il Quotidiano Giuridico

IP & IT

GDPR

Il Far West delle sanzioni del GDPR inizia ora (o è già iniziato?)

lunedì 20 maggio 2019

di **Coraggio Giulio** avvocato in Roma, Capo del Settore Technology dello Studio Legale DLA Piper

Oggi, 20 maggio 2019, cessa l'efficacia della norma transitoria di cui all'art. 22 del D.Lgs. n. 101/2019 secondo cui il Garante per la protezione dei dati personali "avrebbe tenuto conto", ai fini dell'applicazione delle sanzioni amministrative previste dal GDPR della fase di loro prima applicazione.

Il **D.Lgs. 101/2019** aveva fatto scalpore tra gli esperti privacy per due ordini di motivi.

Non è chiaro cosa significhi il termine "tenere conto" ai fini del calcolo delle sanzioni della "**prima applicazione delle disposizioni sanzionatorie**" del Regolamento privacy europeo, soprattutto rispetto ad obblighi che in alcuni casi rispecchiano principi già dettati dal D.Lgs. 196/2003, se non addirittura dalla Legge 675/1996.

È come ammettere che la conformità alla normativa **privacy** prima dell'avvento delle sanzioni del **GDPR** non fosse ritenuta importante dalle aziende che ora si rendono conto che devono attivarsi.

Allo stesso modo, il legislatore italiano sembra non aver tenuto conto che il GDPR è un regolamento comunitario e, in quanto tale, non ha bisogno di implementazione, le sue disposizioni hanno applicazione diretta e lo spazio di discrezionalità lasciato agli Stati Membri è limitato a quanto espressamente indicato dal regolamento stesso. Quindi il Garante non ha potuto emettere sanzioni meno elevate rispetto a quanto disposto dal GDPR.

Ad essere sinceri però, anche il garante privacy francese aveva previsto una moratoria di 12 mesi dall'inizio dell'applicabilità del GDPR ai fini dell'applicazione delle sanzioni. Tuttavia, sappiamo poi come è andata. La sanzione di € 50 milioni emessa dal CNIL contro Google è di gran lunga la più alta sanzione per la violazione della normativa privacy mai adottata. Potrebbe essere addirittura superata però dalle sanzioni che, sulla base delle ultime indiscrezioni, è probabile che siano emesse contro **Facebook** in relazione agli eventi collegati allo scandalo di **Cambridge Analytica**.

Con la disposizione sopra richiamata, sembrava che il legislatore italiano avesse inviato le aziende a "provare" ad essere conformi al GDPR in questi primi mesi. Ma mi viene in mente una famosa citazione da Star Wars del maestro Yoda,

"Provare no! Fare o non fare non c'è provare!".

L'approccio delle aziende italiane in molti casi è stato di "provare" a fare quanto richiesto dal GDPR e di avere un piano di messa in conformità con il GDPR. Tutto ciò è avvenuto principalmente nei mesi precedenti al 25 maggio 2018, con livelli di tensione che sono notevolmente aumentati nei giorni immediatamente precedenti alla scadenza.

Le aziende italiane sono pronte alle sanzioni del GDPR?
Quello che è sorprendentemente accaduto successivamente al **25 maggio 2018** è stata una notevole riduzione del livello di priorità riconosciuto dalle **aziende** alla necessità di conformarsi

al GDPR. Alcune aziende avevano previsto investimenti milionari nel 2018 nel loro programma privacy per poi non allocare quasi alcun importo nel 2019. Come se gli adempimenti richiesti dal regolamento privacy si riducessero a delle procedure e misure tecniche che, una volta adottate, mettono in sicurezza l'azienda per sempre!

Ma lo scenario che abbiamo riscontrato in alcuni casi, è stato che le aziende avevano adottato informative sul trattamento dei dati personali, registri del trattamento e procedure prima del 25 maggio, ma queste non riflettevano in alcun modo l'operatività dell'azienda. Queste misure erano state adottate prima della scadenza, unicamente perché il management aveva scoperto la rilevanza della compliance privacy durante quei giorni in cui la notizia dell'avvenuto di questa nuova normativa era su tutti i giornali. Tuttavia, successivamente altre priorità erano diventate più rilevanti e la situazione di "mera facciata" sopra indicata, era rimasta.

L'inizio delle nuove ispezioni del Garante Privacy

Un primo segnale di allarme l'ha dato il **Garante** per il trattamento dei dati personali che **negli ultimi mesi ha ricominciato le proprie ispezioni con l'ausilio della Guardia di Finanza**. La particolarità che abbiamo riscontrato nelle ispezioni post 25 maggio è data dal livello di dettaglio delle richieste indirizzate alle aziende.

Ci sono infinite liste di informazioni che vengono richieste e soprattutto che vengono verificate dal Garante, anche accedendo ai sistemi informatici delle aziende per verificare la corrispondenza tra quanto indicato nella documentazione e lo stato di fatto.

Le aziende spesso non sono preparate a queste misure. Ciò vale per assurdo sempre più spesso nelle multinazionali che hanno adottato dei programmi di messa in conformità con il regolamento privacy molto complessi. Tuttavia, hanno poi deciso che una localizzazione basata sul trattamento dei dati personali effettivamente svolto dalla società italiana, sull'approccio del garante locale e sulle disposizioni di integrazione del GDPR applicabili fosse eccessivamente onerosa per il gruppo.

La soluzione è stata in molti casi di adottare le medesime procedure, informative, misure organizzative e di sicurezza e adempimenti per tutte le società del gruppo, con registri del trattamento dotati di un livello di tailorizzazione molto limitato. Tutta questa documentazione spesso contiene indicazioni di mero principio che difficilmente possono essere lette come istruzioni specifiche agli incaricati del trattamento. Allo stesso modo, in alcuni casi i documenti non vengono tradotti in italiano, aggiungendo un'ulteriore complicazione perché il Garante valuta solo documenti in italiano.

Quanto sopra indicato avviene spesso in un contesto dove si individua un unico DPO di gruppo a livello globale che è difficilmente accessibile, non ha una conoscenza approfondita della realtà locale, non può essere presente in caso di ispezioni e nella maggior parte dei casi non parla italiano.

Queste circostanze sono considerate negativamente dal Garante nell'ambito di un'ispezione e inevitabilmente aumentano il rischio di subire una sanzione. Tale rischio viene ulteriormente aumentato dal fatto che le aziende non sono a volte pronte per gestire un'ispezione. Le procedure per la gestione delle indagini fiscali o i c.d. dawn raid in materia di antitrust sono molto comuni. Tuttavia, non molte società li hanno adottati con riferimento alle ispezioni privacy.

La sanzione emessa dal Garante ai sensi del GDPR

L'unica sanzione ad oggi emessa dal Garante ai sensi del GDPR è stata pari a **€ 50.000 contro l'Associazione Rousseau** per la mancata adozione delle misure di sicurezza richieste dal Garante, successivamente al verificarsi del **data breach** relativo ai siti web connessi al Movimento 5 Stelle nell'estate del 2017.

Questa decisione è interessante per due motivi.

In primis, è stata emessa dal Garante contro un responsabile del trattamento, invece che il titolare del trattamento. Si tratta di un elemento di novità introdotto dal regolamento privacy europeo. Non è più solo il titolare del trattamento che è responsabile per la conformità con gli obblighi relativi alla disciplina di trattamento dei dati personali.

I fornitori di servizi non sono più "protetti" dal proprio cliente rispetto alle possibili sanzioni. Se si dimostra che l'applicazione della sanzione era conseguenza del loro comportamento scorretto o in violazione del GDPR, possono essere direttamente sanzionati dal Garante.

Ciò non vuol dire però che il titolare del trattamento è esentato dal controllare la conformità alla normativa privacy dei propri responsabili del trattamento. Al contrario, si tratta di un obbligo espressamente previsto dal GDPR che, in caso di mancata osservanza, può dar vita ad una sanzione anche a carico del titolare del trattamento per la condotta dei suoi responsabili del trattamento.

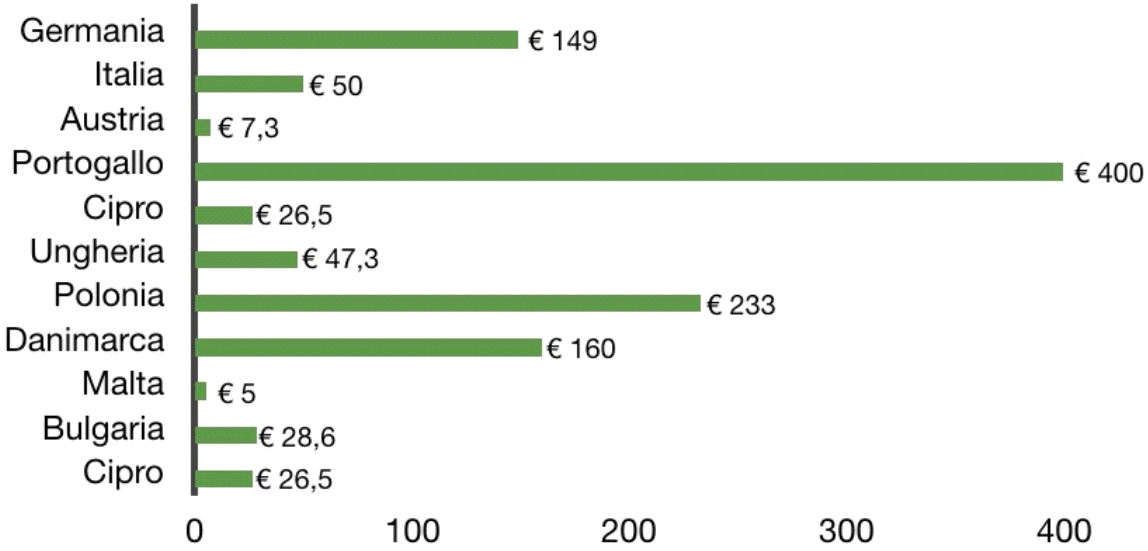
I criteri di calcolo delle sanzioni previste dal GDPR
Un secondo elemento interessante della decisione adottata contro l'Associazione Rousseau riguarda anche l'importo della sanzione. Il Garante non fornisce molte indicazioni sui **criteri seguiti per il calcolo dell'importo**. E ciò rappresenta proprio uno degli elementi di incertezza del GDPR che

· non dispone un importo minimo delle sanzioni;
· prevede solo un massimo con l'unica variante che le sanzioni possono essere fino a € 10 milioni o € 20 milioni, o per le imprese, fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente; e
· detta criteri per il calcolo delle sanzioni molto ampi.
Il Garante infatti deve tener conto dei **seguenti elementi**:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a 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;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati o ai meccanismi di certificazione approvati ai sensi del GDPR e
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.
Tutti questi elementi lasciano un **elevato livello di discrezionalità al Garante nel calcolo della sanzione**, con l'aggravante che – dato il recente inizio dell'applicabilità del GDPR – non ci sono numerose precedenti decisioni (neanche dei garanti stranieri) da utilizzare come benchmark di riferimento.

Vista l'affinità della tipologia di sanzione, è probabile che il Garante terrà conto di alcuni criteri sviluppati negli anni dalle autorità antitrust. Tuttavia, anche alla luce dell'ampissima "forbice" relativa all'importo della possibile sanzione, è probabile che qualsiasi sanzione di importo non irrisorio sfocerà in lunghi contenziosi. A conferma di ciò, Google ha già annunciato che farà ricorso contro la sanzione di € 50 milioni contro emessa dal CNIL.

Quanto è elevato il rischio delle sanzioni privacy?
Lo studio **DLA Piper** sta monitorando le sanzioni che sono state emesse dai Garanti europei nelle principali giurisdizioni. Nel grafico di seguito, non ho inserito la sanzione di € 50 milioni emessa dal CNIL perché ha un importo notevolmente superiore rispetto alle altre sanzioni e avrebbe reso l'immagine illeggibile.



In relazione a ciascun paese è indicato il valore complessivo delle sanzioni emesse ai sensi del GDPR in migliaia di euro. Non si tiene conto della sanzione di € 50 milioni emessa dal CNIL nei confronti di Google.

Da questi dati emerge che tutti i garanti privacy europei hanno emesso sanzioni di importo notevolmente inferiore rispetto al CNIL. La seconda maggiore sanzione è stata emessa dal garante portoghese che in un solo procedimento ha emesso una sanzione di € 400 mila contro un ospedale per accesso abusivo ai dati di pazienti. Ma i garanti tedeschi sono stati i più attivi con 21 procedimenti conclusi in relazione a contestazioni sorte successivamente al 25 maggio 2019.

Non è chiaro se questi dati devono essere di conforto per le società. Non è possibile garantire che questo approccio “light” sarà confermato nei prossimi mesi. Ma è certamente vero che il ”far west” del GDPR è solo agli inizi.