GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Attenti ai dispositivi innocui spesso nascondono trappole

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali

(di Francesco Malfetano, "Il Messaggero", 11 aprile 2018)

Presidente Antonello Soro, l'Internet of Things sta rivoluzionando il modo di vivere la tecnologia con nuove soluzioni e servizi che facilitano la quotidianità e ottimizzano i tempi di produzione. Qual è il prezzo, quali rischi per gli utenti? Soprattutto, fino a che punto ci si può spingere? In che modo gli utenti possono opporsi all'uso illecito dei dati personali?

"Si stima che presto ogni oggetto, persino il nostro abbigliamento, sarà connesso e che in dieci anni vi saranno 150 miliardi di sensori in rete, 20 volte di più della popolazione mondiale. Ogni cosa, dunque, sarà "smart": non solo i telefoni ma anche auto, case, città; l'intemet degli oggetti e l'analisi dei big data convergeranno con l'intelligenza artificiale e i sistemi biometrici; vivremo, dunque, in un pianeta "intelligente". Tutto ciò favorirà certamente, per un verso, un netto miglioramento della qualità della vita, liberandoci - come già oggi è evidente - del peso di molte incombenze quotidiane e dischiudendo possibilità prima precluse".

Però non bisogna sottovalutare i rischi ai quali la "connessione di tutto" espone l'utente.

"Sicuro. In primo luogo va considerato il rischio di hackeraggio di questi dispositivi, non sempre adeguatamente protetti e tuttavia tali da consentire l'accesso a una molteplicità di dati, spesso sensibili, con danni rilevanti per l'interessato. E' pertanto indispensabile verificare - prima dell'utilizzo di ciascun dispositivo, in base alla relativa informativa - le caratteristiche e le implicazioni del trattamento, limitare la categoria dei dati accessibili e, in caso di uso illecito dei propri dati, opporvisi. Non bastasse, rivolgersi al Garante per ottenere la cessazione del trattamento".

Invece cosa può fare l'autorità? Dal 25 maggio entrerà in vigore il nuovo "Regolamento europeo in materia di protezione dei dati personali". Cosa cambia per utenti e aziende?

"L'esigenza di adeguare la normativa all'evoluzione tecnologica, comporta anzitutto un'anticipazione della soglia di tutela dei dati alla fase della progettazione dei sistemi, secondo i criteri di privacy by design e privacy by default, inscrivendo così nelle stesse tecnologie le misure di garanzie per gli utenti. Ma l'innovazione principale concerne la responsabilizzazione del titolare: principio su cui fonda il Regolamento e che impone a imprese e professionisti di adottare strategie aziendali che garantiscano un livello di tutela dei dati personali adeguato al rischio connesso al trattamento e idonee misure preventive".

Il caso Cambridge Analytica e quello Russiagate hanno fatto da detonatore per la questione della profilazione - e più in generale dei Big Data - chiarendo come questo potere sia spesso concentrato nelle mani di pochi. Quali pericoli si nascondono dietro?

"Queste vicende dimostrano come il passaggio dalla profilazione commerciale a quella politico-elettorale determini effetti dirompenti per la democrazia. Attraverso il possesso delle informazioni sulle paure, gli orientamenti, le aspirazioni dei cittadini, si propongono a ciascuno di essi non solo notizie che sovra-rappresentano o, al contrario, sotto-stimano i fenomeni reali così da assecondarne le idee, ma anche progetti politici ritagliati su queste specifiche esigenze, rendendo così possibile la manipolazione del consenso e, in ultima analisi, un pesantissimo condizionamento del risultato elettorale. Il tutto è aggravato dalla concentrazione di tali informazioni (e del conseguente potere di condizionamento) in capo a poche imprese, capaci così di spiegare effetti determinanti su questioni di rilevanza primaria".

Big data e privacy dei dati sulla salute sono conciliabili?

"La normativa di protezione dati (il nuovo Regolamento in particolare) mira, tra l'altro, a coniugare le esigenze di riutilizzo di dati su larga scala - in particolare big data - per fini di utilità sociale con il diritto degli interessati alla protezione delle informazioni che li riguardano. In tal senso, ad esempio, si prevede che - anche qualora non possa svolgersi su dati del tutto anonimi - l'archiviazione di dati per fini di ricerca, anche scientifica, è possibile previa adozione di misure, quali tra le altre la pseudominimizzazione, idonee a minimizzare l'impatto del trattamento sugli interessati".

Le smart city sono al centro della rivoluzione dell'IoT. Siamo pronti a gestire la mole di dati che produrranno? Quanto è sicuro oggi vivere in una casa intelligente?

"Le nostre città stanno divenendo fonti sempre più rilevanti di dati, anche personali, laddove forniscano informazioni su come un soggetto vive lo spazio cittadino. All'incremento dei dati che le smart city producono (funzionale alla loro innovazione e migliore fruibilità) deve, tuttavia, corrispondere una parallela crescita di consapevolezza in ordine alla necessità di proteggere il flusso informativo così generato, per fini tanto di sicurezza cibernetica quanto di tutela della privacy dei cittadini. Esigenza analoga si ravvisa anche rispetto alla "smart home"".

Quanto incide l'apparente "innocuità" di oggetti di uso quotidiano, connessi però al web, sui nostri comportamenti?

"Incide. Talvolta ci induce a sottovalutare la possibilità che essi rappresentino il canale di accesso elettivo per attacchi informatici e hacker capaci di sfruttarne le vulnerabilità. Inoltre, di questi dispositivi sottovalutiamo la capacità di rivelare, mediante l'uso secondario dei dati

raccolti, stili di vita, capacità economica, persino patologie o dipendenze. E' dunque quantomai necessario un utilizzo consapevole e attento di strumenti, quali questi, tanto utili quanto rischiosi".