UNIVERSITÀ DEGLI STUDI DI BOLOGNA

Cybersecurity e Data Protection

Sicurezza informatica, norme e leggi della strategia europea

Giovedì 11 maggio 2017

Relatore: Mariano Angioni

NUOVE REGOLE

Nel maggio 2018 entreranno in vigore le norme dettate dalla Unione Europea in materia di sicurezza delle reti informatiche.

Una cornice di riferimento sulla cybersecurity costituita da due regolamenti e dalle due direttive entro le quali si dovranno collocare tutte le leggi e le applicazioni nazionali.

L’anno appena trascorso, il 2016, sarà ricordato come l'anno che ha dato l’avvio al percorso sul tema della sicurezza informatica. Il futuro di questa tematica in Europa è essenzialmente tutto nelle norme di un ampio pacchetto di riforme attuate dalla UE, approvato, entrato in vigore ed in parte applicabile già da quest’anno:

- il Regolamento n. 679/2016, Regolamento Generale sulla Protezione dei Dati (RGPD), entrato in vigore il 24 maggio scorso, applicabile dal 24 maggio 2018, che sostituisce la Direttiva 95/46/CE;
- il Regolamento n. 910/2014, Regolamento Electronic Identification Authentication and Signature (Regolamento EIDAS), entrato in vigore il 17 settembre 2014, applicabile dallo scorso primo luglio, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che sostituisce il quadro normativo definito dalla Direttiva Europea 1999/93/EC;

- la Direttiva n. 680/2016, entrata in vigore il 24 maggio scorso, sul trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI del Consiglio;
- la Direttiva n. 1148/2016, Direttiva Network and Information Security (Direttiva NIS), entrata in vigore l'8 agosto scorso, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Il Legislatore si è impegnato affinché i contenuti delle succitate disposizioni siano efficaci, funzionino nella pratica e perdurino per almeno una generazione. Sono norme complesse, che richiedono la consulenza di esperti, non solo in questioni giuridiche ma delle complesse problematiche di compliance.

Il Regolamento GPD ed il Regolamento EIDAS, normativamente parlando, non necessitano di recepimento. Il Regolamento EIDAS è già applicabile, il RGPD lo sarà dal 25 maggio 2018. Diversamente, invece, la Direttiva NIS e la Direttiva 680/2016 che dovranno essere recepite con una legge nazionale, e ciò dovrà avvenire sempre entro i primi mesi del 2018.

Dal maggio 2018 avremo quindi un’ampia cornice normativa di riferimento sulla sicurezza informatica, costituta dai due regolamenti e dalle due direttive, entro la quale si collocheranno tutte le leggi a completamento e recepimento delle stesse.

Le simmetrie ed i parallelismi tra i vari testi sono evidenti e confermano l’orientamento univoco adottato dal Legislatore europeo nell’affrontare la tematica della sicurezza informatica. Per capirlo è sufficiente leggere i quattro articoli che in ognuno dei quattro testi si occupano della definizione delle misure di sicurezza. Tutti fanno riferimento all'obbligo di adozione di misure tecniche e organizzative “appropriate” (EIDAS e Direttiva NIS) e “adeguate” (RGPD e Direttiva 680) per “gestire i rischi legati alla sicurezza dei servizi fiduciari prestati” (EIDAS) e per “garantire un livello di sicurezza adeguato al rischio” (RGPD, Direttiva 680 e Direttiva NIS).

Analoghe dirette esistono anche su altri fronti, per esempio in relazione alla notifica di una violazione (prevista sia Regolamento EIDAS che dal RGPD). Entrambi fanno riferimento all'obbligo di notifica all'autorità competente, quindi ad un “organismo di vigilanza” (EIDAS) ed ad una “autorità di controllo” (RGPD) delle violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi. Notifica (comunicazione) che dev'essere effettuata anche alla “persona fisica o giuridica” (EIDAS) e agli “interessati” (RGPD), se per tali soggetti sussistono “effetti negativi” (EIDAS) e un “rischio per i loro diritti e le loro libertà” (RGPD).

Sul termine entro il quale la notifica dev'essere effettuata alle autorità competenti l'EIDAS prevede 24 ore mentre il RGPD ne prevede 72, in entrambi i casi da quando si è venuti a conoscenza della violazione.

L'UE si è quindi concentrata su disposizioni davvero necessarie ed ha evitato dettagli che avrebbero potuto interferire con le tecnologie future. I testi esaltano la chiarezza e la comprensibilità in materia di sicurezza informatica e sono una rara dimostrazione di coerenza e uniformità legislativa e quindi di una opportunità, per i destinatari, che devono applicare norme diverse ma per fortuna omogenee, univoche e chiare al fine di attuare una protezione dei dati e dei sistemi efficace, che conferisce potere al singolo e stimola aziende e autorità pubbliche alla responsabilizzazione.

In questo quadro, alla PA è richiesto uno sforzo ulteriore perché questa, nel corso degli anni, si è dotata di una pluralità di sistemi informativi rigidi e isolati, non adeguatamente protetti, che elaborano e trattano dati parziali che non si integrano fra loro. Sistemi forniti per lo più da aziende private che potrebbero porre la PA nell'impossibilità di attuare un importante e nuovo principio del RGPD: l'interoperabilità, ovvero la possibilità di poter convertire in ogni momento e senza aggravi di costo, la tecnologia alla base del sistema informativo in uso estraendo da essi i dati.