Nuovo Codice privacy

Adeguamento al GDPR: sanzioni e regime transitorio

Enrico Barraco, Andrea Sitzia, Stefano Jacobucci, Silvia Rizzato - Studio legale Barraco

Apparato sanzionatorio del GDPR

Il Regolamento generale sul trattamento dei dati personali 679/2016 (GDPR), in ragione della sua natura di Regolamento, cioè di atto avente portata generale, obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri dell'Unione europea, risponde alla necessità, espressa nel considerando n. 10 del GDPR, di garantire un "livello coerente ed elevato di protezione", assicurare l'attuazione del principio di libertà di movimento, evitando pericolosi fenomeni di "stabilimento strategico", con un trattamento dei dati che dovrebbe essere equivalente in tutti gli Stati membri dell'Unione europea.

L'esigenza sottostante all'apparato sanzionatorio del GDPR è dunque quella di garantire omogeneità di applicazione dello stesso, in ogni Stato membro; tuttavia, questa esigenza è presto sconfessata dall'art. 84, par. 1, GDPR, a norma del quale "gli Stati membri dell'Unione europea stabiliscono le norme relative alle altre sanzioni per le violazioni del presente Regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'art. 83 e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive".

Va anche precisato che la materia penale non rientra tra le materie di competenza dell'Unione europea, pertanto, almeno con riferimento alle fattispecie e alle sanzioni penali, la scelta di rimettere agli Stati membri dell'Unione europea trova una sua concreta giustificazione proprio nella carenza di competenza.

Giusta la distinzione fatta dall'art. 84 GDPR, va subito chiarito che il Regolamento individua due categorie di sanzioni, quelle amministrative e quelle penali. Le prime sono puntualmente individuate dall'art. 83 GDPR, le seconde sono rimesse alla libera determinazione del legislatore nazionale, come si evince dall'art. 84 GDPR, nella parte in cui stabilisce che "gli Stati membri dell'Unione europea stabiliscono le norme relative alle altre sanzioni per la violazione del presente Regolamento", dove per "altre sanzioni" devono intendersi quelle diverse dalle sanzioni amministrative pecuniarie.

Venendo alle sanzioni amministrative pecuniarie, disciplinate dall'art. 83 GDPR, va notato che il principio generale che regge le stesse si rinviene nell'art. 83, par. 1 a norma del quale: "ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie [...] siano in ogni singolo caso effettive, proporzionate e dissuasive".

Viene dunque precisato che le sanzioni sono inflitte casisticamente, cioè "in funzione delle circostanze di ogni singolo caso" sia in aggiunta che in sostituzione delle sanzioni previste in funzione dell'esercizio del potere correttivo di cui all'art. 58, par. 2, GDPR (1).

(1) Quanto al tipo di sanzione, queste vengono individuate dall'art. 58, par. 2, in relazione ai poteri dell'Autorità di controllo, nelle seguenti tipologie:

- avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possano verosimilmente violare le disposizioni del Regolamento;
- ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del Regolamento;
- ingiunzione al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal Regolamento;
- ingiunzione al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del Regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
- ingiunzione al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imposizione di una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

L'esercizio del potere correttivo da parte dell'Autorità nazionale, per l'Italia il Garante della privacy, dev'essere esercitato secondo i seguenti parametri:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

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

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

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

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

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Nel caso in cui sussistano i criteri per applicare la sanzione amministrativa pecuniaria, il Garante potrà irrogare le seguenti sanzioni:

• nel caso di violazione degli obblighi del titolare o del responsabile del trattamento, nonché degli organismi di certificazione e ancora dell'organismo di controllo: fino a 10.000.000 euro ovvero, solo per le imprese, fino al 2% del fatturato mondiale;

• nel caso di violazione dei principi base del trattamento, dei diritti dell'interessato, delle norme sul trasferimento di dati all'estero, di quelle dettate per specifici trattamenti e ancora nel caso di violazione di ordine o limitazione provvisoria o definitiva: fino a 20.000.000 euro ovvero, solo per le imprese, fino al 4% del fatturato mondiale.

Ogni violazione va trattata singolarmente; tuttavia l'art. 83, par. 3, nella logica del concorso formale con assorbimento della pena, stabilisce che se, in relazione allo stesso trattamento o a trattamenti collegati, sono violate varie disposizioni del GDPR l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

Va notato che anche la disciplina delle sanzioni amministrative pecuniarie si espone alla concorrenza normativa del legislatore nazionale; infatti, l'art. 83, par. 7 stabilisce che "ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte le sanzioni amministrative pecuniarie" aggiungendo poi al par. 9 "laddove lo Stato membro non disponga alcunché, si applicano direttamente le sanzioni di cui all'art. 83 secondo i principi di proporzionalità, effettività e dissuasività".

Autorità competente in materia di trattamento dei dati personali

A dare attuazione alla nuova disciplina è l'autorità garante, per l'Italia il c.d. Garante della privacy, che in passato si è dimostrato molto attento al suo ruolo.

Accertata la violazione di quanto stabilito nel GDPR, il Garante adotta la misura che ritiene più corretta e coerente con la natura e l'entità della violazione, secondo quanto stabilito dalla

- ordine di rettifica, cancellazione di dati personali o limitazione del trattamento e notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;

- revoca della certificazione o ingiunzione all'organismo di certificazione di ritirare la certificazione rilasciata, oppure ingiunzione all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

- ordine di sospendere i flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

normativa europea e nazionale e con attenzione alla natura del Titolare del trattamento.
L'art. 58, par. 2, GDPR indica come il Garante provvede in caso d'inadempienza da parte di un titolare o di un responsabile del trattamento.

Adeguamento dell'apparato sanzionatorio del Codice privacy al GDPR

Il GDPR prevede che gli Stati membri dell'Unione europea adottino prescrizioni o misure aggiuntive proprie, purché risultino compatibili con il testo europeo, che rimane la prima fonte della normativa privacy.
Il D.Lgs. n. 101/2018, in materia di sanzioni svolge proprio questa funzione adeguando il Codice privacy al GDPR; tuttavia, la regolamentazione risulta ancora da definire in modo completo, poiché al Garante è assegnato il compito di verificare i vecchi codici di condotta e le vecchie autorizzazioni, con il fine specifico di sostituirli con le ***regole deontologiche***, cioè provvedimenti generali e specifiche misure di garanzia, aventi natura di "*soft-law*".
Rispetto alle sanzioni il nuovo Codice privacy modifica radicalmente il testo previgente prevedendo l'abrogazione degli artt. 161-165 e riscrivendo l'**art. 166, D.Lgs. n. 196/2003**.
1) Sono soggette alla sanzione amministrativa di cui all'***articolo 83, par. 4 GDPR*** le seguenti violazioni:
- uso di linguaggio non conforme nell'informativa diretta al minore infraquattordicenne;
- inosservanza delle prescrizioni del Garante nel caso di trattamento con rischi elevati per l'esecuzione di un interesse pubblico;
- assenza di chiarezza nella redazione delle cartelle cliniche;
- eccesso di dati nel certificato di assistenza al parto;
- mancata informativa circa la natura e la durata del trattamento dei dati di traffico;
- mancata adozione di misure per bloccare il trasferimento di chiamata automatica;
- mancata individuazione di modalità per la manifestazione del consenso all'inclusione in elenchi;
- mancata adozione di misure tecniche e organizzative adeguate al rischio, di garanzia dell'esclusività dell'accesso e da parte del fornitore di servizi e-mail;
- mancata adozione PIA;
- mancata sottoposizione del programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.
2) Sono soggette alla sanzione amministrativa di cui all'***articolo 83, par. 5 GDPR*** le seguenti violazioni:
- trattamento per esecuzione di un compito d'interesse pubblico non fondato su norma di legge o Regolamento;
- trattamento senza il consenso del minore;
- trattamento di dati particolari necessario per motivi d'interesse pubblico fuori dai casi previsti dall'ordinamento;
- accesso a dati genetici, biometrici e relativi alla salute, consentito a terzi fuori dalle prescritte garanzie di trattamento;
- trattamento di dati relativi a condanne penali e reati fuori dai casi di legge;
- trattamento non autorizzato di dati di persone decedute e loro mancata cancellazione o cancellazione contro volontà dell'interessato;
- indicazione delle generalità delle parti nel caso di diffusione di provvedimenti giudiziari per cui è richiesto l'anonimato;
- trattamento dei dati per fini di tutela della salute in violazione delle disposizioni sull'esenzione del consenso sul trattamento dei dati particolari;
- informativa fornita dal pediatra non chiara o agevolmente comprensibile ovvero non analitica nell'individuazione di rischi specifici;
- mancata annotazione dell'informazione con modalità uniformi da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie;
- mancata affissione di appositi cartelli integrativi dell'informativa nel trattamento d'informazioni operate da altri soggetti;
- ritardata informativa a seguito di trattamento in urgenza per la tutela dell'incolumità;
- ammessa visione della cartella clinica a soggetti terzi, fuori dai limiti di legge;
- rilascio del certificato di assistenza al parto recante il nome della madre fuori dai limiti e dai termini di legge;
- comunicazione o diffusione di risultati di profitto degli studenti per finalità diverse dal collocamento;
- conservazione e trattamento di dati raccolti per finalità di archiviazione o ricerca ma trattati per finalità diverse;

- violazione delle regole deontologiche per trattamenti nell'ambito del rapporto di lavoro (art. 111) e sulle informazioni da rendere in caso di ricezione di curriculum (art. 111-*bis*);
- accesso da parte del patronato a dati per i quali non è stato manifestato il consenso;
- trattamento di dati relativi a sinistri fuori dai casi di legge;
- mancata informativa o trattamento senza consenso dell'utente o contraente nel caso di trattamento d'informazioni archiviate su terminale;
- mancata cancellazione di dati relativi al traffico, o conservazione ai fini della contestazione della fatturazione eccedente i sei mesi, o conservazione oltre i termini senza il consenso dell'interessato o, ancora, accessibilità a terzi dei dati di traffico;
- mancanza di dettagli nella fattura;
- mancanza di misure volte a impedire l'identificazione del chiamante.

Sotto il ***profilo penale***, il capo II del Titolo III vede il totale restyling dell'***art. 167***, con cui sono state introdotte le seguenti fattispecie di reato:

• ***trattamento illecito dei dati***: punisce, 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, arreca nocumento all'interessato in violazione di specifiche disposizioni di legge, nonché chi, al fine di trarre per sé o per altri profitto o 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, arreca nocumento all'interessato;

• ***comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala***: si verifica in caso di comunicazione e diffusione, al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, di un archivio automatizzato o una parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala (2) anche quando lo si fa senza consenso quando questo è richiesto per le operazioni di comunicazione e di diffusione;

• ***acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala***: si verifica quando, al fine di trarne profitto per sé o altri, ovvero di arrecare danno, si acquisiscano con mezzi fraudolenti un archivio automatizzato o una parte sostanziale dello stesso contenente dati personali oggetto di trattamento su larga scala.

• ***falsità nelle dichiarazioni***: la norma sanziona chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi, nonché colui che cagioni intenzionalmente un'interruzione o turbi la regolarità di un procedimento dinanzi al Garante o degli accertamenti da questi svolti.

Va segnalato che non sono state riscritte ma solo inasprite le sanzioni nei casi d'inosservanza dei provvedimenti del Garante.

Il regime transitorio

Il GDPR avendo natura di Regolamento ha diretta applicazione nell'ordinamento e specificamente dal 25 maggio 2018 costituisce norma avente la stessa efficacia della legge.

Il nuovo Codice privacy, tanto atteso, ha acquistato piena efficacia solo il 19 settembre 2018, rendendo difficile il coordinamento tra la disciplina nazionale e quella europea; pertanto in molti hanno richiesto una proroga sull'effettività del regime sanzionatorio.

Evidentemente non era possibile disporre un simile provvedimento; tuttavia, il nuovo Codice privacy dispone un ***periodo di otto mesi*** in cui il Garante eserciterà gradualmente il proprio potere sanzionatorio, nei confronti di aziende che comunque debbono ritenersi ritardatarie, laddove alla data del 25 maggio 2018 non abbiano provveduto alla *compliance*.

Va ricordato che l'Autorità ha programmato un piano di attività ispettive per il secondo semestre, durante il quale le sanzioni saranno certamente irrogate.

(2) Per una definizione v. considerando n. 91 del Regolamento e le Linee guida sui responsabili della protezione dei dati del Gruppo (art. 29).