Maggio 2019

Base giuridica del trattamento dei dati ai fini antiriciclaggio: obbligo di legge ma anche interesse pubblico

Nazario Vitale, Funzione Compliance e Antiriciclaggio, AXA Assicurazioni

I destinatari della normativa antiriciclaggio e di contrasto al finanziamento del terrorismo, *ex* D.Lgs. n. 231/2007[1], novellato dal D.Lgs. n. 90/2017[2], sono chiamati a predisporre presidi volti non soltanto ad intercettare fattispecie concrete di chi immette denaro derivante da proventi illeciti nel circuito economico finanziario ovvero imprenditoriale dissimulandone l'origine iniziale, quanto piuttosto ad evitare in via preventiva che tali casistiche si concretizzino ponendo quindi attenzione anche a semplici situazioni oggettivamente anomale ed elusive[3].

Il più grande strumento di prevenzione di cui i soggetti obbligati dispongono e possono avvalersi consiste nella procedura di *Adeguata Verifica della Clientela*[4] che deve essere utilizzata da tutti gli operatori al fine di poter *identificare*, *verificare*, *certificare* chi sia il cliente ed individuare il tipo di operazione o prestazione richiesta; in ogni caso, il corretto assolvimento degli obblighi di adeguata verifica presuppone un approccio basato sul rischio tale da determinare una classe di rischio che risulterà tanto più elevata quanto maggiore risulti essere il grado di opacità riscontrato nelle informazioni richieste e da questi fornite (che si tratti di dati anagrafici piuttosto che dell'indicazione circa l'origine dei fondi o ancora di dati economico-reddituali o ancor più dell'origine storica del patrimonio). Tuttavia, la procedura in questione non si esaurisce con un'unica misura ma in base alla risultanza del profilo di rischio calcolato si pondera la profondità degli ulteriori approfondimenti e la tipologia dei dati da raccogliere (documenti di approfondimento della posizione o inerenti più propriamente l'operazione in sé). L'adeguata verifica della clientela costituisce infatti uno dei basilari e fondamentali punti cardine in materia antiriciclaggio, gravante sui soggetti obbligati affinché entrino in

[1] Attuazione della direttiva UE 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
[2] Attuazione della direttiva UE 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE.
[3] Cfr. Cass. Sez. II, n. 28888/18, Cass. Sez. II n. 8699/07, Cass. Sez. V n. 23071/09.
[4] Artt. 17 e ss. del D.Lgs. 231/2007 e s.m.i.

possesso di tutti quegli elementi che possano consentire di "pesare" il cliente ed intercettare la presenza di un eventuale rischio di riciclaggio.

Il summenzionato processo, quindi, avviene non solo al momento del censimento o di instaurazione del rapporto d'affari con la clientela ma anche in costanza di relazione. Tali misure da approntare come anche le informazioni che vengono acquisite debbono in ogni caso rispettare le garanzie stabilite dalla normativa in materia di protezione dei dati personali. Al quesito sulla liceità della raccolta dei suddetti dati, del loro utilizzo e del relativo trattamento risponde il Regolamento UE 2016/679 dettato in materia di protezione dei dati personali, in particolare all'art. 6 rubricato "*base giuridica del trattamento*", in virtù del quale la base giuridica del trattamento risulta lecita nella misura in cui si prospetti "*almeno una*" delle condizioni espressamente elencate dalla medesima norma, ovvero: a) vi sia il consenso dell'interessato, b) il trattamento risulta necessario per l'esecuzione di un contratto, c) il trattamento è necessario per l'adempimento di un "*obbligo legale*", d) il trattamento è necessario per salvaguardare "*gli interessi vitali dell'interessato*", e) il trattamento è necessario per l'esecuzione di un compito di "*interesse pubblico*" o connesso a "pubblici poteri", f) il trattamento è necessario per il perseguimento del "*legittimo interesse*" del titolare del trattamento. Si precisa che per titolare del trattamento si intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*"[5], identificandosi quindi con il soggetto obbligato così come individuato dalla normativa antiriciclaggio.

E' pacifico che la raccolta ed il trattamento dei dati per finalità antiriciclaggio si iscrive nella previsione dell'adempimento di un "*obbligo legale*" determinandone così la liceità del trattamento dei dati personali a prescindere dal "*consenso*" dell'interessato. In aggiunta, si potrebbe anche sostenere che la legge antiriciclaggio, in realtà, persegue come fine ultimo la diminuzione delle attività criminose ed una conseguente armonizzazione delle regole che trascendono il singolo soggetto obbligato, ma sono rivolte a vantaggio di un'ampia platea di destinatari. A sostegno di ciò, si evidenzia che nella premessa dello schema di decreto legislativo recante attuazione della direttiva (UE) 2015/849 viene precisato che "le *ragioni del nuovo intervento riguardano la necessità di rafforzare il mercato interno riducendo la complessità transfrontaliera, di contribuire alla stabilità finanziaria tutelando la solidità, il funzionamento regolare e l'integrità del sistema finanziario e di salvaguardare la prosperità economica dell'Unione europea assicurando un efficiente contesto imprenditoriale"*. Ciò detto, la base giuridica ex art. 6 del cit. regolamento si basa non solo su di un "*obbligo legale*" ma anche su di un "*interesse pubblico*". Ne consegue che è la stessa normativa sulla protezione dei dati personali che individua una base giuridica lecita nell'obbligo di legge o nel perseguimento del pubblico interesse della normativa AML/CTF[6] dando luogo ad una deroga sul consenso, con la precisazione che tale deroga sussiste unicamente sul solo "*trattamento dei dati*", così da

[5] Art. 4 n. 7 del Regolamento UE 2016/679.
[6] Anti-money laundering and counter terrorism financing.

comportarne l'assoggettamento della normativa antiriciclaggio e di contrasto al finanziamento del terrorismo agli altri principi e obblighi previsti dal "General Data Protection Regulation" (in breve GDPR). Ciò obbliga il destinatario della normativa AML/CTF, tra le altre cose, alla raccolta dei dati ritenuti necessari commisurando il relativo adempimento al grado di rischiosità associato al cliente o all'operazione o prestazione professionale richiesta prestando attenzione a non confluire in quelle circostanze che rendano inopportuno o eccedente un controllo così approfondito; allo stesso modo i dati raccolti dovranno comunque essere trattati esclusivamente ai fini antiriciclaggio, dovrà essere garantita la sicurezza degli stessi, gestirne il relativo accesso ed il mantenimento in un apposito repository per un arco temporale necessario ed adeguato. Tanto è vero che, alla luce dell'art. 5 del Regolamento UE 2016/679, in cui viene sancito il principio della limitazione della conservazione, i dati personali vanno "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*". Ci si chiede, pertanto, quale sia il termine di conservazione massimo ammesso per i principali documenti raccolti per finalità antiriciclaggio e come esso si quantifichi/determini. La quantificazione del periodo massimo di conservazione può avvenire o in base ad una valutazione motivata del Titolare del trattamento ovvero, laddove sia previsto da una norma *ad hoc*, in virtù di una disposizione normativa che, ad altri fini, imponga comunque (e quindi giustifichi) la conservazione di tali dati per un determinato lasso temporale. Proprio la fattispecie da ultimo rappresentata potrebbe individuarsi nell'art. 31 del D.Lgs. n. 231/2007 e s.m.i., rubricato "Obblighi di conservazione", il quale indica il limite temporale di "*10 anni" e specifica chiaramente che il dies a quo in tale computo decorre "dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale*". A dimostrazione della stretta connessione tra la normativa in materia di protezione dei dati e l'antiriciclaggio si evidenzia che già l'originaria legge di recepimento della III direttiva AML dava enfasi a che i dati fossero trattati nel rispetto della normativa sulla Privacy[7] *ex* D.Lgs. n. 196/2003, così manifestando la particolare attenzione che il Legislatore ha riposto su questo delicato tema. Tale richiamo lo si ritiene attuale perché se da un lato è stato mantenuto con il recepimento della IV direttiva[8], dall'altro è stato anche rafforzato con l'indicazione "*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*[9]". In aggiunta, si consideri che la stessa legge di delegazione europea con cui è stato delegato il Governo di dare organica attuazione alla direttiva (UE) 2015/849 rappresenta l'esigenza

[7] Si consideri che già l'originaria legge di recepimento della III direttiva AML all'art. 3 rubricato "principi generali" recita al comma 2 quanto segue: "*I sistemi e le procedure adottati ai sensi del comma 1* (obblighi di adeguata verifica della clientela, di segnalazione delle operazioni sospette, di conservazione dei documenti, di controllo interno, di valutazione e di gestione del rischio) *rispettano le prescrizioni e garanzie stabilite dal presente decreto e dalla normativa in materia di protezione dei dati personali*".
[8] Cfr. art. 16 co. 4 D.Lgs n. 231/2007 e s.m.i.
[9] Cfr. art. 3 co. 9 D.Lgs n. 231/2007 e s.m.i.

di "*rafforzare i presidi di tutela della riservatezza e della sicurezza dei segnalanti, delle segnalazioni di operazioni sospette, dei risultati delle analisi e delle informazioni acquisite anche negli scambi con le FIU*[10] *e incoraggiare le segnalazioni di violazioni potenziali o effettive della normativa di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose o di finanziamento del terrorismo*"[11].

Inoltre, si sottolinea che alcune norme del D.Lgs. n. 231/2007 e s.m.i. effettuano rinvii espressi alla normativa sul trattamento dei dati personali. A titolo esemplificativo, si vedano: l'art. 16, in tema di mitigazione del rischio, in base al quale i presidi e le procedure adottate devono essere in linea con la normativa vigente in materia di protezione dei dati personali, sia ponendo molta attenzione sui sistemi di controllo implementati, sia mediante corsi di formazione del proprio personale; l'art. 32 relativo ai sistemi di conservazione dei dati acquisiti che devono essere "*idonei a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali*"; gli artt. 38 e 39 dettati in materia di Segnalazione di operazione sospetta (in breve SOS), aventi ad oggetto rispettivamente la riservatezza dell'identità del segnalante dell'operazione sospetta e il divieto di "*dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione*".

Riassumendo, si può pacificamente asserire che i destinatari della normativa antiriciclaggio procedono all'analisi e alla valutazione dei rischi di riciclaggio e di finanziamento del terrorismo cui sono esposti nell'esercizio quotidiano delle loro attività come anche alla raccolta, all'utilizzo, alla gestione ed alla conservazione dei dati personali dei clienti perché coperti dal citato regolamento 2016/679 che all'art. 6 individua l'opportuna base giuridica del trattamento dei dati non solo nell'adempimento di un obbligo di legge ma anche di un interesse pubblico. Tuttavia, in considerazione del fatto che, come illustrato, gli operatori sono obbligati comunque al rispetto degli obblighi e dei principi in materia di privacy, è necessario che i destinatari della normativa Aml prestino particolare attenzione all'adempimento degli stessi, in quanto, in presenza di condotte illecite o comunque non conformi, alle sanzioni già previste dal D.Lgs 231/2007 potrebbero aggiungersi quelle previste dal GDPR e dal Codice Privacy Italiano[12].

Volendo inquadrare il sistema sanzionatorio delle due normative oggetto della presente analisi, si precisa che il D.Lgs n. 231/2007 e s.m.i. come anche la normativa sul trattamento dei dati personali (Reg. UE 2016/679 e D.Lgs. n. 196/2003 e s.m.i.) prevedono entrambi sia sanzioni amministrative che di tipo penale, oltre naturalmente alla responsabilità civile in presenza di danni arrecati ad un soggetto. Al fine di avere una visione d'insieme si passerà velocemente in rassegna il quadro sanzionatorio previsto in

[10] Financial Intelligence Unit istituita presso la Banca d'Italia dal D.Lgs. n. 231/2007.
[11] Art. 15 co. 2 lett. g) della L. n. 170/2016.
[12] D.Lgs. n. 196/2003 e s.m.i..

primis dalla normativa antiriciclaggio per poi far cenno a quello previsto in materia di trattamento dei dati.

Per prima cosa, è interessante evidenziare che con il decreto che ha recepito la IV Direttiva la disciplina AML ha subito una profonda depenalizzazione degli illeciti penali in illeciti amministrativi. Coerentemente con la legge di delegazione europea del 12.8.2016 n. 170[13], in particolare l'art. 15, il decreto di recepimento ha voluto arginare il perimetro punitivo penalistico limitando "*la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti, perpetrate attraverso frode o falsificazione, e di violazione del divieto di comunicazione dell'avvenuta segnalazione, prevedendo sanzioni penali adeguate alla gravità della condotta e non eccedenti, nel massimo, tre anni di reclusione e 30.000 euro di multa*". Le sanzioni comminate (siano esse amministrative o penali) devono comunque risultare effettive, proporzionate, dissuasive così da contrastare il grave fenomeno del riciclaggio.

Il testo novellato destina il solo art. 55 alle fattispecie penali, mentre gli illeciti amministrativi sono contemplati negli articoli da 56 a 69. Le fattispecie sanzionatorie, determinate con la tipica sanzione amministrativa che è quella pecuniaria, si possono presentare o in misura determinata, ovvero proporzionale o ancora fissata dalla legge tra limiti minimi e massimi[14] e vengono irrogate in funzione del livello di responsabilità, della gravità e delle conseguenze della violazione, del grado di collaborazione e della capacità patrimoniale del soggetto trasgressore e/o inadempiente. A tutela di quest'ultimo, la L. 689/1981 prescrive all'art. 11 un obbligo di motivazione quale requisito necessario per l'applicazione del quadro sanzionatorio.

In base alle linee guida fornite del MEF a seconda della presenza o meno di ulteriori elementi qualificanti rispetto al mero riscontro della violazione del precetto, le fattispecie previste dal decreto novellato possono distinguersi in "base" (tipizzata) e "qualificata" (consistente nel carattere "grave", "ripetuto", "sistematico", plurimo" della condotta che dà luogo alla violazione)[15]**.** Le nuove regole tipizzate, infatti, prevedono l'applicazione di una sanzione pecuniaria in misura fissa (che oscilla tra i 2.000 euro per violazione degli obblighi di adeguata verifica ovvero inosservanza degli obblighi di conservazione ai 3.000 euro per non ottemperanze delle disposizioni relative all'obbligo di segnalazione delle operazioni sospette) e di una sanzione qualificata da comminare nelle ipotesi di violazioni gravi, ripetute, sistematiche o plurime (che può variare da un minimo di 2.500 euro ad un massimo di € 300.000 euro). Le sanzioni si applicheranno a tutti i soggetti

[13] *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea.*
[14] "*In tema di sanzioni amministrative pecuniarie, ove la norma indichi un minimo e un massimo della sanzione, spetta al potere discrezionale del giudice determinarne l'entità entro tali limiti, allo scopo di commisurarla alla gravità del fatto concreto (Cass. Civ., Sez. I, 24 marzo 2004, n. 5877).*
[15] Cfr. Circolare MEF 6.7.2017 n. DT54071.

obbligati, diversi da quelli di cui all'art. 62 (intermediari bancari e finanziari)[16]. Si aggiunga che il summenzionato decreto prevede anche sanzioni sull'inosservanza degli obblighi di comunicazione da parte dei componenti degli organi di controllo dei soggetti obbligati[17] fino all'importo di 30.000 euro; sulle condotte illecite dell'omessa esecuzione del provvedimento UIF di sospensione dell'operazione sospetta[18] ed inosservanza degli obblighi informativi verso UIF e MEF[19] fino all'importo di 50.000 euro; sull'inosservanza delle limitazioni all'uso del contante e dei titoli al portatore[20] fino all'importo di 250.000 euro.

Da quanto esposto finora si evince chiaramente che la ratio della legge di delegazione europea è quella di depenalizzare e di arginare l'illecito di matrice penalistica.

Focalizzando l'attenzione sul GDPR, l'art. 83 distingue due macro aree sulla base del principio generale di proporzionalità della pena rapportata all'inadempienza di legge. Nella prima rientrano le violazioni di minore gravità, per le quali sono previste sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente: la violazione delle condizioni applicabili al consenso dei minori (il codice privacy si riferisce a minori di anni quattordici) in relazione all' offerta diretta di servizi della società dell'informazione, il trattamento illecito di dati personali che non richiedono l'identificazione dell'interessato, la mancata o errata notificazione e/o comunicazione di un data breach[21] all'Autorità nazionale competente, la violazione dell'obbligo di nomina del DPO, la mancata applicazione di misure di sicurezza, l'assenza di sicurezza e cifratura nella conservazione dei dati. Nella seconda categoria, invece, sono presenti sanzioni più rilevanti in considerazione del maggior peso e rilievo delle fattispecie a cui fanno riferimento ed ammontano fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente: inosservanza dei principi di base del trattamento[22], trasferimento illecito di dati personali ad un destinatario in un

[16] Art. 62 co. 1: "*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 la sanzione amministrativa pecuniaria da 30.000 euro a 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*".

[17] Cfr. art. 59 co. 1 del cit. D.Lgs. 231/2007 s.m.i.

[18] Cfr. art. 58 co. 6 del cit. D.Lgs. 231/2007 s.m.i.

[19] Cfr. art. 60 del cit. D.Lgs. 231/2007 s.m.i.

[20] Cfr. art. 63 co. 1 del cit. D.Lgs. 231/2007 s.m.i.

[21] Cfr. art. 4 n. 12 del reg. 2016/679: *"«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*".

[22] Liceità, correttezza e trasparenza, minimizzazione dei dati, esattezza rispetto alle finalità per le quali tali dati sono trattati, limitazione della conservazione, integrità e riservatezza, responsabilizzazione del titolare

Paese terzo o un'organizzazione internazionale, inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità nazionale di controllo, compravendita di dati a prescindere dalla scelta (consenso) liberamente esercitata dagli interessati.

Affinché le sanzioni siano sempre effettive, proporzionate e dissuasive (cfr. cit. art. 83, co. 1), l'autorità adibita ed incaricata di sorvegliare l'applicazione del cit. reg. (il Garante per la protezione dei dati) dovrà tenere in considerazione circostanze quali la natura, la gravità, la durata della violazione, il carattere doloso o colposo della stessa, le misure adottate per attenuare il danno subito, il relativo grado di responsabilità, i presidi implementati, le categorie di dati personali interessate dalla violazione. I soggetti possibili responsabili dell'illecito sono in riferimento congiunto il titolare ed il responsabile del trattamento. Con riguardo alle sanzioni penali, se da un lato il GDPR non le contempla direttamente, tuttavia contiene un rinvio alle fattispecie previste nel riformato Codice Privacy[23] agli artt. 167 - 170. Tali norme fanno riferimento al trattamento illecito dei dati, alla loro diffusione su larga scala o acquisizione fraudolenta nonché alla falsità nelle dichiarazioni rese al Garante. Ove si dovesse incorrere nella violazione di uno di tali precetti, in base alla norma infranta, è prevista la pena della reclusione da un minimo di sei mesi (ad esempio per trattamento illecito dei dati) ad un massimo di sei anni (in caso di diffusione illecita di dati personali su larga scala).

Il peso delle sanzioni illustrate evidenzia la particolare attenzione e sensibilità del legislatore in tema di antiriciclaggio e di privacy, circostanza che impone agli operatori la massima attenzione e diligenza.

In disparte le questioni attinenti l'eventuale concorso di norme e il regime di cumulo delle sanzioni, che riguardano profili più spiccatamente penalistici e che pertanto esulano dalla presente trattazione, occorre tenere presente che eventuali condotte illecite da parte degli operatori possono violare contemporaneamente gli obblighi imposti dalle due normative, con serio rischio di applicazione congiunta delle sanzioni: a titolo esemplificativo, si veda la violazione degli "*obblighi di conservazione*" dei dati ex art. 31 (ut supra), la cui fattispecie è contemplata sia dal D.Lgs. 231/2007 agli artt. 57 co. 1[24], 55 co. 2[25] e sia dal

---

del trattamento (art. 5 GDPR); liceità della base giuridica del trattamento (art. 6 GDPR); "*condizioni per il consenso*" (art. 7 GDPR); "*trattamento di categorie particolari di dati personali*" (art. 9 GDPR).

[23] D.Lgs. n. 196/2003, come modificato dal D.Lgs. n. 101/2018, entrato in vigore il 19 Settembre 2018.

[24] Art. 57 (Inosservanza degli obblighi di conservazione). - 1. Ai soggetti obbligati che, in violazione di quanto disposto dagli articoli 31 e 32, non effettuano, in tutto o in parte, la conservazione dei dati, dei documenti e delle informazioni ivi previsti o la effettuano tardivamente si applica la sanzione amministrativa pecuniaria pari a 2.000 euro. - 2. Fuori dei casi di cui al comma 1 e salvo quanto previsto dall'articolo 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione amministrativa pecuniaria da 2.500 euro a 50.000 euro.

[25] Art. 55 co. 2: Chiunque, essendo tenuto all'osservanza degli obblighi di conservazione ai sensi del presente decreto, acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta

GDPR agli artt. 5 co. 1, 83 co. 5 lett. a); ovvero il "*divieto di comunicazione*" al cliente o a terzi dell'avvenuta segnalazione ex art. 39, fattispecie anch'essa contemplata tanto dal D.Lgs. 231/2007 all'art. 55 co. 4[26] [27] quanto dal D.Lgs. n. 196/2003 all'art. 167 bis co. 2, 3[28]. Pertanto, occorre rammentare che la liceità del trattamento dei dati e la circostanza per cui l'antiriciclaggio risponda ad un obbligo di legge e persegua un interesse pubblico non esime, in alcun modo, dal regolare rispetto di tutti gli obblighi previsti dalla normativa in materia di privacy, né da eventuali responsabilità relative ad illeciti amministrativi, penali o civili.

conservazione dei predetti dati e informazioni è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro.

[26] Art. 55 co. 4: Salvo che il fatto costituisca più grave reato, chiunque, essendovi tenuto, viola il divieto di comunicazione di cui agli articoli 39, comma 1, e 41, comma 3, è punito con l'arresto da sei mesi a un anno e con l'ammenda da 5.000 euro a 30.000 euro.

[27] Nel caso di intermediari bancari e finanziari le relative sanzioni sono previste all'art. 62 per "*violazioni gravi ripetute sistematiche o plurime*" dalla normativa antiriciclaggio.

[28] Art. 167 bis co. 2, 3: 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione. 3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.