Sanzioni e strumenti di tutela tra G.D.P.R. e Codice Privacy

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»

Ordine degli Avvocati di Torino

Claudio Strata - *Avvocato*

Il GDPR ha previsto e determinato le sanzioni amministrative irrogabili in caso di violazione.

Non contiene, però, disposizioni volte a disciplinare direttamente la responsabilità penale che deriva dall'illecito trattamento dei dati personali.

Tuttavia i singoli Stati membri hanno la possibilità di prevedere sanzioni di carattere penale, poiché il Legislatore europeo ha espressamente demandato la scelta del regime relativo alla responsabilità penale agli Stati stessi.

Le principali disposizioni di riferimento sono il Considerando n. 149 e l'art. 84 del *GDPR*.

Il Considerando n. 149, infatti, sancisce che i singoli Stati debbano poter stabilire le disposizioni concernenti le sanzioni penali applicabili in caso di violazione del Regolamento e in caso di violazione delle norme nazionali adottate in virtù ed entro i limiti posti dal Regolamento.

È, altresì, ammesso che le sanzioni aventi carattere penale, previste dagli Stati membri, possano implicare la sottrazione dei profitti ricavati mediante la violazione del Regolamento, a condizione che venga rispettato il principio del *ne bis in idem*, quale interpretato dalla Corte di Giustizia europea.

Al GDPR si è affiancato il D.Lvo 101/2018 che ha modificato il d.lvo 196/2003 (c.d. Codice Privacy): oltre alle sanzioni amministrative sono state confermate quelle penali, con le modifiche di cui vi darò conto.

Ho il compito di illustrarvi l'attuale quadro sanzionatorio e di tutela e le norme di riferimento.

SANZIONI AMMINISTRATIVE

Sono previste dal GDPR, art. 83.

La competenza per indagini, istruttoria, procedimento e irrogazione delle relative sanzioni è del Garante, ai sensi dell'art. 166 Codice Privacy.

SANZIONI AMMINISTRATIVE – Art. 83 Reg. + art. 166 Codice Privacy

Art. 83 comma 1 G.D.P.R. - Elementi utilizzati per la valutazione, ai fini dell'irrogazione della sanzione:

- Natura, gravità e durata violazione: nei casi in cui la violazione sia "minore" e non crei un rischio significativo per i diritti degli interessati, la sanzione può essere sostituita con un ammonimento.
- Carattere doloso o colposo della violazione.
- Misure adottate per attenuare il danno subito dagli interessati.
- Grado di responsabilità di titolare e responsabile del trattamento.
- Eventuali violazioni precedenti, pertinenti, commesse da titolare o responsabile
- Grado di cooperazione con Autorità di controllo.
- Categorie di dati interessati dalla violazione.
- Notificazione della violazione.
- Rispetto di eventuali prescrizioni imposte precedentemente in merito allo stesso tipo di violazioni.
- Adesione a codici di condotta o meccanismi di certificazione.
- Eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, come benefici finanziari conseguiti o perdite evitate quale conseguenza della violazione.

Art. 83 comma 2: le sanzioni possono essere aggiunte alle misure di cui all'art. 58.2 G.D.P.R. (poteri correttivi) ovvero alternative.

Sanzioni afflittive – art. 83 comma 4 G.D.P.R.:

Fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato annuo mondiale dell'esercizio precedente, nei casi di:

- inosservanza degli obblighi del titolare e del responsabile del trattamento;
- inosservanza degli obblighi dell'organismo di certificazione;
- inosservanza degli obblighi dell'organismo di controllo.

Art. 83 comma 5 G.D.P.R.

Fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato annuo mondiale dell'esercizio precedente, nei casi di:

- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati;
- inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali;
- inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo. Inosservanza di un ordine correttivo dell'autorità di controllo.

Sanzioni correttive – art. 58 comma 2 G.D.P.R.:

Le sanzioni correttive sono connesse ai poteri dell'Autorità di controllo, la quale può:

- rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR;
- rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;
- ingiungere al titolare del trattamento 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 disposizioni del GDPR, anche specificando in che modo ed entro quale termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

- Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;
- Revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- Infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure;
- Ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

STRUMENTI DI TUTELA: RECLAMO, SEGNALAZIONE, RICORSO GIURISDIZIONALE

RECLAMO

GDPR

Per il **reclamo** non sono previste particolari formalità, il GDPR non menziona alcunché circa il suo contenuto.

Ai sensi dell'art. 77 comma 2, l'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78. Ai sensi del considerando 141, ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico.

È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

Art. 142 Codice Privacy

- 1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto.
- 2. Il reclamo è sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali.
- 3. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.
- 4. Il Garante predispone un modello per il reclamo, da pubblicare nel proprio sito istituzionale, di cui favorisce la disponibilità con strumenti elettronici.
- 5. Il Garante disciplina con proprio regolamento il procedimento relativo all'esame dei reclami, nonché modalità semplificate e termini abbreviati per la trattazione di reclami che abbiano ad oggetto la violazione degli articoli da 15 a 22 del Regolamento.

Art. 143 Codice Privacy

- 1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento può adottare i provvedimenti di cui all'articolo 58 del Regolamento nel rispetto delle disposizioni di cui all'articolo 56 dello stesso.
- 2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.
- 3. Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo è deciso entro dodici mesi. In caso di attivazione del procedimento di cooperazione di cui all'articolo 60 del Regolamento, il termine rimane sospeso per la durata del predetto procedimento.
- 4. Avverso la decisione è ammesso ricorso giurisdizionale ai sensi dell'articolo 152.

Le modalità di presentazione…

- Il reclamante potrà far pervenire l'atto utilizzando la modalità ritenuta più opportuna, **consegnandolo a mano** presso gli uffici del Garante (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) **raccomandata A/R indirizzata a: Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 Roma**

b) **messaggio di posta elettronica certificata indirizzata a: protocollo@pec.gpdp.it**

- In sede di prima applicazione, il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell'interessato/a in corso di validità).

Artt. 8/18 Regolamento Garante 1/2019 - procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali

Art. 8

Dopo la presentazione del reclamo di cui all'art. 142:

- Se irregolare o incompleto → ne viene data comunicazione all'istante, con l'indicazione delle cause della irregolarità o incompletezza nonché del termine, di regola non superiore a quindici giorni, entro cui provvedere alla relativa regolarizzazione.
- Il reclamo non tempestivamente regolarizzato è archiviato e può essere esaminato a titolo di segnalazione.

Art. 9 - Trattazione del reclamo

- 1. L'esame del reclamo, nel corso dell'istruttoria preliminare e del successivo procedimento amministrativo eventualmente avviato, è orientato a criteri di semplicità delle forme osservate, di celerità ed economicità, anche in riferimento al contraddittorio. Resta fermo quanto stabilito all'articolo 15 in relazione alla trattazione dei reclami aventi ad oggetto la violazione degli articoli da 15 a 22 del RGPD [diritto di accesso, di rettifica, di cancellazione, di limitazione di trattamento, obbligo di notifica, diritto alla portabilità, di opposizione, profilazione].
- 2. Salvo quanto previsto dall'articolo 57, paragrafo 4, del RGPD, e dall'articolo 156, comma 8, del Codice, il dipartimento, servizio o altra unità organizzativa al quale il reclamo è assegnato cura l'istruttoria senza richiedere alcun contributo spese.
- 3. Il responsabile del procedimento procede, in riferimento alle formalità da osservare, nel rispetto delle disposizioni di cui alla legge 7 agosto 1990, n. 241, e successive modificazioni, con particolare riguardo agli avvisi alle parti, alle comunicazioni interlocutorie previste e al diritto di visione degli atti.

Art. 10 - Istruttoria preliminare

1. Il reclamo regolarmente presentato non comporta la necessaria adozione di un provvedimento del Collegio ai sensi dell'articolo 143, comma 1, del Codice.

2. Il dipartimento, servizio o altra unità organizzativa cui il reclamo è assegnato avvia un'istruttoria preliminare e, fermo restando quanto previsto dall'articolo 8, commi 1 e 2, del presente articolo informa l'istante dello stato o dell'esito del reclamo entro tre mesi dalla data della sua ricezione o della sua regolarizzazione.

3. Il dipartimento, servizio o altra unità organizzativa verifica se sussistono idonei elementi in ordine alle presunte violazioni e alle misure richieste dall'istante.

A tal fine, il dipartimento, servizio o altra unità organizzativa esamina la documentazione pervenuta e può curare l'acquisizione di precisazioni e informazioni in ordine ai fatti e alle circostanze cui si riferisce il reclamo, anche sentendo personalmente o a mezzo di procuratore il titolare o il responsabile del trattamento, mediante richiesta di informazioni o di esibizione di documenti ai sensi dell'articolo 157 del Codice sottoscritta dal dirigente competente, nonché procedendo ai sensi dell'articolo 22.

In tale contesto il dipartimento, servizio o unità organizzativa può invitare il titolare o il responsabile ad eseguire spontaneamente le misure richieste con il reclamo e a comunicare all'Ufficio, entro il termine da quest'ultimo richiesto, la propria eventuale adesione.

4. Al fine di promuovere l'esame organico di questioni, anche pervenute in tempi diversi, che possono rendere opportuna l'adozione di un eventuale provvedimento di carattere generale, l'istruttoria preliminare può essere svolta contestualmente in relazione a **più reclami aventi il medesimo oggetto** o che riguardano il medesimo titolare o responsabile del trattamento, oppure trattamenti di dati tra loro correlati. L'eventuale riunione o separazione di procedimenti è disposta dal dirigente del dipartimento, servizio o unità organizzativa competente. Per i procedimenti di pertinenza di più unità organizzative la riunione o separazione è disposta dal segretario generale.

Art. 11 - Chiusura dell'istruttoria preliminare

1. Al termine dell'istruttoria preliminare, il dipartimento, servizio o altra unità organizzativa competente può concludere l'esame del reclamo archiviandolo, quando:

a) la questione prospettata con il reclamo non risulta riconducibile alla protezione dei dati personali o ai compiti demandati al Garante;

b) non sono ravvisati, allo stato degli atti, gli estremi di una violazione della disciplina rilevante in materia di protezione dei dati personali;

c) si tratta di una richiesta eccessiva, in particolare per il carattere pretestuoso o ripetitivo anche ai sensi dell'articolo 57, paragrafo 4, del RGPD;

d) la questione prospettata con il reclamo è stata già esaminata dall'Autorità, in particolare con un provvedimento collegiale di carattere generale, o può essere esaminata richiamando provvedimenti o questioni già affrontate dal Garante ovvero esprimendo un prudente avviso su questioni che non presentano particolare rilevanza sul piano generale.

2. Nei casi di cui al comma 1 del presente articolo è fornito all'istante un riscontro indicando succintamente le ragioni per le quali, ai sensi del medesimo comma, non è promossa l'adozione di un provvedimento del Collegio.

3. Delle determinazioni di cui al comma 1 è informato il Collegio nei modi di cui all'articolo 36 del presente regolamento.

Art. 12 - Avvio del procedimento per l'adozione dei provvedimenti correttivi e sanzionatori

1. Quando l'esame del reclamo non si conclude ai sensi dell'articolo 11, comma 1, il dipartimento, servizio o altra unità organizzativa avvia, con propria comunicazione al titolare e, se del caso, al responsabile del trattamento, il procedimento per l'adozione dei provvedimenti di cui agli articoli 58, paragrafo 2, e 83 del RGPD.

2. Nel rispetto dell'articolo 166, comma 5, del Codice, la comunicazione di cui al comma 1 contiene:

a) una sintetica descrizione dei fatti e delle presunte violazioni della disciplina rilevante in materia di protezione dei dati personali nonché delle relative disposizioni sanzionatorie;

b) l'indicazione dell'unità organizzativa competente presso la quale può essere presa visione ed estratta copia degli atti istruttori;

c) l'indicazione che entro trenta giorni dal ricevimento della comunicazione è possibile inviare al Garante scritti difensivi o documenti e chiedere di essere sentito dalla medesima Autorità.

3. Ove ne ricorrano i presupposti, la comunicazione di cui ai commi 1 e 2 del presente articolo può essere resa direttamente al titolare e, se del caso, al responsabile del trattamento, qualora tali soggetti vengano sentiti dal dipartimento, servizio o altra unità organizzativa in fase di istruttoria preliminare, ai sensi dell'articolo 10, comma 3, del presente regolamento.

4. Ai sensi dell'articolo 166, comma 5, del Codice, i commi precedenti non trovano applicazione ove la suddetta comunicazione risulti incompatibile con la natura e le finalità del provvedimento da adottare.

Art. 13 - Diritto di difesa

1. Il destinatario della comunicazione di cui all'articolo 12 può esercitare il diritto di difesa mediante la presentazione di deduzioni scritte e documenti, nonché, ove richiesta, con l'audizione personale in merito ai fatti oggetto di comunicazione.

2. Entro trenta giorni dalla data di notifica della predetta comunicazione le deduzioni scritte e i documenti sono inviati all'unità organizzativa competente.

3. Il destinatario della comunicazione può richiedere, con specifica istanza debitamente motivata, una breve proroga. La proroga, di norma non superiore a quindici giorni, può essere concessa secondo criteri di proporzionalità anche in relazione alle caratteristiche operativo/dimensionali dei destinatari stessi e alla complessità della vicenda presa in esame. Il dipartimento, servizio o altra unità organizzativa competente comunica l'accoglimento o il rigetto della richiesta di proroga.

4. Ove sia altresì richiesta un'audizione, con istanza specifica anche allegata alle memorie difensive indirizzate al dipartimento, servizio o altra unità organizzativa competente, la medesima ha luogo presso la sede del Garante nella data fissata dall'Ufficio. Dell'audizione è redatto un sintetico verbale a cura dell'Ufficio. L'eventuale rinuncia all'audizione deve essere comunicata tempestivamente al dipartimento, servizio o altra unità organizzativa competente in relazione all'istruttoria. In sede di audizione i richiedenti svolgono le proprie controdeduzioni, evitando duplicazioni o meri rinvii a quanto già rappresentato negli scritti difensivi. L'audizione delle persone fisiche destinatarie della comunicazione di cui all'articolo 12, comma 2, ha carattere strettamente personale; è consentita la partecipazione con l'assistenza di un avvocato o di altro consulente.

5. La mancata presentazione di controdeduzioni scritte o della richiesta di audizione non pregiudica il seguito del procedimento.

Art. 14 - Decisione del reclamo

1. Valutata la documentazione in atti, l'esame del reclamo è concluso nei modi di cui all'articolo 11, comma 1, quando nuovi elementi sopravvenuti nel corso del procedimento evidenziano l'infondatezza o l'insussistenza dei presupposti per adottare un provvedimento.

2. Fuori dei casi di cui al comma 1, il dipartimento, servizio o altra unità organizzativa competente cura la predisposizione dello schema di provvedimento del Collegio e lo sottopone al segretario generale, trasmettendolo nei modi di cui all'articolo 15 del regolamento del Garante n. 1/2000.

3. Il Collegio provvede con propria deliberazione e adotta, ove necessario, i provvedimenti correttivi e sanzionatori di cui all'articolo 58, paragrafo 2, del RGPD. Il Collegio provvede con propria deliberazione anche quando rileva l'infondatezza del reclamo.

4. Il provvedimento è notificato alle parti a cura del dipartimento, servizio o altra unità organizzativa che ne ha curato l'istruttoria.

5. Quando la condotta è particolarmente risalente nel tempo o ha esaurito i suoi effetti oppure tali effetti sono stati rimossi o sono state fornite idonee assicurazioni da parte del titolare o del responsabile del trattamento, il dipartimento, servizio o altra unità organizzativa competente informa l'istante, ai sensi dell'articolo 77, paragrafo 2, del RGPD, ferma restando l'applicazione dei commi 2, 3 e 4 del presente articolo ove ne ricorrano i presupposti.

Art. 15 - Reclami aventi ad oggetto la violazione degli articoli da 15 a 22 del RGPD

- 1. In relazione ai reclami che abbiano ad oggetto, in via esclusiva, la violazione degli articoli da 15 a 22 del RGPD per i quali l'istante abbia già esercitato, in relazione al medesimo oggetto, i diritti riconosciuti da tali disposizioni nei confronti del titolare del trattamento senza ottenere un idoneo riscontro nei termini di cui all'articolo 12, paragrafo 3, del RGPD, salvi i casi di inammissibilità o manifesta infondatezza, entro quarantacinque giorni dalla data della sua ricezione, il reclamo è comunicato al titolare, con invito ad esercitare entro venti giorni dal suo ricevimento la facoltà di comunicare all'istante e all'Ufficio la propria eventuale adesione spontanea.

- 2. Il reclamo reca in allegato copia della richiesta rivolta al titolare del trattamento e dell'eventuale riscontro ricevuto.

- 3. Qualora l'istante non abbia preventivamente esercitato i diritti di cui agli articoli da 15 a 22 del RGPD con istanza rivolta al titolare del trattamento, se dal reclamo non emergano specifiche e fondate ragioni che ne giustifichino la mancata effettuazione, il dipartimento, servizio o altra unità organizzativa ai quali il reclamo è assegnato invita, entro quarantacinque giorni dalla data della ricezione del reclamo, l'istante a rivolgersi al titolare del trattamento.

- 4. In caso di adesione spontanea da parte del titolare ai sensi del comma 1, il dipartimento, servizio o altra unità organizzativa competente informa l'istante, ai sensi dell'articolo 77, paragrafo 2, del RGPD, e comunica al titolare o al responsabile del trattamento l'avvio del procedimento per l'adozione dei provvedimenti di cui agli articoli 58, paragrafo 2, e 83 del RGPD, ai sensi dell'articolo 166, comma 5, del Codice e nei termini di cui all'articolo 12 del presente regolamento.

Art. 16 – Ordinanza ingiunzione

- 1. Ai sensi dell'articolo 58, paragrafo 2, lettera i), e dell'articolo 83 del RGPD nonché dell'articolo 166 del Codice, il Collegio adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice.
- 2. L'ordinanza ingiunzione o l'atto di archiviazione sono notificati ai destinatari degli stessi a cura del dipartimento, servizio o altra unità organizzativa che ne ha curato l'istruttoria.
- 3. Quando ne ricorrono le condizioni, il provvedimento è altresì trasmesso, a cura del dipartimento, servizio o altra unità organizzativa che ha curato il procedimento sanzionatorio, al dipartimento, servizio o altra unità organizzativa competente in materia di amministrazione e contabilità per l'iscrizione a ruolo dei relativi importi.
- 4. Resta salva l'applicazione dell'articolo 28 della legge 24 novembre 1981, n. 689 [**prescrizione: 5 anni dalla violazione, salvo atti interruttivi**].

Art. 17 – Registro interno delle violazioni e delle misure correttive adottate

1. La decisione sul reclamo ai sensi degli articoli 14 e 15 nonché l'ordinanza ingiunzione ai sensi dell'articolo 16 dispongono altresì, ricorrendone i presupposti, l'annotazione nel registro interno dell'Autorità previsto dall'articolo 57, paragrafo 1, lettera u), del RGPD, delle violazioni e delle misure adottate in conformità all'articolo 58, paragrafo 2, del RGPD.

2. La conseguente annotazione nel predetto registro interno è curata dal dipartimento, servizio o altra unità organizzativa competente.

SEGNALAZIONE

GDPR

Nell'ambito del GDPR, le segnalazioni sono citate ma non regolamentate, pertanto si ritiene che, in materia, possa essere ancora applicabile il Codice Privacy.

Art. 144 Codice Privacy

- 1. Chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.
- 2. I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio.

Art. 19 Regolamento Garante 1/2019 – Esame delle segnalazioni

1. Sono qualificabili come segnalazioni gli atti, diversi dalle richieste di parere e dai quesiti, che non presentano le caratteristiche del reclamo e sono volti a sollecitare un controllo da parte del Garante sulla disciplina rilevante in materia di trattamento dei dati personali.

2. La segnalazione è presentata da un soggetto identificato. L'Autorità può utilizzare le notizie indicate in eventuali segnalazioni che provengono da un soggetto non identificato, qualora ritenga di dover avviare controlli su casi nei quali ravvisa il rischio di seri pregiudizi o di ritorsioni ai danni di soggetti interessati dal trattamento, oppure ricorre comunque un caso di particolare gravità.

3. La segnalazione può essere esaminata dall'Autorità, ma non comporta la necessaria adozione di un provvedimento.

4. Nei casi in cui fatti di possibile rilievo per la disciplina in materia di protezione dei dati personali siano stati riscontrati nell'ambito di verifiche condotte da altre Autorità, la segnalazione può essere esaminata ai fini dell'eventuale accertamento della sussistenza di una violazione. Ove necessario, sono acquisiti ulteriori elementi.

5. Il dipartimento, servizio o altra unità organizzativa competente può, anche tenuto conto di quanto previsto dall'articolo 3 del presente regolamento, concludere l'esame della segnalazione disponendone l'archiviazione quando ricorre uno dei presupposti di cui all'articolo 11, comma 1, oppure in caso di segnalazioni del tutto generiche. Si considerano tali le segnalazioni che si limitano a imputare a un soggetto fatti privi di elementi circostanziati o che non contengono elementi tali da consentire un'agevole individuazione del titolare del trattamento.

6. È fatta salva l'attività di controllo, anche con riferimento a segnalazioni già oggetto di archiviazione ai sensi dei commi precedenti, in caso di sopravvenuti elementi di fatto o di diritto ovvero di diversa ed ulteriore valutazione del Garante.

7. Delle determinazioni di cui al comma 5 è informato il Collegio nei modi di cui all'articolo 36.

Art. 20 - Istruttoria preliminare ed eventuale procedimento amministrativo

1. Fermi restando i casi in cui la segnalazione è archiviata ai sensi dell'articolo 19, comma 5, il dipartimento, servizio o altra unità organizzativa può avviare un'istruttoria preliminare.

2. Nel corso dell'eventuale procedimento amministrativo si osservano le disposizioni per i reclami di cui agli articoli da 9 a 18, anche per quanto riguarda l'informativa al Collegio ai sensi dell'articolo 36, e al segnalante può essere fornito un riscontro.

Ai sensi del combinato disposto tra l'art. 154 Codice Privacy e gli artt. 21 ss Regolamento 1/2019, il Garante ha il potere di irrogare sanzioni ed effettuare controlli senza che vi sia un reclamo o una segnalazione.

Poteri del Garante - Art. 154 Codice Privacy

- 1. Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformità alla disciplina vigente e nei confronti di uno o più titolari del trattamento, ha il compito di:
- a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;
- b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;
- c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-quater;
- d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
- […]

- 3. Per quanto non previsto dal Regolamento e dal presente codice, il Garante disciplina con proprio Regolamento, ai sensi dell'articolo 156, comma 3, le modalità specifiche dei procedimenti relativi all'esercizio dei compiti e dei poteri ad esso attribuiti dal Regolamento e dal presente codice.
- 4. Il Garante collabora con altre autorità amministrative indipendenti nazionali nello svolgimento dei rispettivi compiti.
- 5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante, anche nei casi di cui agli articoli 36, paragrafo 4, del Regolamento, è reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.
- 6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.
- 7. Il Garante non è competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.

Art. 21 - Controlli e provvedimenti adottati senza istanza di parte

1. Nell'esercizio dei compiti di controllo o comunque esercitabili dal Garante, valutati gli elementi in suo possesso e anche in assenza di reclamo, segnalazione o notificazione di violazione dei dati personali, l'Autorità può avviare d'ufficio un'istruttoria preliminare per verificare la sussistenza di idonei elementi in ordine a possibili violazioni della disciplina rilevante in materia di protezione dei dati personali.

2. Nel corso dell'eventuale procedimento si osservano, in quanto applicabili, le disposizioni per i reclami di cui agli articoli da 9 a 18, anche per quanto riguarda l'informativa al Collegio ai sensi dell'articolo 36.

Art. 22 - Attivita` ispettive e di revisione sulla protezione dei dati personali

1. Il dipartimento, servizio o altra unità organizzativa competente in materia di attivita` ispettive e di revisione cura lo svolgimento dell'attivita` ispettiva effettuata ai sensi degli articoli 157 e 158 del Codice nonche' ai sensi dell'articolo 58, paragrafo 1, e dell'articolo 62 del RGPD, tenuto anche conto della programmazione dell'attivita` ispettiva disposta dal Collegio ai sensi dell'articolo 4, comma 1, lettera c), del presente regolamento, sulla base di un ordine di servizio sottoscritto dal dirigente del medesimo dipartimento. Effettuati gli accertamenti relativi agli elementi idonei in ordine alle presunte violazioni, il dipartimento, servizio o altra unità organizzativa inoltra gli atti al segretario generale per l'assegnazione alla competente unità organizzativa ai sensi dell'articolo 14 del regolamento del Garante n. 1/2000, per il seguito di trattazione.

2. Valutata la sussistenza di eventi di particolare rilevanza, il Collegio puo` disporre ulteriori attivita` ispettive, da svolgersi secondo le modalita` di cui al comma 1 del presente regolamento.

3. Il dipartimento servizio o altra unità organizzativa competente in materia di attivita` ispettive e di revisione cura altresi` i controlli di cui al comma 1 nell'ambito delle istruttorie preliminari e dei procedimenti amministrativi comunque avviati presso altre unità organizzative dell'Autorita`, alle quali è restituito l'esito per la successiva trattazione.

4. L'attivita` ispettiva effettuata ai sensi degli articoli 157 e 158 del Codice puo` essere curata dal dipartimento servizio o altra unità organizzativa competente in materia di attivita` ispettive e di revisione ovvero delegata alla Guardia di finanza. La stessa puo` essere altresi` effettuata avvalendosi, ove necessario, della collaborazione di altri organi dello Stato.

5. L'ordine di servizio con cui è disposta l'attivita` ispettiva individua il titolare o il responsabile del trattamento destinatari del controllo, i poteri di indagine utilizzati, l'ambito del controllo, il luogo ove si svolge l'accertamento, il responsabile delle attivita` e gli ulteriori partecipanti, designati d'intesa con i dirigenti dei dipartimenti, servizi o altre unità organizzative; l'ordine di servizio indica altresi` le sanzioni previste ai sensi dell'articolo 83, paragrafo 5, lettera e), del RGPD e degli articoli 166 e 168 del Codice.

6. Nel corso dell'attivita` ispettiva, della quale puo` essere dato preavviso, è possibile, in particolare:

a) controllare, estrarre ed acquisire copia dei documenti, anche in formato elettronico;

b) richiedere informazioni e spiegazioni;

c) accedere alle banche dati ed agli archivi;

d) acquisire copia delle banche dati e degli archivi su supporto informatico.

7. Durante l'attivita` ispettiva il soggetto sottoposto ad ispezione puo` farsi assistere da consulenti di propria fiducia e fare riserva di produrre la documentazione non immediatamente reperibile entro un termine congruo, di regola non superiore a trenta giorni; in casi eccezionali, puo` essere richiesto un differimento di tale termine.

8. Le attivita` di revisione sulla protezione dei dati personali sono avviate ai sensi dell'articolo 58, paragrafo 1, lettera b), del RGPD, presso il titolare o il responsabile del trattamento ovvero presso la sede dell'Autorita`. In tale ultimo caso, l'attivita` si svolge a seguito di convocazione del titolare o del responsabile presso il dipartimento, servizio o altra unità organizzativa competente in materia di attivita` ispettive e di revisione. Nell'ambito delle attivita` di revisione, qualora emergano elementi di criticita` nel trattamento dei dati personali, possono essere avviate attivita` ispettive al fine di rilevare eventuali violazioni della normativa sulla protezione dei dati personali.

9. Dell'attivita` svolta ai sensi dei commi precedenti, con particolare riferimento alle dichiarazioni rese ed ai documenti acquisiti, è redatto processo verbale, una copia del quale viene consegnata al soggetto sottoposto ad ispezione ovvero ad attivita` di revisione.

Ricorso giurisdizionale

Il ricorso giurisdizionale è regolamentato dall'art. 152 Codice Privacy, il quale prevede che «*1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento, sono attribuite all'autorità giudiziaria ordinaria. (1)*

1-bis. Le controversie di cui al comma 1 sono disciplinate dall'articolo 10 del decreto legislativo 1° settembre 2011, n. 150. (2)»

Art. 10 d.lgs. 150/2011

1. Le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo.

2. Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.

3. Il ricorso avverso i provvedimenti del Garante per la protezione dei dati personali, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, è proposto, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento ovvero entro sessanta giorni se il ricorrente risiede all'estero.

4. Decorso il termine previsto per la decisione del reclamo dall'articolo 143, comma 3, del decreto legislativo n. 196 del 2003, chi vi ha interesse può, entro trenta giorni dalla scadenza del predetto termine, ricorrere al Tribunale competente ai sensi del presente articolo. La disposizione di cui al primo periodo si applica anche qualora sia scaduto il termine trimestrale di cui all'articolo 143, comma 3, del decreto legislativo n. 196 del 2003 senza che l'interessato sia stato informato dello stato del procedimento.

5. L'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile.

6. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

7. L'efficacia esecutiva del provvedimento impugnato può essere sospesa secondo quanto previsto dall'articolo 5.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nei casi in cui non sia parte in giudizio, il Garante può presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali. Il giudice dispone che sia data comunicazione al Garante circa la pendenza della controversia, trasmettendo copia degli atti introduttivi, al fine di consentire l'eventuale presentazione delle osservazioni.

10. La sentenza che definisce il giudizio non è appellabile e può prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonché il risarcimento del danno.

SANZIONI PENALI

Dalla relazione illustrativa al d.lgs. 101/2018…

«Quasi tutte le vigenti disposizioni penali (gli art 167 ss. del codice privacy) reprimono comportamenti che, in attuazione dell'art. 83 del Regolamento, dovranno essere puniti con sanzioni amministrative (fa eccezione soltanto il reato di false comunicazioni al Garante).

Di conseguenza, è stata evidenziata l'opportunità di adempiere a tale obbligo procedendo direttamente ad una mirata e limitata depenalizzazione, in modo da scongiurare i rischi di violazione del principio del ne bis in idem tra sanzioni penali e sanzioni amministrative affermato nella giurisprudenza delle Corti europee (su cui ora si tornerà maggiormente nel dettaglio).

In particolare, vanno assicurate le esigenze di proporzione tra fatto e trattamento sanzionatorio che sono sostanzialmente riconducibili al profilo sostanziale del ne bis in idem (peraltro soltanto nei casi in cui la sanzione amministrativa sia inferiore a quella penale ed il suo importo possa, di conseguenza, essere integralmente scomputato); ma il rispetto di dette esigenze non risolve i profili di tensione con l'omonima garanzia processuale, secondo cui un soggetto non dovrebbe essere sottoposto a due procedimenti sanzionatori per il medesimo fatto (idem factum), indipendentemente dall'esito degli stessi (e a prescindere, quindi, dal problema della proporzione della sanzione).»

Art. 167 Codice Privacy

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, 126 e 130 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 e 10 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.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. 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. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. 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.

Comma 1: la condotta, in concreto, consiste nell'operare in violazione delle disposizioni (artt. 123, 126, 130, e provvedimenti di cui all'art.129) in materia di comunicazioni elettroniche.

Potrebbe definirsi una norma parzialmente in bianco. La condotta consiste nell'arrecare nocumento sorretto dalla volontà di ottenere un profitto, arrecando un danno all'interessato. Si tratta di un reato a consumazione anticipata ragione per la quale non si ritiene possibile il tentativo.

Comma 2: prevede un' altra fattispecie punita più gravemente. Rispetto all'altra ipotesi cambia la modalità della condotta consistente nel trattare dati particolari, e relativi a condanne penali e reati, in violazione di legge, regolamento e delle misure di garanzia, al fine di trarre profitto ovvero di arrecare danno, ove per danno si deve ritenere un ipotesi di danno indubbiamente di natura patrimoniale. Il dolo specifico è previsto nella forma alternativa.

Per completezza, circa l'elemento soggettivo, il Garante, come si legge nel Dossier relativo ai lavori parlamentari, suggerisce *di considerare, quale oggetto alternativo del dolo specifico, anche il nocumento, in ragione dell'esigenza di presidiare con la sanzione penale condotte connotate da un simile disvalore, anche quando sorrette dal dolo di danno e non solo da quello di profitto. Tale modifica consentirebbe di assicurare una maggiore continuità normativa con la fattispecie vigente e di evitare gli effetti (anche sui processi in corso) dell'*abolitio criminis *che si dovesse ravvisare, in parte qua, per effetto della novellazione proposta.*

Comma 3: la condotta si sostanzia nel trasferimento di dati verso paesi terzi od organizzazioni internazionali in violazione del Regolamento europeo.

Comma 4: ha carattere processuale e disciplina la procedura con la quale il Pubblico Ministero è tenuto ad informare il Garante allorchè abbia notizia, ovvero quando gli giunge un rapporto dalla PG. Naturalmente, il PM dovrà verificarne la fondatezza.

Comma 5: impone un obbligo di denuncia da parte del Garante verso il PM.

Comma 6: prevede la necessità della sanzione amministrativa pecuniaria irrogata e riscossa dal Garante per ottenere una diminuzione di pena, senza specificarne il *quantum* di riduzione. In assenza di una maggiore precisazione della legge si deve ritenere che la diminuzione sia al massimo di 1/3. Si badi bene che si tratta di una diminuente e non attenuante, poiché non soggetta né a valutazione né a bilanciamento, imposta per legge.

Art. 167bis Codice Privacy

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 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.

Si tratta di un delitto, introdotto dal D.Lgs. 101/2018, punito gravemente da 1 a 6 anni, allorchè chiunque comunichi o diffonda un archivio automatizzato o una parte sostanziale di esso, al fine di trarne profitto o di arrecare un danno.

Per "archivio" si 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, come si rinviene nelle definizioni di cui all'art. 4 del Regolamento UE 679/16.

Perché la condotta sia penalmente rilevante deve trattarsi di "archivio" avente ad oggetto dati trattati su "larga scala" parametro normativamente previsto dall'art. 37 del Regolamento UE con una sua specificazione nelle linee guida elaborate dal WP29 sul Data Protection Officer (DPO), cui si rimanda.

Il **comma 2** punisce la medesima condotta di cui al comma 1, ma si perpetra in assenza di consenso. La previsione di questa nuova e diversa fattispecie penale ha lo scopo di reprimere quei comportamenti che, per vastità di dimensioni, non si esaurirebbero nella mera violazione delle norme sul trattamento.

Il dolo è specifico. Un esempio potrebbe essere la comunicazione o diffusione di un archivio di malati di tumore di un ospedale ad un centro di laboratorio di scienza medica, senza il consenso dell'interessato (avente diritto), al fine di trarne profitto.

Il **III** ed ultimo **comma** è procedurale ed impone di informare al Garante, con la previsione della diminuente, per l'ipotesi di cui si è detto. È possibile, infine, la previsione del delitto nella forma tentata nel caso in cui l'evento non si verifichi o l'azione non venga completata.

La previsione di una nuova e diversa fattispecie penale non coincidente con l'attuale articolo 167 del Codice ha lo scopo di reprimere quei comportamenti che per vastità di dimensioni, coinvolgimento di un numero rilevante di persone offese e, quindi, di dati trattati, finalizzazione dell'azione al profitto, non si esauriscono nella mera violazione delle norme sul trattamento.

Art. 167ter Codice Privacy

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.

Valgono le considerazioni svolte per il reato di cui all'art. 167bis.

Art. 168 Codice Privacy

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.

Si tratta di una fattispecie che, a differenza delle altre finora analizzate, è punita a titolo di dolo generico.

La condotta è data dalla dichiarazione o attestazione mendace di notizie o circostanze o dalla produzione di atti o documenti falsi.

L'ipotesi di un più grave reato potrebbe ravvisarsi nella calunnia.

La disposizione viene poi integrata tramite l'inserimento di un **comma II** con la previsione della sanzione della reclusione fino ad un anno a carico di chi cagiona intenzionalmente una interruzione o turba la regolarità dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante.

Si tratta dunque di un'ipotesi autonoma di reato comune, laddove la condotta attiva si perfeziona attraverso qualsiasi atteggiamento o manifestazione che potremmo definire non consono, come ad es. espressioni verbali particolarmente aggressive che portano ad una interruzione del procedimento o ne turbano la regolarità.

Art. 169 Codice Privacy - abrogato

[1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni [o con l'ammenda da diecimila euro a cinquantamila euro].

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo della sanzione stabilita per la violazione amministrativa. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758 e successive modificazioni, in quanto applicabili.]

Art. 170 Codice Privacy

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.

Tale fattispecie è stata riformulata dal D.Lgs. 101/2018 in ordine alla specificazione del tipo di provvedimenti violati.

Rispetto agli illeciti precedentemente descritti, questo è il primo delitto in cui manca la clausola di riserva espressa. Si tratta sempre di un reato comune.

La condotta è la mancata osservanza di un provvedimento adottato dal Garante ai sensi dell'art. 58 del Regolamento che impone "…una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento" destinato ad una realtà specifica; ovvero di una delle misure di garanzie di cui all'art. 2 *septies* volte ad individuare "*le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, misure di minimizzazione, specifiche modalità di accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché eventuali altre misure necessarie a garantire i diritti degli interessati*"; nonché i provvedimenti generali di cui all'art. 21 comma I del decreto di armonizzazione.

Con riferimento a questi ultimi, si pone il problema di come gestire il trattamento di dati autorizzato da provvedimenti ovvero da autorizzazioni generali che sono state abrogate per effetto del D.lgs 101/2018 le quali verranno sostituite da un unico provvedimento che dovrà essere emanato a seguito di una consultazione pubblica della durata di 90 giorni dall'entrata in vigore del predetto decreto (e cioè dal 19 settembre u.s.) e potrà essere adottato solamente trascorsi 60 giorni dal termine del procedimento di consultazione pubblica.

Secondo alcuni, senza soluzione di continuità, per il periodo transitorio, continuano ad essere efficaci i provvedimenti e le autorizzazioni generali del Garante. Secondo altri invece, in forza dell'art. 27 del D.Lgs. 101/2018 – che ha abrogato l'intero Titolo VI (Adempimenti) del Codice della Privacy- sono cadute (con effetto immediato) le autorizzazioni generali del Garante. Secondo quest'ultima interpretazione, tuttavia, si pone un problema di non facile soluzione. Ad esempio, si faccia il caso del **trattamento di dati giudiziari.** Per tali dati il soggetto chiamato a verificare la possibilità di trattamento dovrà valutare bene se rientra o meno nelle casistiche di cui all'art. 2 *octies* poiché, ad oggi, non sono coperte tutte le ipotesi previste dall'Autorizzazione Generale n. 7 del 2016. Si raccomanda, pertanto, estrema prudenza prima di iniziare un trattamento di dati giudiziari, salvo l'autorizzazione dell'interessato.

Art. 171 Codice Privacy

1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

Art. 38. Disposizioni penali.

1. Le violazioni degli articoli 2, 4, 5, 6, 8 e 15, primo comma lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno. 2. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. 3. Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. 4. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale.

Si tratta di una fattispecie riformulata ovvero parzialmente modificata la quale, rispetto alla previgente versione, pur mantenendo l'applicabilità delle sanzioni di cui all'art. 38 Stat. Lav., si limita alle violazioni commesse con riferimento al solo comma I dell'art. 4 Stat. Lav.

In definitiva, la fattispecie penale punisce tutte quelle violazioni connesse all'impiego di impianti audiovisivi o altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori per esigenze che non siano organizzative e produttive, legate alla sicurezza sul lavoro o alla tutela del patrimonio aziendale, nonché tutte quelle violazioni legate al mancato rispetto della procedura autorizzativa (sindacale o amministrativa) circa l'installazione degli impianti stessi.

Non vengono più sanzionate, come in precedenza, le violazioni connesse al comma II dell'art. 4 cioè relative agli strumenti di lavoro e a quelli di registrazione degli accessi e delle presenze.

Art. 172 Codice Privacy

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.

Bilancio 2018

Nel corso del 2018 sono state adottate 175 ordinanze-ingiunzione, a fronte delle 109 del 2017 ed è stato rilevato un notevole aumento delle somme riscosse pari a 8.161.806 euro, a fronte dei 3.776.694 euro registrati nel 2017 (con una variazione positiva del +116%).

Da registrare inoltre un incremento del 20% delle violazioni amministrative contestate: 707 nel 2018 rispetto alle 589 contestazioni del 2017.

Le contestazioni hanno riguardato la violazione di disposizioni del Codice per illeciti commessi prima della data di applicazione del Regolamento (UE) 2016/679.

Sono invece diminuite le segnalazioni all'autorità giudiziaria: 27 nel 2018 rispetto alle 41 del 2017.

Gli accertamenti, svolti nel 2018 anche con il contributo delle Unità Speciali della Guardia di finanza, Nucleo speciale privacy, hanno riguardato numerosi e delicati settori, sia nell´ambito pubblico che privato.

Per quanto riguarda il settore privato le ispezioni si sono rivolte principalmente ai trattamenti effettuati: dagli istituti di credito, da società per attività di rating sul rischio e sulla solvibilità delle imprese, dalle aziende sanitarie locali e poi trasferiti a terzi per il loro utilizzo a fini di ricerca, da società che svolgono attività di telemarketing, da società che offrono servizi di "money transfer". Oggetto di particolare accertamento anche i trattamenti di dati svolti da società assicuratrici attraverso l'installazione di "scatole nere" a bordo degli autoveicoli e da società che offrono servizi medico-sanitari tramite app.

Per quanto riguarda il settore pubblico l´attività di verifica si è concentrata su enti pubblici, soprattutto Comuni e Regioni, che svolgono trattamenti di dati personali mediante app per smartphone e tablet, con particolare attenzione all'eventuale profilazione e geolocalizzazione degli utenti; sulle grandi banche dati; sul sistema della fiscalità, con speciale riguardo alle misure di sicurezza e al sistema degli audit; sul sistema informativo dell´Istat e sullo Spid.

Piano ispettivo del Garante Privacy – Obiettivi 2019

Principali obiettivi:

- Istituti di credito, sanità, sistema statistico nazionale (Sistan), Spid, telemarketing, carte di fedeltà, grandi banche dati pubbliche.
- L'attività ispettiva, svolta anche in collaborazione con il Nucleo speciale privacy della Guardia di finanza, riguarderà innanzitutto i trattamenti di dati effettuati dalle banche, con particolare riferimento ai flussi legati all'anagrafe dei conti; i trattamenti di dati effettuati dalle Asl e poi trasferiti a terzi per il loro utilizzo a fini di ricerca; la gestione delle carte di fidelizzazione da parte delle aziende; il rilascio dell´identità digitale ai cittadini italiani (Spid); il Sistema Integrato di Microdati (Sim) dell´Istat.
- I controlli si concentreranno anche sull'adozione delle misure di sicurezza da parte di pubbliche amministrazioni e di imprese che trattano dati sensibili, il rispetto delle norme sull'informativa e il consenso, la durata della conservazione dei dati da parte di soggetti pubblici e privati. L'attività ispettiva verrà svolta anche in riferimento a segnalazioni e reclami, con particolare attenzione alle violazioni più gravi.

Telemarketing indesiderato: 600 mila euro di sanzione a Wind Tre

Il Garante per la privacy ha ordinato a Wind Tre S.p.A. il pagamento di una sanzione di 600 mila euro per gravi violazioni della normativa sulla protezione dei dati personali nel corso di attività di marketing telefonico, anche tramite sms.

La sanzione è giunta a seguito di un provvedimento adottato prima dell'entrata in vigore del nuovo Regolamento Europeo, con il quale il Garante, sulla base di numerose segnalazioni, aveva dichiarato illecito il trattamento dei dati dei clienti effettuato dalla società telefonica e vietato l'ulteriore uso di tali dati a fini di marketing. Wind Tre aveva infatti usato senza consenso i dati dei clienti a fini promozionali e sempre senza consenso li aveva comunicati alla rete dei partner commerciali. Il trattamento illecito è derivato principalmente da due violazioni.

La prima ha riguardato la mancata verifica delle liste di chi non desiderava essere contattato a scopi pubblicitari ("black list"), detenute dalla società, nelle quali erano presenti i segnalanti.

La seconda è dipesa da una sistematica e prolungata comunicazione illecita di dati della clientela a terzi, cioè appunto ai partner commerciali. La società infatti aveva erroneamente qualificato la maggior parte dei punti vendita come titolari autonomi, anziché come responsabili del trattamento, incorrendo così in una illecita comunicazione.

Nel definire l'importo dovuto, l'Autorità ha tenuto conto della gravità delle violazioni contestate, come il fatto che siano stati impiegati differenti canali di contatto (telefonate, sms) con esponenziale aumento dell'invasività delle campagne promozionali, ma anche - in termini favorevoli - del fatto che Wind Tre abbia posto in essere autonome iniziative per eliminare le criticità prima ancora dell'adozione del provvedimento di divieto, poi ulteriormente rafforzate per adeguarsi alle novità introdotte dal Regolamento Ue.

La società ha proceduto al pagamento della sanzione nei termini previsti.

Cambridge Analytica

Il Garante per la privacy ha concluso l'istruttoria avviata nei confronti di Facebook per il "caso Cambridge Analytica". Al termine delle verifiche effettuate è risultato che i dati dei cittadini italiani acquisiti tramite l'App "Thisisyourdigitalife" (il test della personalità ideato per raccogliere le informazioni personali oggetto di profilazione), benché non siano stati trasmessi a Cambridge Analytica, sono stati comunque trattati in modo illecito, in assenza di idonea informativa e di uno specifico consenso. Pertanto il Garante ne ha vietato l'ulteriore trattamento e si è riservato di avviare un separato procedimento sanzionatorio.

Nel corso della medesima istruttoria è inoltre emerso uno specifico trattamento di dati personali dei cittadini italiani acquisiti in occasione delle elezioni politiche del 4 marzo 2018, mediante un prodotto, denominato "Candidati", installato sulla piattaforma del social network. Tale prodotto consentiva agli elettori che fornivano il proprio indirizzo postale di avere informazioni sui candidati della propria circoscrizione elettorale e sui loro programmi. Facebook, pur affermando di non registrare informazioni su come gli utenti si fossero orientati su tali profili, conservava i file di log delle loro azioni per un periodo di 90 giorni, per poi estrarne "matrici aggregate" non meglio definite. Inoltre, nel giorno delle elezioni appariva sul newsfeed degli utenti di Facebook un messaggio che sollecitava la condivisione dell'essersi o meno recati al voto e ad esprimere opinioni sull'importanza dello stesso.

Il Garante ha rilevato che queste due funzioni di Facebook, specificamente concepite e rivolte ai cittadini italiani in prossimità delle elezioni, non sono previste tra le finalità indicate nella "data policy" della piattaforma.

I dati personali possono essere raccolti per finalità determinate ed esplicite e successivamente trattati in modo compatibile con tali finalità. A maggior ragione le finalità del relativo trattamento devono essere descritte con estrema precisione quando vengono raccolti dati sensibili, come quelli potenzialmente idonei a rivelare opinioni politiche, in modo tale da consentire agli utenti di esprimere il proprio consenso libero e informato. E dati "sensibili" sono ad esempio le informazioni sull'essersi recati o meno alle urne o le dichiarazioni a favore del voto (rimaste visibili sulla piattaforma anche se, secondo quanto sostenuto da Facebook, non monitorate).

A conclusione dell'istruttoria, il Garante ha dunque ritenuto illegittimo il trattamento di dati realizzato da Facebook in quanto basato su un generico consenso reso dall'utente al momento della registrazione alla piattaforma dopo la lettura di una informativa del tutto inidonea.

Per tali ragioni, ha vietato a Facebook il trattamento di ogni eventuale dato raccolto mediante tali modalità e delle valutazioni espresse dagli utenti a seguito del messaggio che sollecitava la condivisione.

Anche per tale fattispecie l'Autorità si è riservata la contestazione di sanzioni amministrative per gli illeciti trattamenti di dati riscontrati.

Il provvedimento è stato trasmesso all'Autorità di protezione dati dell'Irlanda, Paese dove è insediato lo stabilimento principale di Facebook in Europa, per le valutazioni di competenza, in cooperazione con il Garante italiano.

Lavoro: vietato il controllo massivo e la conservazione illimitata delle email

No al controllo massivo e alla conservazione senza limite delle email. Il Garante per la privacy ha vietato ad una società il trattamento di dati personali effettuato sulle email aziendali dei dipendenti in violazione della normativa sulla protezione dei dati e di quella sulla disciplina lavoristica. La società dovrà ora limitarsi a conservare i dati a fini di tutela dei diritti nel giudizio pendente.

L´Autorità - intervenuta a seguito del reclamo di un dipendente - ha accertato che la società trattava in modo illecito i dati personali contenuti nelle email in entrata e in uscita, anche di natura privata e goliardica, scambiate dal lavoratore con alcuni colleghi e collaboratori. I dati raccolti nel corso di un biennio erano poi stati utilizzati per contestare un provvedimento disciplinare cui era seguito il licenziamento del dipendente poi annullato dal giudice del lavoro.

Nel disporre il divieto l´Autorità ha rilevato numerose e gravi violazioni. La società non ha infatti fornito ai dipendenti alcuna informazione su modalità e finalità di raccolta e conservazione dei dati relativi all´uso della posta elettronica, né con una informativa individualizzata né attraverso la policy aziendale. Un comportamento in contrasto con l´obbligo della società di informare i lavoratori riguardo alle caratteristiche essenziali dei trattamenti effettuati, comprese le operazioni che possono svolgere gli amministratori di sistema (ad es., accesso ai contenuti delle email). La società, inoltre, conservava in modo sistematico i dati esterni e il contenuto di tutte le email scambiate dai dipendenti per l´intera durata del rapporto di lavoro e anche dopo la sua interruzione, violando così i principi di liceità, necessità e proporzionalità stabiliti dal Codice privacy. La società - afferma l´Autorità - anziché mettere in atto un trattamento così invasivo, avrebbe potuto agire in modo più efficiente e più rispettoso della riservatezza dei lavoratori predisponendo dei sistemi di gestione documentale in grado di individuare selettivamente i documenti che avrebbero dovuto essere via via archiviati. Inoltre - continua il Garante - la conservazione estesa e sistematica delle mail, la loro memorizzazione per un periodo indeterminato e comunque amplissimo nonché la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto (ad es. difesa in giudizio, perseguimento di un interesse legittimo) consente il controllo dell´attività dei dipendenti. Controllo vietato dalla disciplina di settore che non autorizza, anche dopo le modifiche del Jobs Act, verifiche massive, prolungate e indiscriminate. Il datore di lavoro infatti pur potendo controllare l´esatto adempimento della prestazione e il corretto uso degli strumenti di lavoro deve sempre salvaguardare la libertà e la dignità dei dipendenti.

Ingiustificata, in particolare, la raccolta a priori di tutte le email in vista di futuri ed eventuali contenziosi, il Garante ha ribadito infatti che la conservazione deve riferirsi a contenziosi in atto o a situazioni precontenziose e non a ipotesi astratte e indeterminate. Il Garante ha ritenuto, infine, non conforme alla legittima aspettativa di riservatezza della corrispondenza l´accesso della società alle email in ingresso sull´account aziendale dopo il licenziamento del lavoratore. Al cessare del rapporto di lavoro la casella di posta elettronica deve essere disattivata e rimossa e al suo posto di devono attivare eventuali account alternativi.

L´Autorità si riserva di valutare con un autonomo procedimento la contestazione di sanzioni amministrative relative agli illeciti riscontrati.

Propaganda elettorale: no all'uso dei dati di ex-pazienti senza consenso - Il Garante sanziona un medico per 16mila euro

L'Autorità per la privacy ha comminato una sanzione di 16mila euro a un medico che ha utilizzato gli indirizzi di circa 3.500 ex-pazienti per inviare lettere a sostegno di un candidato alle elezioni politiche regionali del 4 marzo 2018, senza che gli interessati avessero espresso alcun specifico consenso a riguardo.

Nel corso dell'istruttoria, avviata dal Garante a seguito di alcuni articoli di stampa che segnalavano la vicenda, il medico si è difeso affermando di aver scritto ai suoi ex pazienti, che aveva avuto in cura presso un importante Istituto oncologico, per informarli della sua nuova sede di lavoro, avendo cessato il suo rapporto professionale presso l'Istituto. Con l'occasione, aveva contestualmente espresso il suo sostegno a un candidato alle elezioni, già assessore alla Sanità e al Welfare, e aveva ritenuto di rispettare le norme consentendo ai destinatari di opporsi alla ricezione dei messaggi, mediante un link posto in calce alla mail.

Il Garante ha giudicato un tale trattamento di dati personali illecito per diversi profili.

In primo luogo, il medico non ha reso l'informativa né al momento della registrazione dei dati dei pazienti né alla prima comunicazione, come previsto dal Codice privacy. Questo adempimento è infatti obbligatorio in quanto i dati, nel caso di specie, non risultano raccolti dal medico direttamente presso gli interessati, ma ricevuti dall'Istituto oncologico all'atto della cessazione del rapporto di lavoro. Inoltre, il medico ha utilizzato i dati dei suoi ex pazienti per finalità diverse da quelle di cura, per le quali erano stati raccolti, senza aver acquisito uno specifico e autonomo consenso.

Come chiarito dal Garante nel provvedimento generale in materia di propaganda elettorale del 6 marzo 2014, "i dati personali raccolti nell'ambito dell'attività di tutela della salute da parte di esercenti la professione sanitaria e di organismi sanitari, non sono utilizzabili per fini di propaganda elettorale e connessa comunicazione politica. Tale finalità non è infatti riconducibile agli scopi legittimi per i quali i dati sono stati raccolti".

Nonostante la sanzione sia stata comminata in base al vecchio Codice, i principi che la ispirano restano validi anche in base al nuovo Regolamento Ue, come di recente precisato nel provvedimento dell'Autorità del 7 marzo 2019.