GDPR, il punto della situazione a sei mesi dall'entrata in vigore

intervista a Gabriele Faggioli, CEO di P4I | Presidente Clusit

A sei mesi dall'entrata in vigore del GDPR, quali considerazioni si possono fare sul suo recepimento in Italia?

Dal nostro punto di osservazione, sia accademico che professionale, possiamo dire che le grandi aziende italiane e internazionali hanno avviato in massa e, in parte, portato a compimento progetti di adeguamento al GDPR.

Ci sono interi settori di mercato che, considerando i player più rilevanti, hanno sicuramente fatto moltissimo.

Penso alle banche, alle assicurazioni, alle telco, al settore del fashion e del luxury.

Ma anche la grande distribuzione organizzata. Si tratta di settori di mercato ad altissimo numero di interessati dove, di conseguenza, l'adeguamento al GDPR era essenziale e mandatorio in considerazione anche dei potentissimi sistemi CRM che utilizzano. Da sottolineare che, per la prima volta, abbiamo visto un interesse e un intervento deciso anche da parte di aziende industriali, interessate soprattutto per motivi o di HR o di apparecchiature IoT, quindi connesse.

Completamente diversa è la nostra visione delle PMI e della pubblica amministrazione dove, per motivi diversi, gli interventi appaiono meno incisivi e strutturati.

Soprattutto per le PMI, il GDPR rappresenta un impegno normativo potenzialmente molto impattante e costoso, forse sovradimensionato.

Per questo motivo, per le PMI si dovrebbero adottare rapidamente provvedimenti di semplificazione, anche se sarebbe comunque consigliabile l'utilizzo di tecnologie informatiche esternalizzate, anche al fine di spostare il problema.

In ogni caso, a mio avviso questa terza tornata normativa (dopo la 675 del 1996 e la 196 del 2003) è quella della maturità: mai c'era stata una attenzione così ampia sul tema.

È interessante anche notare come sia cambiato l'approccio alla tematica: la presenza dei DPO oggi aiuta enormemente

a tenere sotto controllo i trattamenti e l'applicazione normativa.

Ma anche la pressione mediatica ha il suo ruolo. Fino a qualche anno fa erano pochissime le aziende con budget dedicati mentre oggi, nello strato alto delle imprese italiane e internazionali, è la regola.

La sicurezza informatica è un tema all'ordine del giorno al C-level e questo è un merito sia normativo che mediatico.

Perchè lei afferma che il GDPR piace più agli avvocati che agli ingegneri?

Perché il GDPR è soprattutto una norma di indirizzo che una norma prescrittiva. Devi fare l'analisi dei rischi, ma non dice come. Devi fare la DPIA, ma non elenca tassativamente quando. Puoi usare come base giuridica il legittimo interesse, ma non sono elencati i casi. Devi adottare misure di sicurezza adeguate, ma non sono elencate quali.

Si tratta quindi di una norma che lascia moltissimo spazio interpretativo e che permette anche applicazioni personalizzate

Per fare un esempio: fino al 25 maggio per tenere le immagini delle telecamere per più di sette giorni occorreva richiedere un'autorizzazione al Garante con tempi di risposta molto

lunghi. Oggi è invece possibile fare una valutazione di impatto e, in pochissimi giorni, fare scelte che prima avrebbero comportato molti mesi di attesa. Certo, senza certezza interpretativa ma con l'obbligo di fare valutazioni serie e approfondite.

Si sono riscontrate variazioni significative di segnalazioni di data breach in Italia da maggio a oggi?
Difficile fare confronti, perché fino al 25 maggio 2018 solo pochissimi soggetti pubblici e privati erano tenuti a notificare le violazioni. In ogni caso, l'obbligo di analizzare tutte le violazioni e di notificare quelle rilevanti pone un problema di gestione strutturata dei casi prima inesistente. Per fare un esempio, la sola perdita di un PC o l'inoltro di una mail a un soggetto sbagliato è un data breach. Come ovvia conseguenza, le casistiche sono tantissime e quotidiane. Per fortuna i casi gravi sono una minor parte ma, indiscutibilmente, i cittadini interessati da almeno un caso sono già stati tantissimi come, peraltro, viene affermato anche dal Garante.

È già possibile delineare una casistica di sanzioni comminate finora a livello europeo?
Ci sono state le prime sanzioni ma è per ora impossibile delinare un trend. Sicuramente, le Autorità si stanno muovendo con la mano leggera, per il momento.
Ma a tendere è probabile che prima o poi arrivi una sanzione veramente pesante. Personalmente, non penso che le sanzioni saranno mai punitive per i casi di interpretazione errata del GDPR quanto, invece, per trattamenti volutamente illegittimi. In ogni caso, quando si trattano i dati di milioni di cittadini in settori come la grande distribuzione organizzata, dove anche la numerosità dei dati oggetto di trattamento è veramente importante, il rischio sanzionatorio non può assolutamente essere sottovalutato.