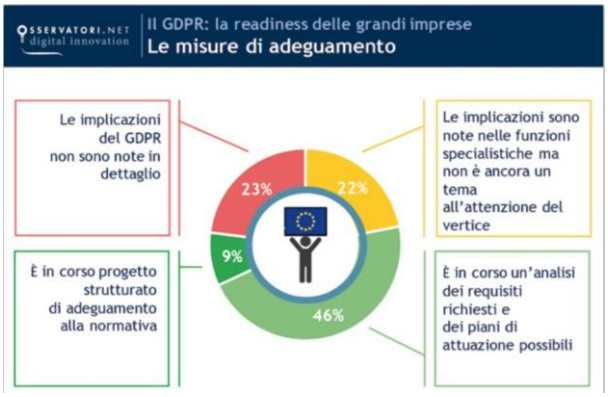
R.it ECONOMIA & Finanza con Bloomberg

Privacy, il fantasma delle regole Ue: ultima chiamata per imprese e PA

Il nuovo regolamento sulla protezione dei dati prevede sanzioni fino al 4% dei ricavi di gruppo. C'è tempo fino a maggio 2018 per adeguarsi, Italia in grave ritardo. Faggioli, ceo P4I: "Pmi buco nero"

Andrea Frollà



C'è un fantasma che si aggira per l'Europa. No, non è quello descritto 170 anni fa da Marx ed Engels, ma il **nuovo regolamento Ue in materia di privacy**, entrato in vigore dal 24 maggio scorso negli Stati membri e pienamente applicabile dal 6 maggio del 2018. Partorite dalla macchina dell'Unione Europa dopo quasi 5 anni di lavoro inteso e tortuoso, le regole scritte da Bruxelles puntano a difendere in modo adeguato i dati personali nell'era digitale, imponendo degli obblighi precisi alle aziende a livello di governance e trattamento delle informazioni.

Il **regolamento generale sulla protezione dei dati (Gdpr)**, che fa parte della riforma che include pure la **direttiva sulla protezione dei dati** trattati dalla polizia e dalle autorità giudiziarie penali, ha visto la luce seguendo il motto "un continente, una legge". E la sua applicazione si estenderà anche alle imprese extraeuropee che offrono servizi all'interno dell'Unione europea. Già questo basta a spiegare quanto la privacy disegnata da Bruxelles sia molto complessa e corposa.

Tra i numerosi princìpi a tracciare la rotta per difendere i dati, e allo stesso tempo ridurre

i costi e la burocrazia che zavorrano le imprese europee, rientrano l'**accesso facilitato ai dati** (più informazioni sulle modalità di trattamento, da comunicare in modo chiaro e comprensibile), la **portabilità delle informazioni** (sarà più semplice trasferire i dati personali da un fornitore di servizio a un altro) e il **diritto di essere informati in caso di violazione**. Oltre a garanzie rigorose per il **trasferimento dei dati fuori dal territorio comunitario**.

L'approccio di Commissione europea, Parlamento Ue e Consiglio per tradurre in norme questi princìpi è stato **promuovere la responsabilizzazione dei titolari del trattamento**, secondo una logica basata sul rischio che premia i soggetti più responsabili e che inaugura l'era della *privacy by design*, cioè la protezione dei dati che parte dalla messa in piedi dei sistemi di tutela. Ad esempio, diventa obbligatorio effettuare una valutazione di impatto quando il trattamento dei dati pone rischi per i diritti delle persone. Oppure ancora, per molte aziende ed enti pubblici è necessario dotarsi di un **Data protection officer (Dpo)**, ossia di una figura specializzata che assicura la corretta gestione delle informazioni. Misure ammorbidite dalla **scomparsa di alcuni oneri amministrativi**, tra cui l'obbligo di notificare particolari trattamenti. Quindi più responsabilità in cambio della semplificazione.

Il carattere spettrale della nuova data protection in salsa europea, che rientra nel più ampio progetto di creazione del mercato unico digitale, non è dettato tanto dalle previsioni del testo, quanto dal processo di avvicinamento delle imprese all'applicazione prevista da maggio 2018. Per capire quanto sia importante adeguarsi e mettersi in regola nei tempi prestabili basta ricordare l'entità delle sanzioni previste. Si passa da violazioni più leggere, che prevedono sanzioni fino a 10 milioni di euro, a quelle più gravi, che possono tradursi in **multe fino al 4% del fatturato di gruppo**. Tanto per dare un ordine di grandezza, se una compagnia come Apple inciampasse nel modo peggiore fra le nuove regole europee si troverebbe a dover sborsare un assegno da quasi 10 miliardi. Ma la pesantezza delle sanzioni previste non deve mettere in guardia solo i big, bensì qualunque azienda o ente pubblico di piccole o medie dimensioni che tratta dati personali.

In Italia il livello di attenzione è in aumento ma se ci si domanda quale sia lo stato dell'arte, vale a dire se le imprese e gli enti si siano mossi a dovere, la risposta è negativa. Anzi, allarmante. Infatti, secondo i dati dell'**Osservatorio Information Security & Privacy** del Politecnico di Milano, oggi **solo un'azienda italiana su cinque conosce nel dettaglio le implicazioni del Gdpr** e sono pochissime (9%) quelle che

hanno già strutturato un progetto per adeguarsi. Se non bastasse, la percentuale di imprese che non prevedono di modificare la governance o di stanziare un budget ad hoc nei prossimi mesi arriva al 50%. Il 46%, quindi molte ma comunque non abbastanza, almeno ha in corso un'analisi dei requisiti richiesti. Uno scenario appare desolante, dovuto a un ritardo al limite del disinteresse.

«Il processo di adeguamento al nuovo regolamento è ben avviato nel caso delle aziende di **maggiori dimensioni, dove il tema è ormai più che noto e i progetti sono in via di sviluppo. Mentre il mondo della piccola e media impresa è un buco nero difficilmente controllabile**. Sicuramente l'uniformità rigida e la complessità delle regole non aiutano l'applicazione - spiega **Gabriele Faggioli**, ceo di P4I (società del gruppo Digital360 che offre servizi di advisory e coaching a supporto di imprese e PA) nonché presidente dell'Associazione Italiana per la sicurezza informatica – **Il tempo per mettersi in regola c'è ma non sono più ammessi temporeggiamenti**. Bisogna partire quanto prima con il registro del trattamenti, cioè mappando dati e applicazioni, per poi procedere con le valutazione dei rischi e tutte le altre misure necessarie».

Come già accennato, un ruolo chiave nella transizione verso le nuove regole lo avrà la figura del data protection officer. «La scelta del Dpo passa dal bivio fra competenza interna o esterna. L'ideale, specialmente per le grandi società, è sempre optare per una risorsa 'casalinga' perché conosce già numerose tipologie di trattamento dei dati effettuati e, aspetto non secondario, innalza il livello di competenze interne dell'organizzazione – spiega l'esperto di P4I - Deve essere un profilo che abbia **il giusto mix di competenze giuridiche e informatiche**. Meglio se è una figura con un'esperienza importante nella compliance e nell'audit, dove l'analisi di processi e rischi è pane quotidiano». Tutti questi temi animeranno un evento dedicato alle imprese, **organizzato da Arrow Ecs Italia con il contributo editoriale di Digital4Trade e** in programma a Milano il prossimo 21 aprile, che prevede la partecipazione dei massimi esperti di normativa europea e sicurezza informatica.