Internet of Things: profili di rischio in termini di privacy e sicurezza dei dati

Author : Federica Maria Calì

Date : 17 Maggio 2019

Negli ultimi anni si è assistito a una vera e propria rivoluzione tecnologica grazie all'avvento dell'Internet of Things e degli *smart objects*: la natura degli oggetti evolve grazie alla possibilità, mediante il collegamento in rete, di comunicare dati su se stessi e di usufruire di informazioni esterne.

L'oramai enorme diffusione di tali dispositivi ha da ultimo portato all'apertura di un dibattito rispetto al loro utilizzo. Essi infatti hanno un forte impatto nella vita quotidiana degli utenti, essendo in grado di estrapolare una serie di dati (riguardanti consumi, abitudini, geolocalizzazione, etc.) che consentono alle aziende di tracciare un **preciso profilo** dei propri clienti, e di utilizzarlo a livello commerciale.

Nel 2017 il mercato Internet of Things (IoT) in Italia e? arrivato a toccare i 3,7 miliardi di euro, con una crescita del 32% rispetto al 2016 spinta sia dalle applicazioni più consolidate che sfruttano la "tradizionale" connettività cellulare (2,2 miliardi di euro, +29%), sia da quelle che utilizzano altre tecnologie di comunicazione (1,5 miliardi di euro, +36%) [fonte: Osservatorio IoT Polimi].

Riportiamo alcune immagini tratte dal rapporto *Buon compleanno IoT* del Polimi.

La crescita del mercato IoT nel 2018

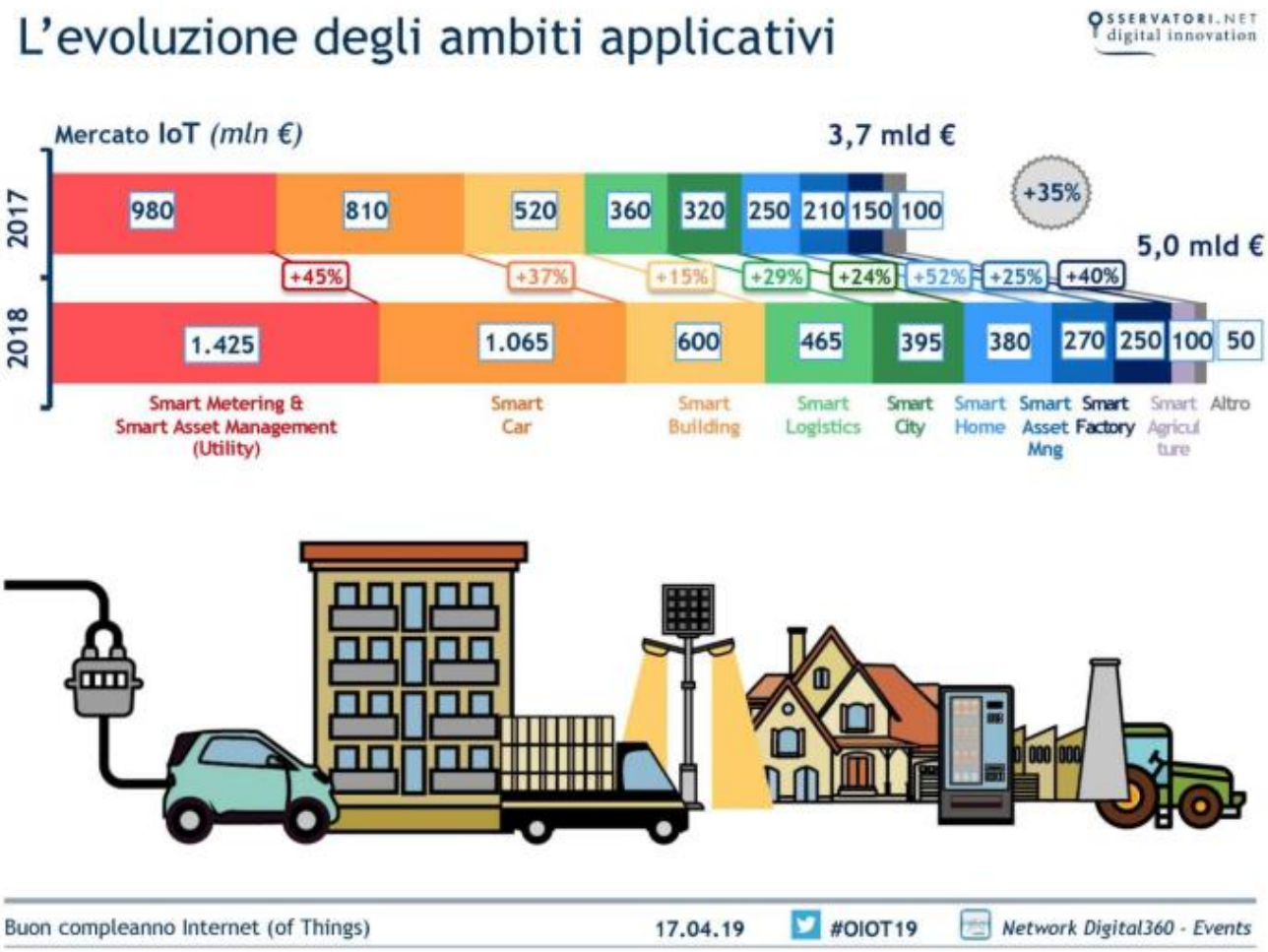
OSSERVATORI.NET digital innovation

Mercato IoT* *(mld €)*

Assinform
Mercato digitale in Italia: 70,3 mld €, +2,3% (+1,6 mld€) rispetto al 2017

** La stima non comprende: wearable consumer, sistemi cablati in campo industriale e domotico, casse audio e Smart TV stand-alone per la Smart Home, soluzioni RFId passive in ambito logistico*

Buon compleanno Internet (of Things) 17.04.19 #OIOT19 Network Digital360 - Events



A fronte di ciò, si è avvertita la necessità di una regolamentazione specifica del rapporto tra **Internet of Things** e **Privacy.**

In particolare negli ultimi mesi abbiamo assistito a un boom degli assistenti vocali, integrati in gran parte di computer, tablet e smartphone, a cui è sufficiente dare un preciso ordine vocale per ottenere una risposta rapida e puntuale. Oggi li conosciamo come Siri, Alexa, Cortana e Google Assistant, ognuno sviluppato da una diversa casa produttrice: Apple, Amazon, Microsoft e Google. Il loro utilizzo risulta particolarmente semplice e intuitivo: tuttavia la loro crescente diffusione, unita alla nascita degli *smart speaker* (dispositivi molto simili a casse Bluetooth, ma che integrano anche le funzioni degli assistenti vocali), ha scatenato molte **polemiche**, legate in particolare alla *privacy* e alla protezione dei dati personali, che molti utenti temono possano essere violati.

Per poter funzionare correttamente, uno *smart assistant* necessita di una connessione a Internet e di un microfono funzionante. Quando pronunciamo un comando vocale, infatti, il nostro assistente personale deve essere in grado di registrare quanto pronunciato e collegarsi a un server tramite il quale decodificare gli ordini impartiti. È proprio tale **costante connessione** a server appartenenti a grandi colossi dell'industria digitale che desta

preoccupazione in molti utenti. Tutto si basa su algoritmi, *machine learning* e sistemi di riconoscimento che raccolgono continuamente un'enorme quantità di dati.

Gli assistenti vocali, quindi, ascoltano, apprendono, si adattano alle esigenze dell'utente, personalizzando l'esperienza e offrono le risposte più adatte a quel tipo di profilo.

Provando ad analizzare alcune tra le principali finalità comuni alla grandissima maggioranza dei dispositivi in grado di supportare uno *smart assistant* può senz'altro citarsi la **possibilità di eseguire ricerche online**. Tale funzione permette di trovare una risposta veloce a moltissime e diverse domande. Uno *smart assistant* permette insomma di sfruttare tutte le possibilità offerte dai motori di ricerca moderni e dalle enciclopedie senza la necessità di uno schermo e di una tastiera.

Altra funzione - utilizzata soprattutto dai giovani, data l'integrazione con applicazioni ormai molto popolari come Spotify - è la possibilità di riprodurre musica, controllando la riproduzione delle proprie playlist e dei propri brani preferiti.

Sarà possibile anche gestire il calendario e quindi chiedere al proprio assistente vocale di ricordare un appuntamento o una riunione.

Tra le **novità** più apprezzate dagli utenti vi è poi il controllo dei *devices* in una *smart home*: un servizio che permette di connettere tutti i propri dispositivi smart e controllarli con la propria voce. Sarà per esempio possibile ordinare di accendere la TV, abbassare il termostato o programmare lo spegnimento delle luci.

Vi sono infine alcuni ambiti, più delicati e non ancora diffusi in tutti i Paesi, in cui gli *smart assistant* sono utilizzati. Ad esempio, da pochi mesi è disponibile il servizio che permette di effettuare telefonate gratis via Internet senza bisogno di schede SIM oppure quello relativo ai pagamenti *online*: la possibilità di gestire l'*online banking* semplicemente con dei comandi vocali è però ancora limitata.

Si possono, dunque, ben comprendere le **preoccupazioni** legate all'utilizzo sempre più diffuso degli assistenti vocali. I dispositivi in cui questi sono integrati ci seguono tutto il giorno, tengono traccia dei nostri gusti, delle nostre preferenze e abitudini, sfruttando in parte queste informazioni per offrire suggerimenti personalizzati sempre più precisi, soprattutto a fini pubblicitari e commerciali.

Inoltre parliamo di dispositivi che restano in ascolto, in attesa di un comando o di una richiesta. Per cui, nonostante le aziende garantiscano la massima riservatezza dei dati raccolti, l'anonimizzazione delle registrazioni e la privacy degli utilizzatori, non sono mancati casi in cui le registrazioni delle conversazioni tra utenti e assistenti vocali siano state spedite per errore via mail ad utenti sconosciuti o siano state pubblicate sui social network, o casi relativi a comportamenti anomali degli stessi dispositivi, che si attivavano senza richiesta o fornivano informazioni su discussioni effettuate in casa in momenti in cui non sarebbero dovuti essere in ascolto attivo.

Di fronte a un siffatto scenario diverse sono le implicazioni che l'uso di tali dispositivi comporta in materia di privacy e di protezione dei dati personali.

Il Regolamento generale sulla protezione dati **(GDPR)** 2016/679 offre importanti garanzie su tali fronti, intervenendo su alcuni punti chiave riguardanti la disciplina dell'IoT. In termini generali, il GDPR dispone che i dati vengano trattati in quanto "adeguati, pertinenti e limitati" rispetto a ciò che è necessario per le finalità perseguite (principio, appunto, della **minimizzazione**).

Nel caso specifico dell'IoT, viene richiesta l'elaborazione di un sistema di gestione della privacy che venga sviluppato fin dalla fase di progettazione del prodotto: non qualcosa di posteriore, quindi, ma di integrato all'oggetto stesso.

Come ha osservato proprio il Presidente dell'Autorità garante per la protezione di dati personali, Antonello Soro: "*Il GDPR prevede l'incorporazione delle misure di protezione dati negli stessi sistemi e dispositivi, in modo che essi siano progettati e configurati in maniera da minimizzare l'uso di dati personali e proteggerli adeguatamente.*
Queste misure compensano quel deficit di consapevolezza nell'utilizzo di dispositivi intelligenti di uso quotidiano, la cui apparente innocuità ci induce a sottovalutarne la potenziale esposizione ad attacchi informatici o comunque la capacità di rivelare, tramite i dati raccolti, stili e tenore di vita, persino patologie o dipendenze. Inoltre, rispetto alla profilazione e al microtargeting che questi dispositivi possono incentivare, risultano determinanti il diritto di opposizione e quello di contestare la decisione automatizzata, nonché di ottenere l'intervento umano nel processo decisionale".

L'**art. 21** GDPR, a protezione dell'interessato, prevede il diritto di quest'ultimo di opporsi, in qualsiasi momento, per motivi connessi alla sua posizione, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 6, par.1, lett.e) o f), compresa la profilazione sulla base di tali disposizioni. In tal caso il titolare del trattamento si asterrà dal trattare i dati personali salvo egli dimostri la presenza di motivi legittimi cogenti che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato, oppure nel caso di accertamento, esercizio o difesa di un diritto in sede giudiziaria.

L'**art. 22** GDPR sancisce inoltre il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo sulla sua persona in modo significativo. Un'**eccezione** a tale disposizione è prevista nel caso in cui la decisione sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, nel caso in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento e infine nel caso in cui si basi sul consenso esplicito dell'interessato. In tali ultimi due casi il titolare del trattamento dovrà porre in essere misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, quale ad esempio il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

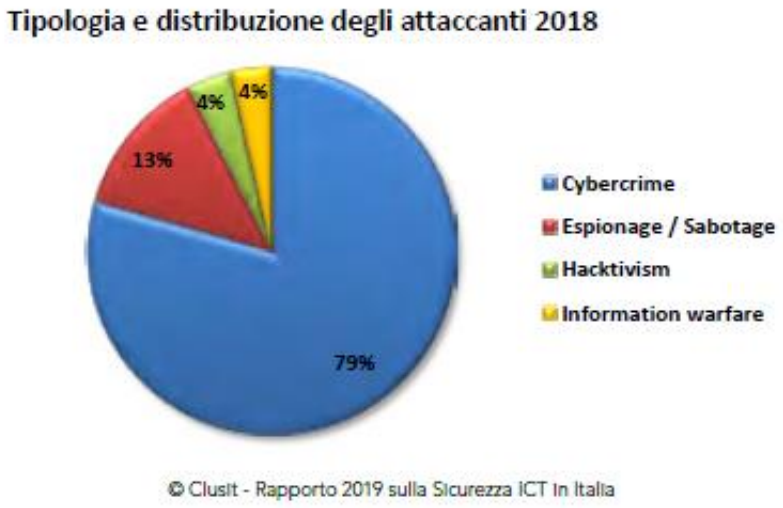
Il considerando n. 90, inoltre, stabilisce l'obbligo per il titolare del trattamento di effettuare una **valutazione d'impatto** antecedente al trattamento, per valutare la particolare probabilità e

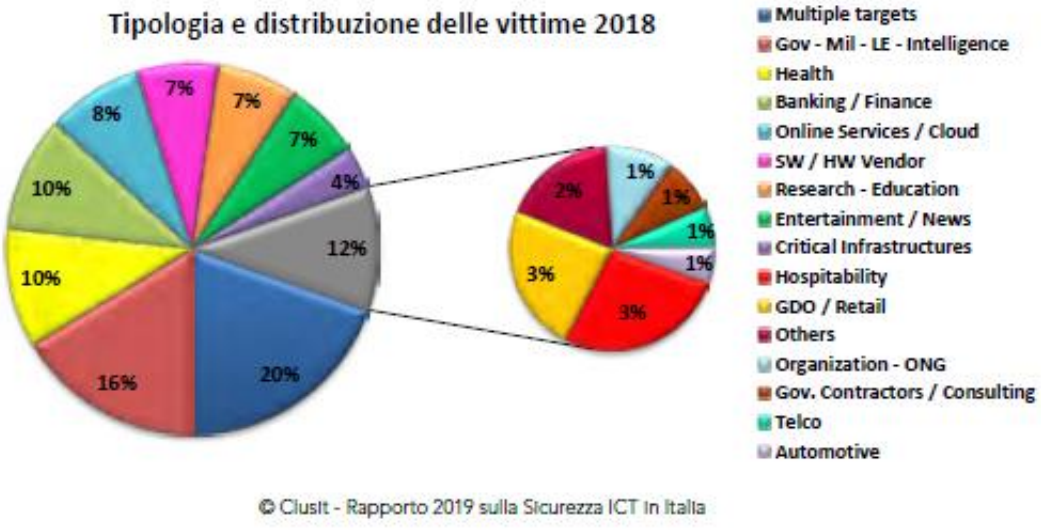
gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento e delle fonti di rischio, soprattutto in caso di trattamenti su larga scala (cioè sui prodotti il cui utilizzo coinvolgerebbe un vasto numero di interessati).

Più precisamente, gli **articoli 35 e 36** della normativa impongono, a questo proposito, una **tutela rafforzata** in caso di rischio elevato: sarà necessario, in quel caso, interpellare l'autorità di controllo (il Garante per la protezione dei dati personali) la quale, entro otto settimane dalla richiesta, dovrà fornire il proprio parere positivo o, in caso contrario, intervenire ammonendo e addirittura inibendo i produttori.

Tutto ciò premesso, non bisogna dimenticare la **sicurezza dei dati e delle informazioni** che noi forniamo. Sono oramai su tutte le cronache gli attacchi che molti dispositivi stanno subendo, con furto di dati o richieste di riscatto.

Dal **rapporto 2019 del Clusit** si evidenzia come gli attaccanti non risparmino nessuno.





La sensibilità su questi temi è ancora molto ridotta. Non bisogna pensare che nell'IoT rientrino solo i *devices* vocali, poiché di tale mondo fanno parte integrante anche gli *smart watch*, gli antifurti, i comandi robotici, la domotica, i dispositivi bio medici, le app mediche, le autovetture, i giocattoli, le *smart city* e le *smart home*, etc.

Tutto ciò che è connesso è facilmente attaccabile. È quindi necessario elevare la nostra **consapevolezza** dei pericoli connaturati negli oggetti connessi. Per innalzare l'asticella della sicurezza è opportuno avvalersi di metodologie che ci possano supportare durante il percorso.

Il primo passo da compiere è quello dell'**analisi dei rischi** che l'implementazione di queste tecnologie comporta. A seguito dell'analisi dei rischi - sia a livello dei diritti e libertà dell'interessato, sia a livello aziendale - è necessario verificare e/o implementare le misure di sicurezza più adatte. In ottica GDPR si potrebbe effettuare una DPIA e una *Privacy by design;* in ottica di scurezza aziendale è necessario verificare la sicurezza logica dei sistemi coinvolti.

Anche in questo caso è necessario un approccio olistico al problema. Il processo deve essere analizzato nel suo complesso dall'inizio alla fine, andando a cercare gli anelli deboli e magari effettuando test e verifiche periodiche.

Articolo a cura di **Federica Maria Calì** e **Stefano Gorla**