Privacy e anti-riciclaggio: due normative in evoluzione alla ricerca di una difficile "sintesi"

Roma, 20 giugno 2018

Ettore Frustaci

BonelliErede

Introduzione

- Le attività richieste dalla normativa in materia di anti-riciclaggio comportano operazioni di «trattamento» dei dati personali dei soggetti da identificare/ monitorare
- Gli adempimenti imposti dall'una e dall'altra normativa si intrecciano e non sempre sono compatibili tra loro:

Per es.

…la normativa AML richiede ai soggetti obbligati di ottenere dai propri clienti informazioni sufficienti a svolgere i compiti loro rimessi – **maggiori le informazioni, migliori le possibilità di svolgere efficacemente i controlli richiesti**

…ma la normativa privacy si basa sul principio di minimizzazione delle operazioni di trattamento – **solo i dati veramente necessari alle finalità del trattamento vanno trattati**

Quale esigenza deve essere privilegiata?

E ancora:

…l'adempimento degli obblighi previsti dalla normativa AML prevede la raccolta e la conservazione (per un lungo periodo di tempo) di una grande quantità di dati personali dei soggetti interessati…

…ma la normativa sulla privacy prevede che possano essere effettuate solo operazioni di trattamento funzionali alle finalità per cui i dati personali sono stati originariamente raccolti…

Come assicurare che tale patrimonio informativo non sia utilizzato per finalità ultronee (marketing diretto; valutazione del merito di credito, ecc.)?

Prima Parte: la situazione precedente all'adozione della c.d. «IV Direttiva Anti-Riciclaggio» e del GDPR

- Coordinamento tra le due normative opportuno ma sempre trascurato

- la disciplina AML nasce prima di quella privacy (L. 197/1991, successivamente sostituita dal D.lgs. 231/2007)

- la disciplina sulla privacy è stata prima regolata dalla l. 675/1996 successivamente sostituita dal D.gls. 196/2003 (c.d. «Codice Privacy»)

L'AML vista nell'«ottica» del Codice Privacy

- attività AML tra quelle necessarie ad adempiere un obbligo di legge (consenso non necessario)

- applicabili tutti gli obblighi ordinariamente previsti, tra cui:

  - informativa preventiva anche sulle attività di AML
  - misure minime di sicurezza per prevenire il rischio di perdita, distruzione o accessi non autorizzati
  - nomina incaricati del trattamento e istruzioni inerenti all'ambito di trattamento consentito

- diritto di accesso escluso «*in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio*»

L'AML vista nell' «ottica» del Codice Privacy – Gli interventi del Garante

- Parere favorevole sullo schema di decreto AML, con qualche riserva sull'eccessiva genericità di alcuni adempimenti e sulla discrezionalità lasciata agli intermediari:
  - collaborazione attiva dei destinatari della normativa AML, **ma nel rispetto delle prescrizioni del Codice**
  - adeguata verifica della clientela, **ma senza la raccolta di dati eccedenti rispetto al perseguimento delle finalità richieste**
  - segnalazione di operazioni sospette, **ma con criteri idonei a consentire di determinare quando sia legittimo sospettare**
  - approccio basato sul rischio, **ma è necessario fissare dei parametri**
- Riconosciuta la legittimità del trasferimenti delle informazioni riguardanti le SOS tra intermediari appartenenti al medesimo gruppo quale perseguimento di un interesse legittimo

La privacy vista nell' «ottica» del Decreto AML

- Nel complesso meri rinvii alle disposizioni del Codice Privacy che non aiutano a definire una disciplina di coordinamento

- Riconosciuto in termini generali l'obbligo di dare applicazione alle disposizioni del Codice Privacy (es. Art. 3 co. 2: «*I sistemi e le procedure adottati* […] *rispettano le prescrizioni e garanzie stabilite dal presente decreto* ***e dalla normativa in materia di protezione dei dati personali***»)

- Limitato in maniera sostanziale il diritto di accesso («*i soggetti obbligati alla segnalazione non possono comunicare al soggetto interessato o a terzi l'avvenuta segnalazione di operazione sospetta o che è in corso o può essere svolta un'indagine in materia di riciclaggio o di finanziamento del terrorismo*»)

- Approccio basato sul rischio. **Come si coniuga con la tutela dei dati personali?**

La privacy nell' «ottica» del Decreto AML…e nei provvedimenti attuativi della Banca d'Italia

- molto scarsi i riferimenti alla tutela della privacy
- nel provvedimento per la tenuta dell'A.U.I., si fa riferimento espresso al Codice Privacy, specificando che:
  - la registrazione deve avvenire nel rispetto dei principi generali in materia di trattamento;
  - è necessaria l'informativa per gli interessati;
  - le operazioni di trattamento devono essere svolte dagli incaricati del trattamento;
  - è necessario rispettare le misure minime di sicurezza
- Complessivamente non vengono forniti chiarimenti rispetto alle problematiche di coordinamento tra le due discipline

E, invece, le problematiche di coordinamento si presentano… sia dal lato privacy

- Provvedimento del Garante Privacy del 28 novembre 2013:

➢ illeciti certi trattamenti di dati personali svolti da Poste Italiane nell'ambito dell'adempimento dei propri obblighi AML

➢ gli obblighi AML devono essere concretamente assolti commisurando il relativo adempimento al grado di rischiosità associato al tipo di cliente,

➢ nel caso in questione il criterio dell´"approccio basato sul rischio" risulta essere stato disatteso da Poste Italiane, la quale, in occasione dell´espletamento dei controlli richiesti dalla normativa vigente, ha effettuato verifiche (comportanti anche il trattamento dei dati personali dell´interessato) obiettivamente eccedenti in rapporto al "profilo di rischio"

…sia dal lato AML

- Interpretazione restrittiva dei Tribunali sull'obbligo di effettuare segnalazioni cc.dd. di secondo livello :

"La segnalazione delle operazioni recanti anomalie formali non è subordinata, dunque, all'evidenziazione dalle indagini dell'operatore di un quadro indiziario di riciclaggio e neppure all'esclusioni in base ad un personale convincimento dello stesso dell'estraneità dell'operazione ad una attività delittuosa, ma ad un giudizio puramente tecnico sulla idoneità di esse, valutati gli elementi oggettivi e soggettivi che le caratterizzano, ad essere strumento di elusione alle disposizioni»

Seconda Parte: la fase intermedia: la revisione della normativa AML

- A distanza di pochi anni l'una dall'altra tanto la normativa in materia di antiriciclaggio che quella in materia di privacy sono andate incontro ad importanti innovazioni

- Meno significative quelle riguardanti l'anti-riciclaggio: sostituzione della direttiva

- Di portata storica quelle riguardanti la privacy: la direttiva viene sostituita da un regolamento direttamente applicabile in tutti gli stati membri

- La decisione di riformare radicalmente la normativa sulla privacy è legata anche all'eccessiva pervasività di controlli effettuati per supposte esigenze di interesse pubblico

L'occasione giusta per trovare una «sintesi»?

- Il primo progetto di riforma è quello della normativa AML
- Le raccomandazioni FATF non affrontavano il problema dell'interazione tra norme AML e norme in materia di privacy
- L'Article 29 Working Party ed il Garante Europeo per la Protezione dei Dati hanno espresso dei pareri sulla bozza di direttiva, finalizzati a sollevare problematiche di lunga data nel coordinamento tra normativa AML e privacy

I suggerimenti dell'Article 29 Working Party e del GEPD

- **<u>Revisione del c.d. divieto di «tipping off», tramite</u>**:
  - minore discrezionalità per stati membri nell'attuazione del divieto;
  - possibilità di circoscrivere la limitazione del diritto di accesso nel tempo;
  - possibilità di escludere SOS che si rilevino infondate o irrilevanti

- **<u>Regime applicabile ai dati sensibili raccolti nell'ambito delle operazioni di adeguata verifica della clientela:</u>**
  - Non viene chiarito se tali dati possano essere utilizzati o meno e con quali limitazioni
  - Rischi di operare scelte arbitrarie e discriminatorie

- **<u>Sproporzione del termine di conservazione delle informazioni raccolte nell'ambito delle attività di adeguata verifica</u>**:

  - possibilità di differenziare la durata degli obblighi di conservazione on a case by case basis

Attenzione limitata alle raccomandazioni fornite…ma con qualche eccezione

- La maggior parte delle segnalazioni effettuate da Article 29 WP e dal GEPD non sono state inserite all'interno della versione finale della nuova direttiva

- La direttiva riconosce però la necessità che le operazioni di trattamento svolte nell'ambito delle attività AML possano perseguire solo le finalità della direttiva stessa e non scopi ultronei

«*Alcuni aspetti dell'attuazione della presente direttiva comportano la raccolta, l'analisi, la conservazione e la condivisione dei dati.* ***Tale trattamento dei dati personali*** […] *dovrebbe essere consentito* ***esclusivamente per gli scopi definiti nella presente direttiva e per le attività previste da essa*** […]. ***In particolare, occorre vietare categoricamente l'ulteriore trattamento dei dati personali a fini commerciali***.»

Parte Terza: il D.lgs. 231/2007 post riforma ed il suo coordinamento con il GDPR

Le disposizioni in materia di trattamento di dati personali nella nuova versione del D.lgs. 231/2007

- Viene riconosciuta espressamente la limitazione dell'utilizzo dei dati raccolti nell'ambito degli adempimento AML al perseguimento delle finalità previste dal Decreto:

Art. 3, co. 9: «*I soggetti obbligati assicurano che il trattamento dei dati acquisiti nell'adempimento degli obblighi di cui al presente decreto avvenga,* ***per i soli scopi e per le attività da esso previsti*** *e nel rispetto delle prescrizioni e delle garanzie stabilite dal Codice in materia di protezione dei dati personali*»

- Viene riconosciuta la necessità di coltivare una cultura aziendale in cui gli obblighi AML siano allineati a quelli imposti dalla privacy:

Art. 16: «*I soggetti obbligati adottano misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi del presente decreto,* ***ivi compresi quelli in materia di protezione dei dati personali***»

I provvedimenti BdI e IVASS in consultazione

- BdI e IVASS hanno recentemente avviato delle consultazioni sulle bozze dei provvedimenti attuativi del nuovo Decreto in materia di:
  - Organizzazione, procedure e controlli in tema di anti-riciclaggio; e
  - Adeguata verifica della clientela

- Nonostante le maggiori attenzioni dedicate alle tematiche privacy dal Decreto, non vengono fornite particolari istruzioni sul coordinamento tra le due normative

- Si fa riferimento alla necessità di raccogliere il consenso degli interessati nel caso di procedure cc.dd. di video-identificazione

I Provvedimenti BdI – IVASS in consultazione

Alcuni adempimenti richiesti rispetto alle attività di adeguata verifica rafforzata (i.e. i casi in cui sussistono elevati rischi di riciclaggio e finanziamento del terrorismo) suscitano alcune perplessità:

- lo svolgimento di attività di adeguata verifica rafforzata richiede l'acquisizione di maggiori informazioni sul cliente e sul titolare effettivo.

- sono espressamente indicate alcune ipotesi da considerarsi **sempre** a rischio elevato (e.g. clienti residenti in paesi ad alto rischio; rapporti di corrispondenza transfrontalieri; PEP; importi insolitamente elevati);

- per le ulteriori ipotesi bisogna rifarsi ai fattori di rischio previsti dal Decreto ed arricchiti dal provvedimento in consultazione e che riguardano:
  - Fattori di rischio relativi al cliente, all'esecutore o al titolare effettivo;
  - Fattori di rischio relativi alla tipologia di prodotto;
  - Fattori di rischio geografici

- tra i fattori di rischio relativi al cliente rientrano, tra l'altro, «*indici reputazionali negativi*», *fermo restando che «[n]el valutare le notizie negative provenienti dai media o da altre fonti informative i destinatari ne considerano la fondatezza e l'attendibilità basandosi, tra l'altro, sulla qualità e sull'indipendenza di tali fonti informative*»

- ***Rimane il rischio che vi sia eccessiva discrezionalità da parte dei soggetti obbligati circa le ipotesi in cui tali attività di adeguata verifica rafforzata trovano applicazione.***

- Altri elementi di perplessità riguardano la necessità (già presente nelle precedenti versioni dei provvedimenti) di raccogliere informazioni che dovrebbero essere acquisite rispetto a soggetti terzi:

  - Parte II, Sezione VI: «*In caso di rischio elevato, sono acquisite e valutate ulteriori informazioni relative al cliente ed al titolare effettivo, tra cui:*
    […]
    - ***la situazione lavorativa, economica e patrimoniale di familiari e conviventi***»
  - Parte IV, Sezione II: «*è inclusa l'acquisizione e la valutazione di informazioni sulla reputazione del cliente e/o del titolare effettivo* […]. ***Rilevano tra l'altro informazioni riguardanti i familiari e coloro con i quali il cliente intrattiene stretti rapporti d'affari***»

Capo III, Sezione IV Provv. IVASS: «*Costituiscono fattori di rischio elevato concernenti i rapporti continuativi e le operazioni* […] *la designazione di uno o più beneficiari non legati al cliente o al titolare effettivo da legami affettivi, di parentela, di affinità, coniugio, unione civile oppure quando i legami dichiarati non sono coerenti con le circostanze di cui l'impresa è comunque a conoscenza*»

- Come coordinare tali adempimenti con gli obblighi di informativa, applicabili anche in caso di raccolta di dati personali presso terzi?

Che cosa cambia con l'introduzione del GDPR

L'impatto del GDPR

- Il GDPR non priva di per sé di efficacia gli obblighi previsti dalla normativa AML

- il Considerando 19 fa riferimento espresso agli adempimenti anti-riciclaggio, giustificando le limitazioni di diritti e obblighi che siano funzionali al perseguimento di tali interessi:

«***Quando il trattamento dei dati personali effettuato da organismi privati rientra nell'ambito di applicazione del presente regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti***, *qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica.* ***Ciò riveste particolare importanza ad esempio nel quadro del riciclaggio***.»

L'impatto del GDPR

- Articolo 6 GDPR: «*Il trattamento è lecito solo se e nella misura in cui ricorre una delle seguenti condizioni:*

  […]

  (c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento»

- Articolo 17 GDPR [Diritto all'oblio]: «[i] *Paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:*

  […]

  (b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello stato membro cui è soggetto il titolare del trattamento»

L'impatto del GDPR

Ciò non vuol dire che l'entrata in vigore del GDPR non abbia effetti rilevanti anche rispetto alle operazioni di trattamento che i soggetti obbligati sono tenuti a svolgere ai sensi della normativa AML:

- Articolo 25: «*il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*»

- Articolo 30: «*ogni titolare del trattamento* […] [tiene] *un registro delle attività di trattamento svolte sotto la propria responsabilità*»

- Articolo 35: valutazione d'impatto sulla protezione dei dati

L'Impatto del GDPR – E' questa la sintesi?

- Nel regime normativo precedente (tanto più a seguito della abolizione dell'obbligo del DPS), l'impatto della normativa privacy finiva per essere assorbito dai preponderanti interessi pubblici perseguiti dall'AML.

- Le misure a tutela della privacy finivano per avere una valenza più formale che sostanziale (informativa; nomina incaricati; nomina responsabile).

- Le innovazioni apportate dal GDPR impongono un nuovo approccio nello svolgimento delle operazioni di trattamento, anche per operazioni di trattamento che siano finalizzate a dare seguito ad obblighi di legge

- Necessario in particolare coordinare l'approccio basato sul rischio con i principi di privacy by default e privacy by design e le esigenze in tema di minimizzazione nell'utilizzo dei dati personali che essi richiedono

L'impatto del GDPR – E' questa la sintesi?

L'occasione giusta per trovare la «sintesi»

- Poco dopo l'entrata in vigore del GDPR, gli intermediari saranno chiamati ad adottare le politiche aziendali richieste dai provvedimenti messi in consultazione da IVASS e BdI

- E' necessaria in particolare l'adozione di un documento ove siano indicate le scelte che il destinatario intende in concreto compiere sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati

- Tale documento dovrà necessariamente tenere conto delle valutazioni effettuate dai medesimi titolari ai fini del loro registro trattamenti, della valutazione d'impatto, nonché più in generale per conformarsi ai principi di privacy by default e privacy by design