ARRIVA LA DATA GOVERNANCE

di MARIA MORO

IL REGOLAMENTO UE SULLA PRIVACY PREVEDE UN APPROCCIO SISTEMICO AL TRATTAMENTO DEI DATI CHE RICHIEDE UNA RESPONSABILITÀ SOLIDALE, VERO CAMBIO DI MENTALITÀ PRIMA CHE DI OPERATIVITÀ NELLE AZIENDE. LE IMPRESE ITALIANE SI STANNO ADEGUANDO, MA SOLO IL 9% HA GIÀ IN CORSO UN PROGETTO STRUTTURATO

Poco più di un anno di tempo per mettersi in linea con il regolamento europeo sulla privacy sembra molto, ma non lo è. Il nuovo *Gdpr* (*General data protection regulation*, regolamento Ue 2016/679) spinge verso l'introduzione di una *data governance*, che implica riorganizzazione della struttura, nuove tecnologie finalizzate al trattamento e sicurezza del dato, e, di conseguenza, importanti investimenti. **Luca Bolognini**, presidente dell'**Istituto italiano Privacy**, disegna le complessità insite nell'adeguamento delle imprese italiane al nuovo regolamento Ue.

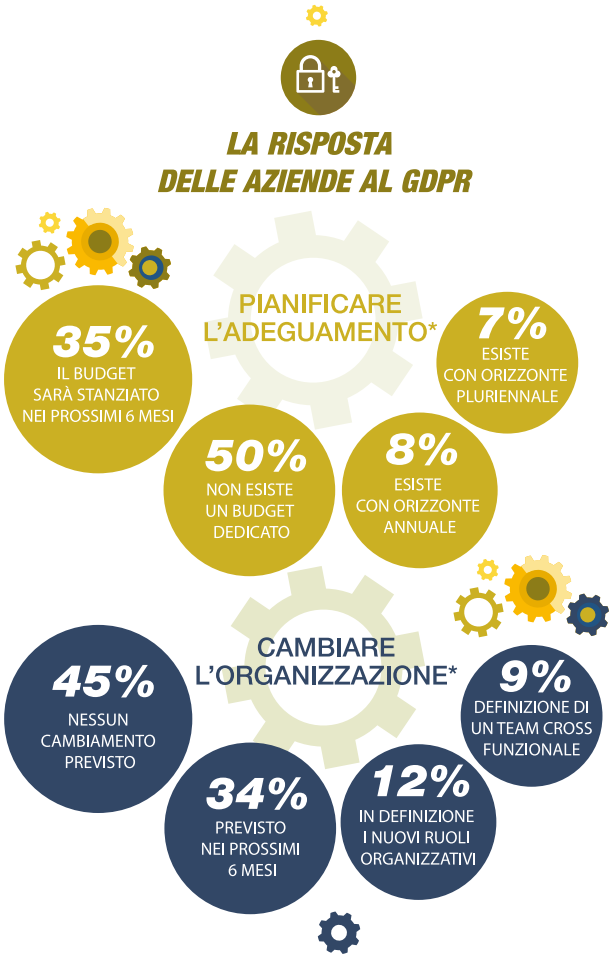
Rispetto a quanto previsto dalla normativa italiana, quali sentieri già tracciati può trovare l'applicazione del Gdpr?

Il regolamento privacy Ue sostituirà solo una parte delle norme imperative nazionali in materia di protezione dei dati: molti obblighi squisitamente italiani resteranno in piedi, ad esempio per quanto riguarda i controlli a distanza sul lavoro o il settore sanitario, e più in generale le misure prescritte dal Garante privacy con i suoi provvedimenti generali. È chiaro che le misure minime di sicurezza di cui all'Allegato B al *Codice privacy* dovranno essere considerate superate, ma questo non significherà non applicare più i criteri in esse contenuti. Semplicemente, si dovrà andare molto oltre come livelli di salvaguardia. Il regolamento cambia il paradigma a cui attenersi: non più una *lista della spesa*" di misure precise e valide per tutti i soggetti che trattano dati, ma la necessità di valutazioni d'impatto e di scelta di misure di sicurezza e salvaguardia che siano *adeguate ai rischi*. Non solo, i rischi e gli impatti da considerare non saranno unicamente tecnologici ma anche *umanistici*, riferiti, ad esempio, alla potenziale lesività di violazioni sui beni della vita, sociali, relazionali, psicologici, economici delle persone fisiche. Non banale.

Come sta rispondendo il sistema imprenditoriale italiano al Gdpr?

Come dicevano i latini, *si vis pacem para bellum* e in un certo senso è il metodo consigliabile anche per la rivoluzione di *compliance privacy* in arrivo. Alcune recenti survey ci raccontano di un panorama imprenditoriale ancora distratto rispetto alla rilevanza dei nuovi obblighi privacy e del rischio cyber: tuttavia la mia percezione è che si stiano facendo strada consapevolezza e urgenza di far fronte alle nuove sfide di *compliance data protection*. Molte grandi e medie aziende hanno già avviato attività utili alla compliance privacy europea, mentre le

***Luca Bolognini**, presidente dell'Istituto italiano Privacy*



*I dati sono raccolti dalla ricerca "Cyber crime: la minaccia invisibile che cambia il mondo" realizzata dall'Osservatorio information security e privacy di Osservatori.net, Politecnico di Milano.

piccole stanno temporeggiando. Se pensiamo che anche una singola violazione di principi generali (articolo 5 del Gdpr) potrà portare a sanzioni fino al 4% del fatturato globale di un'impresa, si capisce come oggi la privacy sia un tema all'ordine del giorno dei board delle multinazionali al pari dell'Antitrust.

Come attrezzare le imprese per mettere in pratica le disposizioni del regolamento?

Alle aziende raccomando azioni combinate tra legge e tecnologia: anche un avvocato esperto, come me, da solo non va da nessuna parte, così come è ingenuo pensare che gli adempimenti Gdpr siano fatti di mera *data security*. Anzi, spesso la *data protection/safety* va bilanciata con la sicurezza: troppa sicurezza può sfondare i limiti imposti dalla privacy, condurre alla violazione di principi e altre norme del regolamento o dei diritti dei lavoratori rispetto ai controlli a distanza. Servono equilibrio, competenza, multidisciplinarietà. In tutti i progetti di *compliance privacy* europea che stiamo avviando ci avvaliamo di una squadra integrata, composta da avvocati, ingegneri Ict, fornitori di tecnologie utili alla *cyber security* e di tool per la gestione automatizzata degli adempimenti, anche documentali, imposti dal Gdpr.

Ben venga, quindi, il data protection officer, figura obbligatoria per enti pubblici e alcune imprese, ma auspicabile in generale per tutte le aziende, meglio se inserito nello staff e sostenuto da un data protection officer esterno: raccomando altre figure in aggiunta, come i data protection designer che siano in grado di trasformare le regole giuridiche in misure pratiche, processi e prodotti *privacy-friendly*.

In che modo il rispetto del Gdpr può risultare efficace in caso di attacchi cyber?

Il principio di responsabilizzazione (*accountability*) ci imporrà di razionalizzare, difendere le nostre scelte e documentarle per dare prova di avere fatto mente locale sui rischi e sulle azioni di mitigazione. Il gioco di squadra fra legali e tecnici sarà la chiave di volta, oltre alla continuità degli interventi e della consulenza. Si interverrà sempre più anche come periti delle assicurazioni che coprono il *cyber risk*. È chiaro che applicare i requisiti legali, logici, organizzativi e tecnici di protezione e sicurezza dei dati personali previsti nel regolamento contribuisce, automaticamente, a prevenire violazioni di dati e a gestire al meglio le fasi successive al loro infausto verificarsi, in primis accorgendosi della *data breach* e quindi, reagendo opportunamente e documentando le evidenze e le scelte. Stiamo parlando di prevenzione continuativa, ciclica, non di interventi spot. Senza contare che nei registri delle attività di trattamento, obbligatori ex articolo 30 regolamento 2016/679 (Ue), si devono indicare le varie misure di sicurezza adottate. Non solo quindi in fase di prevenzione, ma anche in caso di data breach, la collaborazione tra legali, dotati di tool automatizzati di analisi dei rischi, e società esperte in *forensics* e in cyber security aziendale, diventerà fondamentale.