

VIVIANA DALOISO

Il conto alla rovescia è finito. E se – al netto delle notizie che negli ultimi mesi hanno avuto più risonanza mediatica, in primis lo scandalo Cambridge Analytica e l'uso che dei nostri dati personali fanno i social network come Facebook – la percezione del cambiamento è quasi inesistente tra i comuni cittadini, l'Europa delle aziende e delle pubbliche amministrazioni è in fermento per la rivoluzione del nuovo Regolamento sulla protezione dei dati personali.

Il giorno della svolta è domani: da quando, cioè, a dettar legge in tutti i Paesi membri sarà il nuovo principio di "responsabilizzazione" (il termine tecnico inglese è *accountability*) di chiunque effettui operazioni di trattamento dei dati personali altrui nell'ambito della propria attività. Niente di teorico, visto che per la prima volta il "tradimento" della suddetta responsabilità – con tutti i cavilli previsti dalla normativa – comporterà sanzioni fino a 20 milioni di euro per i singoli o fino al 4% del fatturato totale annuo per le imprese. E questo indipendentemente da dove si trova la sua sede legale: le multe, cioè, saranno indirizzate anche a chi lede la privacy dei cittadini europei con server posizionati Oltreoceano o nel lontanissimo Oriente. Una prassi comu-

Multe, denunce, diritto all'oblio Ecco la nuova privacy europea

Al via domani il Regolamento sulla protezione dei dati

ne fino a ieri, specie tra i colossi del web, per sgusciare facilmente tra le cause impugnando deboli legislazioni locali.

Il motto del nuovo Regolamento europeo, d'altronde, è "la persona al centro". Col suo diritto sacrosanto – da difendere, rispettare e anche da imparare – alla privacy. L'utente deve innanzitutto essere informato «in modo semplice e chiaro» sulle finalità, le modalità e l'ambito dei trattamenti dei dati per cui presta consenso: un capitolo che ha costretto la quasi totalità delle aziende a riformulare questionari e newsletter di prassi, quando non a riformularli *ex novo*. Sempre lui, l'utente, può revocare in qualsiasi momento il proprio consenso, può fare richiesta di cancellazione dei pro-

Utenti al centro e nuove responsabilità per le imprese e i colossi dei social. Largo alla figura del "controllore" nelle imprese. Tutti i ritardi italiani

pri dati qualora vengano utilizzati illecitamente (anche dai motori di ricerca come Google), può presentare denuncia all'autorità nazionale se reputa che siano stati violati (e la

stessa autorità deve rispondergli, entro tre mesi). E ancora: deve essere informato tempestivamente delle eventuali violazioni dei propri dati, per cui – anche questa una novità dirompente – ogni titolare del trattamento è tenuto ad adottare misure tecniche e organizzative che tutelino i principi di protezione dei dati (crittografia, controllo degli accessi, sorveglianza degli archivi...). A tal fine, d'altronde, è stata istituita la figura del "Dpo", il responsabile della protezione dei dati, una figura esterna alla struttu-

ra dell'azienda che possiede esperienza e competenza nel campo della privacy e che deve occuparsi della applicazione della normativa: una sorta di "controllore" insomma, la cui consulenza diventa fondamentale in ogni ambito per evitare le sanzioni salatissime previste dal Regolamento.

Adeguarsi a tutte le nuove norme – compresa quella delicatissima della tutela della privacy dei minori, che per utilizzare servizi online d'ora in poi avranno bisogno dell'autorizzazione dei genitori fino ai 16 anni – è complicato, nonostante l'entrata in vigore del Regolamento sia stata annunciata la prima volta a fine 2015. Molti i Paesi membri in ritardo tra cui figura – anche se per una volta non fra le ultime posizio-

ni – l'Italia. In particolare il nostro Paese, complice la situazione politica ancora incerta, paga lo scotto di non aver ancora adottato attraverso il voto del nuovo Parlamento le misure nazionali relative al Regolamento. In sostanza, cioè, manca il decreto attuativo che permette l'entrata in vigore ufficiale delle nuove norme e la sostituzione del vecchio Codice della privacy, datato 2003. E che dunque resta in vigore.

Mentre però le medie e grandi imprese – con centinaia di dipendenti, pc e smartphone aziendali, presenza di server, conservazione di banche dati, presenza di videosorveglianza – sono avvantaggiate nel mettersi in pari con le nuove norme, le situazioni più critiche riguardano le piccole realtà e in particolare i commercianti (che fino ad ora non avevano adottato particolari strategie di trattamento dei dati dei propri clienti) e il mondo della sanità, con la sua mole enorme di dati sensibili da tutelare e diversificare e le incombenze pratiche quotidiane legate alla salute e alla vita dei pazienti. Esemplificativa la richiesta di chiarimento avanzata proprio qualche giorno fa dal Sindacato dei medici italiani (Smi) al Garante della Privacy «affinché vengano precisati alcuni nodi irrisolti» dell'applicazione del Regolamento: «Siamo medici, non burocrati» l'obiezione.

I punti chiave



IL DIRITTO ALL'OBLIO

Sparire si può (anche da Google)

Se i dati personali vengono utilizzati illecitamente si può fare richiesta di cancellazione, e questa norma si applica anche ai motori di ricerca. La cancellazione non trova applicazione quando si scontra con il diritto di cronaca e informazione.



LE SANZIONI

Chi sbaglia paga cifre da capogiro

Nel caso in cui si ritenga che i propri diritti siano stati violati, si può presentare denuncia all'autorità nazionale. Che dovrà indagare e rispondere entro 3 mesi. Le aziende responsabili di violazioni potranno essere multate fino al 4% del loro fatturato totale annuo.



LA REVOCA

L'utente può cambiare idea

Si può revocare il proprio consenso all'utilizzo dei dati personali in qualsiasi momento contattando il responsabile del trattamento dati. Nelle newsletter, in particolare, è obbligatorio inserire un link che permetta all'utente di cancellarsi in ogni momento.



IL CONSENSO

Chiarezza nei moduli da compilare

La richiesta di utilizzo dei dati personali deve essere fatta in modo chiaro e fornendo varie informazioni, tra cui il contatto del responsabile della loro protezione (il "Dpo") e le misure di sicurezza in vigore per proteggerli da eventuali attacchi.



LA TUTELA DEI MINORI

Online serve la firma dei genitori

Per accedere ai servizi della società dell'informazione (come i social network) e prestare il proprio consenso al trattamento dei dati i minori di 16 anni necessitano dell'autorizzazione dei propri genitori. Alcuni Paesi potrebbero portare il limite a 13.



IL RESPONSABILE DEI DATI

In tutte le aziende entra il "Dpo"

Nelle imprese che trattano dati su larga scala e che operano nella pubblica amministrazione scatta l'obbligo del "Dpo", il responsabile della protezione di dati, una figura esterna che vigila sulla applicazione del Regolamento e forma il personale.

L'intervista

L'impegno di Soro nell'allineare le nostre norme a quelle europee: «Ora tocca al Parlamento» Forse già oggi il voto

Un ritardo colmabile. E una sfida da vincere, perché in ballo c'è «la protezione della libertà nella società digitale». Sono giorni febbrili per il Garante della Privacy, Antonello Soro, chiamato a districare gli ultimi nodi interpretativi del Regolamento europeo e mettere in pari un'Italia avvantaggiata grazie alla «lungimiranza» del suo Codice Privacy. **Presidente, a che punto siamo con l'attuazione delle norme? Manca ancora il decreto attuativo delle nuove regole: può spiegare che cosa comporta questa lacuna e che cosa ha fatto il Garante per colmare il ritardo?**

Attualmente, lo schema di decreto legislativo di adeguamento è all'esame delle Commissioni parlamentari per l'espressione del prescritto parere, che dovrebbe proprio avvenire oggi, o – è un auspicio che rinnovo – in tempi rapidi. Naturalmente il Garante non può colmare le lacune legislative o comunque supplire all'assenza di norme pri-

COSA CAMBIA PER GLI UTENTI SOCIAL

I principali contenuti del Gdpr Ue sulla privacy

16 anni

Chi ha meno di 16 anni dovrà avere un genitore o un tutore che acconsenta, a suo nome, ai termini di utilizzo

13 anni

I Paesi membri dell'Ue possono decidere l'età limite per questo passaggio abbassandola fino ai 13 anni

FACEBOOK si è già adeguato: i giovani tra i 13 e i 15 anni devono avere il consenso di un genitore per usare il social

- Il sistema di controllo prevede che l'under16 indichi il contatto sul social o l'indirizzo email del genitore che darà il consenso
- Senza consenso i minori vedono una versione meno personalizzata della piattaforma, con condivisione limitata e annunci meno rilevanti
- Facebook vieterà il riconoscimento facciale a chi ha meno di 18 anni

MESSENGER

La chat di Facebook sta chiedendo agli utenti di aggiornare le impostazioni sulla privacy. Anche qui sarà implementata la soglia dei 16 anni

TWITTER

Anche "l'uccellino azzurro" ha iniziato ad aggiornare i suoi termini di servizio per allinearsi al Gdpr

- Sui minori ha innalzato da 13 a 16 anni l'età minima richiesta agli europei per usare Periscope, il servizio per fare dirette video

SNAPCHAT

La chat di messaggi che scompare richieste, per registrarsi, una mail o un numero di cellulare, ma l'età non viene chiesta

INSTAGRAM

La chat, anch'essa della galassia Facebook, ora consente all'utente di chiedere una copia di tutto quanto ha condiviso sulla piattaforma (foto, video, messaggi). Il limite d'età non è stato aggiornato e al momento resta fermo a 13 anni

WHATSAPP

La chat, sempre di proprietà di Facebook, richiederà un'autorizzazione ai genitori di ragazzi tra i 13 e i 15 anni, ma solo nell'Ue

- In mancanza dell'ok dei genitori, in teoria chi ha meno di 16 anni non potrà utilizzare la chat

TELEGRAM

La chat "a prova di intrusione" in fase di registrazione chiede solo il numero di telefono. Per il momento non sono stati fatti annunci di conformità al Gdpr



Antonello Soro

sta creando un business attorno alla privacy e a queste nuove figure professionali, spesso non abbastanza qualificate. C'è chi promette pacchetti di messa in sicurezza a 19,99 euro per le imprese, su Internet...

Il "Dpo" è una figura centrale nel sistema delineato dal Regolamento: in quanto chiamato a supportare il titolare nelle scelte strategiche sul trattamento, da lui dipende la "scommessa" della responsabilità sulla protezione dei dati. Gli è ascritta una vera e propria funzione di garanzia rilevante anche, per certi versi, sotto il profilo pubblicitario, dovendo assicurare la tutela dei dati dei cittadini, fungendo da referente tanto per loro quanto per il Garante. La qualificazione professionale è dunque indispensabile. Quello del "Dpo" tuttavia non può essere inteso come un "mestiere": è una funzione, anche di rilievo essenziale.

Viviana Dalloiso

Il Garante: «All'Italia manca ancora il decreto attuativo»

Quale svolta nella nuova normativa? «I diritti delle persone sono fortemente rafforzati in ogni ambito»

Gdpr (la sigla del Regolamento europeo sulla privacy, ndr) è la sinergia tra la responsabilizzazione del titolare e il rafforzamento dei di-

ritti dell'interessato. Se, infatti, il principio della prima autonomia imprese e amministrazioni nella gestione del trattamento, dall'altro lato i diritti (conoscitivi e di controllo) dell'interessato sono significativamente rafforzati, con il riconoscimento non solo dell'oblio e della portabilità dei dati, ma anche della revoca e dell'opposizione. **Come cambia il ruolo del Garante?** Il Garante rafforza notevolmente la sua funzione al pari delle altre Autorità di protezione dati, che pur non di-

smettendo le vesti di istituzioni di prossimità divengono snodi essenziali di un sistema europeo di protezione delle libertà nella società digitale. **Cosa sarà del nostro Codice sulla privacy?** Il Codice italiano viene integrato, in parte abrogato e in generale coordinato con il nuovo quadro giuridico europeo, con il quale molte delle sue previsioni – penso alle più avanzate e lungimiranti – sono compatibili. I trattamenti per fini di polizia e giustizia penale vengono auto-

Come regolamentare la nuova figura del "Dpo"? «Non è un mestiere, servono competenza e professionalità»

nomizzati e disciplinati dal decreto legislativo di recepimento della direttiva 2016/680, che si applica specificamente a questa mate-

ria. Quanto ai provvedimenti sinora adottati, essi continueranno ad applicarsi in quanto compatibili con il nuovo quadro giuridico europeo, mentre con provvedimento generale il Garante individuerà (aggiornandole o viceversa) le prescrizioni delle autorizzazioni generali emanate, con particolare riguardo ai trattamenti di dati genetici, biometrici, relativi alla salute. **Un commento sulla figura dei "Dpo", i responsabili della protezione dei dati: secondo gli addetti ai lavori si**