisione delle informazioni, idonee a garantire la corretta osservanza delle prescrizioni dettate in materia di prevenzione del riciclaggio e del finanziamento del terrorismo (art. 39, co. 3).

L'adozione delle politiche e procedure di gruppo diventa, pertanto, una condizione al ricorrere della quale è possibile la comunicazione infra-gruppo:

- nel previgente regime il divieto di comunicazione dell'avvenuta segnalazione non impediva le comunicazioni tra gli intermediari finanziari appartenenti al medesimo gruppo, anche se situati in Paesi terzi, a condizione che applicassero misure equivalenti a quelle previste dalla III Direttiva antiriciclaggio;

- nel nuovo regime, il divieto non impedisce la comunicazione tra gli intermediari bancari e finanziari ovvero tra tali intermediari e le loro succursali e filiazioni controllate a maggioranza e situate in Paesi terzi, a condizione che le medesime succursali e filiazioni si conformino a politiche e procedure di gruppo, ivi incluse quelle relative alla condivisione di informazioni, idonee a garantire la corretta osservanza delle prescrizioni dettate in materia di AML/CFT.

Pertanto, in assenza delle politiche e procedure di gruppo, ovvero laddove le succursali e filiazioni controllate a maggioranza e situate in Paesi terzi non vi si conformino, sussiste un divieto di comunicazione infra-gruppo.

L'art. 39 prevede altresì, al co. 5 (in analogia con quanto previsto dall'art. 46, co. 6), i casi relativi allo stesso cliente o alla stessa operazione, che coinvolgano due o più intermediari bancari e finanziari: il divieto di comunicazione non impedisce la condivisione tra intermediari, 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, fermo restando quanto previsto dagli artt. 42, 43 e 44 del Codice privacy.

Una volta che le Autorità di vigilanza di settore interverranno disciplinando tale aspetto, i soggetti obbligati vigilati dovranno conformarsi, pena la sanzione di cui al nuovo art. 62, co. 1, ai sensi del quale: *"nei confronti degli intermediari bancari e finanziari responsabili, in via esclusiva o concorrente, di violazioni gravi, ripetute o sistematiche ovvero plurime delle disposizioni di cui al Titolo II, Capi I, II e III, di quelle in materia*

di procedure e controlli interni di cui agli articoli 15 e 16 del presente Decreto, delle relative disposizioni attuative adottate dalle autorità di vigilanza di settore nonché dell'inosservanza dell'ordine di cui al comma 4, lettera a), si applica lo sanzione amministrativa pecuniaria da euro 30.000 a euro 5.000.000 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".

Inoltre, l'art. 62, co. 2 e 3, prescrive che *"fermo quanto disposto dal comma 1, 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 di cui al comma 1 o l'inosservanza dell'ordine di cui al comma 4, lettera a) ovvero hanno inciso in modo rilevante sull'esposizione dell'intermediario al rischio di riciclaggio o di finanziamento del terrorismo. Qualora il vantaggio ottenuto da/l'autore della violazione sia superiore a 5.000.000 di euro, la sanzione amministrativa pecuniaria è elevata fino al doppio dell'ammontare del vantaggio ottenuto, purché tale ammontare sia determinato o determinabile"* e che *"nelle ipotesi di cui al comma 2, tenuto conto della gravità della violazione accertata e nel rispetto dei criteri di cui all'articolo 67, le autorità di vigilanza di settore, secondo le rispettive competenze, hanno il potere di applicare la sanzione amministrativa accessoria 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"* ([23]).

Nel nuovo regime, la violazione del divieto imposto dall'art. 39, co. 1, rimarrà altresì sanzionata – *ex* art. 55 – con l'arresto da sei mesi a un anno e con l'ammenda da 5.000 euro a 30.000 euro, salvo che il fatto costituisca più grave reato.

5. Conclusioni

In attesa di capire come verrà declinato in termini pratici l'obbligo di dotarsi di politiche e procedure di gruppo per lo scambio di informazioni ai fini AML/CFT, è difficile prevedere un obbligo di scambio di dati personali della generalità dei clienti nei gruppi bancari/finanziari o di categorie o gruppi di clienti (quali, ad esempio, tutte le persone politicamente esposte o tutti i clienti con un profilo di rischio maggiore).

Sarà interessante valutare le modalità con cui le capogruppo:

([23]) Per completezza, si segnala che l'art. 62, co. 5, punisce con la sanzione amministrativa pecuniaria da euro 3.000 a 1.000.000 anche i revisori legali e le società di revisione legale con incarichi di revisione su enti di interesse pubblico o su enti sottoposti a regime intermedio responsabili di violazioni gravi, ripetute o sistematiche ovvero plurime delle disposizioni di cui al Titolo II, Capi I, II e III, di quelle in materia di procedure e controlli interni di cui agli artt. 15 e 16, delle relative disposizioni attuative adottate dalla Consob.

- assicureranno che le sedi in un altro Stato membro rispettino le disposizioni locali che recepiscono la IV Direttiva;

- imporranno alle succursali o filiazioni controllate a maggioranza e situate in Paesi terzi, che applicano obblighi minimi in materia di AML/CFT meno rigorosi di quelli applicati sul suo territorio, di applicare gli obblighi dello Stato membro della capogruppo stessa, anche in materia di protezione dei dati, nella misura consentita dal diritto interno del Paese terzo;

- nei casi in cui l'ordinamento di un Paese terzo non consente l'attuazione delle politiche e delle procedure di gruppo, assicureranno che le succursali o le filiali controllate a maggioranza situate in detto Paese terzo applichino misure supplementari per far fronte in modo efficace al rischio di riciclaggio o di finanziamento del terrorismo e ne informino le competenti autorità del loro Stato membro d'origine;

- consentano la condivisione delle informazioni all'interno del gruppo, con particolare riguardo alle informazioni relative al sospetto che i fondi provengano da attività criminose o siano collegati al finanziamento del terrorismo di cui è stata fatta segnalazione.

L'obbligo di condivisione delle informazioni atterrà certamente alle SOS effettuate ed ai soggetti riguardati dalle segnalazioni stesse.

Le modalità di scambio dei dati, che a rigore sarà obbligatorio, dovranno essere regolamentate in apposita *policy*/procedura formalizzata a livello di gruppo, secondo la strategia dettata dalla capogruppo e nel rispetto delle normative locali dei Paesi di origine delle singole società del gruppo. In particolare, la *policy* potrà limitare l'accesso a tali informazioni ai soli responsabili delle strutture che dovranno valutare l'operatività dei clienti e l'apertura di nuovi rapporti ai fini antiriciclaggio; ciò al fine di evitare un accesso indiscriminato con il conseguente rischio che l'informazione relativa all'avvenuta SOS trapeli, con violazione del disposto dell'art. 39 del D.lgs. 231/2007.

In secondo luogo, verrà richiesto ai gruppi di rafforzare l'approccio globale al rischio di riciclaggio in termini di adozione di *policy*/procedure coerenti per tutte le realtà del gruppo (compatibilmente con la normativa locale applicabile a ciascuna), secondo la strategia dettata dalla capogruppo, che tuttavia non è detto che debba prevedere un obbligo di condividere infra-gruppo i dati relativi alla clientela *tout court*, senza che ciò sia giustificato da una specifica esigenza sottostante. Infatti, il principio secondo cui *"nel caso dei gruppi, ai quali la presente normativa riserva specifiche disposizioni, si ravvisano esigenze di coordinamento ma anche di conoscenza integrata della clientela"* (cfr. Provvedimento Banca d'Italia marzo 2011) ormai non può che essere interpretato alla luce della sopra richiamata previsione della IV Direttiva secondo la quale il presupposto per la condivisione delle informazioni è che ricorra il sospetto che "*i fondi provengano da attività criminose o siano collegati al finanziamento del terrorismo*".

Alla luce di quanto precede, con riguardo all'approccio globale richiesto, si ritiene che la *policy* di gruppo dovrà ragionevolmente prevedere:

1. innanzitutto una condivisione ed uniformazione dei criteri e delle modalità di adeguata verifica della clientela e, in tale ambito, di attribuzione dei profili di rischio;

2. in secondo luogo, con specifico riguardo alla condivisione di informazioni:

   – il già richiamato obbligo in capo a ciascuna società di comunicare alle altre società del gruppo le SOS effettuate;

   – il riconoscimento a ciascuna società del gruppo che stia valutando l'operatività di un determinato cliente in relazione ad un possibile sospetto di riciclaggio o finanziamento al terrorismo della facoltà di richiedere alle altre società del gruppo se abbiano rapporti con il cliente stesso e, in tal caso, le informazioni da esse raccolte nell'ambito dell'adeguata verifica della clientela;

   – la creazione di un *database* condiviso dei nominativi dei clienti classificati ad alto rischio da ciascuna società del gruppo, alimentato da e accessibile a tutte le società del gruppo. Le informazioni inserite nel database potrebbero limitarsi ai dati identificativi del cliente, senza neppure dare evidenza della/e società del gruppo con la/e quale/i il cliente abbia rapporti in essere.

Infine, come sopra indicato con riguardo alla condivisione delle informazioni sulle SOS, nella definizione delle regole di gruppo si dovrà garantire che lo scambio di informazioni sia funzionale esclusivamente alla prevenzione del rischio AML/CFT e che siano inibiti utilizzi differenti dei dati scambiati; ciò in considerazione della rilevanza delle informazioni stesse e dei danni che a ciascuna società del gruppo potrebbero derivare da fughe di notizie (si pensi, ad esempio, al rischio di sanzioni in caso di violazioni dell'art. 39 o ai danni derivanti da contestazioni da parte dei clienti per la divulgazione di informazioni ad essi attinenti).

La *policy* dovrebbe quindi essere strutturata in modo tale da evitare un accesso indiscriminato alle informazioni condivise, ad esempio riservando alle sole strutture antiriciclaggio delle società del gruppo l'accesso al *database*.