PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3784 di giovedì 19 maggio 2016

Il nuovo GDPR: quando "investire" diventa "sprecare"

E' nuovo di pacca: il nuovo Regolamento Europeo sulla Protezione dei Dati Personali, conosciuto con il nome di GDPR, è sbarcato in Europa, e porta con sé molti quesiti e dubbi. Di Eleonora Bottonelli.

Il 25 e il 26 maggio 2016 esperti mondiali di settore, legislatori, autorità ed esponenti di multinazionali si sono incontrati a Berlino durante l'EDPD, per avviare una discussione su alcune sfumature non ancora chiare.

Opportuno sarebbe analizzare tre punti chiave, tra i tanti trattati: la natura del Regolamento, la nuova figura del DPO e le implicazioni pratiche nel giro di due/tre anni. Queste ultime hanno, infatti, avuto ben poco spazio nei dibattiti, che hanno assunto più una forma tecnico-legale ad uso e consumo degli uffici legali delle multinazionali che, si ricorda, sono una minima percentuale delle attività che saranno coinvolte dall'entrata in vigore del Regolamento.
Procedendo con ordine: alcune affermazioni nel Regolamento rimangono generiche e hanno sollevato alcune perplessità; si afferma infatti che l'onere della prova spetta alle aziende, che devono dimostrare di aver attuato "tutte le misure adeguate, ragionevoli e necessarie" in maniera documentale.

Questo approccio appartiene alla Common Law più che alla Roman Law a cui siamo abituati. Di base le nostre leggi si limitano a una lista di "non fare", che sottintendono che tutto ciò che non è scritto è permesso se non altrimenti specificato, con tutti i difetti del caso.
Mentre il Sig. Albrecht, un parlamentare europeo, afferma risolutivamente "E' una legge, non una linea guida!", molti altri ospiti dell'EDPD non sono stati così zelanti: un ufficiale dell'Interpol ha infatti espresso perplessità sulla reale possibilità di applicare, nella realtà, una regola così generica (chi stabilisce infatti cosa è "adeguato, ragionevole e necessario" ?).

Secondo punto: la nuova figura del DPO (Data Protection Officer).
Mai occasione più propizia per vedere i movimenti interni a questo settore: all'EDPD è stato chiaro che molti si stanno già muovendo per questa nuova Caccia all'Oro. Che questo sia un bene o un male è ancora troppo presto per saperlo, ma il rischio è che qualcuno ci lasci la carriera: il DPO è una figura di taglio dirigenziale che avrà il compito di essere il "cattivo" di turno. Non solo sarà il responsabile per l'Impact assesment e della reale attuazione del programma di Protezione dei Dati, ma risponderà sia all'azienda, sia ai Garanti, anche attraverso i cosidetti "whistle blowing" (segnalazioni anonime dei dipendenti di ipotetiche violazioni dei colleghi).
Nel caso di pubbliche amministrazioni sarà responsabile anche verso i cittadini, che potranno rivolgersi a lui per questioni riguardanti l'uso dei propri dati personali. Ciliegina sulla torta: il DPO si prende tale impegno come persona fisica.

Queste considerazioni sottendono alcuni risvolti sociali e di mercato, non molto prese in considerazione all'EDPD.

Il GDPR non è solo una legge, ma una vera e propria rivoluzione legale e sociale (in un mondo sempre connesso, la regolamentazione a protezione dei dati era solo questione di tempo).
Tutto ciò sarebbe magnifico, se non fosse che l'Europa (sistema anglo-sassone escluso) non è pronta per un tale cambio di mentalità: andando a parlare con piccole e medie imprese come Consulente, ci si accorge immediatamente che nessuno sa di cosa si stia parlando. Si pensa che la sicurezza dei dati e della loro integrità sia un problema di "IT e computer", e dicono, o

pretendono, di non avere i soldi per fare gli investimenti richiesti.
In due anni la legge entrerà pienamente in vigore: ci saranno una miriade di procedimenti in tribunale e di multe salate, e molte aziende potrebbero chiudere per questo (le sanzioni possono arrivare al 4% del fatturato o 20 milioni di euro). Per citare uno dei tanti avvocati presenti all'EDPD: "Sarà la nostra fortuna".
Non c'è alcuna educazione in questo settore, nessuna conoscenza di base, e improvvisamente il verbo "investire" del Garante Europeo Buttarelli diventa il verbo "sprecare" delle piccole e medie imprese, che vedranno questo nuovo meccanismo come un'ennesima tassa da pagare con il sangue, non sapendo che invece è stato studiato per aiutare anche i processi interni e migliorare le performance.
Quando questo accadrà, vi sarà un ennesimo motivo di malcontento verso le istituzioni europee da controllare, con i prevedibili risvolti politici non da sottovalutare.
Un modo per evitare, o almeno contenere, tutto ciò potrebbe essere organizzare dibattiti pubblici sull'argomento, creando, in parallelo, dei fondi ad hoc e una migliore via di comunicazione tra le istituzioni Europee, le piccole/medie imprese e i cittadini. Queste ultime due categorie, infatti, non possono usufruire di un ufficio legale come le multinazionali.

Eleonora Bottonelli

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Direttiva (Ue) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

---