MAG
95-12.02.18

DEBUTTO IN SOCIETÀ (per azioni)

Lo studio La Scala è il primo, tra i grandi player del settore, a tagliare il traguardo. I soci diventano azionisti. E nella governance entra anche il collegio sindacale

LA TERZA VITA di F2i

CERVED: l'ufficio legale sarà una LAW FIRM

BÄR & KARRER: ecco perché lavoriamo tanto con L'ITALIA

LEGALCOMMUNITY ENERGY AWARDS 2018

NUOVA PRIVACY, siamo **IN RITARDO**

MAG ne ha parlato con Maria Roberta Perugini, partner di Jacobacci. «Norme sottovalutate». Ecco come si dovrà procedere per adeguarsi. E gli studi legali non faranno eccezione

Il 25 maggio diventerà applicabile la nuova privacy europea. La sensazione però è che in Italia si sia già tutti in ritardo. In effetti, nel corso dell'anno e mezzo trascorso dall'entrata in vigore del GDPR, diversi organismi hanno effettuato ricerche per analizzare il livello di consapevolezza delle imprese e di attivazione per l'adeguamento.
I risultati sono sempre coerenti nell'evidenziare che, ancora oggi, più della metà degli operatori (soprattutto se Pmi) non ha reale consapevolezza dell'impatto della nuova normativa e non ha avviato azioni per adeguarsi.
Purtroppo si tratta di un problema rilevante. La nuova privacy è un tassello (insieme ad altri, ad esempio le misure per lo sviluppo delle infrastrutture digitali e quelle per l'incentivazione del commercio elettronico transfrontaliero) di un progetto molto più ampio per la creazione di un mercato unico digitale che la Ue ha definito, condiviso e perseguito sin dal 2015.
«Dobbiamo considerare la *compliance privacy* come uno strumento essenziale per sostenere e incentivare i nuovi modelli di sviluppo economico fondati sull'innovazione», dice in questa intervista **Maria Roberta Perugini**, partner di Jacobacci. «La trasformazione digitale crea nuovi mercati di sbocco e l'ampliamento di quelli tradizionali. Crea nuovi prodotti e servizi, nuovi processi di produzione e vendita, nuove relazioni nel mondo del lavoro».
La Ue, nella sua comunicazione di maggio scorso sulla revisione intermedia della strategia per il mercato unico digitale, ha sottolineato come il rispetto della vita privata e la protezione dei dati personali siano due condizioni che garantiscono la fiducia dei consumatori verso l'impresa e di conseguenza la stabilità, la sicurezza e la competitività dei flussi commerciali mondiali. «Le imprese che non riusciranno a realizzare la transizione sono inesorabilmente destinate a restare indietro», sottolinea l'avvocata.

Il GDPR va visto in questo contesto e ognuno deve fare la sua parte, compresi i legislatori nazionali, che hanno la responsabilità fondamentale di compiere interventi tempestivi sul quadro legislativo nazionale in un'ottica di armonizzazione con la normativa europea.
La legge di delega al Governo per adeguare il quadro normativo nazionale alle disposizioni del Regolamento è di ottobre scorso (quindi, già in grande ritardo sulla tabella di marcia) e prevede un termine di ulteriori sei mesi per l'emanazione di appositi decreti: in pratica, fino all'inizio di maggio.

«Un adeguamento **"standard"** è perfettamente **inutile**, a prescindere dai costi sostenuti per attuarlo. Il **25 maggio** è solo il **punto zero** di un percorso che **comincia** e che **continua** finché l'impresa opera trattamenti»

In attesa dei decreti delegati, però, alcune nuove disposizioni in materia sono state inserite nella legge europea 2017 e poi nella legge di Bilancio 2018, mentre un ulteriore specifico provvedimento a fine anno ha modificato la disciplina del registro delle opposizioni e dunque del telemarketing...
Sì, ma queste innovazioni, in parte perché sono intervenute su temi molto specifici e in parte per il contenuto perlomeno opinabile, certamente non stanno contribuendo a dare chiarezza e organicità al quadro normativo in materia e anzi – in alcuni casi – sembrano addirittura contrastare con specifiche norme del GDPR.

Che atteggiamento riscontra tra imprese e soggetti interessati?
Purtroppo, nella mia esperienza professionale constato che moltissime realtà imprenditoriali sono ancora oggi ignare del ruolo fondamentale giocato nello sviluppo economico dalle norme a protezione dei dati personali. Queste, anzi, assai spesso vengono sottovalutate, affrontate con un approccio formalistico e interpretate (con fastidio) come richiesta di adempimenti amministrativi aggiuntivi, privi di rilevanza sostanziale.

Bene, allora da cosa bisogna cominciare?
Dal convincersi che la soluzione è sviluppare una reale capacità di *data governance*. Moltissime organizzazioni non hanno consapevolezza effettiva della mole dei dati che trattano e delle loro caratteristiche, e neppure

sanno con esattezza dove sono archiviati e da chi e come sono utilizzati... È chiaro che in queste condizioni non solo non è possibile alcuna efficace gestione del rischio di *data breach*, ma neppure vi sono i presupposti per effettuare quel salto di qualità nella gestione delle informazioni aziendali.

E quindi?
La prima cosa da fare dunque è un'analisi approfondita dell'azienda. I risultati di questa analisi sono la base per verificare il livello di conformità effettivo dell'ente al GDPR e per individuare le azioni da assumere al fine di raggiungere una conformità piena (*gap analysis*), e ciò sia sotto il profilo della sicurezza sia sotto quello documentale e organizzativo.

E a questo punto?
Una volta individuati i propri obiettivi di *accountability*, l'impresa deve definire un primo piano per soddisfarli. A conclusione di questi passaggi, l'impresa sarà in grado di produrre il proprio modello di gestione privacy. A questo punto – e solo a questo punto – dovranno e potranno essere operate le azioni concrete volte all'attuazione degli specifici interventi individuati, diretti alla implementazione del modello di gestione privacy aziendale.

Esiste un modello valido per tutti?
Un adeguamento "standard" è perfettamente inutile, a prescindere dai costi sostenuti per attuarlo. Il 25 maggio è solo il punto zero di un percorso che comincia e che continua finché l'impresa opera trattamenti. È importante la partecipazione attiva dell'ente alla progettazione e attuazione di un percorso personale di conformità, anche condotto con il supporto di consulenti esperti, costituisce l'ottimale strumento per giungere a gestire in autonomia la compliance nel continuo.

Adeguarsi sarà costoso? E quanto?
Certamente, operare per la compliance comporta dei costi. Ma è l'unico strumento per mitigare il rischio di sanzioni che con il GDPR possono arrivare fino a 20 milioni di euro o – se superiore – al 4% del fatturato mondiale annuo di gruppo.

Chi è il Dpo? Cosa fa?
Possiamo dire che il Dpo è una "misura di sicurezza": questa figura è esplicitamente prevista e regolamentata dal GDPR. È uno strumento fondamentale dell'*accountability*, il "direttore d'orchestra" del sistema di trattamento aziendale.

«A mio parere è necessaria una **competenza multidisciplinare**, che però ad oggi è estremamente **difficile da trovare** in una sola persona: credo che per il momento si affermerà maggiormente la scelta di costituire un *team*, magari guidato da un legale con **esperienza** in materia di *privacy* ma che comunque annoveri anche altri componenti, perlomeno con competenze informatiche, di ***cybersecurity*** e di ***governance*** **aziendale**.»

Lo deve fare l'avvocato? Il general counsel? Un tecnico?
Può essere un individuo o un team, così come in house o esterno, nominato sulla base di un contratto di servizi. La mia impressione è che, per il ruolo chiave che assume nell'ottica della conformità dell'ente, le realtà più complesse, non possano prescindere dall'avere un Dpo dedicato, e pertanto interno.

Con quali competenze?
A mio parere è necessaria una competenza multidisciplinare, che però ad oggi è estremamente difficile da trovare in una sola persona: credo che per il momento si affermerà maggiormente la scelta di costituire un team, magari guidato da un legale con esperienza in materia di privacy ma che comunque annoveri anche altri componenti, perlomeno con competenze informatiche, di cybersecurity e di governance aziendale.

Anche gli studi legali dovranno provvedere?
Gli studi legali operano trattamenti di dati personali come e più degli altri enti: certamente devono adeguarsi alla nuova normativa e ritengo che abbiano particolare interesse a farlo, visto che custodiscono le informazioni più preziose e riservate dei loro clienti. Anche tra gli studi legali vige la stessa regola delle imprese: chi ha consapevolezza dei rischi e delle opportunità legati all'innovazione, considera l'adeguamento al GDPR una priorità e un'opportunità; chi al contrario non ne è consapevole, si gira dall'altra parte o si limita a un adeguamento formale.

E sono pronti, gli studi?
Bisogna capire innanzitutto che la sicurezza non è solo un tema di *cybersecurity*, che pure è un aspetto essenziale: la sicurezza, prima ancora che dalla tecnologia, passa attraverso la conoscenza e il controllo dei propri processi di trattamento. È inutile avere a disposizione sofisticati firewall quando si consente ai collaboratori di utilizzare il proprio pc personale per accedere ai server, di navigare con device personali sulla wifi di studio senza un'adeguata configurazione degli accessi o di collegare al pc di studio hard disk esterni non autorizzati.

Per i consulenti sarà un buon filone di business. Ma per svolgere un'adeguata attività serviranno competenze multidisciplinari o è un lavoro solo per avvocati?
Un servizio di consulenza efficace in questo campo deve sapere collegare aspetti legali e possibili soluzioni tecniche e organizzative, per mettere l'azienda in grado di identificare gli interventi necessari assegnando le relative responsabilità, pianificare e ottimizzare gli interventi. È ovvio che per tutto questo sia necessario un approccio multidisciplinare (legale, governance, tecnico, organizzativo) e olistico che è nuovo con riferimento alla compliance privacy ma che non è esattamente assimilabile neppure alle attività di adeguamento ad altre normative.

Insomma, l'avvocato da solo non basta più?
Non basta più, così come il tecnico informatico, anche se esperto di cybersecurity, e l'esperto di governance aziendale: tutti però sono elementi essenziali e la stretta collaborazione tra di essi e i referenti aziendali, che sono i veri attori del trattamento, è la chiave per una consulenza di successo. ■