Cyber safety e GDPR: in gioco i diritti e le libertà delle persone fisiche

Date : 27 febbraio 2018

Qualunque analisi in tema di sicurezza con riferimento alla normativa sulla protezione dei dati personali rimanda immediatamente alla necessità di adottare adeguati interventi di tipo informatico a protezione dei dati oggetto di trattamento.

L'approccio è corretto ma, specie alla luce del nuovo Regolamento europeo in materia di protezione dei dati personali (meglio noto con l'acronimo inglese GDPR), non può essere ricondotto esclusivamente ad adempimenti di *cyber security*.

Invero, sia il codice privacy - agli artt.31 e ss., così come nel disciplinare tecnico di cui all'allegato B - che l'attuale sezione seconda del capo IV del Regolamento fanno espresso riferimento (tali sono i rispettivi titoli) a misure di "sicurezza dei dati".

In particolare, l'art.32 del GDPR, sebbene non elenchi più in modo tassativo le misure minime come previsto dal D. L.vo 196/2003, individua una serie di misure (dalla pseudonimizzazione alla resilienza dei sistemi, alle procedure di *back-up* e *disaster recovery*, a varie attività di *testing*) che ribadiscono la natura prettamente informatica del concetto di sicurezza riferito ai dati personali.

L'intero impianto del Regolamento, tuttavia, è costruito attorno ad un principio che va ben oltre la mera sicurezza del dato in sé e che riguarda, invece, la sicurezza dei diritti e delle libertà delle persone fisiche.

Il concetto emerge anche nel già menzionato art.32, nella parte in cui prescrive al titolare di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento nonché del "*rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*".

Viene poi ripreso, quale parametro modulare di riferimento, nei successivi artt. 33 e 35: nella disciplina in tema di *data breach* costituisce il discrimine per la notifica all'Autorità di controllo (non tutte le violazioni di dati, infatti, debbono essere notificate all'Autorità di controllo, ma solo

quelle che mettono a rischio diritti e libertà degli interessati), mentre, con riferimento alla valutazione di impatto dei trattamenti sulla protezione dei dati, il rischio per i diritti e le libertà degli interessati rappresenta uno dei presupposti della DPIA (*Data Protection Impact Assessment*), ma solo qualora si versi in un'ipotesi di "rischio elevato".

Da quanto esposto appare chiaro che la *ratio* del concetto di sicurezza nel GDPR non è tanto la protezione del dato in sé quanto piuttosto della persona che dal trattamento di quel dato può subire lesioni ai suoi diritti e alle sue libertà.

Si tratta di un concetto molto ampio di sicurezza il cui significato è, forse, più facile cogliere nella duplice accezione inglese di "*security*" e "*safety".*

Con il primo termine s'intende l'insieme di misure volte a prevenire e contrastare atti di interferenza illecita esterna nei confronti di un sistema, mentre il secondo si riferisce alla sicurezza sotto il profilo della progettazione, della costruzione e della manutenzione di un sistema affinché il sistema stesso non pregiudichi l'incolumità o la salute delle persone.

In quest'ottica, un sistema (informatico e non) può dirsi *secure* se è invulnerabile rispetto ad attacchi esterni, mentre è *safe* se è improbabile che causi danni alle persone.

La conferma che il Regolamento graviti attorno al concetto di *safety* emerge non solo dagli articoli sopra citati, ma anche dal disposto di cui all'art.25, in tema di *privacy by design* e *by default* (volti rispettivamente ad attuare, in concreto, i principi di minimizzazione e limitazione delle finalità) che, a sua volta, impone di tenere conto, tra l'altro, dei "*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*".

Un sistema che tratta dati personali sarà, dunque, sicuro (*safe*) solo se sarà fisiologicamente in grado di tutelare i diritti e le libertà delle persone; al contempo, però, lo stesso dovrà essere sicuro (*secure*) anche rispetto ad eventuali situazioni patologiche rappresentate da pericoli esterni.

L'impostazione del GDPR, sotto questo profilo, non è dissimile da quella adottata dal legislatore europeo (recepita in Italia, da ultimo, con il D. L. vo 81/2008) in tema di tutela della salute e della sicurezza nei luoghi di lavoro, in cui, trattandosi di salute dei lavoratori, il concetto di *safety* risulta sicuramente più immediato.

Entrambe le normative si basano sul *risk assessment*.

La valutazione dei rischi costituisce, infatti, sia nel GDPR che nella normativa anti-infortunistica sul lavoro il presupposto necessario per procedere all'adozione di misure di prevenzione e protezione idonee ad eliminare o ridurre alla fonte i rischi riscontrati e, solo in seconda battuta, si tratta di un'attività volta a soddisfare l'onere, posto in capo al titolare del trattamento o al datore di lavoro, di dimostrare la *compliance* normativa.

In entrambi i casi l'analisi dei rischi deve confluire in un documento ed è soggetta a costante revisione qualora intervengano variazioni dei rischi a seguito di modifiche dell'attività di

trattamento o dell’attività produttiva.

Non solo.

Entrambe le normative prevedono la designazione di un responsabile che collabori con il titolare o il datore: nel primo caso, la normativa ha introdotto la figura del responsabile per la protezione dei dati personali (*Data Protection Officer*, DPO, nell’acronimo inglese), nel secondo quella del responsabile del servizio di prevenzione e protezione dei rischi (RSPP).

Si tratta di due figure (indifferentemente interne o esterne all’azienda), in possesso di comprovate conoscenze e qualità professionali, a cui vengono attribuite funzioni di consulenza, cooperazione, coordinamento e vigilanza. Alcune differenze emergono solo in relazione all’autonomia finanziaria ed organizzativa che l’art.38, 2° co., GDPR prevede in maniera più marcata rispetto al D. L.vo 81/2008 e, per contro, un maggior coinvolgimento nell’individuazione e valutazione dei rischi da parte del RSPP (art.33, 1° co., lett. a), D. L.vo 81/2008) rispetto al DPO, il quale deve fornire al titolare un parere in merito alla DPIA, solo se richiesto (art.39, 1° co., lett. c), GDPR).

Si potrebbe legittimamente obiettare che nel caso di beni immateriali, come i dati personali, sia fuori luogo far riferimento al concetto di *safety*, concetto strettamente legato all’incolumità fisica delle persone, nonché tentare un parallelo con la disciplina in tema di sicurezza sui luoghi di lavoro in cui oggetto di tutela è esplicitamente la salute dei lavoratori.

Siffatta critica, a parere di chi scrive, non convince per due ordini di motivazioni.

Da un lato, si osserva come, da anni, la più attenta dottrina (Rodotà) abbia elaborato, sulla falsariga dell’*habeas corpus*, teorizzato nella Magna Carta e trasfuso nell’art.13 della nostra Costituzione, il diritto di *habeas data*, ovverosia il diritto all’inviolabilità ed integrità del corpo digitale.

Si tratta di un diritto che va oltre la mera autodeterminazione del singolo in ordine ai dati personali che lo riguardano, innanzitutto perché ribalta la prospettiva (è una libertà rispetto al potere dispositivo altrui, a prescindere dal controllo attivo che il soggetto può rivendicare sui suoi dati) ed in secondo luogo perché si riferisce non ai dati singolarmente considerati (sarebbe come tutelare ogni singolo capello o pelo di un corpo fisico) bensì il corpo digitale, ovverosia il complesso dinamico delle informazioni che rappresentano l’individuo nel mondo digitale.

Riconoscere una *safety* digitale, significa dunque riconoscere che oggetto di tutela non sono più i singoli dati in sé ma ogni individuo nella sua interezza e dimensione digitale.

Dall’altro lato, il parallelo con la normativa anti-infortunistica sul lavoro consente di sviluppare un approccio culturale alla materia che, allontanandosi dall’ottica del soggetto singolo, proponga una tutela collettiva del diritto alla protezione dei dati personali.

Per comprendere meglio il parallelo è sufficiente ricordare come a seguito della rivoluzione industriale la diffusione delle macchine e delle lavorazioni pericolose aumentò in modo

impressionante il numero degli infortuni sul lavoro e delle malattie professionali, ma solo una regolamentazione del lavoro di stampo collettivo riuscì a garantire una tutela effettiva del diritto alla salute del singolo lavoratore. Oggi, di fronte alla c.d. rivoluzione digitale ed alla impellente necessità di garantire un'adeguata protezione della privacy e dei dati personali dei cittadini, può essere utile ricordare l'evoluzione normativa in tema di sicurezza sui luoghi di lavoro e sottolineare come la prima legge italiana in materia fu la legge 11 febbraio 1886, n. 3657 a tutela del lavoro dei fanciulli negli opifici industriali, nelle cave e nelle miniere ed il primo intervento volto ad assicurare, attraverso un sistema di prevenzione, la tutela della integrità fisica del prestatore d'opera fu il Regolamento generale per la prevenzione degli infortuni del 1899 (R. D. 18 giugno 1899, n.230), emanato alcuni decenni dopo l'inizio del processo italiano di industrializzazione.

Concludendo, la vera sfida del GDPR, nella sua concreta applicazione, sarà quella di riuscire a garantire, attraverso i nuovi strumenti tecnico-organizzativi (DPIA, *privacy by design* e *by default*, DPO), una tutela non tanto dei dati in sé quanto delle persone da quei dati rappresentati.

Per vincere questa sfida occorre andare oltre il concetto di *cyber security* e provare ad approcciare la materia sotto il diverso profilo della *cyber safety*.

A cura di: **Monica A. Senor**