Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

Il nuovo impianto sanzionatorio penale del Codice della privacy coordinato al GDPR. Le principali novità in materia di reati privacy

Introduzione al nuovo impianto sanzionatorio penale del Codice della privacy come novellato dal d.lgs. 101/2018 di coordinamento al GDPR

di Alessandro Del Ninno, Professore e Avvocato

Il nuovo Codice della privacy come risultante dalle modifiche e integrazioni introdotte dal recente decreto legislativo 101/2018 presenta rilevanti novità in merito all'impianto sanzionatorio penale (applicabile a far data dal 19 Settembre 2018): dopo che le prime bozze legislative del decreto di coordinamento avevano quasi del tutto depenalizzato i reati privacy contenuti nella precedente versione del Codice della privacy, la scelta definitiva del Legislatore è stata di segno totalmente opposto: non solo sono stati confermati i reati già precedentemente noti e previsti dal Codice privacy (dal trattamento illecito di dati personali alla falsità nelle dichiarazioni al Garante; dalla inosservanza dei provvedimenti del Garante fino alle violazioni dei divieti di controllo a distanza dei lavoratori e di indagine sulle loro opinioni), riordinando e rimodulando le relative sanzioni, ma sono stati altresì introdotte nel Codice nuove ipotesi di reato: la comunicazione e diffusione illecita di dati oggetto di trattamento su "larga scala"; l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala; l'interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante.

L'unica ipotesi di reato previgente abrogata dal decreto di coordinamento è quella sulla omessa adozione delle misure minime di sicurezza previste dal previgente articolo 33 del Codice della privacy, reato prima previsto all'articolo 169 del Codice: il che è ovviamente coerente con l'inesistenza - nel Regolamento Generale UE 679/2016 sulla protezione dei dati – "GDPR" – della categoria delle "misure minime di sicurezza". Come è noto, difatti, nel previgente Codice della privacy le misure di sicurezza nel trattamento dei dati personali erano distinte in misure di sicurezza *idonee* (art. 31) e *minime* (art. 33). Il GDPR non prevede alcuna diversificazione (si può affermare che le misure di sicurezza ad oggi previste dall'articolo 32 del Regolamento UE sono solo quelle idonee) e sanziona in via amministrativa la violazione degli obblighi di sicurezza con l'applicazione di una sanzione fino a 10 milioni di Euro o - per le imprese - fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Il nuovo impianto sanzionatorio del "nuovo" (o, meglio, novellato) d.lgs. 196/2003 recante il Codice della privacy si basa su sette articoli (dall'art. 167 all'art. 172) che compongono il Capo II "*Illeciti Penali*" del Titolo III ("*Sanzioni*"). Sono previste nove diverse ipotesi di reato

(più l'articolo 172, che è norma di chiusura sulla pena accessoria della pubblicazione della sentenza di condanna per uno dei delitti previsti) che a loro volta si articolano prevedendo diverse condotte delittuose, sia di base che aggravate. Ad esempio, il reato unitario di "*trattamento illecito di dati personali*" di cui all'art. 167 del Codice contempla delitti anche molto diversi tra di loro e che vanno dai reati base per la violazione degli articoli 123 (recante le regole sul trattamento dei dati di traffico nell'ambito della fornitura di un servizio di comunicazione elettronica), 126 (che regola il trattamento dei dati relativi all'ubicazione – si pensi ai servizi di geolocalizzazione o georeferenziazione ormai ordinari e incorporati in app e *devices* – prescrivendo che possono essere trattati tali dati solo se anonimi o se l'utente o il contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento), 129 (con le regole che fissano le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico) e 130 [recante l'obbligo di richiedere il consenso preventivo (*opt-in*) al "contraente" o all'"utente"per l'invio di materiale mediante posta elettronica, fax, Mms o Sms], fino ai reati aggravati di trattamento dei dati personali di particolare natura di cui all'art. 9 del GDPR (dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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) in violazione delle regole deontologiche o delle misure di garanzia predisposte dal Garante, o di trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza di cui all'art. 10 del GDPR in violazione delle norme previste (si attende anche uno specifico decreto del Ministro della Giustizia), per finire col reato aggravato di trasferimento illecito 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 GDPR.

E' inoltre da notare, come meglio si approfondirà in successivo articolo di commento specifico articolo per articolo, che mentre per integrare (e dunque sanzionare) le condotte delittuose di cui al reato di *trattamento illecito dei dati personali* è necessario – oltre al dolo di profitto o di danno ("*al fine di trarre profitto per sè o altri ovvero al fine di arrecare danno*") – anche il verificarsi di un effettivo "*nocumento*"arrecato all'interessato (che diventa dunque elemento oggettivo e costitutivo del reato), per i reati di comunicazione e diffusione illecita di dati oggetto di trattamento su "larga scala", di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala, di interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante è invece sufficiente il solo dolo di profitto o danno, non essendo richiesto anche l'effettivo verificarsi di un nocumento all'interessato per integrare la fattispecie di reato. Infine, per i reati di falsità nelle dichiarazioni al Garante, di inosservanza dei provvedimenti del Garante e per le violazioni dei divieti di controllo a distanza dei lavoratori e di indagine sulle loro opinioni, il reato si commette con la mera condotta oggettiva della falsità, inosservanza o violazione.

Ancora, una interessante novità introdotta dal decreto di coordinamento 101/2018 al Codice della privacy è quella della previsione – per talune ipotesi di reato, non per tutte - di una stretta cooperazione tra Autorità Giudiziaria e Garante della privacy nell'area della erogazione delle sanzioni amministrative (di competenza del Garante) eventualmente coincidente con l'area di rilevanza penale delle infrazioni al Codice. Una cooperazione – per così dire – bidirezionale. E' difatti previsto che il Pubblico ministero, quando ha notizia dei reati di trattamento illecito dei dati personali, o di comunicazione e diffusione illecita di dati oggetto di trattamento su "larga scala"o di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala ne informa senza ritardo il Garante (al fine delle valutazioni connesse agli accertamenti amministrativi di competenza). Al contrario, il Garante trasmette al Pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato e la trasmissione degli atti deve avvenire al più tardi al termine dell'attività di accertamento delle violazioni. Tale novità (soprattutto la relazione motivata) determinerà probabilmente l'apertura di un numero maggiore di procedimenti penali per violazione delle norme privacy rispetto al passato, quando il Garante procedeva alla mera comunicazione della notizia di reato alle competenti Procure.

L'intersecarsi dei piani sanzionatori penale e pecuniario-amministrativo ha anche un altro effetto, disciplinato dall'art. 167, comma 6, del nuovo Codice della privacy che difatti prevede che "*Quando per lo stesso fatto è stata 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*". Tale comma 6 è mutuato dall'art. 187-*terdecies* del d.lgs. 58/1998 sugli abusi di mercato: ove vi sia una convergenza sul medesimo fatto di sanzioni pecuniarie (amministrative o disposte dall'autorità giudiziaria quale conseguenza del reato), la pena pecuniaria penale è diminuita (per l'imputato o per la persona giuridica) se il Garante ha già comminato e riscosso per il medesimo fatto la diversa sanzione amministrativa pecuniaria prevista dal Codice o dal GDPR.

Il particolare interesse connesso all'impianto sanzionatorio penale del nuovo Codice della privacy risiede nella considerazione che tali norme rappresentano una sorta di chiusura del cerchio: mentre difatti il GDPR ha dettato le norme sulle violazioni e sanzioni amministrative pecuniarie (art. 83) e sui criteri per l'individuazione e la ripartizione della responsabilità civilistica (art. 82) – determinandosi in sede di coordinamento operato dal d.lgs. 101/2018 la totale abrogazione nel previgente testo del Codice della privacy sia delle sanzioni amministrative (al Titolo III, Capo I, "*Sanzioni Amministrative*" è rimasto solo il nuovo articolo 166 che reca importanti criteri di applicazione delle sanzioni amministrative pecuniarie previste dal GDPR ad ipotesi di violazione di norme del Codice) che dell'art. 15 del vecchio testo normativo (che prevedeva il risarcimento del cosiddetto danno da trattamento dei dati personali) – mancava del tutto - essendo ovviamente materia riservata alla competenza

nazionale di ciascuno Stato membro – la regolamentazione delle violazioni e delle sanzioni penali. Il Considerando n. 149 del GDPR – difatti – prevede che siano gli Stati membri a stabilire le proprie disposizioni relative a sanzioni penali per violazioni del Regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del GDPR. Tuttavia, precisa il Considerando, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non deve essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia UE (ci si riferisce ovviamente alla Giurisprudenza della Corte che ha chiarito l'applicazione di tale principio e del divieto di applicare per lo stesso fatto una sanzione amministrativa e anche una sanzione pecuniaria di natura penale, come una multa).

Inoltre, il successivo Considerando 152 del GDPR ulteriormente chiarisce che se necessario in altri casi, ad esempio in caso di gravi violazioni del Regolamento, gli Stati membri procedono ad attuare un sistema che preveda sanzioni – anche penali - effettive, proporzionate e dissuasive.

Dunque i titolari e responsabili del trattamento italiano nonché le loro persone autorizzate al trattamento (tutte le norme penali del Codice sono dirette a "*Chiunque*" commetta i reati previsti) dovranno tenere in considerazione il GDPR e il Codice della privacy per l'impianto sanzionatorio complessivo di natura amministrativa, civilistica (GDPR) e penale (Codice della privacy). Ed è in tale prospettiva che il presente contributo di analisi generale dell'impianto sanzionatorio penale introdotto dal d.lgs. 101/2018 al Codice della privacy sarà a breve seguito da un successivo commento pratico – articolo per articolo – delle norme di cui agli artt. 167-172 del nuovo Codice.

Infine, merita concludere la presente analisi ricordando le necessarie norme di coordinamento transitorio dettate dagli articoli 24 e 25 del d.lgs. 101/2018 (dunque esterne al Codice della privacy).

L'articolo 24 ("*Applicabilità delle sanzioni amministrative alle violazioni anteriormente commesse*") prescrive che le disposizioni che, mediante abrogazione, hanno sostituito sanzioni penali prima previste dal Codice della privacy con le sanzioni amministrative previste dal GDPR [un caso su tutti: il trattamento in violazione dell'obbligo di acquisire il consenso ai sensi del "vecchio" articolo 23 del Codice – ora abrogato - che costituiva reato di trattamento illecito dei dati, mentre oggi la violazione dell'art. 6, comma 1, lettera (a) del GDPR sul consenso quando costituisce la base giuridica del trattamento è sanzionata in via amministrativa fino a 20 milioni di Euro o – per le imprese - fino al 4% del fatturato mondiale, se superiore] si applicano anche alle violazioni commesse anteriormente alla data del 19 Settembre 2018, data di entrata in vigore del decreto di coordinamento e del nuovo Codice della privacy (si pensi ad eventuali procedimenti penali pendenti per il reato di trattamento illecito di dati personali per violazione dell'art. 23 del "vecchio" Codice della privacy). Ciò sempre che il procedimento penale non sia stato a tale data definito con sentenza o con decreto divenuti irrevocabili. Se i procedimenti

penali per i reati depenalizzati sono stati definiti prima del 19 Settembre 2018 con sentenza di condanna o decreto irrevocabili, in tale caso il giudice dell'esecuzione revoca la sentenza o il decreto, dichiarando che il fatto non è previsto dalla legge come reato e adotta i provvedimenti conseguenti.

Ai fatti commessi prima della data di entrata in vigore non possono in ogni caso: (a) essere applicate sanzioni amministrative pecuniarie per un importo superiore al massimo della pena originariamente prevista o inflitta per il reato, tenuto conto del criterio di ragguaglio di cui all'articolo 135 del codice penale; (b) essere applicate le sanzioni amministrative accessorie, salvo che le stesse sostituiscano corrispondenti pene accessorie.

Il successivo articolo 25 del d.lgs. 101/2018 (rubricato "*Trasmissione degli atti all'autorità amministrativa*") costituisce il coordinamento e completamento procedurale dei principi stabiliti all'articolo precedente. La norma stabilisce difatti che entro il 19 Dicembre 2018 l'autorità giudiziaria penale dispone la trasmissione all'autorità amministrativa competente degli atti dei procedimenti penali relativi ai reati trasformati in illeciti amministrativi, salvo che il reato risulti prescritto o estinto per altra causa alla medesima data.

Se l'azione penale non è stata ancora esercitata, la trasmissione degli atti è disposta direttamente dal pubblico ministero che, in caso di procedimento già iscritto, annota la trasmissione nel registro delle notizie di reato. Se il reato risulta estinto per qualsiasi causa, il pubblico ministero richiede l'archiviazione a norma del codice di procedura penale; la richiesta ed il decreto del giudice che la accoglie possono avere ad oggetto anche elenchi cumulativi di procedimenti.

Se l'azione penale è stata esercitata, il giudice pronuncia, ai sensi dell'articolo 129 del codice di procedura penale, sentenza inappellabile perchè il fatto non è previsto dalla legge come reato, disponendo la trasmissione all'autorità amministrativa competente degli atti dei procedimenti penali relativi ai reati trasformati in illeciti amministrativi Quando è stata pronunciata sentenza di condanna, il giudice dell'impugnazione, nel dichiarare che il fatto non è previsto dalla legge come reato, decide sull'impugnazione ai soli effetti delle disposizioni e dei capi della sentenza che concernono gli interessi civili.

Una volta ricevuti gli atti, l'autorità amministrativa (cioè, quasi sempre, il Garante) notifica gli estremi della violazione agli interessati residenti nel territorio della Repubblica entro il termine di novanta giorni e a quelli residenti all'estero entro il termine di trecentosettanta giorni dalla ricezione degli atti. Entro sessanta giorni dalla notificazione degli estremi della violazione l'interessato è ammesso al pagamento in misura ridotta, pari alla metà della sanzione irrogata, oltre alle spese del procedimento (e il pagamento determina l'estinzione del procedimento).

Interessante notare come l'articolo 25 – esclusivamente per il caso di conversione di reati in illeciti amministrativi soggetti a sanzione – prevede che "*si applicano, in quanto*

compatibili, le disposizioni di cui all'articolo 16 della legge 24 novembre 1981, n. 689". Si ammette, cioè, solo in tali casi e in quanto compatibile, l'applicabilità dell'art. 16 con il relativo pagamento di una somma in misura ridotta pari alla terza parte del massimo della sanzione prevista per la violazione commessa (quindi un importo inferiore alla metà sanzione comminata) o, se più favorevole e qualora sia stabilito il minimo della sanzione edittale, pari al doppio del minimo edittale, oltre alle spese del procedimento.

Stesso richiamo alla applicabilità dell'articolo 16 della legge 24 novembre 1981, n. 689 non è invece effettuato dal nuovo articolo 166 del Codice della privacy, che detta gli importanti criteri in base ai quali le violazioni delle nuove norme del novellato Codice della privacy devono essere sanzionate sul piano amministrativo in base alle due diverse ipotesi previste dall'articolo 83, comma 4 del GDPR (fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore) e 83, comma 5 (fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore). Difatti i commi 7 e 8 dell'art. 166 si limitano a prevedere che nell'adozione dei provvedimenti sanzionatori da parte del Garante si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689 (dunque non anche l'articolo 16 con la previsione della definizione mediante pagamento in misura ridotta di un terzo) e che entro il termine di trenta giorni (o sessanta se il trasgressore risiede all'estero) previsto per la proposizione del ricorso avverso il provvedimento sanzionatorio comminato dal Garante, il trasgressore e gli obbligati in solido possono al massimo definire la controversia mediante il pagamento di un importo pari alla metà della sanzione irrogata.