Privacy e Sicurezza: Come cambia lo Scenario e i Riferimenti Normativi nel Nuovo Regolamento Generale sulla Protezione dei Dati

Date : 20 aprile 2016

Manca poco, ormai, all'entrata in vigore del Nuovo Regolamento europeo sulla privacy, il quale apporterà alcune modifiche alla disciplina relativa alla protezione dei dati personali.

Uno dei campi in cui il Regolamento prevede delle novità è quello delle "**Misure di sicurezza**", sul quale vogliamo soffermare la nostra attenzione. Rispetto all'attuale Codice Privacy (D.Lgs. 196/2003), che prevede una bipartizione tra misure di sicurezza minime e idonee (le prime specificatamente individuate agli artt. 33-34 e all'Allegato B del Codice stesso, mentre le seconde non ben definite in quanto variano in base a una serie di parametri che devono essere valutati da ciascun titolare del trattamento), la normativa europea individua un corpus unico di misure di sicurezza che dovranno essere applicate tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento (compreso l'eventuale rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche).

Il nuovo regolamento europeo sulla protezione dei dati, infatti, prevede all'**art. 32**, che il titolare del trattamento e il responsabile del trattamento mettano in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, altre, se del caso:

a) la **cifratura** dei dati personali e la **pseudonimizzazione**;

b) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;

c) la **capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per **testare, verificare e valutare** regolarmente l'**efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

A ben vedere, non si tratta di misure di sicurezza del tutto nuove rispetto al vecchio impianto normativo, soprattutto se le confrontiamo con i contenuti del Documento Programmatico sulla Sicurezza (noto anche come “DPS”), che costituiva una misura di sicurezza obbligatoria sino a qualche anno fa.

Una vera novità, invece, è rappresentata dalla “pseudonimizzazione” - che prevede che i dati personali non “possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile” - e dall’utilizzo della “crittografia”.

Occorre evidenziare, però, per non incorrere in errore, che il regolamento non impone – sempre o in qualunque caso - l’uso della pseudonimizzazione o della crittografia (l’utilizzo delle locuzioni “tra le altre” e “se del caso” è eloquente), ma obbliga i titolari o i responsabili del trattamento a valutare – caso per caso – quelli che possono essere i rischi inerenti a quello specifico trattamento e attuare, di conseguenza, misure per limitare tali rischi, come, ad esempio, proprio la cifratura e la pseudonimizzazione dei dati (come ribadito nella parte in cui si specifica “per garantire un livello di sicurezza adeguato al rischio”). Pertanto, è necessario effettuare, prima, un’analisi di rischio (in alcuni casi sarà necessaria una vera e propria “Valutazione d’impatto sulla protezione dei dati”) e poi, se è il caso, adottare le misure di cifratura o pseudonimizzazione.

Le restanti indicazioni normative, invece, individuano i requisiti generici di sicurezza (es. sicurezza di reti e di sistemi d’informazione) che un sistema deve soddisfare per garantire la compliance privacy rispetto alla nuova regolamentazione europea e mettere in sicurezza tutto l’ambiente in cui l’informazione viene trattata:

- **riservatezza**, ovvero la protezione dei dati trasmessi o conservati per evitarne l’intercettazione e la lettura da parte di persone non autorizzate;
- **integrità**, come conferma che i dati trasmessi, ricevuti o conservati siano completi e inalterati;
- **disponibilità**, come conferma che i dati siano accessibili e i servizi funzionino anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.

Di dubbia interpretazione, invece, appare il termine “**resilienza**” (magari potremmo interpretarlo come obbligo di adottare misure volte a limitare l’impatto di un attacco a una serie di informazioni/ dati o risorse, evitando il perpetrarsi di ulteriori danni, o come capacità di reazione di un sistema a fronte di un evento che metta a rischio la sicurezza delle informazioni e dei dati trattati), ma è facile comprendere come lo stesso sia strettamente legato anche alle ulteriori misure indicate alle lettere seguenti c) e d).

In particolare, il punto d) delle misure indicate all’art. 32, introduce quel principio di “rendicontazione” che prevede l’obbligo del Titolare del trattamento di conformarsi agli adempimenti derivanti dalla nuova normativa e di dimostrare tale conformità (e, quindi, il rispetto di tutti obblighi in capo allo stesso), anche mediante l’adozione di politiche interne e di

meccanismi atti a garantire il rispetto del Regolamento stesso. Il titolare del trattamento, infatti, deve attuare i requisiti di sicurezza dei dati e mettere in atto meccanismi per assicurare la verifica dell'efficacia delle misure.

Ciò vuol dire che non solo si chiede al Titolare del trattamento (o al suo Responsabile) di adottare determinate misure di sicurezza (previa analisi dei rischi) e dimostrarne la conformità alla nuova regolamentazione europea, ma si chiede altresì di dimostrare che dette misure abbiano effettivamente funzionato durante il corso dei trattamenti effettuati (sulla scorta di quanto avviene nella redazione dei Modelli di Gestione e Organizzazione in base al D.Lgs. 231/2001).

Appare utile, infine, un confronto con le disposizioni previste, e ad oggi ancora vigenti, dal d.lgs. n. 196/2003 (Codice privacy). L'art. 31 stabilisce che *"i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*. In più, ai sensi dell'art. 33 del Codice privacy, i titolari del trattamento sono tenuti ad adottare le **misure minime** volte ad assicurare un **livello minimo di protezione dei dati personali**. In particolare, per i trattamenti di dati effettuati con strumenti elettronici le misure di sicurezza idonee per garantire la sicurezza dei dati personali consistono *"nell'autenticazione informatica, nell'adozione di procedure di gestione delle credenziali di autenticazione, nell'utilizzazione di un sistema di autorizzazione, nell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, nella protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; nell'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi, nell'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari"*.

Da una rapida comparazione, quindi, possiamo affermare che gli articoli dei due testi legislativi (italiano ed europeo, vecchia e nuova normativa) che affrontano la tematica delle "misure di sicurezza" non sono in antitesi, ma anzi, quanto riportato nel D.Lgs. 196/2003 costituisce la base e il punto di partenza per sviluppare un più completo "Data Protection Program" (sulla scorta del vecchio DPS), finalizzato a consentire al titolare del trattamento di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici e idonei modelli organizzativi (in relazione ai trattamenti effettuati per le varie finalità perseguite e in base alle modalità e agli strumenti utilizzati).

A cura di: **Graziano Garrisi**, Avvocato del Foro di Lecce dal 2008. Fa parte del Digital & Law Department dello Studio Legale Lisi, occupandosi principalmente di consulenza legale in materia di privacy e diritto delle nuove tecnologie, nonché nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e D.Lgs. 196/2003. Socio fondatore e membro del Direttivo di ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei

documenti) è Socio fondatore anche di ABIRT (Advisory Board Italiano dei Responsabili del Trattamento dei dati personali). Relatore in numerosi convegni e autore di pubblicazioni in materia di diritto delle nuove tecnologie. Iscritto all'elenco Anorc Professioni Responsabile Trattamento dei Dati Personali.