Decreto GDPR e sanzioni penali

In Italia, le sanzioni penali continueranno ad avere un ruolo fondamentale per la **salvaguardia** del diritto alla protezione dei dati personali.

Il decreto di adeguamento al GDPR, in vigore dal 19 settembre, conferma infatti le svariate **fattispecie di reato** previste dal Codice della Privacy e ne introduce addirittura di nuove.

E' importante tenere presente che non è sufficiente rispettare le norme in materia di protezione dei dati personali, ma, in ossequio del principio di *accountability*, i titolari dovranno dimostrare di essere consapevoli delle modalità di trattamento e di conservazione degli stessi.

Con l’approvazione e la pubblicazione in Gazzetta Ufficiale del Decreto Legislativo di adeguamento al Regolamento Generale sulla Protezione dei Dati (GDPR) l’Italia si conferma uno dei paesi europei con la normativa sulla privacy **più complessa e articolata.**

“Clausole di apertura” del GDPR

Il legislatore italiano ha infatti deciso di avvalersi di quasi tutte le cosiddette

“clausole di apertura” del GDPR

ossia di quelle disposizioni del Regolamento che consentono agli Stati membri di mantenere o introdurre norme specifiche ulteriori per la protezione dei dati personali.

In particolare, il legislatore ha deciso di avvalersi della facoltà, concessa dal GDPR a tutti gli Stati membri, di prevedere sanzioni penali per alcune violazioni della normativa sulla privacy.

Queste sanzioni vanno ad aggiungersi alle sanzioni amministrative già previste dal Regolamento.

Questa scelta, pur presentando alcune criticità, è coerente con il preesistente regime sanzionatorio delineato dal D.Lgs. 196/2003 (Codice della Privacy), ma non mancano le novità.

Le Criticità

Prescindendo da qualsiasi valutazione sull'opportunità di procedere all'abrogazione *in toto* del Codice della Privacy, la depenalizzazione è giustificabile solo **qualora si ritenga che le sanzioni amministrative** introdotte dal GDPR per ciascuna delle fattispecie interessate dalla depenalizzazione siano sufficientemente dissuasive, **non essendo sufficiente fare riferimento a presunti problemi in punto di *ne bis in idem*.**

Vediamo quali sono:

Le fattispecie di reato dopo il decreto di adeguamento al GDPR

La scelta operata dal nostro legislatore è stata quella di **modificare il quadro sanzionatorio** delineato dal previgente Codice della Privacy, lasciando però sostanzialmente **inalterate svariate fattispecie incriminatrici ed introducendone di nuove.**

Ecco una panoramica delle fattispecie di reato che permangono o sono state introdotte nel nostro ordinamento dopo il **19 settembre 2018,** data di entrata in vigore del decreto di adeguamento.

Trattamento illecito di dati

L’articolo **167 del Codice della Privacy**, norma che nelle intenzioni della **Commissione ministeriale incaricata di aggiornare il Codice avrebbe dovuto essere abolita *in toto*,** è stato riformulato in modo da continuare a punire penalmente diverse condotte consistenti nell’arrecare **nocumento all’interessato**, in violazione di alcune specifiche e limitate disposizioni normative, come ad esempio alcuni dei requisiti sul trattamento dei dati sensibili e sul trasferimento internazionale di dati.

In sostanza, si è deciso di mantenere in vita **le sanzioni penali previste per le violazioni più gravi richiamate dal previgente articolo 167.**

Tuttavia, per garantire maggiore conformità al principio del ***ne bis in idem,*** si è ritenuto di stabilire che ove per gli stessi fatti venga applicata una sanzione amministrativa, a norma del Codice o del Regolamento, la pena debba essere diminuita.

Da notare è anche l'aggiunta, rispetto al testo dell'articolo 167 contenuto nello schema di decreto pubblicato a maggio, **di fattispecie di danno e di violazioni non lucrative.**

È stata infatti accolta la richiesta avanzata dal Garante e dalle Commissioni parlamentari di punire le condotte di cui **all'articolo 167**

1. **non solo quando sorrette da una volontà di trarre profitto,** ma anche ove

2. sussista una volontà di arrecare un danno ad altri.

Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

Il decreto di adeguamento introduce **all'articolo 167-bis del Codice della Privacy** una fattispecie di reato del tutto nuova che punisce la **comunicazione e la diffusione di dati personali oggetto di trattamento su larga scala, in violazione di certi requisiti normativi, quali il consenso dell'interessato (ove richiesto).**

Quanto all'elemento soggettivo del reato, sono punite le condotte sorrette da una **volontà di recare danno ad altri o di trarre profitto per sé o altri.**

Si tratta di una riformulazione del **reato di "comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone"** contenuto nello schema di decreto esaminato nel mese di maggio dal Garante e dal Parlamento.

Tale riformulazione riduce notevolmente la portata applicativa di questa nuova fattispecie incriminatrice e potrebbe comportare alcuni problemi interpretativi.

Infatti, **il reato si configura solo quando la comunicazione o la diffusione riguardi un "archivio automatizzato" di dati personali** (o una sua parte sostanziale).

Quest’ultimo non viene definito dal decreto.

Tuttavia, ai fini del GDPR per **“archivio”** s’intende “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.”

Inoltre, la fattispecie di cui all’articolo 167-bis richiede che i dati contenuti nell’archivio **siano oggetto di trattamento su larga scala.**

Né nel decreto di adeguamento, né nel GDPR si dà **alcuna definizione di trattamento su larga scala,** anche se il considerando **91 del GDPR** fornisce alcune utili indicazioni:

i trattamenti su larga scala ricomprendono quei trattamenti che ***“mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato.”***

Infine, il reato di cui all'articolo **167-bis** è configurabile solo qualora la **diffusione o comunicazione dei dati avvenga in violazione di specifiche e limitate disposizioni normative,** per lo più applicabili a quei soggetti che trattano **dati professionalmente o per obbligo di legge.**

Da tutto ciò deriva che questa **nuova fattispecie di reato potrà trovare applicazione soltanto in un numero molto limitato di casi.**

Nei casi sopra citati il fatto è **punito con la reclusione da uno a sei anni, ma la pena è diminuita** ove per gli stessi fatti **venga anche applicata una sanzione amministrativa.**

Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

Il decreto di adeguamento introduce all'**articolo 167-ter del Codice della Privacy** un'altra fattispecie incriminatrice del **tutto nuova**, la quale punisce con **la reclusione da uno a quattro anni:**

«chiunque, al fine di trarne profitto ovvero di arrecare danno ad altri, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala».

Si tratta in qualche modo del **rovescio della medaglia del reato di cui all'articolo 167-bis,** visto che ad essere punita è l'acquisizione invece della comunicazione dei dati.

Per il resto, valgono considerazioni analoghe a quelle sopra svolte.

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

L'articolo 168 del Codice della Privacy, così come novellato dal decreto di adeguamento, mantiene sostanzialmente invariata la punibilità, con la reclusione da sei mesi a tre anni, di:

«chiunque dichiari o attesti il falso al Garante, reato già previsto dal previgente articolo 168 del Codice».

La disposizione viene però integrata tramite l'inserimento al secondo comma dello stesso articolo di una **nuova fattispecie di reato,** che punisce 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».

Si tratta di una fattispecie fortemente **ispirata all'articolo 340 del Codice Penale**, che sanziona l'interruzione di un ufficio o servizio pubblico o di un servizio di pubblica necessità, dal quale riprende, per coerenza col principio di eguaglianza, il massimo edittale.

Vale la pena ricordare che il GDPR non prevede specifiche sanzioni amministrative per condotte di questo tipo, peraltro particolarmente odiose.

Pertanto, il ricorso al diritto penale pare qui specialmente giustificato, come peraltro dimostra il fatto che analoghe fattispecie penali sono state introdotte in altri Stati membri.

Ad esempio, in Lussemburgo, l'interruzione dei compiti dell'autorità di controllo (Commission nationale pour la protection des données) è punita con la reclusione fino ad un anno.

Inosservanza di provvedimenti del Garante

Il decreto di adeguamento ha **ripristinato il reato di inosservanza di provvedimenti del Garante già previsto dall'articolo 170 del previgente Codice della Privacy,** reato che era stata eliminato nello schema di decreto presentato al Parlamento.

Tale reato è stato reinserito nel Codice su insistenza delle Commissioni parlamentari e dello stesso Garante, il quale aveva fatto opportunamente notare come l'abrogazione dell'articolo 170 risultasse in contrasto con l'introduzione di una fattispecie di reato analoga nel decreto legislativo che attua la Direttiva 2016/680 sul trattamento dei dati personali in ambito penale.

Difatti, **se l'abrogazione dell'articolo 170 fosse stata mantenuta**, si sarebbe determinata l'irragionevole conseguenza per cui se a non osservare un provvedimento del Garante fosse stato un funzionario di polizia o un magistrato si sarebbero integrati gli estremi di un reato, mentre se a fare lo stesso fosse stato un qualsiasi altro soggetto si sarebbero applicate esclusivamente sanzioni amministrative.

Con l'entrata in vigore del decreto di adeguamento rimane quindi punibile, **con la reclusione da tre mesi a due anni, chiunque, essendovi tenuto,** non osservi un provvedimento adottato dal Garante.

Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

Il decreto di adeguamento conferma i reati già previsti all'articolo 171 del previgente Codice **per le violazioni delle norme dello Statuto dei lavoratori in materia di controlli a distanza dei lavoratori e indagini sulle loro opinioni politiche, religiose o sindacali.**

Le violazioni connesse **al controllo a distanza dei lavoratori** sono oggetto di un numero sempre maggiore di segnalazioni inviate dal Garante all'autorità giudiziaria, e i precedenti giurisprudenziali certo non mancano in questo campo.

Ad esempio, la Cassazione ha recentemente stabilito che l'installazione di un sistema di videosorveglianza in grado di controllare a distanza l'attività dei lavoratori in mancanza di accordo con le rappresentanze sindacali aziendali integra reato anche se la stessa sia stata preventivamente autorizzata per iscritto da tutti i dipendenti (si veda la sentenza n. 22148/2017).

La riformulazione delle norme sul controllo a distanza dei lavoratori da parte del Jobs Act ha però creato non poche difficoltà interpretative *(in particolare rispetto all'uso dei moderni sistemi digitali di controllo)*, al punto da sollevare dubbi di compatibilità col principio di tassatività.

A questo proposito, si sarebbe potuto pensare di intervenire ulteriormente sulle norme in questione proprio durante l'adeguamento del nostro ordinamento al GDPR, ma i tempi stretti dettati dall'entrata in vigore del Regolamento hanno sicuramente lasciato poco spazio a riflessioni di più ampio respiro.

Depenalizzazioni

Tutti gli altri reati previsti dal **previgente Codice della Privacy sono stati depenalizzati.**

A questo proposito, vale la pena ricordare come non si sia ritenuto di mantenere il reato di cui **all'articolo 169 del Codice** relativo alle misure di sicurezza.

Come già ricordato, la depenalizzazione del reato in questione è giustificata dal fatto che, con l'entrata in vigore del GDPR, le misure minime di sicurezza previste dal Codice sono abolite, e le nuove misure di sicurezza previste dal GDPR non presentano un livello di dettaglio tale da risultare compatibile con un principio cardine del diritto penale: **il principio di tassatività**

N.B. : Il principio di tassatività vincola il giudice nel suo giudizio, nel senso che il fatto concreto può essere considerato reato solo se è ricondotto in uno dei casi espressamente previsti dalla legge.

È quindi totalmente preclusa l'analogia nell'interpretare una norma penale.

L’opera complessiva di depenalizzazione posta in essere con il decreto di adeguamento è completata dall’articolo 24 dello stesso.

Quest’ultimo prevede infatti che **agli illeciti depenalizzati commessi prima dell’entrata in vigore del decreto stesso** *(ossia prima del 19 settembre 2018)* si applicano **le sanzioni amministrative introdotte in sostituzione delle previgenti sanzioni penali.**

Ciò purché il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili.

Qualora, invece, siano intervenuti sentenza o decreto irrevocabili, questi potranno essere revocati dal giudice dell’esecuzione perché il fatto non è più previsto dalla legge come reato.

IN CONCLUSIONE

In presenza di **una violazione** si possono avere le seguenti conseguenze:

l'autorità di controllo può imporre al titolare delle misure procedurali o tecniche di natura correttiva, da attuare nell'immediatezza, compreso il potere di **limitare, sospendere o addirittura bloccare i trattamenti**;

- se la violazione comporta danni agli interessati, il titolare, insieme al responsabile del trattamento, dovrà provvedere al risarcimento dei danni, materiali e morali;

- la violazione può portare a **danni reputazionali** a carico del titolare *(es. a seguito di un data breach)* con gravi conseguenze sull'attività dell'azienda;

- la violazione può comportare responsabilità per mancato rispetto delle pattuizioni contrattuali con altri titolari o contitolari;

- la violazione può portare all'applicazione di **sanzioni amministrative** da parte dell'autorità di controllo;

- la violazione può portare all'applicazione di **eventuali sanzioni penali**, se lo Stato si è avvalso della possibilità di introdurre tali sanzioni all'interno del suo ordinamento, come previsto dal regolamento europeo.

Sanzioni amministrative

In base all'articolo 83, sono le autorità di controllo nazionali (Garante) a provvedere affinché le **sanzioni amministrative** siano **effettive, proporzionate e dissuasive**. In base al principio di coerenza, l'intervento delle autorità dovrà essere equivalente tra i vari Stati.

Al momento di infliggere una sanzione pecuniaria, l'autorità di controllo dovrà considerare vari criteri per stabilire il tipo di sanzione da applicare e l'eventuale importo:

- la **natura, la gravità** *(più violazioni in un singolo contesto, o separate violazioni)* **e la durata della violazione** *(quindi se il titolare si è attivato tempestivamente)* tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno *(in relazione agli abitanti del paese)* e il livello del danno da essi subito *(in caso di **violazioni minori**, con rischio non significativo per gli interessati, l'autorità può procedere con un semplice avvertimento)*;

- il **carattere doloso o colposo** della violazione *(una violazione intenzionale verrà considerata più grave)*;

- se la violazione ha portato un profitto al titolare;

- le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento **per attenuare il danno** subito dagli interessati;

- 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;

- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

- il **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

- le categorie di dati personali interessate dalla violazione;

- 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;

- 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;

- l'adesione ai codici di condotta o ai meccanismi di certificazione.

Sanzioni penali

Il legislatore italiano, col decreto di adeguamento del Codice Privacy, ha sostanzialmente confermato le fattispecie penali previste dal Codice, introducendo la previsione del **danno** come elemento caratterizzante in alternativa allo scopo di **profitto**.

Quindi non si terrà contro del solo profitto economico dell'autore dell'illecito ma anche del danno arrecato agli interessati, compreso il danno d'immagine e reputazionale della vittima, in tal modo coprendo le fattispecie di **revenge porn**.

I resti previsti dal Codice sono:

- il trattamento illecito dei dati,
- la comunicazione e la diffusione illecita di dati personali oggetto di trattamento su larga scala,
- l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala,

- la falsità nelle dichiarazioni al garante,
- l'interruzione dell'esecuzione di compiti e poteri del garante,
- l'inosservanza dei provvedimenti del garante.

L'art. 167 del Codice stabilisce che: **“Quando per lo stesso fatto è applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita”.** La norma, però, appare del tutto indeterminata rispetto ai criteri per stabilire la diminuzione.

Inoltre, i reati previsti dall'art. 167 bis e 167 ter del Codice hanno come elemento caratterizzate il **trattamento su larga scala**, concetto già introdotto dal regolamento e sostanziato dai pareri del Working Party art. 29 (oggi European Data Protection Board). L'attuazione della norma penale potrebbe creare problemi di tassatività essendo il concetto estraneo alla normativa criminale.

Le violazioni

Il regolamento europeo distingue **due gruppi di violazioni**.

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

a) inosservanza degli **obblighi del titolare e del responsabile del trattamento** a norma degli articoli 8 (consenso dei minori), 11 (trattamento che non richiede identificazione), da 25 a 39 (privacy by default, contitolari del trattamento, rappresentanti non stabiliti nell'Unione, responsabili del trattamento, registro dei trattamenti, sicurezza, notifica delle violazioni, valutazione di impatto, DPO), 42 e 43;

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'articolo 41, paragrafo 4.

2) Un secondo gruppo di violazioni, per il quale sono previste sanzioni **fino 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore. Riguardano:

a) inosservanza dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) inosservanza dei diritti degli interessati a norma degli articoli da 12 a 22;

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 degli Stati membri adottate a norma del capo IX;

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 ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

In ogni caso le sanzioni devono essere considerate un'arma dissuasiva, non certo una punizione, nel senso che, come precisato da Isabelle Falque-Pierrotin, Presidente del gruppo Articolo 29, si terrà conto del graduale adeguamento necessario per una regolamentazione complessa come il GDPR, e ogni violazione sarà soppesata alla luce della sua gravità.

Le sanzioni saranno, quindi, proporzionate anche all'azienda, in modo da non costringerla a chiudere l'attività.

Sanzioni correttive

L'autorità di controllo ha il potere di irrogare sanzioni correttive. Essi 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.