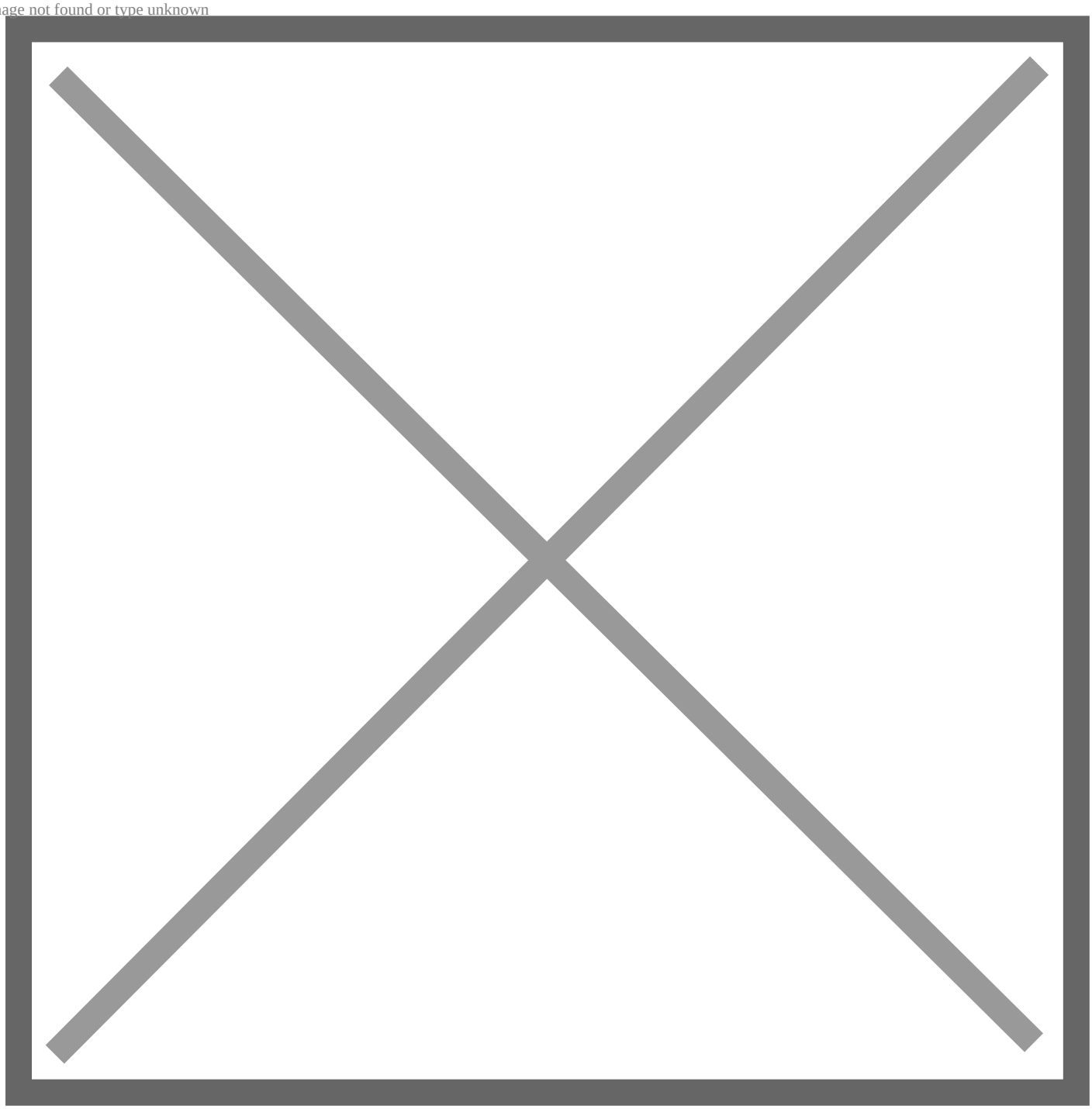
Image not found or type unknown



INTERNET

Il Gdpr non basta: la privacy è sempre a rischio

ECONOMIA 14_12_2018

img
Image not found or type unknown

Privacy sul Web

Ruben Razzante

Image not found or type unknown

Nell'ultimo anno si è fatto un gran parlare di Gdpr (Nuovo regolamento europeo sulla privacy) e si è chiarito che la regolamentazione entrata nella sua piena operatività il 25 maggio di quest'anno potenzia le tutele per gli utenti italiani ed europei e limita i margini di manovra dei titolari del trattamento dei nostri dati, imponendo loro tutta una serie di vincoli rispetto alla profilazione. Gli Stati Uniti, fin dall'epoca del crollo delle Torri Gemelle, hanno intensificato la vigilanza sugli aspetti più rilevanti della circolazione dei dati, ma sono comunque rimasti indietro rispetto al Vecchio Continente, dal quale hanno imparato tanto e hanno ancora tanto da imparare in termini di rispetto della privacy.

La negoziazione a Bruxelles per la definizione dei contenuti del Gdpr tra colossi della Rete e rappresentanti degli Stati nazionali è stata molto aspra e movimentata, considerati gli elevati interessi in gioco. Nonostante questo, continuano a verificarsi episodi, sia in Europa che negli Usa, che confermano la difficoltà di assicurare sufficienti

tutele ai nostri dati.

Si parla spesso, anche nell'ultimo periodo, di vendita dei dati degli utenti da parte dei colossi della Rete. Recentemente una lunga e approfondita indagine del New York Times ha rivelato come decine di app iOS e Android abbiano utilizzato in modo inappropriato i dati di localizzazione degli utenti vendendoli a terzi e violando la loro privacy.

I dati sulla posizione dovrebbero restare anonimi, slegati dall'individuo specifico e utilizzati solo per creare e analizzare aree generali. Il New York Times ha però scoperto che alcune app tracciano i movimenti degli utenti con estrema precisione, consentendo di identificare senza particolari difficoltà le singole persone, di conoscerne le abitudini e mostrare loro pubblicità molto mirate.

Il rischio che si crea è quello che chi ha accesso ai dati grezzi, inclusi dipendenti o clienti, possa comunque facilmente identificare una persona senza il suo consenso. E' possibile seguire qualcuno che si conosce, semplicemente individuando un telefono che rimane regolarmente in un determinato indirizzo. La maggior parte delle app testate dal New York Times monitora infatti posizioni molto precise, non solo aree generali. Tra queste figura WeatherBug, che ha condiviso i dati con oltre 40 società, o l'app sportiva The Score, che chiede agli utenti di attivare la geolocalizzazione per offrire consigli e notizie sportive mirate e che ha trasferito i dati a 16 società pubblicitarie.

In Italia, l'Antitrust ha sanzionato due società di Facebook a causa di violazioni del codice di consumo per un totale di 10 milioni di euro, imponendo loro, inoltre, di pubblicare una dichiarazione rettificativa sul sito internet e sull'app per informare i consumatori. L'Autorità ha infatti accertato che, in contrasto con gli artt. 21 e 22 del codice del consumo, il social network induce gli utenti a registrarsi in modo ingannevole, senza informarli adeguatamente al momento dell'iscrizione dell'attività di raccolta dei loro dati a fini commerciali. Non è chiaro se l'utilizzo dei dati sia necessario per la personalizzazione del servizio e se essi saranno usati per campagne pubblicitarie mirate. Inoltre, è stato riconosciuto che - in violazione degli artt. 24 e 25 del codice del consumo - Facebook attua una pratica aggressiva poiché condiziona i consumatori costringendoli, senza il loro consenso, alla trasmissione dei propri dati a siti terzi per finalità commerciali.

LinkedIn – social network legato al mondo del lavoro acquisito nel 2016 da Microsoft – ha utilizzato i dati di 18 milioni di non iscritti per realizzare annunci mirati su Facebook. E' quanto emerge dall'ultimo rapporto pubblicato dalla Data Protection

Commission irlandese, che comunica altresì che l'azienda ha sospeso la pratica contestata e che sta collaborando con la commissione nelle indagini sulle misure di sicurezza della piattaforma. Linkedin non è certo l'unico ad aver utilizzato in tempi recenti i dati degli utenti senza rispettarne la privacy. Per far luce sullo scandalo Cambridge Analytica, il Parlamento del Regno Unito ha confermato di aver ordinato il sequestro di alcuni documenti riservati sul colosso Facebook dopo che questo aveva ammesso di aver utilizzato i numeri di telefono dei suoi utenti per realizzare annunci mirati e di aver dovuto anche affrontare una violazione particolarmente grave da parte di alcuni hacker russi.

Google aveva già annunciato la chiusura, prevista ad agosto 2019, del suo social network Google+, dopo che era emerso che un bug aveva permesso l'accesso alle informazioni personali di 500mila profili. Ora è saltato fuori un altro bug che riguarda i dati, potenzialmente a rischio, di 52,5 milioni di persone. Google ha quindi anticipato la chiusura del social network da agosto ad aprile del 2019. A individuare quest'ultimo bug sono stati i tecnici di Google che sostengono di non aver rilevato abusi di alcun tipo. Non si può essere certi però che non ce ne siano stati.

Tutti questi episodi dimostrano ancora una volta la vulnerabilità della Rete, la precarietà della nostra privacy e la necessità di unire soluzioni legislative, deontologiche e tecnologiche per limitare al minimo gli abusi sui nostri dati, vero petrolio dell'economia digitale.