PaginaQ
Pisa
http://www.paginaq.it

Sicurezza o riservatezza? Quando il diritto alla privacy diventa "by design"

Author : Redazione

Date : 23 maggio 2015

Privacy o sicurezza. Le agende dei governi, europei e non, impongono in questi ultimi mesi una scelta. L'Italia ha rischiato di essere il primo Paese a fare ricorso alle *"remote computer searches"* per l'acquisizione di dati e comunicazioni all'interno di sistemi informatici, mentre l'Assemblea Nazionale francese ha acconsentito all'utilizzo di una "scatola nera", che installata presso i fornitori di servizi internet per la raccolta dei metadati degli utenti, permetterebbe di individuare chi trasmette le informazioni con un comportamento simile a quello dei terroristi.

Oltreoceano, intanto, una petizione contro la nuova legge anti-terrorismo canadese, che estende i poteri dei servizi di intelligence, porta la firma di 200mila persone. La risposta legislativa alla minaccia terroristica, insomma, passa per la sorveglianza attraverso i Big Data. E la privacy?

Secondo **Ann Cavoukian**, la tutela dei dati personali può e deve essere affiancata, non solo alla sicurezza dei cittadini ma anche alla garanzia degli interessi economici in campo sul fronte dei Big Data.

Direttore esecutivo del *Privacy and Big Data Institute* alla Ryerson University di Toronto, Ann Cavoukian ha di recente tenuto un workshop dal titolo *"Privacy in the era of Big Data"* presso l'Università di Pisa.

Qui, al centro SoBigData, i dati vengono trattati garantendo la protezione delle informazioni sensibili, senza compromettere la possibilità di analisi ulteriori, utili allo sviluppo di servizi. Gli spostamenti in auto di una parte della popolazione, ad esempio, possono essere analizzati attraverso algoritmi di clustering che individuano gruppi di movimenti simili, senza che venga data l'opportunità a chi compie un eventuale attacco di inferire dati personali del singolo individuo.

La trasformazione che viene applicata ai dati sfrutta il principio del *"Privacy by Design"* (Pbd) ideato da Cavoukian intorno agli anni ‘90, ma ancora così attuale da costituire una linea guida per il Gruppo di lavoro ex Articolo 29, l'organismo consultivo a Bruxelles per la protezione dei dati, ed essere inserito all'interno del nuovo regolamento europeo sulla privacy in via di emanazione.

Quello proposto da Cavoukian, *Privacy commissioner* in Ontario dal 1997 al 2014, resta "un nuovo paradigma": "Non possiamo pensare alla privacy nel momento in cui i dati degli utenti vengono utilizzati. Occorre tutelare questi

dati sin dal momento in cui vengono raccolti".

A garanzia del controllo degli utenti sui propri dati personali Cavoukian ha introdotto inoltre il concetto di *"SmartData"*, sviluppato da **George Tomko**, dell'*Identity, Privacy and Security Institute* (Ipsi) di Toronto: la tutela dei dati è delegata ad agenti intelligenti virtuali, che divulgano le informazioni dell'utente solo quando si presentano determinati criteri personali stabiliti per il loro rilascio. Una più efficace protezione dei dati sensibili, dunque, deve essere integrata sin dalla progettazione di sistemi informatici, infrastrutture di rete e pratiche commerciali: così la privacy degli utenti viene garantita di default.

Un'esigenza resa ancora più evidente in rapporto alle nuove tecnologie *Internet of Things*: "Il monitoraggio delle terze parti – secondo Cavoukian - rimuove il controllo di un individuo sui dati che lo riguardano. Per questo occorre concentrarsi sulla prevenzione: è molto più facile ed economico integrare sin da subito misure che tengano conto della privacy all'interno dei dispositivi".
Un messaggio che fa eco ai commenti del Garante della privacy in Italia **Antonello Soro**, che su internet delle cose ha deciso di avviare una consultazione pubblica. Big data e privacy, dunque, non si escludono a vicenda, anzi. L'attenzione alla privacy, come valore aggiunto al
prodotto, può addirittura divenire un fattore competitivo sul mercato: "Le organizzazioni continueranno ad applicare data analytics per generare nuove intuizioni e innovazioni, portare avanti i loro obiettivi strategici e servire al meglio i consumatori".

Tra le linee guida di Pbd compare anche il protocollo di sicurezza *"end-to-end"* recentemente adottato da WhatsApp, che permette la conoscenza del contenuto delle conversazioni solo a mittente e destinatario. Un protocollo che potrebbe non essere più applicabile nel Regno Unito, dopo gli annunci del neo-rieletto primo ministro David Cameron, che ha dichiarato di non voler ammettere mezzi di comunicazione non accessibili all'intelligence britannica.

"La sorveglianza – ha spiegato Ann Cavoukian – è l'antitesi della privacy", ma anche dello sviluppo tecnologico: con la sorveglianza si mettono a rischio "i diritti umani individuali, i diritti di proprietà e le libertà civili che costituiscono i motori concettuali di innovazione e creatività".

Martina Miliani