ItaliaOggi Sette

Il 25 maggio diventa pienamente operativo il regolamento 2016/679 (Gdpr). Fra i dubbi

Privacy a norma Ue al debutto Obblighi e sanzioni? Un puzzle

Pagine a cura
DI ANTONIO CICCIA MESSINA

Il 25 maggio 2018 comincia l'era della privacy europea. Il regolamento Ue 2016/679 diventa operativo. Diventano operative le norme sugli adempimenti e sulle sanzioni. Ma i lavori legislativi sono ancora in corso.

A dire il vero, molte cose sono applicabili in un quadro di norme compiute e definite. Ma ci sono anche tante altre cose per cui il legislatore o il Garante della privacy devono ancora scrivere regole.

Si tratta di pezzi importanti della disciplina della protezione dei dati. Primo su tutti, le semplificazioni per le Pmi. Dappertutto si legge che per le piccole e medie imprese la normativa sarà ritagliata e ridotta e adeguata alle relative dimensioni. Il problema è che è stato usato tanto inchiostro per scrivere che queste semplificazioni si faranno, e neanche una goccia per scrivere quali sono queste semplificazioni.

Il richiamo è fatto, naturalmente, ai legislatori e non alle autorità garanti.

È il legislatore che deve indicare le scelte di minimizzazione dell'impatto economico della normativa privacy sulle realtà economiche piccole. Realtà, queste, dalle quali non sono venuti, statisticamente, grossi rischi per la privacy delle persone. Altro settore che andrà seguito negli stessi termini è quello degli studi professionali. Qualche cosa è stato detto per gli studi individuali (sia con riferimento alla esclusione della nomina del responsabile della protezione dei dati sia per altri adempimenti, come la valutazione di impatto privacy). Ma, come per le Pmi, ci sono spazi per ulteriormente adeguare la normativa alla dimensione, ad esempio, di un piccolo studio associato.

Ci sono, poi, altri adempimenti e altri istituti, in cui il Regolamento è intervenuto e ha dettato le regole di principio, lasciando il dettaglio ai singoli operatori, i quali si trovano a dover decidere, nel loro caso concreto, la portata pratica di norme generalissime. E, quindi, il regolamento è certo formalmente applicabile, ma da un punto di vista sostanziale si mette l'operatore in grosse difficoltà.

Facciamo un esempio. C'è la regola per cui le misure di sicurezza devono essere adeguate. La norma è compiuta, esprime un principio generale e, da questo punto di vista, non manca di nulla (articolo 32).

Passiamo, però, alla concreta attuazione. Sarà la singola impresa a dover dire se è adeguato, per accedere ai computer aziendali e alla rete aziendale, una credenziale basata sulla parola chiave o se ci vuole una autenticazione forte (biometria, token ecc.).

Ancora un altro caso. C'è un'altra regola che dice che chi tratta dati sensibili o biometrici o genetici «su larga scala» deve nominare un responsabile della protezione dei dati. Come prima, la norma è compiuta, esprime un principio generale e, da questo punto di vista, non manca di nulla (articolo 37). Passiamo, però, alla concreta attuazione. Sarà la singola impresa a dover dire se i suoi trattamenti interessano o no una larga scala. E sarà giudicata per questo, anche con sanzioni amministrative pesanti.

Di fronte a questo, l'approccio giusto e sulla stessa lunghezza d'onda del regolamento europeo, è l'approccio basato sul rischio. Traduciamo. Si cerchino i possibili buchi nella rete, i focolai di possibili incendi. Altrimenti detto: si individui dove i dati personali conservati possano essere attaccati o possono subire un danno perché soggetti a smarrimento. Si intervenga a diminuire quel rischio e si cominci a costruire attorno un apparato documentale. Cominciare dalla sicurezza è un metodo assolutamente compatibile con il progetto del regolamento, che pretende di progettare la privacy e di avere la privacy come impostazione predefinita nella organizzazione dell'ente pubblico o dell'impresa.

La minimizzazione del rischio di perdita o di attacco ai dati significa mettere al riparo le persone, la cui identità è disegnata da quei dati. Siamo in un'epoca in cui lo sparpagliamento delle informazioni, senza alcuna prevedibilità e senza alcuna possibilità di controllo, mette le informazioni (cioè l'identità) di ogni persona nelle mani di tantissime persone. Questo a causa della cosiddette rete, che è uno strumento per collegare, ma anche uno strumento per catturare.

Gli operatori economici e gli enti pubblici possono usare i dati delle persone, molto spesso anche senza il loro consenso, ma devono «pagare» questa disponibilità con i doveri di custodia dei dati. Posso trattare i tuoi dati (perché il diritto di una persona sui suoi dati non è assoluto), ma devo proteggere i tuoi dati. Lo pretende la funzione sociale delle attività economiche, lo pretendono i principi di buon andamento e imparzialità dell'attività amministrativa.

Il dovere di custodia dei dati ha ricadute sul piano della responsabilità per danni, la quale non a caso, prevede a carico dell'operatore economico e dell'ente pubblico l'onere di provare la propria «innocenza» e cioè che il danno non è loro imputabile.

Questo quadro, di valori e di obiettivi, sostiene lo sforzo che imprese sono chiamate a fare, barcamenandosi tra norme che presentano ancora tanti buchi come una groviera.

ItaliaOggi Sette

I casi aperti e i chiarimenti necessari

Principi	Legittimo interesse/norma molto vaga	Esempi concreti per poter determinare se si può omettere di chiedere il consenso
	Dati particolari/norma vaga nella parte in cui si riferisce a dati resi manifestamente pubblici	Chiarire portata operativa della disposizioni
	Accesso	Chiarire se sono accessibili i risultati delle profilazioni
	Rettifica	Chiarire se sono rettificabili i dati valutativi
	Trattamento unicamente automatizzati	Chiarire cautele per le particolari categorie di dato
Responsabile del trattamento	Clausole contrattuali	Chiarire quando saranno disponibili le clausole contrattuali tipo
Registri del trattamento	Soggetti esonerati	Chiarire che cosa significa trattamento occasionale o trattamento non rischioso
Valutazione di impatto privacy	Soggetti tenuti/soggetti esonerati	Chiarire quando saranno disponibili gli elenchi dei soggetti obbligati e non obbligati
Dpo	Criteri di nomina obbligatoria	Precisare in concreto quando ricorre la larga scala del trattamento
	Conflitto di interesse	Fare elenco delle posizioni di conflitto di interesse
Certificazioni	Casi e modalità	Precisare quando si avvierà il sistema delle certificazioni
Sanzioni amministrative	Vaghezza della forbice edittale	Precisare termini della graduazione in concreto

Dieci domande al regolamento Ue

Uno studio medico con tre professionisti deve nominare il Dpo?
Il commercialista che tiene la contabilità aziendale deve essere nominato responsabile esterno del trattamento?
Quando c'è larga scala ai fini della nomina di Dpo?
Quando ci sarà lo schema tipo della designazione di responsabile esterno?
I componenti dell'organismo di vigilanza (dlgs 231/2001) possono essere nominati Dpo?
Quando ci sarà l'elenco dei casi in cui non si deve scrivere la valutazione di impatto privacy?
Chi è esonerato dalla tenuta del registro dei trattamenti?
Quali sono i casi di legittimo interesse?
Il medico può scegliere se chiedere o non chiedere il consenso?
Posso tenere l'amministratore di sistema?