PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4425 di Mercoledì 13 marzo 2019

Codici di condotta ed enti di monitoraggio nel GDPR

Gli articoli 40 e 41 del regolamento generale europeo sulla protezione dei dati fanno riferimento allo sviluppo di codici di condotta e all'introduzione di enti di monitoraggio. Un'iniziativa cerca di dare pratica attuazione a queste indicazioni.

Il regolamento generale europeo non solo dà precise indicazioni sui comportamenti che devono tenere i titolari e responsabili, ma offre anche dei preziosi ausili, sotto forma della elaborazione di codici di condotta, che possono aiutare gli stessi titolari e responsabili a rispettare puntualmente le disposizioni del regolamento. Anche se la responsabilità finale, in tema di scelta delle misure di protezione dei dati, compete al titolare, il regolamento prevede esplicitamente una riduzione di responsabilità, in caso di violazioni delle regole, ove il titolare possa dimostrare di aver effettuato il trattamento in conformità a codici di condotta, debitamente approvati e monitorati.

I lettori certo ricordano che la situazione non è molto diversa da quella esistente in Italia fino a poco tempo fa. L'autorità Garante nazionale aveva pubblicato dei codici di condotta per i giornalisti, per gli investigatori privati e per altri soggetti, che dovevano trattare con particolare cautela i dati personali, di cui venivano in possesso nel corso della loro attività professionale. Questi codici di condotta erano stati elaborati congiuntamente da rappresentanti di associazioni di categoria ed infine approvati e pubblicati dall'autorità Garante. Mancava tuttavia un aspetto fondamentale, per completare il cerchio della sicurezza, che discende dal fatto che non erano stati individuati i soggetti che potessero monitorare la corretta applicazione di questi codici. Se pertanto un titolare, in buona o cattiva fede, violava questi codici, era l'autorità Garante ad intervenire a posteriori.

L'impostazione data dal nuovo regolamento invece è completamente diversa, in quanto non solo dà indicazioni precise sulle modalità con cui devono essere sviluppati i codici di condotta, ma introduce anche la figura di organismi accreditati, che possono effettuare il monitoraggio del rispetto di questi codici.

In altre parole, siamo quasi davanti a un sistema di certificazione, in cui una azienda dichiara di rispettare determinate norme, nella fornitura di beni e servizi, ed un ente terzo di certificazione, debitamente accreditato dall'Istituto Nazionale Accredia, rilascia una certificazione iniziale e le certificazioni successive, circa il rispetto di quanto l'azienda ha dichiarato.

Ci troviamo davanti evidentemente ad una situazione assai più garantistica, rispetto a quella precedente, in quanto un titolare non solo dispone di strumenti oggettivi che gli permettano di trattare dati nel pieno rispetto di leggi e regolamenti, ma dispone anche di un ente terzo, che tiene sotto controllo le sue attività di trattamento e ne certifica la correttezza.

Il problema nasce nel momento in cui si si devono stabilire, a livello europeo, le modalità con cui sviluppare un codice di condotta e successivamente le modalità con cui si deve individuare l'organismo di certificazione, impartendo istruzioni sulle modalità con cui questo organismo deve svolgere la sua attività di monitoraggio.

Per questa ragione il comitato europeo per la protezione dei dati, organo di coordinamento europeo delle attività di trattamento, ha pubblicato una linea guida, sulla quale si richiedono le valutazioni di tutti i soggetti interessati.

Il titolo della linea guida è il seguente:

Guidelines1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

Adopted on 12 February 2019

L'obiettivo di questa linea guida è quello di dare preziose indicazioni sulle modalità con cui è possibile rispettare ed attuare i dettati degli articoli 40 e 41 del regolamento europeo, con modalità omogenee a livello europeo. Si confida così che sarà possibile allineare il livello di protezione dei dati nei vari paesi, armonizzando le difformità oggi esistenti, ad esempio ai codici di condotta per i giornalisti, applicati nel Regno Unito, rispetto ai codici applicati in Italia.

Da notare che il tema viene trattato non soltanto negli articoli menzionati, ma anche in una serie di *considerando*, ad esempio i numeri 77,81,98,99,148,168 ed altri articoli.

L'importanza di queste linee guida è sottolineata dal fatto che esse permettono al titolare di trattare dati personali in vari paesi europei, nella certezza di adottare misure omogenee di protezione.

L'obiettivo di queste linee guida è quello di chiarire le procedure e le regole che si devono seguire nella impostazione, nell'approvazione e nella pubblicazione di codici di condotta, validi sia a livello nazionale, sia a livello europeo.

Inoltre queste linee guida indicano i criteri minimi che devono essere richiesti da un Garante nazionale, prima di avviare il riesame e la valutazione finale sul codice, proposto, ad esempio, dalle associazioni di categoria. Dando indicazioni sulle modalità con cui deve essere condotta la valutazione di correttezza di un codice, si offrono anche indicazioni ad enti terzi, che potrebbero essere autorizzati ad effettuare il monitoraggio iniziale e susseguente circa la attuazione del codice in questione.

È ben vero che la nostra autorità Garante ha già indicato Accredia come l'organismo di accreditamento degli enti di certificazione, che presto o tardi verranno coinvolti, ma è anche vero che questi organi di certificazione devono operare secondo linee guida non solo accurate, ma anche omogenee in tutta Europa. Queste linee guida inoltre mettono in guardia i lettori circa il fatto che un codice di condotta approvato potrebbe anche essere elemento garantistico, se i dati devono essere trasferiti fuori dell'unione europea, ma per questo tema verranno sviluppate successive linee guida.

Infine, le linee guida analizzano in profondità i criteri di accreditamento, facendo presente che l'accreditamento di un ente di certificazione si applica solo a uno specifico codice, sulla base di un'approvazione dell'autorità Garante nazionale. Ciò significa che se un ente di certificazione desidera assumere questo ruolo in relazione a più codici, dovrà ottenere una autorizzazione specifica, per singolo codice, dall'autorità Garante nazionale.

Poiché il comitato europeo per la protezione dei dati è aperto a suggerimenti e commenti su queste linee guida, le metto a disposizione dei lettori per un eventuale intervento su di esse.

Adalberto Biasiotti

---

www.puntosicuro.it