ATTUALITÀ

Dammi tre parole... Internet of Things!

di **Fondazione AIDR** · 6 settembre 2021, 15:24

di Biagino Costanzo, Dirigente d'azienda e Socio AIDR

"Gli uomini sono diventati gli strumenti dei loro stessi strumenti." (Henry David Thoreau)

IoT, ecco tre lettere magiche, Internet of Things o ancora Internet delle cose o, se vogliamo, degli oggetti e non stiamo parlando soltanto di computer, smartphone e tablet, ma soprattutto degli oggetti che ci circondano all'interno delle nostre case, al lavoro, nelle città, nella vita di tutti i giorni. L'Internet of Things nasce proprio qui: dall'idea di portare nel mondo digitale gli oggetti della nostra vita quotidiana.

Questo acronimo così semplice e rapido viene oramai citato da anni, migliaia e migliaia di volte al giorno e in tutto il mondo in conversazioni, incontri, dibattiti, riunioni (ora, soprattutto, conference-call...) e come spesso accade sfugge il più delle volte come sia rivoluzionario tutto quello che vi è dietro.

Sono trascorsi più di 50 anni dalla nascita di Internet e più di 20 da quando è stata coniata l'espressione Internet of Things, IoT ovvero quel percorso nello sviluppo tecnologico in base al quale, attraverso la rete Internet, potenzialmente ogni oggetto dell'esperienza quotidiana acquista una sua identità nel mondo digitale. Come detto, l'IoT si basa sull'idea di oggetti "intelligenti" tra loro interconnessi in modo da scambiare le informazioni possedute, raccolte e/o elaborate.

Le tecnologie afferenti l'IoT in questi ultimi anni hanno avuto una evoluzione esponenziale e si sono moltiplicate, allo stesso modo di come si sono evoluti gli ambiti di applicazione. Pensiamo alle auto intelligenti, alla casa intelligente, alla vasta famiglia degli "smart": smart city, smart factory, smart building, smart retail, smart health, smart metering, smart environnment, smart agricolture, smart logistics, e smart lifecycle. Tutto questo grazie alla interconnessione degli oggetti intelligenti.

È d'obbligo però approfondire e riflettere sulle opportunità e i rischi che derivano dalla connettività di questi oggetti.

L’IoT è di fatto un paradigma tecnologico dal potenziale applicativo sconfinato, in grado di incidere su competitività delle imprese, efficienza delle pubbliche amministrazioni e la qualità della vita.

Queste tre lettere vanno bel oltre la semplice definizione ma si traducono concretamente nel nostro quotidiano, andando oltre gli oggetti intelligenti, appunto, assumendo un pieno significato nelle reti che interconnettono questi oggetti stessi.

Pensiamo all’ automotive, con le auto inizialmente rese connesse solo per motivi assicurativi tramite box Gps-Gprs e che oggi escono dalle fabbriche già dotate di connettività a bordo. All’ambito delle fabbriche, dove le tecnologie IoT stanno contribuendo sia in termini di distribuzione che dell’intero sistema, oppure alle abitazioni dove negli anni siamo passati dal semplice impianto di allarme, alla evoluzione della domotica cablata a soluzioni wireless sempre più alla portata di tutti, caratterizzate da servizi in cloud e dall’uso crescente dell’intelligenza artificiale.

Possiamo continuare con l’illuminazione pubblica delle nostre città dove ora si è in grado di regolare la loro luminosità sulla base delle condizioni di visibilità, oppure ai semafori che si sincronizzano per creare la cd onda verde per il passaggio di un mezzo di soccorso.

L’Internet of Things è quindi uno schema che non conosce, potenzialmente, confini applicativi. Nel mondo vi sono, ça va sans dire, Paesi più avanzati sulla materia e altri meno ma in tante zone oramai abbiamo la localizzazione dei dispositivi medicali nei presidi di pronto soccorso, oppure gli sci che inviano informazioni sullo stato della neve, o dall’autovettura che dialoga con l’infrastruttura stradale per prevenire incidenti. Nel mondo produttivo, inoltre, l’IoT aiuta lo scambio dei dati dagli impianti di produzione ai manufatti per la gestione del loro ciclo di vita.

Però, come accennavo prima, tutto questo, ovvero che tutti gli oggetti possono diventare “intelligenti” connettendosi alla rete e scambiando informazioni su di sé e sull’ambiente circostante, è altrettanto vero che questo processo non avviene in tutti gli ambiti, in tutti i posti e con la stessa velocità.

Chiaramente questo dipende dall’esistenza di soluzioni tecnologiche consolidate, dagli equilibri competitivi in un determinato mercato e, infine, dal bilancio tra il valore dell’informazione e il costo di creazione della rete di oggetti intelligenti.

È necessario ribadire che il paradigma dell‘IoT è incontrovertibilmente proteso verso il futuro. Sappiamo che alla base del concetto di Internet of Things c’è una rete di oggetti “intelligenti” in grado di comunicare tra loro, ma dobbiamo chiederci quali sono i trend tecnologici che

decideranno il futuro dell'Internet of Things?

Si è partiti da tecnologie quali reti cellulari, WiFi, NFC, Bluetooth, RFId e siamo ora ai Big Data, Blockchain, artificial Intelligence, sempre più decisivi nel sistema IoT, perché in grado di rafforzare nuove funzionalità, nuovi servizi e nuove opportunità di business.

Tutto questo ha alimentato la nascita di tante startup, molto attive nell'ambito, appunto, dell'IoT e che sono propedeutiche a favorire le tendenze dell'innovazione Digitale e a sviluppare un vero processo della cd "digital trasformation" in molti settori.

Non soffermandoci agli ambiti propri delle applicazioni militari e industriali che meritano capitoli a parte, l'Internet delle cose è sempre più presente nel nostro quotidiano, basti pensare alla possibilità di installare su ogni oggetto che ci circonda un *chip*, un sensore elettronico, di fatto un piccolissimo calcolatore, dotato di un indirizzo internet necessario per poter colloquiare con altri calcolatori vicini e lontani. Oggi, chi di noi non è connesso, tutti i giorni e a tutte le ore, ad uno smartphone ma nel giro di un lustro è presumibile che ognuno potrà (o forse dovrà) essere connesso a centinaia di oggetti intelligenti, a loro volta connessi tra di loro e collegati in una grande rete globale. In questo quadro si inserisce anche l'intelligenza artificiale ma, come ho avuto già modo di ribadire, sarebbe assurdo che succedesse l'impensabile ovvero che l'intelligenza artificiale superi l'insuperabile, ovvero quella umana!

Come è noto dall'intelligenza artificiale, in Giappone, è arrivata Xiaoice, la donna virtuale che fa compagnia 24 ore su 24 a milioni di cinesi, inoltre questo chatbot, dalle sembianze femminili, non solo risponde in chat ai suoi utenti, ma li contatta quando sono tristi o depressi. Il problema però è epocale, culturale, umano in questo caso, una cosa è usare l'IA per facilitare la vita quotidiana, il lavoro, la salute dell'essere umano, un'altra è usarla per sostituire la vita vera che riguarda l'umanità con i suoi dolori, le gioie, l'amore, il sesso, le emozioni, il sudore, le soddisfazioni. Il rifugiarsi su un qualcosa di virtuale, impalpabile, che fa tutto quello che vuoi, ma NON ESISTE, per la semplice paura di confrontarsi con una persona vera, paura insomma, semplicemente di vivere la propria vita, è davvero *il problema dei problemi,* ma bellamente sottovalutato.

Se pensiamo che solo questo algoritmo ha coinvolto più di 600 milioni di utenti, in maggioranza uomini di nazionalità cinese e giapponese con reddito basso, possiamo farci una idea sull'entità di questo fenomeno.

Xiaoice appare sullo schermo con le sembianze di una ragazza intorno ai 18 anni che scherza e coinvolge i propri partner scherzando con loro e inviando testi e immagini sessualmente espliciti. E nel frattempo raccoglie informazioni mirando a diventare la fidanzata ideale di più uomini nello

stesso momento.

È infatti, a questo punto, diviene naturale e necessario interrogarsi anche su quali implicazioni possano esistere in materia di privacy e di sicurezza in questa materia e per i dispositivi connessi.

Quando, per esempio, un attore malevolo vuole attaccare dei dati, inficiando quindi, in qualsiasi modo, uno dei tre parametri che ne definiscono la sicurezza, custoditi e gestiti da una parte ma proprietà di un'altra parte, se viene dunque attaccato un sistema che tratta dati di terzi, la privacy di questi dati viene di sicuro messa in pericolo.

Bisogna mettere in sicurezza questo "terreno", tecnologico/scientifico/cibernetico, il quale sta divenendo la base, artificiale se vogliamo, ma indispensabile non solo per il funzionamento della società ma per la vita stessa dei singoli umani sempre più dipendenti e incapaci di vivere al di fuori di essa.

È essenziale un'alfabetizzazione estesa dell'uso del web.

Nelle scorse settimane a seguito dell'attacco hacker alla Regione Lazio è venuto fuori un turbinio di annunci, considerazioni, riflessioni preoccupate come se fosse una novità. Ma l'incalzare recrudescente degli attacchi hacker di questi ultimi anni, in Italia e in tutto il mondo, e nel 2020-21 in particolare (per intensità e gravità), deve imporre un diverso e concreto approccio a questa materia.

Ben venga la costituenda ANC (Agenzia Nazionale di Cybersecurity), su disposizione del Governo Draghi e guidata dal Prof. Baldoni ma essa deve avere tutti i poteri, le risorse economiche e competenze tali per essere davvero IL potente strumento di analisi e prevenzione a questi reati.

Stiamo vivendo un periodo pericolosissimo a livello di tenuta collettiva, economica, sociale e sottovalutare questo mutamento epocale può essere devastante anche e soprattutto in questo campo. (https://www.aidr.it/sicurezza-digitale-una-nessuna-e-centomila/)

C'è molta disattenzione, superficialità, se non supponenza, in giro, su queste tematiche. In molti sono convinti che anche e tutta la tecnologia può essere gestita e domata e quindi alimenta questa intensa fase commerciale e spinta ad un consumo passivo, acritico, fornendo al pubblico sempre nuove opportunità e strane esperienze. È naturale che all'occhio del consumatore tutto questo può significare solo progresso, un miglioramento rispetto al passato, ma questa visione semplicistica inerente allo sviluppo dell'ambiente intelligente non coglie i rischi sia sociali che ambientali né il cambiamento antropologico delle generazioni future rispetto a quelle precedenti.

Bisogna superare una sorta di paura, strisciante timore, ansia che si possa venir buttati fuori dal godere di queste tecnologie ed esserne esclusi o allo stesso tempo pensare e sospettare che, nel futuro, tutto questo venga un giorno imposto dall'alto con intenti manipolatorie e liberticide.

Quindi ancora una volta il fattore umano resta sostanziale in tutte le cose della nostra esistenza e ancor di più oggi se parliamo di tecnologia, scienza, IoT.

È sempre l'essere umano, si spera con una solida intelligenza e non certo "artificiale", a dover sapere affrontare organizzare e armonizzare questi cambiamenti epocali e non penso solo a quelli tecnologici e scientifici, per garantire una società sicura, evoluta e sempre attenta all'interiorità e soggettività di ogni singolo, così da evitare il caos.

Un giorno le macchine riusciranno a risolvere tutti i problemi, ma mai nessuna di esse potrà porne uno." (Einstein)

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/09/06/dammi-tre-parole-internet-of-things/

© 2026 Istituzioni24