Come spiegare alle PMI perché il Regolamento Europeo sulla Privacy non è come tutte le altre norme e cambierà davvero lo scenario della circolazione del dato digitale in azienda

Date : 14 febbraio 2017

Fino ad ora per un avvocato proporre una consulenza su temi relativi a privacy e/o cybersecurity ad un piccolo/medio imprenditore italiano, dava la stessa imbarazzante sensazione di essere considerato alla stregua di un operatore di un call center che ti chiama alle nove di sera per proporti la sottoscrizione di un contratto con un nuovo operatore telefonico.

Considerato che nel nostro Paese il 99,9% della totalita? delle imprese è costituito da imprese di piccole e medie dimensioni che producono il 68% della ricchezza italiana con 12 milioni di persone impiegate, la vita di noi consulenti è indiscutibilmente complessa. È altrettanto indiscutibile, tuttavia, che dobbiamo proteggere questa fondamentale risorsa del Paese giustificando l'atteggiamento talvolta rude degli imprenditori con il fatto che tutte queste realtà si sono dovute scontrare con una rivoluzione digitale impensabile prima del nuovo millennio.

Il Regolamento Europeo 2016/679, infatti, introduce alcuni innovativi principi in tema di protezione dei dati direttamente applicabili a tutte le realtà aziendali Europee. In questo articolo, ne vorrei solo presentare alcuni per dimostrare come l'applicazione di tale normativa che, tra l'altro prevede profili sanzionatori di sicuro interesse per il piccolo/medio imprenditore (da 10 a 20 milioni di euro o dal 2% al 4% del fatturato dell'azienda), costituisca un primo passo concreto verso una seria responsabilizzazione delle società sul tema.

Partiamo dal primo comma dell'art. 40 il quale recita che: "Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle **esigenze specifiche delle micro, piccole e medie imprese**". L'inciso dedicato specificamente alle PMI è di particolare rilevanza perchè dimostra come il Legislatore Europeo, nell'aver ritenuto applicabile tale norma a tutte le realtà societarie europee abbia compreso come sia impensabile, o quantomeno estremamente complesso, chiedere l'applicazione di standard articolati che solo realtà strutturate sono in grado di rispettare grazie alla loro organizzazione e alle loro risorse economiche. Detto questo,

le direttrici in tema di cybersecurity più significative da seguire per le PMI sono:

1. **Un cloud più "prudente"**: il titolare del trattamento del dato (data controller) è obbligato a scegliere un responsabile del trattamento del dato (data processor) che sia in possesso di idonee misure tecniche e organizzative volte alla protezione dei dati. Questo principio trova la sua applicazione nella scelta del fornitore cloud e nelle necessarie attività di audit di seconda parte successive all'instaurazione del rapporto commerciale con quest'ultimo.
2. **Cifratura**: nel limite di quanto è concretamente fattibile la cifratura e la pseudonomizzazione dovranno essere dei principi da applicare in ogni contesto aziendale.
3. **Privacy Impact Assessment**: in pratica dovranno essere messi in atto quell'insieme di processi funzionali al fine di realizzare, attraverso lo studio delle modalità di trattamento dei dati, un'analisi dei rischi e conseguentemente di individuare le misure idonee a neutralizzarli.
4. **Data Breach**: dal maggio del 2018 tutte le realtà aziendali italiane dovranno notificare entro 72 ore al Garante per la Protezione dei Personali, ogni violazione di dati personali subita all'interno del proprio sistema informatico.

Quest'ultimo aspetto è molto importante perché garantirà, in primis, di avere una più corretta percezione del fenomeno e, inoltre, obbligherà le società a investire direttamente o indirettamente sui processi di gestione degli incidenti informatici che sono alla base della sicurezza informatica.

In sostanza, l'articolo 33 del Regolamento impone ad ogni società l'obbligo di notificare all'autorità nazionale (nel nostro caso il Garante per la Privacy) qualsiasi violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata

Tale notifica deve:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione;
2. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Tutto questo in 72 ore. Ne discende che è necessario che tutte le aziende sono sostanzialmente "costrette" ad adottare una procedura che preveda tale notifica, soprattutto se si considera che tale notifica deve essere fatta anche in caso di distruzione o perdita di dati per cause differenti da un attacco informatico, come, ad esempio, il banale furto di un laptop di un dipendente che contenga dati personali di clienti o di dipendenti.

La cosa però più rilevante è che, nel caso in cui la violazione dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati, il Regolamento obbliga il titolare del trattamento a comunicare tale violazione anche a ciascun interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati personali.

La comunicazione del data breach all'interessato deve essere effettuata utilizzando un linguaggio semplice e chiaro e deve contenere un'accurata descrizione della natura della violazione dei dati personali, nonché suggerimenti e raccomandazioni su come poter attenuare i potenziali effetti negativi derivanti dalla violazione dei suoi dati personali. Tuttavia, si può essere esonerati dalla notifica all'interessato, ove:

1. a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione;
2. b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
3. c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. d) i contenuti delle comunicazioni violate sono interamente cifrati.

Sappiamo bene che l'ipotesi d) è avveniristica poiché la cifratura completa dei dati mette a dura prova l'operatività aziendale e quella c) è demandata alla valutazione ex post di un giudice. Rimane quindi da capire quali siano le misure idonee atte a scongiurare tale rischio. Il Regolamento 679/2916 ci viene in supporto stabilendo che "l'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (art. 32)". Pertanto, l'obiettivo è molto semplice: le aziende per evitare il rischio di un enorme danno reputazionale dovranno nel prossimo futuro adottare il codice di condotta che verrà presumibilmente stilato dalle associazioni di categoria e validato dal Garante della Privacy oppure affrontare un complesso meccanismo di certificazione (ad es. 27001 ISO/IEC). Vi sono ancora molti interrogativi su quali saranno gli standard che dovranno essere rispettati, ma un dato è certo: sicuramente questo tipo di approccio cambierà il volto di molte PMI in Italia ed è compito nostro accompagnarle verso un processo che sia effettivo, ma anche compatibile con le dimensioni e l'operatività aziendali.

Riferimenti:

Camilla Bistolfi, Luca Bolognini, Enrico Pelino, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, 2016

Franco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016

Adalberto Biasotti, *Il nuovo regolamento europeo sulla protezione dei dati*, EPC, 2016

A cura di: **Giuseppe Vaciago**