DB non solo diritto bancario

www.dirittobancario.it

APPROFONDIMENTI

Antiriciclaggio | Governance e controlli

Il trattamento dei dati personali nel nuovo AML Package

Andrea Fedi, Partner, Legance

12 Novembre 2025

Di cosa si parla in questo articolo

AI Act | AML | GDPR | Regolamento Antiriciclaggio

Indice dell'articolo

*Il presente contributo analizza il tema del **trattamento dei dati personali** in ambito **antiriciclaggio** alla luce delle novità introdotte dal nuovo Regolamento (UE) 2024/1624 (**Regolamento Antiriciclaggio**) parte del c.d. **AML Package**.*

1. Introduzione

Non c'è stata era, nella storia dell'uomo, in cui la **disponibilità di informazioni e la capacità di metterle in relazione** non sia stata un **centrale strumento di potere e fonte di responsabilità**. Non sta in questo, dunque, il tratto distintivo nel mondo odierno; semmai lo è la capacità – acquisita oggi grazie alla scienza e alla tecnica informatica – di:

- riprodurre con relativa facilità enormi quantità d'informazioni,
- stivarle in spazi informatici virtuali,
- rapportarle, confrontarle e combinarle,

in maniera tale da dischiuderne appieno tutte le potenzialità.

Il **trattamento dei dati** (personali o non personali) **è dunque divenuto semplice, efficace e pervasivo**, propagandosi in tutte le attività di progetto, amministrazione e/o supervisione: da quelle economiche, a quelle militari o politiche, a quelle di vigilanza, contrasto[1] o controllo pubblico (specialmente con la vittoriosa progressione dei sistemi di *Artificial Intelligence*).

Questo **fenomeno riguarda** inevitabilmente **anche l'antiriciclaggio**:

- sia dal punto di vista delle **autorità pubbliche** preposte alla sorveglianza,
- sia da quello dei **soggetti obbligati**.

In questo ambito, assumono particolare rilievo le disposizioni del recente AML Package, costituito:

- dalla Direttiva UE 31 maggio 2024 n. 1640 (di seguito, **Direttiva Antiriciclaggio**),
- dal Regolamento UE 31 maggio 2024 n. 1620 (di seguito, **Regolamento AMLA**) e
- dal Regolamento 31 maggio 2024 n. 1624 (di seguito, **Regolamento Antiriciclaggio**),

da leggere in combinato disposto con le norme:

- del Regolamento UE 27 aprile 2016 n. 679 (di seguito, **GDPR**) e del D.Lgs. 30 giugno 2003 n. 196 come modificato dal D.Lgs. 10 agosto 2018 n. 101 (di seguito **Codice Privacy)** (il GDPR e il Codice Privacy sono d'ora innanzi richiamati con il sintagma: **Normativa Privacy**) e
- del Regolamento (UE) 13 giugno 2024 n. 1689 (di seguito, **AI Act**) e della legge 8 agosto 2025 n. 132 (di seguito, **Legge IA**) (l'AI Act e la Legge IA sono d'ora innanzi richiamati con il sintagma: **Normativa AI**).

L'incrocio tra la nuova normativa **verticale** sull'antiriciclaggio e quella **orizzontale** su dati personali e AI, oltre che necessario, si dimostra interessante e pregno di conseguenze giuridiche perché le disposizioni presentano molti aspetti meritevoli di uno sguardo attento e trasversale.

2. Principi fondamentali del trattamento

Sono molti i tipi di dati oggetto di trattamento[2] a fini antiriciclaggio, da parte pubblica e da parte privata:

- dati personali comuni[3] (di seguito, **dati comuni**),
- dati personali appartenenti a categorie speciali[4] (di seguito, **dati sensibili**),
- dati personali giudiziari penali[5] (di seguito, **dati penali**),
- dati non personali[6].

È infatti più che evidente che le operazioni di verifica e controllo antiriciclaggio (incluse le procedure di adeguata verifica e quelle per la segnalazione di operazioni sospette: "**SOS**") immancabilmente coinvolgono: sia dati non personali (informazioni non riferibili a una persona fisica, ad es. tutte quelle che riguardano società e persone giuridiche), sia dati comuni di una persona fisica (basti pensare a nome, cognome, luogo e data di nascita), ma anche, più che frequentemente, notizie su persone politicamente esposte e loro parenti e affini (dati sensibili) e/o dati su procedimenti o provvedimenti penali (dati penali).

Ebbene, ogni operazione di trattamento – anche in ambito antiriciclaggio – deve rispettare il GDPR, il cui art. 5 declina i sei **principi fondamentali** per ogni trattamento di dati personali (*ergo*: anche quelli a fini antiriciclaggio):

- **Liceità, correttezza e trasparenza** nei confronti del soggetto interessato
- **Specificità dei fini** per i quali il trattamento è consentito
- **Minimizzazione** del trattamento
- **Qualità** dei dati
- **Durata congrua** della conservazione dei dati
- **Misure di sicurezza**.

Da parte sua, laddove si faccia uso di sistemi AI, l'AI Act prescrive numerosi requisiti, differenziati a seconda che si tratti di sistemi ad alto rischio, a rischio limitato o a rischio minimo, sistemi di AI per finalità generali:

- **trasparenza**
- **qualità dei dati**
- **sistemi di gestione dei rischi**
- **sicurezza**.

Tutti tali temi trovano richiamo nell'AML Package[7], che: da una parte, ribadisce l'**applicazione concorrente** delle sue norme e di quelle del GDPR[8], dall'altra detta **regole attuative** dei principi contenuti nella Normativa Privacy e nella Normativa AI.

Ora, a parte le difficoltà del combinato disposto tra discipline tanto prolisse quali quelle di cui discutiamo, l'aspetto che inizialmente colpisce è legato all'art. 2-decies del Codice Privacy, a mente del quale "*I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali* ***non possono essere utilizzati****, salvo quanto previsto dall'articolo 160-bis*" (che prevede che la validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme restano disciplinate dalle pertinenti disposizioni processuali). Viene quindi da chiedersi se il mancato stretto rispetto delle norme sulla protezione dei dati personali e sul rispetto dei diritti fondamentali possa rendere i dati inutilizzabili, salvo che all'interno di un procedimento giudiziario.

3. Base giuridica del trattamento

Ogni trattamento di dati personali deve poggiare su una delle basi giuridiche contemplate dal GDPR. Tali basi giuridiche sono diverse a seconda che si tratti di:

- **dati comuni**,
- **dati sensibili** o
- **dati penali**[9].

Con riferimento a quanto precede, le basi giuridiche del trattamento legittimo ai sensi del GDPR sono peraltro molto diverse a seconda che il trattamento sia effettuato da un'autorità o da un soggetto obbligato.

- Per quanto riguarda le autorità, i trattamenti possono essere giustificati dall'esistenza di un compito di **interesse pubblico** o connesso all'esercizio di pubblici poteri (art. 6.1.e GDPR per i dati comuni), o dalla necessità del trattamento per motivi di **interesse pubblico "rilevante"** (art. 9.2.g GDPR per i dati sensibili), o, ancora, dalla circostanza che il trattamento avvenga **sotto il controllo dell'autorità** o comunque **in base al diritto unionale o nazionale** (art. 10 GDPR per i dati penali)[10].
- Per quanto riguarda i soggetti obbligati, la base giuridica può invece consistere nell'indispensabilità di adempiere **obblighi legali** (art. 6.1.c GDPR per i dati comuni e art. 10 GDPR per i dati penali) o in motivi di **interesse pubblico "rilevante"** (art. 9.2.g GDPR per i dati sensibili).

Non basta tuttavia una mera norma giuridica o l'esistenza di un generico interesse pubblico per giustificare il trattamento.

Innanzitutto, con riferimento ai dati sensibili, tale interesse deve essere "rilevante" (e non basta a questo riguardo la natura dell'organizzazione che opera il trattamento).

In secondo luogo e in linea più generale, il trattamento secondo il GDPR deve essere sempre **proporzionato** e l'interesse pubblico deve essere **riconosciuto da una norma** che: ne precisi i contorni di liceità e le modalità di trattamento, identifichi il titolare dello stesso, perimetri i dati personali trattabili e la finalità del trattamento, nonché il periodo massimo di conservazione dei dati (considerando 45 e art. 6.3 e 9 GDPR).

In questa cornice valoriale, gli artt. 2-ter e 2-sexies del Codice Privacy[11] stabiliscono che:

- il riconoscimento dell'interesse pubblico può essere contenuto in norme **di legge o di regolamento**, ma, **nel caso dei dati sensibili**, tali norme devono ulteriormente specificare: il tipo di dati, le operazioni eseguibili e lo specifico motivo d'interesse pubblico, nonché le misure appropriate e specifiche a tutela dei diritti fondamentali;
- la comunicazione dei dati è permessa solo se prevista **da legge o regolamento**[12].

Ecco dunque spiegata la radice di vari passaggi delle norme dell'AML Package che insistono sull'esistenza di un **interesse pubblico**[13], stabiliscono **particolari cautele**[14], nonché regole su **conservazione**[15] **e trasparenza**[16] e, infine, dettano cautele *ad hoc* per **i dati sensibili e i dati penali**.

A questo ultimo proposito si segnala che:

1. l'art. 9 della Direttiva Antiriciclaggio consente il trattamento di dati sensibili o penali da parte delle autorità, ma **solo nella misura necessaria** e con l'applicazione di **garanzie adeguate**, cui deve aggiungersi che il trattamento è ammesso solo da parte di **personale autorizzato e competente** e con **misure tecniche e organizzative** secondo standard tecnologici elevati, a tutela della sicurezza;
2. il considerando 152 Regolamento Antiriciclaggio ordina di **non prendere decisioni basate solo sui dati sensibili** se non strettamente pertinenti alle finalità antiriciclaggio;

- l'art. 76 Regolamento Antiriciclaggio permette il trattamento ai **soggetti obbligati** di **dati sensibili** o **penali**, a condizione però che:
- *per i dati sensibili*: gli interessati siano **informati**, i dati siano **qualitativamente adeguati**, le decisioni adottate **non** diano luogo a risultati **discriminatori o distorti**, siano adottate **misure che consentano un elevato livello di sicurezza**;
- *per i dati penali*: i dati riguardino l'**ambito del riciclaggio** e reati presupposto, le procedure adottate dai soggetti obbligati consentano di **distinguere** tra accuse e condanne,
- *in entrambi i casi*, il trattamento sia finalisticamente limitato **unicamente** alla prevenzione del riciclaggio e del finanziamento del terrorismo[17] (dunque, a rigore, le banche di dati sensibili o penali dei soggetti obbligati **non possono essere usate** per valutare l'affidabilità di controparti o per *due diligence*, ma nemmeno per valutazioni ai sensi del D.Lgs. 231/2001.).

Quid juris, nel caso in cui le disposizioni che precedono non siano rispettate?

Sembra fondato ritenere che, se la violazione sia imputabile all'autorità, l'eventuale procedimento sanzionatorio possa essere impugnato per violazione di legge ed eccesso di potere.

Sia che la violazione sia stata compiuta dall'autorità sia che sia stata compiuta dal soggetto obbligato, possono poi essere innescate le sanzioni monetarie e non monetarie che il Garante Privacy ha il potere di irrogare e, eventualmente, può anche originarsi un obbligo di risarcimento del danno civile.

4. L'accesso ai dati

I casi di accesso ai dati sono sviluppati nell'AML Package in tre direzioni:

- Accesso di un'autorità ai dati di un'altra autorità
- Accesso di un privato ai dati di un'autorità
- Accesso dell'operatore privato interessato da un procedimento o indagine.

Ebbene, anche con riferimento alle problematiche relative all'accesso, le disposizioni dell'AML Package tentano un allineamento con i principi e i requisiti imposti dalla Normativa Privacy.

- Innanzitutto, si sottolinea che l'accesso alle informazioni deve essere effettuato in modo da evitare **qualsiasi rischio di "divulgazione"** di informazioni riservate[18] e rispettando il principio del *need to know*[19].
- In secondo luogo, si stabilisce che le autorità responsabili dei registri centrali debbano dare accesso ai dati dei soggetti interessati solo a persone aventi un "**interesse legittimo**"[20] (che siano privati o altre autorità).

Detto termine riecheggia in maniera evidente l'interesse legittimo contemplato dal GDPR, che ne fa una base giuridica per il trattamento, ma "**a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato**"[21] e solo per quanto riguarda **i dati comuni** (non per i dati sensibili o penali)[22].

Coerentemente, si ritiene che anche le autorità dovranno dare o negare l'accesso tenendo conto del tipo di dati che sarebbero disvelati e **bilanciando** gli interessi dei soggetti che chiedono l'accesso e i diritti dei soggetti i cui dati sarebbero oggetto di accesso.

Fin qui, si tratta di interpretare organicamente l'AML Package con la Normativa Privacy.

La Direttiva Antiriciclaggio introduce però una novità, ossia dei casi di **interesse legittimo 'presunto'** per determinate categorie di soggetti (ONG, accademici, giornalisti), limitando altresì le informazioni sui loro accessi che gli organismi responsabili dei registri centrali devono dare ai soggetti interessati[23].

Altri aspetti rilevanti dell'AML Package in termini di accesso e *data governance* sono poi le disposizioni che subordinano a particolari cautele il **trasferimento all'estero** di dati personali a favore di altre autorità[24] e le **limitazioni, imposte al diritto all'accesso** ai propri dati da parte dell'interessato soggetto ad accertamenti e indagini, al fine di non frustrare l'obiettivo delle indagini stesse[25] e assicurare il rispetto delle regole di trattamento dei dati sensibili e penali[26]. Relativamente a ciò, la Direttiva Antiriciclaggio e Regolamento Antiriciclaggio richiamano, quale fondamento della limitazione, la possibilità, offerta al diritto nazionale dall'art. 23 GDPR[27], di condizionare e circoscrivere i diritti d'accesso ai dati qualora si tratti di proteggere indagini penali o altri importanti casi d'interesse pubblico (art. 23.1, d, e, h). Questa possibilità, in Italia, è stata colta dall'art. 2-undecies del Codice Privacy, che fa espresso riferimento alla normativa antiriciclaggio (lett. a)[28].

5. I trattamenti automatizzati e l'AI

Un aspetto di particolare interesse dal punto di vista delle interrelazioni tra AML Package, Normativa Privacy e Normativa AI è l'indagine sul se, quando e come sia possibile un **trattamento automatizzato** dei dati a fini antiriciclaggio[29]: vuoi quando sia l'autorità a sfruttare le nuove tecnologie per la sorveglianza e la repressione, vuoi quando i soggetti obbligati si avvalgano di questi strumenti tecnologici per adempiere ai loro doveri.

Un trattamento automatizzato può invero esemplificativamente accadere in tre casi.

- Il primo è quello che si materializza quando l'autorità pubblica o il soggetto obbligato si valgono di tecniche di **profilazione**[30] di persone fisiche (art. 4(4) GDPR), per trarne indicazioni, anche basate su precedenti analisi antiriciclaggio, sull'attività, localizzazione geografica o affidabilità di persone fisiche, ivi inclusi gli aspetti di loro affidabilità in relazione alla *compliance*.
- Un secondo aspetto appare sulla scena quando le **decisioni**, dell'autorità o del soggetto obbligato, **sono adottate in modo esclusivamente automatizzato** (art. 22 GDPR), in ipotesi per condurre l'adeguata verifica o per avviare indagini e controlli o decidere se effettuare una SOS.
- L'ultimo aspetto, il terzo, viene alla ribalta laddove una verifica o una decisione sia istruita ed eventualmente presa **mediante sistemi AI**[31], che esemplificativamente assegnino un determinato punteggio (AML *scoring*[32]) a categorie di soggetti o di operazioni.

Il legislatore unionale ha intercettato tutti e tre tali temi con le disposizioni dell'AML Package, ribadendo tuttavia l'opportunità di far uso delle nuove tecnologie con il limite dei **diritti fondamentali** e del principio di **non discriminazione**[33].

In effetti, il Regolamento Antiriciclaggio contiene una disposizione specifica (art. 76.5).

Per spiegarne il contenuto e le interrelazioni con la Normativa Privacy e la Normativa AI è tuttavia bene partire dal considerando 150, che riconosce l'interesse dei soggetti obbligati, al fine di gestire gli adempimenti di *compliance* antiriciclaggio, di far uso di tecniche di profilazione o di sistemi per l'assunzione di decisioni automatizzate, precisando chiaramente che, in questi ambiti, dovrà trovare **applicazione congiunta** sia quanto previsto dal Regolamento Antiriciclaggio, sia quanto disposto dalla Normativa Privacy.

Approfondiamo, allora, cosa prevedano la Normativa Privacy e la Normativa AI sui trattamenti automatizzati.

La Normativa Privacy

Ai sensi della Normativa Privacy, il soggetto che tratta in maniera automatizzata i dati degli interessati deve, prima di tutto, fornire **informativa** ai soggetti profilati o incisi da altro trattamento o decisione automatizzata[34] e, poi, altresì, deve consentire loro il **diritto d'accesso**[35]. Con riferimento a questi profili di trasparenza, è peraltro importante ricordare che, a seguito delle sentenze della CGUE[36], l'interessato ha diritto ad avere informazioni funzionali, rilevanti, pertinenti, intelligibili e fondate su una buona qualità dei dati presi in esame.

Dovranno essere poi rispettati l'art. 21 e l'art. 22 GDPR.

La prima disposizione prevede il diritto dell'interessato di **opporsi alla profilazione**, opposizione che può essere superata dal soggetto *profilante* solo se dimostra l'esistenza di motivi legittimi 'poziori' per continuare con il trattamento[37].

La seconda disposizione subordina la legittimità di una decisione basata **unicamente** su un trattamento automatizzato alla ricorrenza di alcune condizioni[38]. Orbene, nel caso, che ci occupa, cioè quello del soggetto obbligato che prenda una decisione automatizzata in materia di antiriciclaggio (ad esempio, la decisione di fare una SOS), l'adozione di una decisione esclusivamente automatizzata resta sottoposta alla verifica che tale decisione sia **ammessa da una norma di diritto applicabile**, la quale deve d'altra parte prevedere specifiche garanzie e tutele (vieppiù considerato che, nell'ambito del quale ci stiamo interessando, potrebbero essere oggetto di trattamento dati sensibili; art. 22.4 GDPR).

La Normativa AI

Per quanto riguarda l'AI Act, va invece ricordato l'art. 5.1 che elenca le pratiche vietate di *artificial intelligence* e proibisce l'**immissione sul mercato**, la **messa in servizio** o l'**uso** di sistemi AI:

- di *social scoring* che producano un trattamento pregiudizievole o sfavorevole in contesti sociali **diversi** da quelli in cui i dati sono stati raccolti o che siano **sproporzionati o ingiustificati** (art. 5.1.c AI Act); e/o
- di *crime prediction* o *crime forecasting* unicamente sulla base della profilazione o della valutazione della personalità (quando non sono sistemi di puro supporto alla decisione umana) (art. 5.1.d AI Act).

AML Package

Il legislatore dell'AML Package si dimostra ben consapevole di questo quadro regolamentare e detta una norma, l'art. 76.5 del Regolamento Antiriciclaggio, che legittima la possibilità di adottare decisioni anche unicamente automatizzate (incluso attraverso sistemi di AI), ma con tre specifici limiti:

- I dati che vengono considerati ai fini della decisione sono solo quelli che emergono dalle procedure di **adeguata verifica**;
- Qualsiasi decisione automatizzata è soggetta a un **significativo intervento umano** (e, ai sensi dell'art. 75.4.g, le informazioni generate dall'AI possono essere condivise nell'ambito dei partenariati solo se l'AI è stata oggetto di **adeguata sorveglianza umana**[39]),
- Il soggetto inciso dalla decisione deve poter ottenere **una spiegazione** della decisione e deve poterla **impugnare** (con esclusione della decisione di effettuare una SOS).

Si tratta di diritti **accrescitivi** delle tutele dei soggetti interessati rispetto a quanto previsto sia dalla Normativa Privacy. In primo luogo, difatti, l'art. 75.5 – unitamente ai requisiti del diritto all'intervento umano[40] e alla spiegazione[41] – si applica a tutte le decisioni automatizzate e non solo a quelle esclusivamente automatizzate né, tanto meno solo a quelle interamente automatizzate previste da una norma di legge[42].

L'AML Scoring

Alla luce della Normativa AI, sembra problematico – e l'AML Package non dipana espressamente il dubbio –l'uso di sistemi di AML *forecasting*, che potrebbero in ipotesi rientrare nel divieto di *crime prediction*. È mia opinione tuttavia che i sistemi di AML *forecasting* siano da ritenersi leciti.

La stessa Commissione UE, nei suoi Orientamenti relativi a pratiche di intelligenza vietate[43] ha infatti ricordato che:

- Il rispetto della normativa settoriale dell'Unione, ad esempio in materia di **antiriciclaggio**, può far sì che la pratica di IA non rientri nell'ambito del divieto di cui all'articolo 5, paragrafo 1, lettera c), dell'AI Act, quando la norma specifica il **tipo di dati** che possono essere utilizzati come pertinenti e necessari per lo **scopo di valutazione specifico legittimo** e garantisce che il trattamento sia **giustificato e proporzionato** al comportamento sociale, (punto 177 degli Orientamenti); e
- Sono legittimi i sistemi di valutazione del rischio che **non** riposino **unicamente** sulla profilazione o valutazione della personalità, ma prevedano un **significativo intervento umano** basato su dati oggettivi e verificabili e condotto da persone competenti e formate (par. 5.2.3 degli Orientamenti): il che è espressamente quanto richiesto dall'art. 75.5 del Regolamento Antiriciclaggio.

Va però ricordato che i sistemi AI di *AML forecasting* devono utilizzare dati di *scoring* che non provengano da contesti diversi dall'antiriciclaggio e devono essere proporzionati e giustificati, tenuto conto del fatto che tali sistemi di AI sono ad alto rischio (All. III, 6.d, AI Act) e, perciò, devono essere spiegabili ai sensi dell'art. 86 AI Act e dell'art. 75 Regolamento Antiriciclaggio.

6. I partenariati per la condivisione di informazioni

Uno degli aspetti più interessanti dell'AML Package risiede proprio nei partenariati per la condivisione delle informazioni, la cui definizione normativa è: "un meccanismo che consente **la condivisione e il trattamento** delle informazioni **tra soggetti obbligati** e, se del caso, **le autorità competenti** di cui al punto 44, lett. a), b) e c), **ai fini** della prevenzione e della lotta contro il riciclaggio, i reati presupposto associati e il finanziamento del terrorismo, a livello **nazionale** o su base **transfrontaliera**, e indipendentemente dalla forma di tale partenariato"[44].

Si deve subito notare l'elasticità della locuzione di "meccanismo"[45] e l'espressa chiusura della definizione sull'irrilevanza delle "forme". Possiamo dunque ritenere che un partenariato possa essere eretto sia nella forma della rete d'imprese ai sensi dell'art. 3, D.L. 10 febbraio 2009 n. 5 (puro contratto o soggetto giuridico) o della società consortile (persona giuridica) e forsanche tramite clausole statutarie o direttive della capogruppo ex art. 2497 c.c. o modelli di organizzazione e gestione ex D.Lgs. 231/2001[46].

Nella prospettiva *data protection*, uno snodo fondamentale sarà costituito dall'identificazione del ruolo privacy[47] dei vari *partner* che, a seconda dei casi potranno essere tutti **titolari autonomi** del trattamento, ma potrebbero anche assumere la posizione di **contitolari** (art. 26 GDPR)[48] e, in alcuni casi, anche di **responsabili del trattamento** (artt. 28 GDPR).

La strada scelta civilisticamente tra le varie forme di *partnership* e quella selezionata per individuare i ruoli *privacy* avrà importanti ricadute in termini di *governance* e di **responsabilità** e anche, per quanto qui c'interessa, di **trasferimento dei dati** (con la possibilità di implementare norme vincolanti d'impresa ai sensi dell'art. 47 GDPR per i trasferimenti transfrontalieri).

Il partenariato ha comunque una **finalità bloccata** (la condivisione di informazioni a fini antiriciclaggio) e solo a tal titolo possono essere trasferite e utilizzate le relative informazioni (*purpose limitation* ai sensi dell'art. 5 GDPR), sia che al partenariato partecipino solo soggetti obbligati, sia che partecipi un'autorità[49].

In ogni eventualità, resta chiaro che i partenariati devono rispettare la Normativa Privacy. Quindi devono essere certamente predisposte le **informative privacy** (ai sensi degli artt. 13 e 14 GDPR), devono essere assegnati ruoli e responsabilità **all'interno e all'esterno** del partenariato (artt. 29 e 28 GDPR), devono essere rispettate le **norme di sicurezza** (art. 32 GDPR)[50] e valutata la necessità di nominare un **DPO** (art. 37 GDPR), etc.

Il Regolamento Antiriciclaggio però pone, esso stesso, una particolare enfasi su uno degli adempimenti privacy previsti dal GDPR, il ***data processing impact assessment*** (DPIA, art. 35 GDPR) che va effettuato **prima** di qualsiasi trattamento[51] e che potrebbe essere anche oggetto di **consultazione con il Garante Privacy** ex art. 36 GDPR. Una forma specifica di consultazione preventiva con il Garante è prevista del resto dall'art. 75.2 Regolamento Antiriciclaggio, che prevede che i soggetti obbligati informino i supervisori dell'intenzione di costituire un partenariato e questi ultimi si consultino con l'autorità nazionale competente in materia di *data protection* per verificare l'esistenza di meccanismi a tutela del rispetto GDPR e l'avvenuta effettuazione della DPIA[52]. Sarà veramente interessante verificare 'sul campo' se questo tipo di accertamento sarà interpretato come controllo '**formale**' (l'esistenza di meccanismi e di una DPIA, senza verifica del merito) o '**sostanziale**' (l'adeguatezza dei meccanismi e la coerenza

logica della DPIA). A questo proposito, si segnala altresì che l'art. 75.6 e 75.7 Regolamento Antiriciclaggio prevede che i partner definiscano politiche e procedure per lo scambio delle informazioni e, se richiesto dalle autorità di supervisione, devono commissionare un *audit* indipendente sul funzionamento del partenariato.

Quanto alla *data retention*, i documenti e le informazioni scambiate nell'ambito di un partenariato sono conservate per almeno 5 anni ai sensi dell'art. 77.3 Regolamento Antiriciclaggio.

7. I gruppi

Un altro contesto in cui i dati e le informazioni possono (e, anzi, devono) circolare ai fini del potenziamento del contrasto al riciclaggio è quello dei gruppi[53], che il Regolamento Antiriciclaggio definisce con particolare larghezza, anche al di là del loro ambito concettuale *corporate* ai sensi del codice civile. Sono infatti considerati membri di un "gruppo":

- non solo le società avvinte da un rapporto di controllo societario (una *parent* e le sue *subsidiaries*, dirette e indirette, nelle forme del controllo di diritto e di fatto),
- ma anche le imprese legate tra loro da una relazione ai sensi dell'articolo 22 della direttiva 2013/34/UE relativa ai bilanci di esercizio e consolidati (art. 2.41 Regolamento Antiriciclaggio).

Nell'ambito dei partenariati e dei gruppi[54] viene **disinnescato il divieto di comunicazione** di dati e informazioni altrimenti previsto dall'Art. 73.1 Regolamento Antiriciclaggio[55].

La condivisione, come nei gruppi così nei partenariati, può avvenire sia su base nazionale, sia su base transfrontaliera, ma sempre a condizione che siano rispettate le politiche e procedure del partenariato (art. 75.6 Regolamento Antiriciclaggio) o le **politiche e procedure del gruppo** (art. 16.3 e 73.3 Regolamento Antiriciclaggio). Nell'ipotesi del gruppo non è prevista l'obbligatorietà di una DPIA preventiva (come per i partenariati), ma sono comunque obbligatorie **garanzie** di riservatezza e protezione dei dati[56], una **valutazione d'impatto** secondo l'art. 16 Regolamento Antiriciclaggio e, nel caso in cui una filiale estera sia soggetta a una normativa meno stringente sulla protezione dei dati, l'impresa madre deve adottare **misure supplementari**[57] (ad esempio in sede di norme vincolanti d'impresa si sensi dell'art. 47 GDPR o di accordi di esportazione dei dati, art. 46.2.c GDPR).

Interessante notare che il Regolamento Antiriciclaggio prescrive espressamente una valutazione d'impatto e la redazione di politiche e procedure a livello di gruppo, il che dovrebbe quantomeno spingere per una revisione della stanca interpretazione nazionale per cui i Modelli 231 devono essere redatti a livello di società singola e non di gruppo.

8. Le misure di sicurezza e la pseudonimizzazione

Dappertutto nell'AML Package viene ribadita l'esigenza di garantire la sicurezza del trattamento delle informazioni. Ad esempio:

- nel considerando 61 e 77 e negli articoli 16.10, 17.2.c e 19.7 Direttiva Antiriciclaggio si prescrive agli Stati Membri di assicurare **misure adeguate nel trattamento da parte delle FIU e delle autorità** (e a maggior ragione per il trattamento dei dati sensibili – cfr. art. 70.1.c Direttiva Antiriciclaggio) e il punto è ripreso dal considerando 45 e dall'art. 47.3.a Regolamento Autorità Antiriciclaggio;
- nell'art. 75.4.e Regolamento Antiriciclaggio particolari regole sono dettate con riferimento al trattamento dei dati nel contesto dei partenariati;
- l'art. 76.2.d Regolamento Antiriciclaggio ribadisce la necessità di rispettare le misure di sicurezza richieste dal GDPR per il trattamento di **dati sensibili** da parte dei soggetti obbligati.

Le misure di sicurezza devono essere: sia tecniche (come ad esempio: cifratura e/o pseudonimizzazione[58]), sia organizzative (ossia legate alle regole interne che disciplinano le credenziali di accesso, il *need to know*, i controlli interni, etc.).

Ovviamente le indicazioni che precedono si sommano agli obblighi di sicurezza (anche informatica) che derivano dall'AI Act o dalla varia legislazione sulla *cybersecurity* (DORA, NIS2, etc.).

[1] Il Regolamento (UE) 2024/1689 (cd. AI Act), all'art. 3(46), definisce le «**attività di contrasto**» come le attività svolte **dalle autorità di contrasto o per loro conto** a fini di prevenzione, indagine, accertamento o perseguimento di **reati** o esecuzione di **sanzioni penali**, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. Sono «attività di contrasto» tutte (a) le autorità pubbliche competenti in materia di **prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali**, incluse la salvaguardia contro leminacce alla sicurezza pubblica e la prevenzione delle stesse; oppure (b) gli **organismi o entità** incaricati dal diritto dello Stato membro di esercitare **l'autorità pubblica e i poteri pubblici** a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse. **Il considerando 59 dell'AI Act indica però che i sistemi AI delle FIU che svolgono compiti in materia di antiriciclaggio non dovrebbero essere consideraticome sistemi AI ad alto rischio utilizzati da un'autorità di contrasto**.

[2] Ai sensi dell'art. 4(2) GDPR è **trattamento praticamente qualsiasi operazione o insieme di operazioni,** compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

[3] Art. 4(1) GDPR: **costituisce dato personale** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

[4] Cioè, secondo l'art. 9.1 GDPR, i dati personali che rivelino l'**origine razziale o etnica**, le **opinioni politiche**, le **convinzioni religiose o filosofiche**, o l'**appartenenza sindacale**, nonché trattare dati **genetici**, dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla **salute** o alla **vita sessuale** o all'**orientamento sessuale** della persona.

[5] Art. 10.1 GDPR: dati personali relativi alle **condanne penali** e ai **reati** o a connesse **misure di sicurezza**.

[6] Ossia tutti i dati che non sono personali (Regolamento UE 1807/2018).

[7] Direttiva Antiriciclaggio:

- considerando 40, 43, 52, 61 e 124 e artt. 12 e 22 sulle limitazioni all'**accesso** e sulla **minimizzazione**,
- considerando 56 e art. 16.7 sugli obblighi di **informazione** e l'**aggiornamento** dei dati,
- considerando 59 e art. 10.20 sui periodi di **conservazione**,
- considerando 61, 65 e 87 e artt. 19.6 e 37.2 e 3 sulla **competenza ed eticità** nell'uso dei dati e dei *big data* da parte delle autorità,
- considerando 77 e art. 30.2 sulla **cifratura e pseudonimizzazione** dei dati da parte delle autorità,
- considerando 122 e 131 sul rispetto **GDPR**,
- considerando 43 e artt. 48 e 51 sui **trasferimenti extraunionali** di dati,
- 58.3 e 4 sull'**anonimizzazione delle decisioni** e sull'oblio,
- 70 sulle regole particolari per **dati sensibili e dati penali**.

Reg. AMLA:

- considerando 18 e art. 11.7 sul periodo di **conservazione** e sulla **limitazione della condivisione**,
- considerando 45 e art. 47.3 sulla **pseudonimizzazione**,
- 25.3 sull'**anonimizzazione delle decisioni**,
- 98 sulla **base giuridica del trattamento**, il coordinamento con le **autorità privacy** e la limitazione dei diritti d'**accesso**.

Regolamento Antiriciclaggio:

- 9.2.a.vi sulle **politiche privacy** dei soggetti obbligati,

- considerando 46 e art. 16 sulla condivisione di informazioni in **gruppi transfrontalieri** e art. 73.5 sulla condivisione di dati tra **soggetti obbligati ubicati in Paesi diversi**,
- considerando 120 sulla **minimizzazione**,
- considerando 147 e art. 75 sui **partenariati** per la condivisione delle informazioni,
- considerando 150 e 171 sull'applicazione del **GDPR**, particolarmente con riferimento alla **qualità dei dati**, alle pratiche di **profilazione** e alle **decisioni automatizzate**,
- considerando 151 e 152 sulle **finalità specifiche** per il trattamento e sull'uso di dati sensibili,
- considerando 153 e art. 77 sulla **conservazione** dei dati,
- considerando 157 sulle limitazioni al diritto **d'accesso**,
- 76 sul trattamento di **dati sensibili e di dati penali**.

[8] Così anche le Guidelines on data protection for the processing of personal data for anti-money laundering/countering the financing of terrorism purposes (Committee of the Convention for the protection of individuals with regard to automatic processing of data) che indicano le necessità di (i) cautela quando si considera la base legale dell'interesse pubblico, (ii) prevenzione di una raccolta eccessiva di dati, (iii) valutare I casi di contitolarità del trattamento nei partenariati, (iv) attenzione alle regole specifiche sul trattamento dei dati sensibili, (v) rispetto delle finalità specifiche del trattamento, (vi) problematicità della base legale costituita dal consenso e attenzione ai limiti del trattamento basato sull'interesse pubblico, (vii) condizioni e requisiti per il trattamento automatizzato, (viii) misure di sicurezza.

[9] In Italia, poi, il novellato Codice Privacy contiene numerose integrazioni e precisazioni, pur muovendosi obbligatoriamente nel solco del GDPR.

[10] Si segnala che l'art. 2-sexies.2., l e q del Codice Privacy (**per i dati sensibili**) considera animati da un interesse pubblico rilevante i trattamenti di dati sensibili per attività di controllo e ispettive e le attività sanzionatorie e di tutela e l'art. 2-octies.3.m (**per i dati penali**) ammette il trattamento se necessario ai fini degli adempimenti antiriciclaggio. Non si può mancare di sottolineare, però, il gravissimo ritardo del Ministero della Giustizia che, ai sensi dell'art. 2-octies del Codice Privacy, avrebbe dovuto emanare un D.M. per identificare ulteriori casi di trattamento legittimo dei dati penali.

[11] Inoltre, ai sensi dell'art. 2-quinquiesdecies del Codice Privacy, il Garante Privacy può adottare provvedimenti a carattere generale che impongono particolari misure e cautele quando il trattamento presenti rischi elevati.

[12] **Solo per i dati comuni** (non per quelli sensibili o penali) è ammessa la comunicazione, ancorché non prevista da legge or regolamento, a condizione che sia necessaria per l'esecuzione del compito d'interesse pubblico e il Garante Privacy non si sia opposto dopo 45 giorni dalla ricezione della notifica

[13] Direttiva Antiriciclaggio: considerando 43 (interesse pubblico sotteso alla normativa antiriciclaggio), 122 (applicazione concorrente del GDPR); Regolamento AMLA: considerando 77 (compiti di interesse pubblico e consultazione con EDPS) e art. 98 (collaborazione con EDPB)

[14] Tra le cautele mi sembra significativo l'aver previsto una nuova figura nell'organigramma delle FIU, ossia il **Responsabile dei Diritti Fondamentali** ex art. 20 Direttiva Antiriciclaggio.

[15] Per es. art. 77 Regolamento Antiriciclaggio.

[16] Direttiva Antiriciclaggio: considerando 56 e 124.

[17] Anche l'art. 2-ter.2 del Codice Privacy ammette la comunicazione di dati trattati per l'esecuzione di interessi pubblici a terzi che li intendono trattare **per altre finalità solo laddove previsto dalla legge**.

[18] Considerando 26 della Direttiva Antiriciclaggio e considerando 75 del Regolamento AMLA. Il concetto di "**diffusione**" è delineato dal Codice Privacy come "il dare conoscenza dei dati personali a soggetti indeterminati, in qualsiasi forma, anche mediante la loro messa a disposizione o consultazione". Il linguaggio appare particolarmente ampio e, mi sembra, pone particolari e, in certa misura, insospettati obblighi. Ad esempio, la conservazione di dati su cloud e/o la loro accessibilità a sistemi di AI che li

usano per training e/o arricchimento può diventare una divulgazione laddove il fornitore del cloud o del sistema AI non abbia sistemi robusti di protezione o non applichi la segregazione dei dati e l'impresa che di essi si avvale non abbia effettuato adeguata due diligence e chiesto appropriate garanzie.

[19] Considerando 59 della Direttiva Antiriciclaggio.

[20] Considerando 30, 40, 42, 43, 44, 130 e 134 e artt. 12 e 13 della Direttiva Antiriciclaggio.

[21] Proprio per questo si ritiene che il trattamento basato sul legittimo interesse necessiti di un esercizio di valutazione e bilanciamento rispetto ai diritti dei terzi, cd. *legitimate interest assessment*

[22] Art. 6.1.f GDPR

[23] Considerando 41 della Direttiva Antiriciclaggio.

[24] Considerando 43 e 61 e artt. 16.7 e 51 della Direttiva Antiriciclaggio.

[25] Considerando 124 e art. 22 della Direttiva Antiriciclaggio, considerando 157 Regolamento Antiriciclaggio. Limitazioni in questo senso sono ammesse dall'art. 23 GDPR e sono coerenti con il Codice Privacy che, all'art. 2-undecies.1.a, stabilisce che i diritti degli interessati non possono essere esercitati quando possa derivarne un **pregiudizio effettivo e concreto** agli interessi tutelati in base alle disposizioni antiriciclaggio.

[26] Art. 98.2 Regolamento AMLA.

[27] Linee guida dell'EDPB sull'art. 23 AI Act, punto 24.

[28] Anche in questo caso però esistono limitazioni: la natura primaria o secondaria della norma, l'esistenza di misure dirette a disciplinare gli ambiti, una comunicazione motivata e resa senza ritardo all'interessato, etc. (vd. comma 3, art. 2-undecies, Codice Privacy).

[29] eventualmente anche con l'uso di sistemi AI

[30] Costituisce **profilazione** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di 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 fisica o, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona (considerando 71 e art. 4.(4) GDPR)

[31] Secondo l'art. 3(1) dell'AI Act è un sistema AI un sistema **automatizzato** progettato per funzionare con livelli di **autonomia** variabili e che può presentare **adattabilità** dopo la diffusione e che, per obiettivi espliciti o impliciti, **deduce** dall'input che riceve come generare output quali **previsioni**, **contenuti**, **raccomandazioni** o **decisioni** che possono influenzare ambienti fisici o virtuali.

[32] Vd. sotto sub 5

[33] Il considerando 27 della Direttiva Antiriciclaggio invita gli Stati membri a fornire agli organismi responsabili dei registri centrali adeguate tecnologie per verifiche automatizzate, ma pur sempre con il limite dei diritti fondamentali e della non discriminazione.

[34] Considerando 60 e art. 13.2(g) GDPR

[35] Art. 15.1.h che precisa che, in sede di accesso vanno fornite **informazioni significative** sul processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

[36] CGUE sentenza 27 febbraio 2025 (C-203/22) e 7 dicembre 2023, C634/21.

[37] Torna dunque ancora una volta la necessità di un esercizio di valutazione contrapposta e di bilanciamento di interessi.

[38] a) che sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) che sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; o c) che si basi sul consenso esplicito dell'interessato.

[39] La **sorveglianza umana** è prevista dall'art. 14 AI Act quale requisito ineludibile dei sistemi di AI ad alto rischio. Secondo il considerando 73 dell'AI Act, le misure di sorveglianza umana dovrebbero in particolare garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo. È inoltre essenziale, se del caso, garantire che i sistemi di IA ad alto rischio includano meccanismi per guidare e informare la persona fisica alla quale è stata affidata la sorveglianza umana affinché prenda decisioni informate in merito alla possibilità, ai tempi e alle modalità di intervento, onde evitare conseguenze negative o rischi, oppure affinché arresti il sistema, qualora non funzionasse come previsto.

[40] Per di più, l'intervento umano deve essere "**significativo**" secondo il Regolamento Antiriciclaggio.

[41] In realtà che esista un diritto alla spiegazione secondo il GDPR è stato per molto tempo dubbio. Ne parla infatti il considerando 71, ma gli artt. 132.f e 14.2.g parlano solo di "informazioni significative sulla logica utilizzata". La recente giurisprudenza ha però decisamente visarto sull'esistenza di tale diritto.

[42] Allo stesso modo, il diritto alla spiegazione è bensì previsto dall'AI Act (art. 86), ma per fattispecie estranee a quella oggetto di esame. L'art. 3.3 della Legge IA, dal canto suo, prevede anch'esso il requisito della spiegabilità, ma solo per sistemi di AI a fini generali.

[43] Orientamenti del 29.7.2025 C(2025) 5052. In merito, gli Orientamenti fanno proprio il caso di un istituto bancario tenuto alle verifiche antiriciclaggio sulla base della normativa e chiariscono che, nella misura in cui le norme antiriciclaggio siano rispettate, si tratterà di un sistema di AI non vietato, **ma comunque ad alto rischio** (con conseguente applicazione di tutto il corpus di cautele e guarentigie previste dall'AI Act per questi sistemi, pur legittimi, ma rischiosi)

[44] Art. 2.1.57 Regolamento Antiriciclaggio.

[45] Il considerando 45 Regolamento Antiriciclaggio usa la definizione egualmente anfibia di "strutture in cui i soggetti obbligati potrebbero condividere proprietà, gestione e controlli della conformità".

[46] Nel caso di entità pubbliche, il partenariato può essere disposto per legge, regolamento o atto amministrativo.

[47] Vd. art. 75.6.b Regolamento Antiriciclaggio.

[48] Nella Direttiva Antiriciclaggio i partenariati vengono iscritti nell'ambito delle strutture che condividono proprietà, gestione o controllo della conformità.

[49] Vd. considerando 80 Regolamento AMLA e considerando 147 e 149 e artt. 73.4 e 75.1 e 75.3 Regolamento Antiriciclaggio.

[50] Vd. anche art. 75.e Regolamento Antiriciclaggio.

[51] Considerando 148 e art. 75.4.h Regolamento Antiriciclaggio.

[52] Sembra trattarsi di una consultazione diversa da quella prevista dall'art. 36 GDPR. Quest'ultima viene richiesta dal titolare del trattamento al Garante Privacy, quando, a valle della DPIA, resti, nel merito, un rischio residuo elevato. Viceversa, la consultazione disciplinata dall'art. 75 Regolamento Antiriciclaggio è chiesta, non dal titolare del trattamento, ma dall'autorità di supervisione e sembra piuttosto un meccanismo di controllo formale.

[53] Considerando 43 Regolamento Antiriciclaggio.

[54] Art. 73.3 e 73.4 Regolamento Antiriciclaggio.

[55] La condivisione di informazioni, al di fuori di gruppi o partenariati, è ammessa anche tra determinate categorie di soggetti obbligati, ma **solo se si tratta di informazioni attinenti "la stessa operazione" che li coinvolge** (art. 75.5 Regolamento Antiriciclaggio).

[56] Considerando 43 Regolamento Antiriciclaggio.

[57] Considerando 46 e art. 17 Regolamento Antiriciclaggio.

[58] In merito alla quale è significativa la recente sentenza CGUE 4 settembre 2025, procedimento C-413/23 P.