



Dichiarazione di Mauritius sull'Internet delle cose

Balaclava, 14 ottobre 2014

L'Internet delle Cose è ormai divenuto parte integrante della nostra vita. Sempre più numerosi sono i dispositivi connessi ad Internet ed in grado di comunicare fra sé, spesso senza che l'utente ne sia consapevole. Sono dispositivi che possono semplificarci la vita, per esempio nella sanità, nei trasporti e nel settore dell'energia: la loro interconnessione può cambiare il modo in cui facciamo le cose. Ma l'Internet delle Cose può anche rivelare particolari molto personali sulla vita di chi possiede questi dispositivi, grazie ai sensori in essi presenti.

Il diritto all'autodeterminazione è un diritto inalienabile di tutti gli esseri umani. Lo sviluppo della persona non può dipendere da quello che imprese e governi fanno di ciascuno di noi. La proliferazione dell'Internet delle Cose aumenta il rischio che ciò avvenga.

Le Autorità per la protezione dei dati e la privacy riunite a Mauritius hanno pertanto esaminato le potenzialità e gli effetti dell'Internet delle Cose durante la 36ma Conferenza Internazionale tenutasi a Balaclava, il 13 e 14 ottobre 2014. Quattro oratori, in rappresentanza del settore privato e del mondo universitario, hanno descritto alle Autorità gli impatti positivi che l'Internet delle Cose può avere sul vissuto quotidiano, ma anche i rischi che esso comporta. Gli oratori hanno esaminato, inoltre, i passi necessari per garantire che i dati personali e la vita privata delle persone continuino ad essere tutelati.

Il dibattito sviluppatosi successivamente ha condotto alle osservazioni e conclusioni indicate qui di seguito:

- I dati raccolti attraverso i sensori nell'Internet delle Cose si caratterizzano per un ordine di grandezza elevato in termini di qualità, quantità e delicatezza. Ciò significa che è molto più consistente la possibilità di compiere analisi inferenziali in ambiti molto più sensibili, e che aumenta la probabilità di identificare i singoli individui. Considerando che già oggi identificabilità e protezione dei "big data" rappresentano una sfida di grande rilevanza, è indubbio che la difficoltà di questa sfida aumenti in misura considerevole alla luce dei "big data" derivati dai dispositivi connessi nell'Internet delle Cose. Dunque, i dati in oggetto dovrebbero essere considerati e trattati come dati personali.
- Benché ad oggi non sia ancora noto il modello di business adottato da molte imprese del settore, è evidente che il valore dell'Internet delle Cose non si esaurisce nei dispositivi in quanto tali. Il profitto deriva dai nuovi servizi collegati all'Internet delle Cose nonché dai dati.
- Oggi siamo tutti consapevoli di quanto pervasiva sia la connettività, e forse i giovani e le generazioni future lo sono in misura ancora maggiore: per loro è impensabile un mondo senza connessioni. Tuttavia, non dovrebbe essere lasciato soltanto a loro il compito di capire se i loro dati siano protetti o meno. Questa responsabilità deve essere condivisa fra tutte le parti interessate a livello sociale, affinché si continui a nutrire fiducia nell'interconnessione dei sistemi. Centrale è, a tal fine, il ruolo della trasparenza: chiunque offra dispositivi operanti nell'Internet delle Cose deve indicare con chiarezza quali dati raccoglie, per quali scopi, e per quanto tempo li conserva, eliminando ciò che è del tutto imprevedibile per il cliente. Al momento dell'acquisto di un dispositivo o di un'applicazione operante nell'Internet delle Cose, occorre fornire informazioni idonee, sufficienti e comprensibili. Oggi, le informative privacy non sempre offrono informazioni chiare e comprensibili, e difficilmente si può ritenere che un consenso prestato sulla base di informative del genere sia un consenso informato. Occorre un cambio di mentalità da parte delle aziende per far sì che le informative privacy cessino di essere soprattutto uno strumento utile a tutelare le aziende stesse da eventuali azioni legali.
- Un trattamento di dati ha inizio con la raccolta dei dati. Tutte le tutele devono essere in atto fin dalle fasi iniziali. Incoraggiamo la messa a punto di tecnologie che facilitino a monte l'integrazione dei requisiti di protezione dei dati e tutela della privacy dei consumatori secondo approcci innovativi. La protezione della privacy sin dalla fase di progettazione (privacy by design) e come default (privacy by default) non dovrebbero più essere considerate una peculiarità, divenendo semmai un punto di forza nell'offerta commerciale di tecnologie innovative.
- L'Internet delle Cose pone, inoltre, sfide significative in termini di sicurezza; anch'esse devono essere affrontate. Un firewall di per sé non è più sufficiente. Un approccio utile a minimizzare i rischi per le persone consiste nel consentire trattamenti solo in sede locale, ossia sul dispositivo stesso. Se ciò non fosse praticabile, le aziende dovrebbero garantire la cifratura dei dati end-to-end così da proteggere le informazioni da interferenze indebite e/o manomissioni.
- Le Autorità per la protezione dei dati e la privacy continueranno a monitorare gli sviluppi dell'Internet delle Cose. Si impegnano ad assicurare l'osservanza sia della legislazione in materia di protezione dei dati e privacy vigente nei propri Paesi, sia dei principi in materia di privacy concordati in ambito internazionale. In presenza di violazioni delle norme applicabili, intraprenderanno le azioni opportune in via unilaterale ovvero attraverso strumenti di cooperazione internazionale.
- Alla luce delle enormi sfide che attendono gli sviluppatori dell'Internet delle Cose, le Autorità di protezione dati ed i singoli, tutti i soggetti interessati dovrebbero dar vita ad un dialogo forte, attivo e costruttivo rispetto alle implicazioni dell'Internet delle Cose e dei big data da esso derivati, in modo da favorire una sensibilizzazione generale con riguardo alle scelte da compiere.

Jacob

Presidente

Conferenza

Kohnstamm

del

internazionale

Comitato

sulla

privacy

Mauritius

Esecutivo

Autorità

Drudeisha

per

la

protezione

Madhub

Presidente

dei

dati