Il GDPR questo sconosciuto, per ora

scritto da goal | 9 Luglio 2018

di Antonio Fiorentino*

Dal 25 maggio 2018 entrerà pienamente in vigore nel nostro Paese il regolamento europeo n. 2016/679 sulla protezione dei dati personali, noto con l'acronimo GDPR (General Data Protection Regulation), emanato il 24 maggio 2016.

Come al solito non mancano difficoltà e ritardi nelle attività di adeguamento da parte dei soggetti obbligati (imprenditori, professionisti, enti pubblici, ecc.) a causa della complessità della materia e degli interventi da eseguire, nella consapevolezza che il GDPR cambierà il modo di intendere la protezione della privacy. Anche per questo, è necessario agire immediatamente, in quanto tutte le aziende pubbliche e private che saranno trovate non conformi si esporranno a sanzioni fino a 20 milioni di euro o fino al 4% del fatturato globale annuo, senza scuse per i trasgressori, che hanno avuto due anni di tempo per mettersi in regola.

Qualsiasi impresa che si occupa di dati sensibili dovrebbe prestare molta attenzione a questo nuovo regolamento, tuttavia sembra che la maggior parte di esse, come pure molti studi professionali, enti privati e talvolta persino qualche istituzione pubblica fatichi a capire di cosa si tratti. La facilità di adeguamento alle normative del passato induce anche questa volta a prestare poca attenzione alla cosa e a considerare il GDPR l'ennesimo regolamento a cui doversi adeguare solo formalmente per non incorrere in sanzioni. Ma questa volta non è cosi, basti pensare che persino colossi d'oltreoceano come Facebook e Google stanno correndo ai ripari. La percezione che si ha, almeno in Italia, è che tutti sappiano di questa novità ma non abbiano un'idea precisa di

cosa sia e di come si debba affrontare. L'adeguamento, quindi, potrebbe essere critico, molti sono "lontani", persino da un punto di vista culturale, dal programmare le azioni necessarie. Moltissimi non hanno compreso che il GDPR segna un mutamento storico, giuridico ma anche politico ed economico di grandissima importanza, non solo perché si passa da un sistema basato su direttive di armonizzazione e legislazioni nazionali di attuazione a un regolamento di immediata applicazione in tutti gli stati membri, ma anche perché questo regolamento è una straordinaria occasione di svecchiamento dei processi e mira in fondo a una riorganizzazione delle aziende soprattutto dal punto di vista tecnologico, dando una fortissima spinta verso il digitale. Quindi il vero rischio che si corre sottovalutando il GDPR non tanto è quello di prendere una multa, ma è quello di uscire dal mercato.

Siamo dunque di fronte a un cambiamento radicale delle leggi sulla protezione dei dati nell'Unione europea (UE), che non è progettato soltanto per rafforzare e unificare la protezione dei dati per le persone all'interno dell'Unione, ma anche per regolare l'esportazione di dati personali dei cittadini europei al di fuori dell'UE. Quel che si vuol regolare è l'utilizzo dei dati personali che qualsiasi organizzazione (pubblica o privata) detiene. Si tratta insomma di un nuovo schema legislativo che regola la vita di tutti e che ha l'obiettivo principale di restituire ai cittadini il controllo dei propri dati personali, unificando le normative all'interno dell'UE e semplificando il contesto normativo per le attività internazionali.

Va sottolineato che non si tratta di una direttiva con tempi lunghi di recepimento da parte degli stati dell'Unione europea e una conseguente montagna di decreti attuativi da definire prima che si possano vedere i suoi effetti, è un regolamento vincolante per tutti, che riguarda cioè tutte le organizzazioni (enti pubblici, imprese, professionisti) e che sarà applicato in tutti i 26 stati membri, i quali devono

istituire un’apposita autorithy sulla privacy, ove non l’abbiano già fatto. La scelta di adottare un regolamento manifesta la volontà del legislatore europeo di creare un quadro giuridico omogeneo e unitario in tema privacy, tale da prevenire la frammentazione dell’impianto originario. Il GDPR sostituisce le vecchie normative ovvero direttive preesistenti (quali la Direttiva 94/46/EC e il DL 196/2003), ma il governo italiano non ha ancora emanato il provvedimento previsto dalla legge delega che “raccordi” la nuova normativa con quelle precedenti. Visto l’esito delle elezioni del 4 marzo 2018 appare piuttosto improbabile che un nuovo governo possa approvare tale provvedimento entro il mese di maggio 2018 (6 mesi a far data dal novembre 2017, giorno in cui è entrata in vigore la legge 25 ottobre 2017, n. 163).

L’adozione del regolamento rappresenta, a vent’anni dalla direttiva madre, una svolta nell’approccio dell’Unione europea alla tutela dei dati personali intesi quali informazioni relative a una persona fisica, identificata o identificabile, anche indirettamente, attraverso altre informazioni ovvero la profilazione del cittadino mediante numeri di identificazione, nome, indirizzo fisico o e-mail, foto, dettagli sulla posizione bancaria, post sui social, informazioni mediche, l’Internet Protocol address (IP), eccetera. In realtà la normativa di adempimenti veri e propri non ne richiede tantissimi, ma i soggetti che gestiscono i dati personali (tra cui le imprese) dovranno sempre e comunque:

- comunicare le violazioni dei dati personali (data breaches) e cioè gli accessi ingiustificati ai dati all’autorità nazionale ogni volta che risulta un rischio per i diritti e la libertà degli individui;
- garantire all’interessato il diritto all’accesso dei proprio dati;
- garantire il diritto all’oblio, e cioè il diritto alla cancellazione definitiva dei dati se la conservazione di tali dati viola il regolamento o i diritti riconosciuti

dall’Unione europea o dagli stati membri cui è obbligato il titolare del trattamento;

- garantire la portabilità dei dati, ovvero che i dati personali siano non solo accessibili e utilizzabili dal titolare, ma anche spendibili in altri contesti semplicemente su richiesta;
- garantire in maniera strutturale la privacy dei dati La privacy deve essere intesa come la maniera in cui i dati personali nascono e vengono trattati fin dal principio. I concetti di privacy by design e privacy by default sono interamente nuovi nel panorama giuridico. Essi richiedono, infatti, che la protezione dei dati faccia parte del progetto di sviluppo dei processi aziendali per tutti i prodotti e servizi e che le impostazioni di privacy siano configurate in modo predefinito, inoltre è l’impresa (società, ditta individuale, ecc.), quale soggetto gestore dei dati, che deve poter giustificare la detenzione dei dati: se cioè dei dati risultano essere obsoleti e sono in un database che viene violato, l’impresa deve dimostrare che quei dati erano lì per una ragione specifica e legittima, altrimenti scatta la sanzione;
- dotarsi di un responsabile della protezione dei dati, denominato Data Protection Officer (DPO). Questo nel caso che l’impresa rientri nella categoria cui viene fatto l’obbligo di avere una figura simile. Un tale obbligo grava, per esempio, sulle pubbliche amministrazioni, sulle imprese che raccolgono dati dal pubblico su vasta scala, quelle che trattano strutturalmente dati personali per i loro clienti, utenti o interlocutori come ad esempio i call center, le assicurazioni, le società di gestione del personale ecc. Il DPO è direttamente responsabile, fra l’altro, della comunicazione al garante della privacy e agli interessati delle eventuali violazioni, entro le 72 ore dalla scoperta della violazione stessa. Gli interessati devono avere la possibilità di interagire con questa

figura per tutti i problemi che riguardano la gestione dei loro dati personali;
- predisporre la richiesta di consenso che l'impresa dovrà ottenere dall'interessato attraverso un'autorizzazione esplicita e non ambigua al trattamento dei dati In altre parole le imprese non potranno più sottoporre al cliente lunghi e illeggibili termini e condizioni scritti in pagine e pagine scritte in un linguaggio spesso molto faticoso e complicato. La richiesta di consenso dovrà essere chiaramente distinguibile da altre materie e scritta in un linguaggio chiaro e comprensibile.

Gli adempimenti per le imprese, in realtà per tutti i soggetti gestori dei dati, non sono dunque pochi. Ma considerare l'arrivo del GDPR come un'imposizione vorrebbe dire perdere di vista lo scenario generale. Il problema vero è che la legge cambia strutturalmente la filosofia della gestione dei dati dei dipendenti e dei clienti, superando la vecchia privacy con i concetti di trasparenza e responsabilità. Il principio base della legge – Privacy by default and by design – non pone obblighi stringenti all'impresa su come organizzare i suoi database, non è invasivo, ma pone un principio di responsabilità che prima non c'era. Se succede qualcosa ai dati custoditi l'impresa ne è responsabile.

La responsabilità concreta può essere accertata soltanto nel caso di una denuncia di violazione. Il modello è simile a quello della sicurezza sul lavoro: finché non ci sono incidenti, non c'è sanzione. Così come, ad esempio, nel caso di un operaio che subisce un grave infortunio a causa della mancata adozione di adeguati sistemi di protezione per negligenze o omissioni del datore di lavoro, solo al verificarsi dell'infortunio "emerge" l'inosservanza degli obblighi sulla sicurezza, così solo nel momento in cui c'è una violazione della sicurezza dei dati, un Data breach (furto d'identità, di dati sensibili ecc.), diventa chiaro che l'impresa non ha messo in atto misure sufficienti a proteggere

i dati personali altrui che gestisce.

Per non incorrere nelle sanzioni, ci sono una serie di azioni molte precise che i soggetti gestori dovranno fare nell'immediato:

- procedere all'analisi dei dati custoditi, ossia verificare a cosa servono i dati posseduti e come vengono utilizzati, perché accade sovente che una buona percentuale di quei dati non è veramente necessaria all'attività aziendale, e proseguire con accertamento del modo in cui vengono conservati;
- curare il rinnovo continuo della documentazione relativa alla Con la nuova legge il consenso del trattamento dei dati personali e la relativa informativa non sono eterni, vanno aggiornati periodicamente;
- attuare un programma di formazione dei dipendenti su come vanno gestiti i dati;
- implementare procedure predefinite di contenimento, avviso e informazione per esempio in caso di data breach.

Le imprese italiane sono dunque chiamate ad affrontare una sfida decisiva e devono attivarsi sia per scongiurare i rischi di vedersi infliggere pesantissime sanzioni, sia per fare un salto di qualità culturale, smettendo di considerare la privacy come un mero adempimento burocratico. Il GDPR infatti ridisegna gli scenari del mercato digitale e richiede a professionisti e manager d'impresa un netto cambiamento di mentalità, per rimanere al *passo con i tempi*, ma anche per sfruttare le nuove opportunità di crescita che questo regolamento offre.

* *Odcec Napoli nord*