PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3701 di giovedì 21 gennaio 2016

Nuovo regolamento generale europeo sulla protezione dei dati

Anticipazioni sul documento che verrà ufficialmente pubblicato in Gazzetta Ufficiale della Unione Europea presumibilmente tra marzo e aprile. Di Adalberto Biasiotti.

Mi è gradito ricordare a tutti i lettori che questo nuovo regolamento generale, che verrà applicato con minime varianti in tutta l'unione europea, ha fatto scomparire del tutto la parola "privacy". È bene che sin da adesso ci abituiamo a non utilizzare più questa parola, che spesso è causa di confusione e non di chiarezza.
Ciò premesso, andiamo a esaminare questo regolamento, di cui non esiste ancora la traduzione in italiano, ma che per molti aspetti può essere recuperata da una precedente traduzione, messa a disposizione durante la lunga e sofferta fase di elaborazione del testo.

Il documento si compone di ben 139 "considerando", vale a dire una serie articolata di premesse, che servono a inquadrare i motivi per cui i successivi articoli sono stati elaborati.
Indi il documento è articolato in 11 capitoli, alcune di quali sono dotati di sezioni.

Il capitolo primo dà indicazioni generali sulle finalità del regolamento, gli obiettivi, l'ambito territoriale e, molto importante, da tutta una serie di definizioni che speriamo vengano tradotte in italiano in modo comprensibile, evitando alcune clamorose confusioni, che erano presenti nella precedente traduzione.
Mi auguro caldamente che il nostro Garante possa influenzare i traduttori europei, in modo da evitare che un responsabile del trattamento diventi un incaricato!

Il secondo capitolo è dedicato alla illustrazione di principi generali di trattamento, che in linea di massima non sono molto diversi da quanto già era stato precedentemente definito. Vengono inserite alcune indicazioni particolari sul trattamento di dati di minori, cioè soggetti che hanno meno di 13 anni, e vengono date indicazioni in merito al trattamento di dati che vengono classificati con l'espressione "pseudo anonimi".

Molto più interessante è **il terzo capitolo**, dove vengono illustrati in dettaglio i diritti degli interessati. Questo capitolo è stato ampliato in modo significativo, anche rispetto al nostro decreto legislativo 196/2003, perché nelle cinque sezioni, in cui esso è articolato, vengono presi in esame in grande dettaglio tutti gli aspetti di questi diritti. Una innovativa prescrizione riguarda l'utilizzo di una informativa iconica, che deve essere uguale in tutta l'unione europea e che tende a superare i problemi posti dalle troppe lingue europee, nelle quali la informativa viene offerta, girando per vari paesi. Per dir la verità, non sempre questa informativa iconica è di immediata comprensione ma dopo poco sono convinto che tutti gli interessati, vale a dire 300.000.000 di europei, potranno capirla facilmente.

Viene illustrato in dettaglio il modo in cui è possibile esercitare il diritto di accesso. Ampio spazio viene dato al diritto di rettifica e cancellazione, anche alla luce delle recenti sentenze della corte di giustizia europea, che ha ampliato in maniera significativa i diritti alla cancellazione dell'interessato. Un'altra sezione che prima non esisteva riguarda il diritto all'obiezione e soprattutto alle modalità con cui, se consentita, è possibile sviluppare la profilazione. Sappiamo tutti che oggi i grandi motori di ricerca adottano tecniche di profilazione sempre più sofisticate, in modo da colpire il bersaglio di un eventuale messaggio

pubblicitario. Ancora una volta, vengono messe in evidenza alcune limitazioni ai diritti degli interessati, che non possono evidentemente opporsi a trattamenti legati all'applicazione di tasse, indagini criminali e via di seguito.

Il quarto capitolo è oltremodo importante perché individua i soggetti che sono preposti al trattamento dei dati. Il data controller equivale al nostro titolare ed il data processor equivale al responsabile del trattamento di dati personali.

Questo capitolo è particolarmente importante perché comincia a mettere in evidenza alcuni strumenti, che occorre utilizzare, prima durante e dopo l'avvio di un processo di trattamento di dati personali. Il primo strumento viene chiamato **data protection by design**, il secondo viene chiamato **data protection by default**. Sono preziosi strumenti di analisi del trattamento, che vengono integrati successivamente da altri strumenti.
Viene anche meglio evidenziata la figura del contitolare, che in Italia era stato introdotto un poco tardivamente.

Un fatto oltremodo sorprendente è legato alla scomparsa dell'incaricato del trattamento di dati personali, secondo la formulazione italiana, che perde questo nome e non ne assume alcun altro! Ovviamente esisteranno decine di migliaia di persone fisiche che tratteranno dati personali, su indicazione di data controller e data processor, ma questi soggetti sono senza nome ed ecco perché io li ho battezzati **data handler ex articolo 27**, che è l'unico punto nel quale si fà riferimento a questi soggetti.

Vengono illustrate le modalità con cui deve essere documentata la modalità di trattamento e la piena disponibilità a cooperare con il garante nazionale. La seconda sezione è tutta dedicata alla sicurezza dei dati, che richiede la introduzione di misure, proporzionate ai rischi. Ampio spazio è dedicato al **data breach**, ossia alla violazione dei dati, con indicazioni di quando e come bisogna informare il garante coinvolto ed eventuali interessati, anch'essi coinvolti.
Tutta la terza sezione è dedicata alla illustrazione di come devono essere protetti i dati per l'intero loro ciclo di vita. Viene qui illustrato un altro aspetto fondamentale di sicurezza, che raccomanda di condurre una **analisi di rischio di trattamento**, per alcune particolari categorie di trattamento. Questa analisi di rischio deve essere revisionata almeno una volta all'anno e sulla base di essa deve essere sviluppato un quarto strumento di valutazione e protezione, vale a dire il **data protection impact assessment**. Quest'ultimo deve essere aggiornato ogni due anni. Si passa infine ad illustrare i casi in cui è richiesta una **consultazione preventiva** con il garante, prima di avviare o addirittura impostare una trattamento di dati che potrebbero avere aspetti critici.

Nella quarta sezione viene illustrato un nuovo personaggio, mai conosciuto in precedenza, il data protection officer. Questo soggetto merita estrema attenzione perché la sua designazione è obbligatoria per tutti gli enti pubblici e per tutti i titolari che trattino dati di più di 5000 interessati, nonché i titolari che sviluppino attività rischiose di trattamento. È bene ricordare ai lettori che questo personaggio esiste già da molti anni nell'ambito delle istituzioni europee e quindi avremo molto da imparare dall'esperienza già maturata, per trasferirla in un contesto nazionale.

Si tratta di un soggetto che evidentemente può dare molto fastidio all'interno di un'azienda ed ecco la ragione per la quale il regolamento si preoccupa di proteggerlo in tutti i modi possibili, ad esempio garantendo una durata minima del contratto, nonché l'attribuzione di risorse adeguate per svolgere la propria funzione. Si tratta di un professionista di elevato livello, che conosce a fondo i problemi tecnici e legali, legati al trattamento di dati personali, e che opera in piena autonomia, con la possibilità di "fare la spia" all'autorità garante, se le sue indicazioni non vengano rispettate dal data controller o data processor.

La quinta sezione dedicata alla illustrazione di **codici di condotta**, di cui in Italia abbiamo già avuto una buona esperienza, ad esempio con il codice di comportamento per i giornalisti o per le ricerche storiche.
Del tutto innovativa è invece la disposizione del regolamento che permette ai garanti nazionali di rilasciare delle patenti di buon livello di protezione al trattamento dei dati. La disponibilità di queste patenti, che vengono chiamate **European data protection seals**, attenua, ad esempio, le sanzioni che potrebbero essere applicate in caso di violazione delle norme.
Poiché le autorità nazionali difficilmente dispongono di risorse sufficienti per gestire questa attività, esse possono stipulare degli accordi con società esterne, che vengono accreditate dalle autorità nazionali. Mi piace ricordare che questo schema non è dissimile da quello che attualmente ha scelto il ministero dell'interno, per verificare la qualità delle prestazioni che vengono offerte dagli istituti di vigilanza privata. Il ministero ha riconosciuto un certo numero di enti di certificazione terzi, accettando le valutazioni che essi rilasciano.

Il capitolo quinto è interamente destinato alle modalità con cui è possibile trasferire dati in paesi terzi e le modalità con cui organismi internazionali, come ad esempio l'Unesco, potrebbero trattare dati personali.
Credo sia superfluo ricordare ai lettori i problemi che sono nati quando la corte di giustizia europea ha dichiarato che l'accordo

Safe harbor, che consentiva appunto questo trasferimento tra Europa e Stati Uniti, non era soddisfacente.
Come già avviene oggi, la commissione europea può riconoscere un certo numero di paesi, la cui legislazione in tema di protezione dati personali è accettabile, verso i quali quindi il trasferimento è libero. Oggi ciò vale ad esempio per Hong Kong, Nuova Zelanda e altri. Per altri paesi invece è possibile stabilire le famose **binding corporate rules**, che sono una sorta di protocollo di sicurezza, che deve governare lo scambio di dati tra paesi europei e altre nazioni. È anche possibile adottare delle **clausole di salvaguardia**, individuate dal data controller e data processor, che devono però essere validate dall'autorità garante nazionale.
Ho già menzionati in precedenza lo European data protection seal, che può essere tenuto come riferimento per un ulteriore modalità di trasmissione sicura di dati in un paese terzo.
Vengono poi poste alcune limitazioni alla comunicazione di dati, che potrebbero essere imposti dalla magistratura inquirente o giudicante di questi paesi terzi.

Tutto il capitolo sesto è dedicato alla illustrazione del ruolo e delle funzioni delle autorità nazionali di supervisione, come ad esempio il nostro garante. Queste autorità devono essere indipendenti, imparziali, dotate di adeguate risorse e vengono date in indicazioni su come scegliere i componenti di queste autorità. La sezione seconda illustra i doveri e i compiti delle autorità che, in linea di massima, non sono molto diverse da quelle attualmente in vigore, salvo la nuova possibilità di certificare i trattamenti presentati dai data controller o data processor.
È esplicitamente imposto il vincolo che la gestione dei reclami degli interessati debba essere fatta gratuitamente, salvo casi affatto particolari.

Il settimo capitolo è dedicato alla cooperazione e coerenza delle attività svolte dai vari garanti nazionali. L'opera di vigilanza sull'attività di queste garanti, che hanno un certo margine di discrezionalità, anche se normalmente inferiore rispetto a quello oggi in vigore, è affidata allo **European data protection board**. Sempre nell'ottica di evitare fughe in varie direzioni delle varie autorità garanti, il principio di coerenza delle eventuali disposizioni emanate diventa fondamentale.
Il capitolo si conclude con una illustrazione del ruolo e delle funzioni dell'European data protection board, di cui fa parte il rappresentante di ogni autorità garante e lo **European the data protection supervisor**.

Il capitolo ottavo è dedicato alla illustrazione dei rimedi, responsabilità e sanzioni, illustrando la differenza fra il procedimento di tutela amministrativa e quello di tutela giudiziaria, come già avviene oggi in Italia. Assai interessante è il fatto che, in caso di applicazione di sanzioni, vi è una responsabilità solidale del data controller e data processor, che sono quindi intimamente coinvolti nella trattamento dei dati, salvo diverse pattuizioni contrattuali, che dovrebbero essere ben evidenziate.
I vari paesi hanno libertà di stabilire sanzioni amministrative efficaci, proporzionate e dissuasive, che non è detto siano esclusivamente economiche. Ad esempio una sanzione applicabile potrebbe essere quella di sottoporre una azienda birichina ad un audit regolare, ad esempio a scadenza ogni anno. Ben più drammatiche sono le sanzioni economiche, indicate nel regolamento, che possono giungere sino a 100.000.000 di euro oppure al cinque % del fatturato dell'azienda; come se non bastasse, la Commissione può deliberare in futuro di aumentare questi limiti. Sono cifre spaventose, ma l'esperienza ha dimostrato come una pesante sanzione sia uno strumento di educazione estremamente efficace. La prova si ha in Italia, laddove i gestori telefonici, che ripetutamente vengono sanzionati dal garante, non cambiano per niente i loro comportamenti. Si vede che certi comportamenti portano profitti assai più alti di quanto non possa essere la sanzione relativa.

Il capitolo nono indica disposizioni afferenti a specifiche attività di trattamento e illustra in particolare alcune peculiarità del trattamento applicabili ai dati sanitari, ai dati personali dei dipendenti, a dati legati alla sicurezza sociale, a dati trattati per finalità scientifiche e per i servizi di archivio. Un articolo è dedicato specificamente ai problemi di trattamento di dati religiosi.

Il decimo capitolo, che illustri i decreti delegati attuativi, ricorda che è possibile elaborare dei formati standardizzati per dare attuazione alle disposizioni del regolamento e l'esempio più evidente, come accennato in precedenza è quello del formato standard di informativa.

Il capitolo undicesimo, che fa riferimento alle disposizioni finali, indica i precedenti testi legislativi o direttive che vengono superati da questo regolamento.

In Annesso1 la presentazione iconica della informativa, che mi auguro tutti vorranno studiare attentamente e che potrebbe essere già applicata fin da oggi, per chi ha voglia di cavalcare la tigre.

Adalberto Biasiotti

Leggi anche " Le nuove icone della privacy"

---

www.puntosicuro.it