PRIVACY/ Da oggi in vigore il regolamento Ue: ecco i dieci errori da non commettere

Responsabili dati, non tuttofare

Sanzioni per mancato adeguamento? Nessuno stop

DI ANTONIO CICCIA MESSINA

Il responsabile della protezione dei dati non è un factotum; le sanzioni non sono sospese; il responsabile esterno non è il Dpo. Sono alcuni degli scivoloni che possono capitare nei primi giorni di operatività del Regolamento Ue sulla privacy, che oggi è all'esordio. Nonostante l'assenza di un decreto italiano di coordinamento. E proprio mentre il Gdpr muove i suoi primi passi, **Antonello Soro**, presidente del Garante per la protezione dei dati, ieri a Bologna durante la convention dei Responsabili della protezione dei dati, fa un appello al parlamento: si faccia in fretta a mandare avanti lo schema di decreto attuativo della legge 163/2016. «L'idea che», ha detto Soro, «da domani ci possa essere una sopravvivenza di norme sulle quali il legislatore è in cammino, non va bene». E potrebbe continuare a causare errori. Come i dieci che analizziamo qui di seguito e che sono ovviamente da evitare fin da subito.

FORMALISMI

Dappertutto si sente dire che il Regolamento ha un approccio basato sul rischio. Seguendo questa impostazione vanno privilegiate scelte da cui deriva un incremento di sicurezza delle reti, dei dispositivi, dei locali e così via. Meglio avere una buona sicurezza e una buona organizzazione. Un errore è scambiare la privacy europea con la stesura di moduli e moduli. Un comportamento virtuoso è dotare i propri uffici, computer, server di sistemi di protezione fisica e tecnologica.

TECNICISMI

Un errore è di pensare che la disciplina della protezione dei dati sia solo un problema di sicurezza informatica. La sicurezza informatica è certamente importante, ma è solo un corno del problema. Posso avere un sistema informatico sicuro e custodire dati inesatti e, quindi, violare clamorosamente la privacy. La privacy è preoccuparsi dell'effetto che fa l'uso dei dati sulla vita delle persone, è attivare condotte virtuose e rispettose.

INFORMAZIONI

Sotto la vigenza del Codice della Privacy (dlgs 196/2003) si parlava di informative e si citava, appunto, questo decreto legislativo. Lasciare a disposizioni degli interessati modelli di informativa contenenti quel riferimento può essere indicativo della mancata presa in esame del regolamento europeo. Di per sé avere un modello di informativa buono nei contenuti, anche se con un riferimento normativo scorretto non è di per sé invalidante. Peraltro le informazioni devono essere, appunto, esaustive nel merito. Meglio correre ai ripari e inserire i riferimenti giusti e anche le informazioni in linea con il regolamento.


Antonello Soro

RESPONSABILI INTERNI

Sulla scorta delle norme del codice della privacy, enti pubblici e privati hanno nominato responsabili interni del trattamento. Si tratta di una organizzazione che non ha più ragion d'essere con questa denominazione. L'organizzazione può mantenere centri interni di imputazione di attività. Ma non bisogna continuare come se nulla fosse.

RESPONSABILI ESTERNI

Non sono da confondere con il responsabile della protezione dei dati. Hanno compiti diversi: solo i responsabili esterni trattano dati per conto del titolare.

AUTORIZZATI AL TRATTAMENTO

I vecchi incaricati del trattamento non si chiamano più così. Si chiamano autorizzati al trattamento. Meglio ricordarsene nei moduli in preparazione.

DPO

Il responsabile della protezione dei dati (Rpd, all'italiana, Dpo all'inglese) è una figura importante, ma non è un factotum. Nominare un Rpd e affidargli tutta la privacy vuol dire non aver compreso bene il suo ruolo. Il Responsabile della protezione dei dati non è un gestore degli adempimenti privacy, ma è un soggetto che informa, consiglia, ma anche sorveglia. E non può sorvegliare se stesso per non essere in clamoroso conflitto di interesse. In questo ultimo mese di maggio 2018, si sono viste procedure di gara per l'affidamento contemporaneamente degli adempimenti per l'adeguamento al regolamento europeo sulla protezione dei dati e per la funzione di responsabile della protezione dei dati. Si tratta di un approccio criticabile, proprio alla luce dell'obbligo di evitare il conflitto di interesse: il Rpd non può valutare se ha condotto un buon adeguamento del trattamento dei dati. Altro errore è assumere come Responsabile della protezione dei dati un soggetto esperto, tanto per coprire una casella. Il responsabile della protezione dei dati deve sapere quello che fa, altrimenti si espone a responsabilità.

RESPONSABILITÀ DEL RPD

Si sente dire e si legge che il Responsabile della protezione dei dati non è responsabile. Attenzione a non fraintendere. L'affermazione è vera se si vuol sostenere che il Responsabile della protezione dei dati non è il parafulmine del titolare del trattamento, che rimane l'unico responsabile per le violazioni del regolamento Ue. Ma attenzione un cattivo consiglio o un cattivo parere del responsabile della protezione dei dati espone quest'ultimo a responsabilità contrattuale nei confronti del titolare.

AMMINISTRATORI DI SISTEMA

Un errore è pensare che siccome non sono nominati dal Regolamento Ue sono da licenziare.

Tutti i presidi della sicurezza sono validi ai fini della dimostrazione del proprio grado di responsabilizzazione.

SANZIONI

È un errore pensare che tanto il Garante per sei mesi non applicherà sanzioni. È una falsa notizia: se al Garante arriverà una notizia di illecito non potrà che esercitare i poteri assegnati dal Regolamento, a prescindere dall'eventuale sospensione del provvedimenti del 22 febbraio 2018 sul monitoraggio.

IN ITALIA CI SI LAMENTA DEGLI ADEMPIMENTI. MA IN USA SONO PIÙ STRINGENTI ANCORA

In California data protection super-rafforzata

La data protection in California è ancora più protection. Nel paese della Silicon Valley, infatti, la privacy dei consumatori è una cosa talmente seria che i consumatori residenti possono contare su garanzie più stringenti rispetto ai consumatori europei e quindi- considerando il livello già molto alto della protezione Ue, ai consumatori dell'intero globo terrestre.

Spigolando nella privacy policy di una notissima piattaforma di mail marketing, è possibile leggere una clausola «unica», destinata esclusivamente ai californians. Gli utenti delle piattaforme digitali che sono residenti in California infatti possono ottenere, per giunta per iscritto, non solo la lista dei dati personali che la piattaforma trattiene ma anche le tipologie dei servizi offerti ed accettati che la piattaforma comunica a terze parti per campagne di marketing proprie di quest'ultima. Non solo. Le piattaforme sono costrette - su richiesta degli utenti - anche a dare nomi e indirizzi delle società terze, indicando chiaramente a quale mail inviare la richiesta.

Una disclosure piena del tragitto del dato personale, che è stato magari depositato con consapevolezza su di una piattaforma, ma poi segue percorsi indiretti e incontrollabili dal suo titolare se non perdendo tantissimo tempo nella lettura della valanga di informative che formalmente tutte le aziende sono costrette a inviare.

In questo caso, il Gdpr non c'entra visto che la questione riguarda un paese extra Ue. Ma qui val la pena di evidenziare, curiosamente, che la normativa dello Stato della California, che offre natali e sede ai più disruptive brand digitali, è quella decisamente più stringente a tutela dei propri cittadini.

E non è finita qui. La California ha dichiarato di volersi adeguare al Gdpr e prevede di approvare the Consumer right to privacy act 2018 entro novembre.

Se le aziende italiane state piangendo calde lacrime per i nuovi adempimenti richiesti dal Regolamento europeo, che entra in piena efficacia proprio oggi, possono consolarsi. Qualcuno laggiù in Silicon Valley sta già tremando.

Claudia Morelli