

Gli effetti del regolamento Ue 2016/679: manca la determinazione dell'importo minimo

Dati, sanzioni senza sfumature

Non sono previste distinzioni tra violazioni gravi o lievi

Pagina a cura
di ANTONIO CICCIA
MESSINA

Il regolamento Ue 2016/679 sulla protezione dei dati dispone sanzioni amministrative per punire le violazioni di molti precetti del regolamento medesimo. L'apparato sanzionatorio ha il fulcro nell'articolo 83, che prevede due fasce di massimi edittali, senza indicazione di minimi edittali. In estrema sintesi ci sono due gruppi di sanzioni: il primo relativo alle violazioni degli adempimenti e degli obblighi; il secondo relativo alle violazioni di principi e diritti. I due massimi edittali sono decisamente elevati: 10 milioni di euro (o in alternativa 2% del fatturato totale mondiale annuo) e 20 milioni di euro (in alternativa 4% del fatturato totale mondiale annuo).

Il sistema regolamentare comprende le norme sulla graduazione della sanzione in concreto, l'istituzione di un casellario degli autori delle violazioni e il rinvio al legislatore nazionale per l'adozione di norme di coordinamento. Sempre sul piano della descrizione della normativa, si consideri che vi è un numero molto copioso di violazioni livellate nella sanzione massima, ma senza una differenziazione e una distinzione, nella fattispecie astratta, tra violazioni formali e violazioni sostanziali, tra violazioni lievi e gravi. Dal piano della descrizione si deve passare al piano della valutazione orientata all'applicazione.

All'approssimarsi del 25 maggio 2018, data a decorrere della quale cominceranno ad applicarsi le disposizioni del regolamento, tra cui il citato articolo 83, si impongono alcune riflessioni.

La questione parte da una considerazione di fatto e cioè l'assenza di determinazione del minimo edittale. In materia si deve dare almeno uno sguardo alla legge 689/1981, legge quadro sulle sanzioni amministrative pecuniarie, la quale dedica l'articolo 10 alla quantificazione dell'importo e al rapporto tra limite minimo e limite massimo. Nel dettaglio l'articolo 10 citato fissa al primo comma l'ambito edittale generale: la sanzione amministrativa pecuniaria consiste nel pagamento di una somma non inferiore a 10 euro e non superiore a 15 mila euro.

Il medesimo articolo 10 aggiunge che le sanzioni proporzionali non hanno limite massimo. La disposizione in esame chiude dichiarando che fuori dei casi espressamente stabiliti dalla legge, il limite massimo della sanzione amministrativa pecuniaria non può, per ciascuna violazione, superare il decuplo del mini-

Le sanzioni	
VIOLAZIONI IN MATERIA DI...	SANZIONE
registro trattamenti	Fino 10 mln/oppure se più elevato fino 2% fatturato totale mondiale annuo
documento valutazione dei rischi	
documento di valutazione di impatto privacy	
procedure data breach	
accordo con contitolari	
contratto di responsabile esterno	
contratto con sub-responsabili	
nomine rappresentante nella Ue	
istruzioni agli autorizzati	
consultazione preventiva	
nomina e attività responsabile della protezione dei dati	
obblighi di enti di certificazione	
obblighi dell'ente di controllo sui codici di condotta	
principi del trattamento	Fino 20 mln/oppure se più elevato fino 4% fatturato totale mondiale annuo
condizioni di liceità del trattamento	
disciplina del consenso	
diritto di trasparenza e informative	
diritto di accesso	
diritto di rettifica	
diritto alla cancellazione dei dati	
diritto alla limitazione del trattamento	
diritti relativi alla portabilità dei dati	
diritto di opposizione al trattamento	
diritti relativi alle decisioni automatizzate e alla profilazione	
disciplina dei trasferimenti dati estero	
inosservanza ordini dell'autorità di controllo	
inosservanza obblighi previsti dal leggi nazionali in settori specifici	

Federprivacy fissa i punti cardine

Nomina Dpo, revisione consensi, valutazione di impatto privacy, procedure data breach, contratti con i responsabili esterni, diritti degli interessati: sono i sei punti fermi che enti pubblici e aziende private devono curare con priorità per attuare il regolamento Ue sulla privacy n. 2016/679. A illustrarli è la circolare n. 1/2018 di Federprivacy, che analizza i problemi della transizione dal Codice della privacy al Regolamento Ue, operativo dal 25 maggio 2018. Ecco alcuni chiarimenti:

Principi. I consensi raccolti anteriormente al 25/5/2018 legittimano le operazioni di trattamento a decorrere da quella data, ma solo se le modalità di acquisizione del con-

senso risultano conformi alle prescrizioni del Regolamento fin dall'inizio o in virtù di integrazione/modifica anteriore al 25/5.

Valutazione. Se le operazioni di trattamento presentano un rischio elevato e se sono conformi a un provvedimento di verifica preliminare del Garante della privacy (art. 17 Codice della privacy), non è necessario redigere entro il 25/5/2018 la Valutazione di impatto privacy.

Responsabili esterni. A decorrere dal 25/5/2018 la disciplina, contrattuale o con atto equivalente tra titolari del trattamento e responsabili esterni, deve essere conforme all'art. 28 del regolamento Ue.

— © Riproduzione riservata —

mo. La norma è inserita in una legge ordinaria ed è pertanto derogabile da legge o atto forza di legge successivo. La norma è, comunque, significativa per il fatto di stabilire, senza vincoli per il legislatore, un'unità di misura del rapporto tra minimo e massimo.

Rammentando quanto sopra è di evidenza che nel regolamento Ue ogni singola violazione prevede una forbice amplissima e che l'unica graduazione sta nelle singole decisioni dell'Autorità garante.

Vi è da chiedersi se questo stato della legislazione comporti qualche criticità. La ri-

sposta è affermativa, e questo senza dubbio almeno sul piano dei principi di proporzionalità delle sanzioni. Si consideri un esempio degli innumerevoli che si potrebbero fare. Si prenda un articolo del regolamento Ue, per esempio l'articolo 12, e si verifichino tutte le condotte esposte a sanzione amministrativa pecuniaria.

Espongono al medesimo trattamento sanzionatorio, fino a 20 milioni o fino al 4% del fatturato, sia: 1) violazioni formali, come il ritardo di un giorno nel dare le dovute comunicazioni all'interessato; l'omissione di avvisi ripetitivi

di norme di regolamento; sia 2) violazioni sostanziali, come la compromissione del diritto alla trasparenza, formulate in termini vaghi (usare misure «appropriate», rifiutare istanze «manifestamente infondate»).

Tutto l'articolo 12 è, poi, scomponibile in innumerevoli violazioni, contestabili separatamente: per esempio il titolare del trattamento effettua comunicazioni trasparenti, intelligibili e facilmente accessibili, con un linguaggio chiaro (specie se destinate a minori), ma non concise, oppure concise, ma con un linguaggio non chiaro. L'analisi proposta per

l'articolo 12 è riproponibile per tutte le norme richiamate dai paragrafi 4 e 5 dell'articolo 83 del Regolamento 2016/679.

Il problema, dunque, è sia compatibile una situazione normativa in cui sostanzialmente qualunque violazione sia suscettibile di: a) nessuna sanzione (si ricordi la possibilità alternativa dell'ammonizione rispetto alla sanzione pecuniaria amministrativa); b) di sanzione di un euro; c) o di una sanzione di 20 milioni di euro o di cifra superiore calcolata in percentuale.

Il problema è se tutto ciò sia coerente con i principi e le prescrizioni previste: a) dall'articolo 23 della Costituzione: «Nessuna prestazione personale o patrimoniale può essere imposta se non in base alla legge»; b) dall'articolo 3 della Costituzione, ovvero principio di uguaglianza formale e sostanziale; c) dall'articolo 1 della legge 689/1981: «Nessuno può essere assoggettato a sanzioni amministrative se non in forza di una legge che sia entrata in vigore prima della commissione della violazione».

In effetti una forbice così ampia (da zero a 20 milioni di euro o cifra superiore calcolata in percentuale) rimette, sempre e costantemente, la determinazione della sanzione all'Autorità amministrativa di controllo e successivamente al giudice.

La dilatazione gassosa della forbice sanzionatoria unita all'affidamento della sanzione stessa alla determinazione in concreto dell'autorità amministrativa svela l'irragionevolezza della norma sanzionatrice: a livello normativo abbiamo un'unica misura sanzionatoria, che si risolve in una applicazione generalizzata non aderente alla specificità delle singole condotte e determina una ingiustificata discriminazione tra soggetti. È sufficiente, a tacitare l'ansia del rispetto del principio di legalità e del principio di riserva assoluta di legge sulle sanzioni, il fatto che l'autorità amministrativa competente possa modulare l'irrogazione della sanzione a seconda della valenza degli elementi oggettivi e soggettivi delle fattispecie? In questo quadro si inserisce l'articolo 13 della legge 163/2017, che, non a caso, ha delegato il governo ad «adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (Ue) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse». La strada legislativa, tra l'altro, appare l'unica coerente.

— © Riproduzione riservata —