LAVOCE.INFO - 10 APRILE 2018

Facebook è roba che scotta. Parola della Commissione Ue

di Andrea Ciffolilli

Trasparenza, portabilità, diritto all'oblio: sono i cardini del regolamento Ue sulla protezione dei dati, in vigore dal 25 maggio. Per aziende e organizzazioni che li trattano ci sono nuovi obblighi e sanzioni severe. Basterà per mettere fine agli abusi?

Dati facili da raccogliere

Sui social network capita spesso di barattare, forse con eccessiva indifferenza, il consenso di accesso alle nostre informazioni personali con l'uso, apparentemente gratuito, di qualche applicazione.

Il tema del possibile utilizzo illecito di questi dati è finito sotto i riflettori con il caso di Cambridge Analytica, società di consulenza che raccoglie e analizza grandi volumi di dati personali e offre servizi di comunicazione strategica ai partiti politici. Avrebbe così acquisito informazioni relative a 50 milioni di profili Facebook, violandone le condizioni di utilizzo. Infatti, i dati sono stati utilizzati per attività commerciali come la vendita di servizi finalizzati a persuadere le persone a votare Donald Trump, Brexit e altro, pur essendo stati raccolti, per mezzo di una app, per scopi di ricerca scientifica. È improbabile che si tratti di un caso isolato ed è difficile prevedere quali possano essere le conseguenze di operazioni simili.

Siamo però alle porte di un cambiamento importante: la riforma delle norme Ue sull'uso dei dati che entra in vigore il 25 maggio 2018 (Gdpr – General data protection regulation) e che dovrà essere rispettata da tutte le aziende che lavorano nel mercato digitale europeo, anche se legalmente al di fuori dei nostri confini (per esempio, Facebook, Google o Amazon).

Il nuovo regolamento introduce regole più severe che garantiscono agli utenti un maggiore controllo delle proprie informazioni personali. Semplifica al tempo stesso il contesto normativo in cui operano le imprese, che finora si sono dovute confrontare con 28 diverse leggi nazionali, mentre adesso ci sarà un solo insieme di norme uguali in tutti i paesi e un solo interlocutore, l'autorità di supervisione nazionale (in Italia, il Garante per la protezione dei dati personali). Ciò dovrebbe favorire la concorrenza e l'innovazione nel settore dei "big data".

Nuovi obblighi per le aziende

Tra i risvolti più interessanti della riforma vi sono quelli che riguardano la maggior tutela dei diritti fondamentali delle persone: cosa succederebbe se un evento simile al famigerato caso Cambridge Analytica-Facebook si verificasse dopo il 25 maggio? In che misura la riforma ci protegge dagli abusi?

Il regolamento introduce maggiore trasparenza, poiché richiede di fornire agli utenti informazioni chiare su chi sta trattando i dati e perché. L'utente ha inoltre diritto di richiedere l'accesso e la

portabilità dei dati personali, ossia di trasmetterli a un altro social network o un altro fornitore di servizi *cloud*.

Altrettanto importante è il diritto all'oblio, ossia alla cancellazione dei dati, se non vi sono motivi legittimi per la loro conservazione. E se i dati vengono smarriti o rubati, la società che ne è responsabile (per esempio, Facebook) dovrà comunicarlo sia alla persona che all'autorità di vigilanza entro 24 ore e fornire la documentazione sulla violazione entro tre giorni. Altrimenti si rischiano multe salate, fino al 4 per cento del fatturato annuo globale, oltre che risarcimenti. Costi che si aggiungono alle possibili perdite in borsa, com'è successo a Facebook all'indomani dello scandalo. È lecito perciò chiedersi se gli obblighi introdotti dalla riforma siano eccessivi, soprattutto quando riguardano aziende piccole. Né è chiaro in che misura sia stata fatta, almeno in Italia, una attività di informazione adeguata sul nuovo regolamento da parte delle istituzioni competenti. Tra gli obblighi merita sicuramente un cenno la necessità di nominare un responsabile della privacy (Dpo – *data protection officer*) che riguarda principalmente i soggetti più grandi che svolgono, come attività principale, monitoraggio regolare e sistematico dei dati personali su larga scala (operatori sanitari, banche e compagnie assicurative, per esempio).

Figura 1 – Cosa cambia con la riforma della privacy?

In generale, i "big data", che inglobano anche informazioni personali, possono essere una grande risorsa se impiegati a vantaggio della collettività, per esempio per migliorare la puntualità dei servizi pubblici, per l'agricoltura di precisione, per studiare e monitorare le malattie. Possono anche assicurare ottime opportunità commerciali, se utilizzati in modo corretto e trasparente, nel rispetto della privacy. Ma chi approverebbe lo scambio di dati che, senza la volontà dei legittimi proprietari, svelino posizioni politiche, credenze religiose, appartenenza etnica o aspetti intimi come, ad esempio, orientamenti sessuali e trasgressioni? O il traffico di dati sanitari, per proporre selettivamente servizi diagnostici o assicurativi?

Al di là dei dubbi sull'informazione adeguata ai soggetti che devono rispettarlo, il nuovo regolamento sulla privacy garantisce una maggiore protezione, obbligando le aziende che trattano i

dati a ripensare le modalità con cui svolgono le attività di analisi, gestiscono gli accessi ai propri servizi e fanno pubblicità. La riforma amplia la giurisdizione in cui le autorità europee possono intervenire e applicare sanzioni, facilita indagini congiunte e introduce il principio per cui le misure di protezione della privacy devono essere “adeguate” piuttosto che “minime”, com’è adesso. Ciò implica che chi gestisce i dati deve dimostrare, in tempi brevi e certi, di aver fatto tutto il necessario per rispettare le norme. Proprio il contrario di ciò che è successo nel caso Cambridge Analytica, quando Facebook ha ammesso che qualcosa era andato storto solo molto tempo dopo la violazione. Difficile giudicare ora l’efficacia della riforma, ma si tratta di un passo in avanti e dovremmo essere soddisfatti che sia l’Europa a dare il buon esempio.