FIMAA FORMA

WEBINAR

26 MARZO 2021

Antiriciclaggio e Privacy

Le sanzioni amministrative e penali

Relatori:

Dott. Michele Pizzullo

Avv. Eleonora Morolli

Le norme in materia di antiriciclaggio

La materia dell'antiriciclaggio, negli ultimi anni, ha conosciuto una rapida evoluzione su iniziativa del Legislatore europeo, successivamente all'emanazione della direttiva 2005/60/Ce, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamenti del terrorismo, nonché della direttiva 2006/70/Ce che ne reca le misure di esecuzione. Queste disposizioni hanno trovato attuazione nel nostro Paese con il **decreto legislativo 21 novembre 2007, n. 231** (cd. «decreto Antiriciclaggio»), che ha introdotto anche sanzioni penali e amministrative.

Il riciclaggio e il finanziamento del terrorismo e la criminalità organizzata, ad esso legati, restano problemi significativi a livello di Unione europea, il che danneggia l'integrità, la stabilità e la reputazione del settore finanziario e costituisce una minaccia per il mercato interno e la sicurezza interna dell'Unione stessa. Al fine di affrontare tali problemi e integrare e rafforzare l'applicazione delle norme antiriciclaggio, è stata emanata la **direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio**, meglio nota come **IV direttiva antiriciclaggio**, recepita in Italia dal **decreto legislativo 25 maggio 2017, n. 90**, che, a sua volta, ha modificato e integrato il vecchio decreto antiriciclaggio 231/2007, senza però abrogarlo, e alla quale è attribuibile il merito e la funzione di aver posto le basi di un nuovo modello di prevenzione del riciclaggio, inteso a rafforzare i presidi di contrasto alla criminalità economica. In tale quadro normativo, è divenuto, in particolare, sempre più determinante e incisivo il ruolo svolto da professionisti quali avvocati, notai e commercialisti, nonché intermediari bancari, assicurativi, finanziari e non finanziari. Di recente, con il **decreto legislativo 4 ottobre 2019, n. 125**, entrato in vigore l'11/11/2019, è stata recepita la **direttiva UE 2018/843 del Parlamento europeo e del Consiglio**, ossia la **V direttiva antiriciclaggio**, che modifica le direttive 2009/138/CE e 2013/36/UE, e introduce modifiche e integrazioni al d.lgs. 90/2017.

Le norme in materia di trattamento dei dati personali

La riforma attuata dal Regolamento UE 2016/679 (GDPR) si basa su diversi pilastri (che sono componenti fondamentali): norme coerenti, procedure semplificate, azioni coordinate, coinvolgimento degli utenti, informazioni più efficaci e rafforzamento dei poteri destinati a far rispettare le norme.

Il suo scopo è, infatti, la *definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea*.

Attribuendo ai titolari e ai responsabili del trattamento dei dati personali delle persone fisiche il cd. *principio di responsabilità*, il Regolamento, all'art. 1, «*considera la tutela del diritto alla protezione dei dati personali come diritto fondamentale delle persone fisiche e stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati; protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*».

In quest'ottica, il principio cardine del GDPR è costituito dall'«**autodeterminazione informativa**», una condizione necessaria per il libero sviluppo della personalità del cittadino e anche un elemento essenziale di una società democratica.

Il 19/09/2018 è entrato in vigore il **d.lgs. 10 agosto 2018, n. 101** (cd. *Codice della privacy*), recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati», che ha abrogato la direttiva 95/46/CE «Regolamento generale sulla protezione dei dati (GU Serie Generale n.205 del 04-09-2018)» e ha introdotto disposizioni per l'adeguamento della normativa nazionale italiana, precedentemente regolata dal d.lgs. 30 giugno 2003, n. 196, alle disposizioni del GDPR.

Le sanzioni in materia di antiriciclaggio

L'osservanza degli obblighi è presidiata da un articolato sistema di sanzioni, penali e amministrative. Il sistema sanzionatorio, inizialmente previsto dal d.lgs. 231/2007, è stato integralmente modificato dal d.lgs. 90/2017 e ulteriormente corretto dal d.lgs. 125/2019, in coerenza con le previsioni comunitarie che stabiliscono l'adozione di sistemi sanzionatori basati su misure effettive, proporzionate e dissuasive nei confronti delle persone fisiche e delle persone giuridiche direttamente responsabili della violazione e degli organi di direzione, amministrazione e controllo che, con condotte negligenti o omissive, abbiano agevolato o reso possibile la violazione. Le sanzioni penali sono ora previste limitatamente ai casi di gravi condotte perpetrate attraverso frode o falsificazione e ai casi di violazione del divieto di comunicazione dell'avvenuta segnalazione di operazioni sospette. Sono stabilite sanzioni amministrative sia per violazioni gravi, ripetute o sistematiche ovvero plurime sia per quelle prive di tali requisiti. Per le prime sono sanciti importi più consistenti, compresi fra un minimo e un massimo edittale; per le seconde sono indicate somme contenute, in misura fissa. La gravità delle violazioni è determinata sulla base di criteri specificamente indicati. Previsioni particolari riguardano le violazioni degli obblighi segnaletici da cui siano derivati vantaggi economici al soggetto responsabile.

In conformità della disciplina comunitaria, il d.lgs. 231/2007 aveva adottato una nozione di riciclaggio che comprende anche le attività di autoriciclaggio, vale a dire l'impiego in attività economiche o finanziarie dei proventi illeciti da parte di coloro che hanno commesso o concorso a commettere il reato presupposto (art. 2).

Nel sistema di repressione penale, invece, l'autoriciclaggio è stato considerato per lungo tempo come un post-factum non punibile. Solo la legge 15 dicembre 2014, n. 186 (art. 3, comma 3) ha introdotto uno specifico reato nell'ordinamento penale italiano (art. 648 ter.1 del codice penale).

Le sanzioni amministrative pecuniarie (d.lgs. 231/2007 e s.m.i.)

Art. 56 - Inosservanza degli obblighi di adeguata verifica e dell'obbligo di astensione. Ai soggetti obbligati che, in violazione delle disposizioni in materia di adeguata verifica della clientela del presente decreto omettono di acquisire e verificare i dati identificativi e le informazioni sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale si applica la sanzione amministrativa pecuniaria **pari a 2.000 euro**. Fuori dei casi sopra previsti e salvo quanto previsto dall'art. 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione **da 2.500 euro a 50.000 euro**. Le dette sanzioni si applicano anche nell'ipotesi di violazione dell'obbligo di astensione di cui all'art. 42.

Art. 57 - Inosservanza degli obblighi di conservazione. 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**. Fuori dei casi sopra previsti e salvo quanto previsto dall'art. 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione **da 2.500 euro a 50.000 euro**.

Art. 58 - Inosservanza delle disposizioni relative all'obbligo di segnalazione delle operazioni sospette. Salvo che il fatto costituisca reato, ai soggetti obbligati che omettono di effettuare la segnalazione di operazioni sospette, si applica una sanzione **pari a 3.000 euro**. Salvo che il fatto costituisca reato e salvo quanto previsto dall'art. 62, commi 1 e 5, nelle ipotesi di violazioni gravi, ripetute o sistematiche ovvero plurime, si applica la sanzione **da 30.000 euro a 300.000 euro**. Le medesime sanzioni si applicano anche in caso di violazione della comunicazione o della segnalazione (art. 36, commi 2 e 6), nonché ai soggetti tenuti alla comunicazione o alla segnalazione (art. 37, comma 3). Nel caso di violazioni gravi, ripetute o sistematiche ovvero plurime producono un vantaggio economico, l'importo massimo della sanzione: a) è elevato fino al doppio dell'ammontare del vantaggio medesimo, qualora detto vantaggio sia determinato o determinabile e, comunque, non sia inferiore a 450.000 euro; b) è elevato fino ad un milione di euro, qualora il predetto vantaggio non sia determinato o determinabile. Ai soggetti obbligati che omettono di dare esecuzione al provvedimento di sospensione dell'operazione sospetta, disposto dalla UIF, si applica la sanzione **da 5.000 euro a 50.000 euro**.

Le predette violazioni, se isolate, vengono considerate violazioni di minore gravità e sono ridotte da uno a due terzi.

Le sanzioni in materia di privacy

L'art. 83 del GDPR autorizza le autorità di controllo degli Stati membri a infliggere sanzioni amministrative pecuniarie in relazione a violazioni del regolamento. Il livello delle sanzioni e le circostanze delle quali le autorità nazionali tengono conto nel decidere se infliggere una sanzione, nonché il tetto massimo di tali sanzioni sono anch'essi fissati nell'articolo 83. Il regime sanzionatorio è pertanto armonizzato in tutta l'Unione europea.

L'art. 84 del GDPR attribuisce, comunque, in materia una certa discrezionalità agli Stati membri nel momento in cui stabilisce che gli stessi determinano le sanzioni per le violazioni del Regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e prendono tutti i provvedimenti necessari per assicurarne l'applicazione.

E' importante tenere presente che non è sufficiente rispettare le norme in materia di protezione dei dati personali, ma, in ossequio di responsabilizzazione (*accountability*) del titolare del trattamento lo stesso dovrà dimostrare di essere consapevole delle modalità di trattamento e di conservazione dei dati dell'interessato, insomma dovrà essere consapevole e dovrà *rendere conto del proprio operato*.

Il titolare del trattamento, tenuto conto della natura, del contesto e della finalità del trattamento, deve garantire, ed essere in grado di dimostrarlo (appunto, renderne conto), che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi pregiudicare i diritti e le libertà dell'interessato. E non è sufficiente adottare misure di conformità alle norme stabilite dal GDPR, ma occorre anche documentarle (principio di trasparenza) e garantirne l'efficacia.

Sanzioni correttive e impugnazioni

L'autorità di controllo ha il potere di irrogare **sanzioni correttive** che consistono nel:

- rivolgere avvertimenti al titolare o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare le norme;
- rivolgere ammonimenti al titolare o al responsabile del trattamento ove i trattamenti abbiano violato le norme;
- ingiungere al titolare o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;
- ingiungere al titolare o al responsabile del trattamento di conformare i trattamenti alle norme, specificando eventualmente le modalità e i termini per la conformità;
- imporre una limitazione provvisoria o definitiva al trattamento, sospendere temporaneamente il trattamento, o vietare del tutto;
- ordinare la rettifica, la cancellazione o l'aggiornamento dei dati personali;
- revocare le certificazioni o ingiungere all'organismo di certificazione di ritirare le certificazioni rilasciate se i requisiti non sono soddisfatti;
- infliggere le sanzioni amministrative pecuniarie;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Impugnazioni

I provvedimenti adottati dalle autorità di controllo possono essere impugnati dinanzi all'autorità giudiziaria.

I criteri per l'applicazione delle sanzioni

A norma dell'art. 83 del GDPR, spetta alle autorità di controllo nazionali (Garante) provvedere affinché **le sanzioni amministrative siano effettive, proporzionate e dissuasive**. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa l'autorità di controllo, in ogni singolo caso, tiene debito conto dei seguenti elementi:

- a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- b) il carattere doloso o colposo della violazione;
- c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli artt. 25 e 32 del GDPR;
- e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- g) le categorie di dati personali interessate dalla violazione;
- h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- i) qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- j) l'adesione ai codici di condotta approvati ai sensi dell'art. 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42 del GDPR;
- k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Le sanzioni amministrative pecuniarie

In termini di applicazione delle sanzioni amministrative, il GDPR prevede due livelli di violazioni.

Nel primo livello di violazioni, **le sanzioni possono arrivare fino a 10 milioni di euro oppure al 2% del fatturato mondiale annuo della società se superiore**, se riguardano:

a) inosservanza degli obblighi del titolare e del responsabile del trattamento dei dati personali, a norma degli articoli 8 (Consenso dei minori), 11 (Trattamento che non richiede identificazione), da 25 a 39 (riguardanti, rispettivamente, la protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, i contitolari del trattamento, i rappresentanti dei titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione, il responsabile del trattamento, il trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento, il registro dei trattamenti, la cooperazione con l'autorità di controllo, la sicurezza del trattamento, la notifica di una violazione dei dati all'autorità di controllo, la comunicazione di una violazione dei dati personali all'interessato, la valutazione di impatto sulla protezione dei dati, la consultazione preventiva con l'autorità di controllo, la designazione del responsabile della protezione dei dati (DPO), il tempestivo e adeguato coinvolgimento del responsabile della protezione dei dati, i compiti assegnati al responsabile della protezione dei dati), 42 (Certificazione rilasciata dai competenti organismi o dall'autorità di controllo competente) e 43 (Organismi di certificazione);

b) inosservanza degli obblighi dell'organismo di certificazione, a norma degli articoli 42 e 43;

c) inosservanza degli obblighi dell'organismo di controllo a norma dell'art. 41 (ossia un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente), par. 4, a norma del quale, fatti salvi i compiti e i poteri dell'autorità di controllo competente, l'organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente, adotta le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento, e informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

Nel secondo livello di violazioni (art. 83, par. 5, GDPR), sono previste **sanzioni fino 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**, qualora sia riscontrata:

a) inosservanza dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5 (principi applicabili al trattamento di dati personali), 6 (Liceità del trattamento), 7 (Condizioni per il consenso) e 9 (Trattamento di categorie particolari di dati personali);

b) inosservanza dei diritti degli interessati a norma degli articoli da 12 a 22 (comportanti, rispettivamente, l'adozione di misure appropriate in tema di informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato, le informazioni che il titolare del trattamento deve fornire qualora i dati personali siano raccolti presso l'interessato; le informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato; da parte dell'interessato, il diritto di accesso ai dati, il diritto di rettifica dei dati, il diritto alla cancellazione dei dati («diritto all'oblio»), il diritto di limitazione di trattamento dei dati, l'obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento, il diritto alla portabilità dei dati, il diritto di opposizione al trattamento dei dati personali che lo riguardano, il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione;

c) inosservanza dei trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale, a norma degli articoli da 44 a 49;

d) inosservanza di qualsiasi obbligo ai sensi delle legislazioni adottate dagli Stati membri;

e) inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo, o il negato accesso in violazione dei poteri spettanti ad ogni autorità di controllo, di cui all'articolo 58, paragrafo 1;

- alle quali si aggiunge l'inosservanza delle prescrizioni di cui alle autorizzazioni generale del Garante per la privacy di cui all'art. 21, del d.lgs. 101/2018 (adeguamento Codice Privacy) o di cui al provvedimento di cui all'art. 21, comma 1, del d.lgs. 101/2018 (prescrizioni in materia di dati a trattamento speciale).

Le sanzioni penali in materia di antiriciclaggio

Le norme sanzionatorie in materia di prevenzione del riciclaggio e del finanziamento del terrorismo sono basate su misure **effettive, proporzionate e dissuasive**, applicabili alle persone fisiche e alle persone giuridiche responsabili delle violazioni. In tale prospettiva, le **fattispecie penali**, contenute nell'art. 55 del d.lgs. 231/2007, modificato dal d.lgs. 125/2019, sono circoscritte alle sole condotte di **grave violazione** degli obblighi di **adeguata verifica** e di **conservazione**, perpetrate attraverso **frode o falsificazione**, nonché del **divieto di comunicazione** dell'avvenuta segnalazione.

Art. 55 - Fattispecie incriminatrici.

*1. Chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione è punito con la reclusione **da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro**. Alla medesima pena soggiace chiunque essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, in occasione dell'adempimento dei predetti obblighi, utilizza dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione.*

*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 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**.*

3. Salvo che il fatto costituisca più grave reato, chiunque essendo obbligato, ai sensi del presente decreto, a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, fornisce dati falsi o informazioni non veritiere, è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro.

*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**.*

Le sanzioni penali in materia di privacy

Il legislatore italiano, a seguito della legge 25 ottobre 2017, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione Europea – Legge di delegazione europea 2016-2017 – è dovuto intervenire in un campo, già regolamentato dal Codice della Privacy, introdotto, come si è detto, nel nostro ordinamento con il d.lgs. 196/2003. L'ampia discrezionalità lasciata dalla cd. «Legge di delegazione europea», se da un lato ha consentito un più libero recepimento nei singoli Paesi degli Stati membri, dall'altro non ha fornito indicazioni rilevanti su molti aspetti di notevole importanza, tra i quali, senza dubbio, l'inquadramento giuridico delle violazioni in materia di trattamento dei dati con la concreta difficoltà del discriminare tra la sanzione amministrativa e quella penale.

Nel d.lgs. 10 agosto 2018, n. 101, con il rischio di violare il principio del *ne bis in idem* (principio, com'è noto, che vieta di essere puniti due volte per la medesima violazione di legge), è stata decisa una rivisitazione del Codice della privacy che armonizzasse il precedente assetto normativo con le nuove esigenze comunitarie; non dunque la depenalizzazione dei reati, ma modifiche degli stessi con, addirittura, l'aggiunta di ulteriori fattispecie al d.lgs. 196/2003 (artt. 167 *bis* e 167 *ter*), confermando, tuttavia, l'abrogazione dell'art. 169 (Omessa adozione di misure minime di sicurezza). **Le sanzioni prevedono misure che vanno da 6 mesi fino ad arrivare, nei casi più gravi, a 6 anni di reclusione** per i reati di: (i) art. 167. Trattamento illecito di dati (reclusione da sei mesi a 3 anni); (ii) art. 167 *bis*. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (reclusione da 1 a 6 anni); (iii) art. 167 *ter*. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (reclusione da 1 a 4 anni); (iv) art. 168. Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (da 6 mesi a 3 anni); (v) art. 170. Inosservanza dei provvedimenti del Garante (da 3 mesi a 2 anni).

Art. 167. Trattamento illecito di dati.

1. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123 (dati relativi al traffico), 126 (dati relativi all'ubicazione) e 130 (comunicazioni indesiderate) o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.*

2. *Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 ("Trattamento di categorie particolari di dati personali") e 10 ("Trattamento dei dati personali relativi a condanne penali e reati") del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.*

3. *Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.*

Le novità maggiormente interessanti riguardano l'introduzione dei commi 4, 5 e 6. Essi, infatti, rappresentano il "salvacondotto" per la reintroduzione delle fattispecie penali, a seguito della loro abrogazione nella prima bozza del d.lgs. 101/2018 e tipizzano quei correttivi utili al fine di scongiurare il rischio di violare il principio del *ne bis in idem*. I commi 4 e 5 prevedono un meccanismo di coordinamento tra Pubblico ministero e Garante, cui è demandata l'azione giudiziaria nei rispettivi campi, penale e amministrativo. Vige, infatti, l'obbligo per il Pubblico Ministero di informare il Garante circa la sopravvenienza di una notizia di reato (4° comma), e per il Garante l'obbligo di comunicare al PM qualora presuma l'esistenza di un reato (5° comma). Il sesto comma, invece, intende limitare il carico afflittivo della convergenza tra sanzione penale ed amministrativa, stabilendo che, qualora per la stessa violazione sia stata comminata una sanzione amministrativa, la pena per il reato sia diminuita.

Art. 167 bis. Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarre 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.

Nel secondo comma, il quale prevede la medesima sanzione rispetto al primo, sono tutelati quei dati per il cui trattamento è richiesto il consenso. Ad essere punita, nel caso di specie con la reclusione da uno a sei anni, è la condotta di chi comunica o diffonde un archivio automatizzato, o parte di esso, contenente dati personali oggetto di trattamento su larga scala, arrecando nocimento all'interessato. Per "archivio" deve intendersi "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico". Una definizione di questo termine è fornita dalle linee guida sul processo decisionale automatizzato e profilazione (WP251): «*Il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano.*». Conseguentemente, un trattamento parzialmente automatizzato è un trattamento automatizzato che prevede in qualche misura l'intervento umano.

Un trattamento manuale è una qualsiasi operazione di trattamento (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) **effettuato esclusivamente attraverso l'agire umano, che può essere effettuato sia in formato sia cartaceo che digitale.**

Art. 167 ter. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti 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 quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

Il nuovo articolo 167 ter introduce il reato di acquisizione fraudolenta di dati personali. Ai fini della sussistenza del reato è indispensabile l'utilizzo di mezzi fraudolenti e, come nel caso dell'art. 167 bis, la condizione del trattamento su larga scala.

Lo schema tipico alla base della redazione di fattispecie penalmente rilevanti è quella di prevedere reati ordinati secondo un ordine crescente, che parte da quello con una sanzione minore fino ad arrivare a quello con una sanzione maggiore. Nei reati contro la persona, all'interno del codice penale, ad esempio, vi è un ordine ascendente che fa sì che l'istigazione a delinquere (art. 414 c.p.) preceda l'associazione per delinquere (art. 416 c.p.) che, a sua volta, precede l'associazione di tipo mafioso (art. 416 bis c.p.). Qui la sanzione è inferiore rispetto a quella degli articoli precedenti, dal momento che viene punita "solo" l'acquisizione fraudolenta dei dati, ma non anche l'utilizzo successivo o l'eventuale diffusione.

Analogamente al precedente art. 167 bis, viene effettuato un rinvio all'art. 167 per l'attuazione del meccanismo di coordinamento tra Pubblico Ministero e Garante e per la diminuzione della sanzione penale, qualora successiva alla sanzione amministrativa per lo stesso fatto.

Art. 168. Falsità nelle dichiarazioni al Garante e interruzione nell'esecuzione dei compiti o dell'esercizio dei poteri del Garante.

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.

2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

Il primo comma punisce chiunque dichiari o attesti falsamente notizie o circostanze o produca atti o documenti falsi. Si tratta di due diverse condotte: la prima prevede la attestazione, ovvero l'attività di redazione di atti afferenti dichiarazioni di terzi; la seconda, invece, si riferisce ai "fatti" dei quali il soggetto ha diretta percezione o che ha compiuto direttamente.

Il secondo comma punisce chi cagiona un'interruzione o chi arrechi un turbamento all'attività del Garante. Anche in questo caso le condotte tipizzate sono due: l'interruzione individua il mancato svolgimento dell'attività, indipendentemente dal fatto che questa sia temporanea o definitiva; il turbamento si riferisce, invece, ad un'alterazione del regolare svolgimento dell'attività la quale, pur non comportando la cessazione della stessa, sia tale da pregiudicare in maniera apprezzabile il perseguimento degli obiettivi cui la stessa è finalizzata.

In entrambi i commi, il bene giuridico tutelato è, senza dubbio, il corretto svolgimento delle funzioni amministrative del Garante, il regolare ed ordinato andamento dell'attività della pubblica amministrazione.

Art. 170. Inosservanza dei provvedimenti del Garante.

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2 septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni.

A differenza delle disposizioni precedenti, che prevedono reati comuni, con il termine “chiunque” deve intendersi che potrà commettere la violazione soltanto il destinatario del provvedimento inosservato.

La condotta tipica consiste, pertanto, nell’inosservanza di più “classi” di provvedimenti del Garante da parte del destinatario dell’atto, obbligato a conformarvisi in virtù di espressa previsione. La condotta di inosservanza è ad ampio spettro: concerne, infatti, non soltanto la mera omissione, ma anche la trasgressione mediante modalità comportamentali “attive”.