

## Internet of Things

Enrico Menduni

### INTERNET NON È DI SOLA PERTINENZA DEGLI UMANI

1. Internet viene generalmente, ma non correttamente, considerata una rete operata e controllata da umani: un *network* di computer connessi fra loro attraverso reti di telecomunicazione, comandati da un atto umano. In una prima fase ciò è avvenuto generalmente da posizioni stanziali; in una seconda – che si colloca nel nostro millennio – anche in mobilità e con apparecchi diversi dai computer.
2. In realtà è tecnicamente possibile che un computer si connetta con un destinatario preordinato, o che gli è stato comunicato, senza intervento o controllo umano, ricevendo e inviando informazioni; una possibilità che preesiste a Internet, grazie al possibile utilizzo di reti di comunicazione radio o in cavo, e che Internet ha enormemente potenziato e semplificato.
3. Tipicamente le prime aree in cui tale connessione fuori dal controllo umano si determina sono essenzialmente tre: a) aggiornamento *software* e manutenzione; b) monitoraggio remoto dell'attività; c) *malware*.
4. L'avvento della telefonia cellulare 3G e la diffusione di schede SIM che è possibile inserire in dispositivi di vario tipo hanno permesso di estendere tale possibilità e di renderla accessibile anche a utenti non professionali.
5. L'esclusività attribuita agli umani nell'operare e/o controllare la comunicazione in Internet appare dunque concettualmente sempre più fragile. Per meglio comprenderlo, può essere utile analizzare due tipologie di applicazioni, sempre più interlacciate e sovrapponibili: i sensori e l'identificazione a radiofrequenza.

### WSN (*WIRELESS SENSORS NETWORK*)

6. Una considerazione iniziale riguarda i dispositivi mobili, di cui milioni di persone sono oggi dotati, e che dispongono di molteplici sensori digitali miniaturizzati (accelerometri e giroscopi, termometri e barometri, misuratori dell'esposizione alla luce, apparati di geolocalizzazione ecc.) necessari alle varie funzioni dell'apparecchio. Pertanto ciascuno dei loro utenti, quando comunica, diffonde anche (a un unico destinatario ma sempre più spesso, nel web 2.5 del *social networking*, praticamente a tutti gli utenti connessi) un complesso di informazioni; molte di esse hanno la forma di metadati di cui spesso l'utente nemmeno si rende conto.
7. Inoltre, anche grazie alle stesse tecniche di miniaturizzazione delle componenti e alla possibilità di approvvigionarsi di energia dall'ambiente, si diffondono sempre più apparecchi non presenziati (anch'essi possono essere fissi o mobili) che registrano e diffondono informazioni a destinatari dedicati o alla generalità degli utenti.
8. Si definisce WSN (*Wireless Sensors Network*) una rete di sensori, collocati stabilmente o in mobilità, dedicati al monitoraggio di fenomeni fisici nell'ambiente naturale o antropico, in grado di inviare dati e di ricevere istruzioni. Parametri come la pressione atmosferica, il traffico su un'autostrada, la radioattività, il livello dell'acqua in

un bacino, i passaggi degli spettatori attraverso un varco in uno stadio sono alcuni esempi delle quantità rilevate.

### RFID (*RADIO FREQUENCY IDENTIFICATION*)

9. La RFID (*Radio Frequency Identification*) è una tecnologia per il tracciamento o l'identificazione basata su minuscolo dispositivo in genere chiamato semplicemente *tag* (cartellino, etichetta). Nella sua forma più semplice esso consiste in un supporto che alloggia un'antenna e in un *microchip* di memoria che contiene dati che possono essere letti e/o scritti, senza fili, da un apposito lettore che fornisce l'energia necessaria per la trasmissione (RFID passiva). Il lettore a sua volta deve essere connesso a un sistema informativo per la gestione dei dati e per il loro trasferimento. Appartengono a questa tipologia i *tag* incorporati in carte di credito, banconote, documenti, articoli merceologici, libri di una biblioteca, e che presentano molti vantaggi rispetto ai codici a barre precedentemente (e ancora largamente) usati<sup>1</sup>. Anche in Italia dal 26 ottobre 2006 tutti i passaporti rilasciati hanno un microchip biometrico (anche con impronte digitali e firma del titolare) inserito nella copertina.

10. Nella RFID attiva, il *tag* è dotato anche di una batteria, possibilmente ricaricabile, che gli consente di connettersi senza fili e di inviare dati autonomamente, o quando è attivato in remoto (RFID semi-attiva, che consente un notevole risparmio di energia, ma ne limita gli usi). Anche la RFID attiva ha ormai costi molto contenuti, dimensioni minuscole, una vasta gamma di applicazioni ed è disponibile in commercio anche per utenti non professionali.

11. Collocato su un oggetto mobile (ma anche su un animale o una persona), il *tag* RFID ne traccia gli spostamenti, ad esempio avvertendo una centrale remota quando l'oggetto esce da un raggio di azione predeterminato. Anche la centrale remota può essere mobile: tipicamente, uno *smartphone*. I dispositivi antifurto montati su questi telefoni cellulari appartengono a questa tipologia. Un RFID può anche connettersi con una porta disponendone la chiusura o l'apertura; ad esempio il RFID collocato sul collare di un cane (ma anche inserito sotto la pelle) può permettere a quel cane di entrare in casa, ma non ad altri animali. Naturalmente esistono altre applicazioni meno innocenti. Ad esempio il fornitore di un dispositivo o di un *software* può essere informato, in genere – ma non necessariamente – quando l'utente lo consente, del luogo in cui esso si trova (*Location reporting*) e quindi tenere traccia non solo degli indirizzi Internet visitati, ma anche dei luoghi fisici (*Location history*), utilizzando questi dati per le proprie attività ed eventualmente vendendo questi dati ad altre applicazioni e *social network* che possono beneficiarne, personalizzando i contenuti offerti in base a tali dati.

12. Anche i singoli cittadini, se dotati di *tag* RFID (ad esempio per motivi sanitari) oppure provvisti oggetti personali che ne sono provvisti, possono vedere messa in discussione la propria privacy e ciò ha determinato normative, provvedimenti e risoluzioni politiche in ambito nazionale e comunitario<sup>2</sup>.

---

<sup>1</sup> I principali vantaggi sono: non è necessario il contatto fisico tra lettore e codice, che può essere anche non visibile; la velocità di lettura è assai maggiore; è possibile un'efficiente cifratura dei dati.

<sup>2</sup> Si vedano in particolare: Conferenza internazionale delle Autorità di protezione dei dati e della privacy, *Risoluzione sull'identificazione attraverso radiofrequenze (RFID)*, Sidney, 20 novembre 2003; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale

13. Occorre notare infine che le connessioni necessarie alle connessioni RFID e WSN non si avvalgono obbligatoriamente di Internet ma preferiscono in gran parte dei casi utilizzare reti semplificate, economiche, con protocolli particolari, come il caso di ZigBee<sup>3</sup>.

#### ESIGENZE DI *NETWORKING* E DI AUTOMAZIONE

14. Nel loro complesso, le tecnologie digitali sopra descritte, che discendono peraltro da tecnologie militari o spaziali, rispondono a pressanti e molteplici esigenze della società contemporanea. Tra esse possiamo indicare, a puro titolo di esempio:

- a. diagnostica, medicina e assistenza a distanza di bambini, anziani, malati; aiuti e supporti per disabili;
- b. monitoraggio dell'ambiente, previsioni metereologiche e segnalazione precoce degli eventi naturali (frane, slavine, movimenti tettonici), misurazione dell'inquinamento dell'aria e dell'acqua;
- c. monitoraggio del pericolo di incendio (in particolare nelle foreste) e attivazione di dispositivi antincendio;
- d. monitoraggio di strutture e impianti anche non presenziati, controllo di apparecchi;
- e. controllo del traffico e della navigazione, conduzione di veicoli, loro localizzazione;
- f. sorveglianza e allarme;
- g. domotica (*smart homes*);
- h. monitoraggio di reti e di strutture distributive, flotte di veicoli, catene di negozi e magazzini.

15. L'emergere di queste esigenze mostra anche, in negativo, quanti dati che sarebbero molto utili al progresso della società rimangano inutilizzati a questo scopo, per diverse motivazioni:

- a. perché gli ambienti fisici in cui sono generati non sono connessi (ad esempio: contatori analogici del gas, dell'acqua o elettrici);
- b. perché i dati non vengono captati (modalità, tempi e consumi nell'utilizzo di macchine; frequenze di passaggi di utenti e visitatori; ricorrenze di eventi) o soltanto visionati (telecamere di controllo);
- c. per le difficoltà di dialogo tra database, anche digitali, raccolti da soggetti diversi, con protocolli, tecnologie, finalità differenti.

---

europeo e al Comitato delle regioni: *L'identificazione a radiofrequenza (RFID) in Europa. Verso un quadro politico*, 15 marzo 2007; Oese, *Radio Frequency Identification (RFID). A focus on information security and privacy*, 14 gennaio 2008 (DSTI/ICCP/REG(2007)9/FINAL); Direttiva 2009-136-CE, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, 25 novembre 2009; Risoluzione del Parlamento europeo del 6 luglio 2011 su un approccio globale alla protezione dei dati personali nell'Unione europea (2011/2025(INI)).

<sup>3</sup> Uno dei principali standard di comunicazioni wireless. Dal 2002 è attiva la ZigBee Alliance per la certificazione dei prodotti (ormai più di 600 in una vasta gamma di settori: domotica, audio energia, salute, sicurezza, sistemi informativi, telefonia, personal computer ecc.).

16. Si tratta di esigenze di *networking* di società ormai molto complesse, che mettono sotto pressione le reti di telecomunicazione come accadde nel XIX secolo (secondo il famoso esempio di Ithiel De Sola Pool<sup>4</sup>) quando lo sviluppo del telegrafo elettrico fu posto al servizio del controllo del crescente traffico ferroviario, ormai caotico e pericoloso. Le linee telegrafiche furono anzi posate, per risparmiare territorio e processi autorizzativi, sul sedime delle strade ferrate: qualcosa del genere, in modalità immateriale, sta avvenendo oggi.

17. Siamo dunque in presenza di tre grandi tendenze:

- a. raccogliere molti più dati, specie sulle criticità delle società contemporanee;
- b. sostituire ovunque possibile ai misuratori analogici dedicati a una sola funzione dispositivi multifunzionali in grado di dialogare in rete (*smart grids*);
- c. mettere in rete database dispersi o non convenientemente utilizzati, anche per la non-interoperabilità dei protocolli utilizzati.

18. È altamente probabile che tali tendenze si realizzino collocando alcuni dei processi relativi fuori della diretta operatività umana e, tendenzialmente, rendendo il controllo sempre più remoto o automatizzato. Il prezioso aiuto offerto dai sensori collocati in posizioni critiche e rischiose (ad esempio sulle pendici di un vulcano, all'interno di un macchinario in movimento, in un teatro di guerra) sarebbe sminuito se a essi dovessero essere associati i costi, i rischi e le complicazioni di un costante intervento umano in presenza.

19. Occorre tener conto del sovraccarico informazionale che si riverserà sulle reti di comunicazione a seguito di tali processi, che eleveranno esponenzialmente il numero dei comunicanti, sganciandolo da sole considerazioni demografiche: il numero degli esseri umani comunicanti diventa una sola delle variabili da considerare per calcolare la necessaria capienza delle reti.

20. La quantificazione probabilistica di questi *overload* rappresenta un problema assai complesso che qui può essere solo enunciato, ma che avrà conseguenze tecnologiche ed economiche di grande peso, che coinvolgeranno tutti gli operatori di comunicazione, gli utenti e tutte le tecnologie di comunicazione, particolarmente quelle *wireless*, sia terrestri che satellitari. Si tratterà probabilmente di un *cocktail* di tecnologie, com'è già avvenuto con le reti delle precedenti generazioni, ma con quali ingredienti e quali proporzioni ancora non può essere definito con esattezza. Conseguentemente, anche l'uso delle bande di frequenza sarà sottoposto a una forte sollecitazione. Le connessioni di queste problematiche allo sviluppo del Wi-Max, la tecnologia Internet *wireless* terrestre a lunga distanza, sono evidenti, ma sono coinvolte anche le comunicazioni radio su altri protocolli e il complesso delle reti di comunicazione.

## VERSO L'INTERNET DELLE COSE

21. L'espressione "*Internet of Things*" (IoT) designa un probabile sviluppo della rete Internet in cui al tradizionale scambio informazionale umano-umano, si affiancano progressivamente processi comunicativi umano-oggetto (e oggetto-umano) e oggetto-

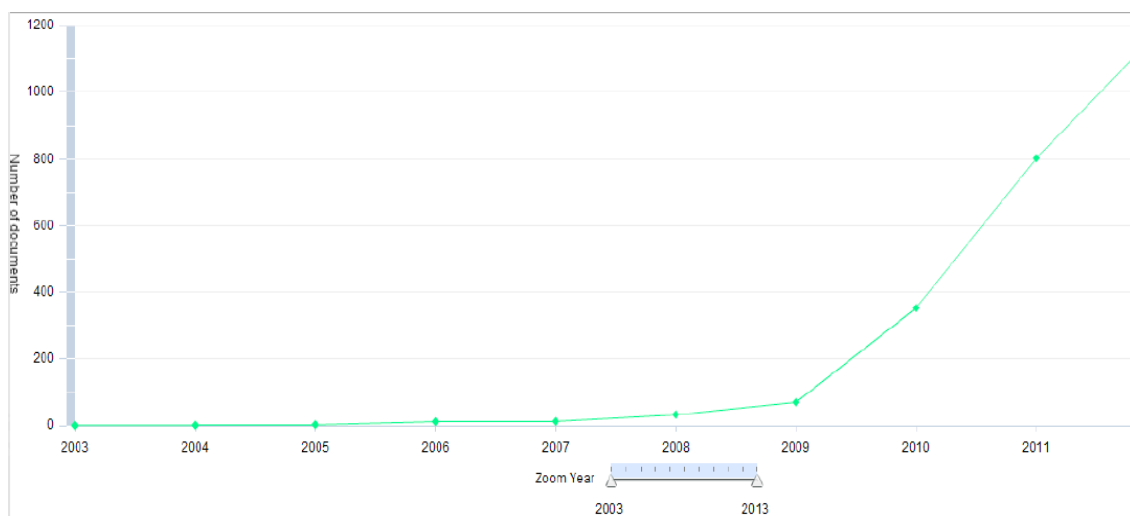
---

<sup>4</sup> Ithiel De Sola Pool, *Technologies of Freedom*, tr.it. *Tecnologie di libertà. Informazione e democrazia nell'era elettronica*, Torino, Telecom Italia-Utet, 1995.

oggetto, nei quali i processi di questa terza tipologia tendono a rappresentare, almeno quantitativamente, la maggioranza dei transiti. Ciò comporta non solo le dinamiche di information *overload* sulle reti di telecomunicazione a cui abbiamo precedentemente accennato, ma anche un ridisegno delle infrastrutture, delle piattaforme e delle interfacce per corrispondere alle nuove interazioni, andando oltre la *human computer-interaction* che in larga parte le ha sinora ispirate.

22. Una nuova configurazione teorica e tecnica, dunque, cui la comunità scientifica si è applicata con lungimiranza. Una ricerca delle pubblicazioni scientifiche su “*Internet of Things*” sul database Scopus mostra una crescita esponenziale dei documenti a partire dal 2009 circa.

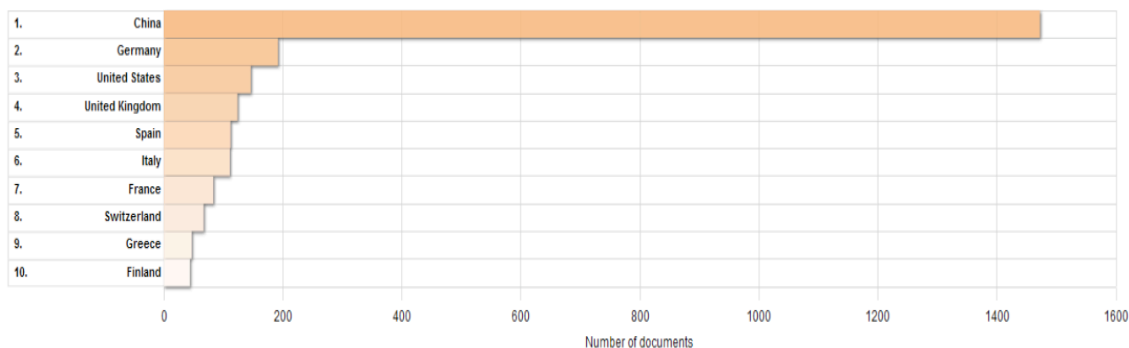
Figura X  
Internet of Things in Publications (database Scopus)



Fonte: Kimmo Ahola Tekes, 2013

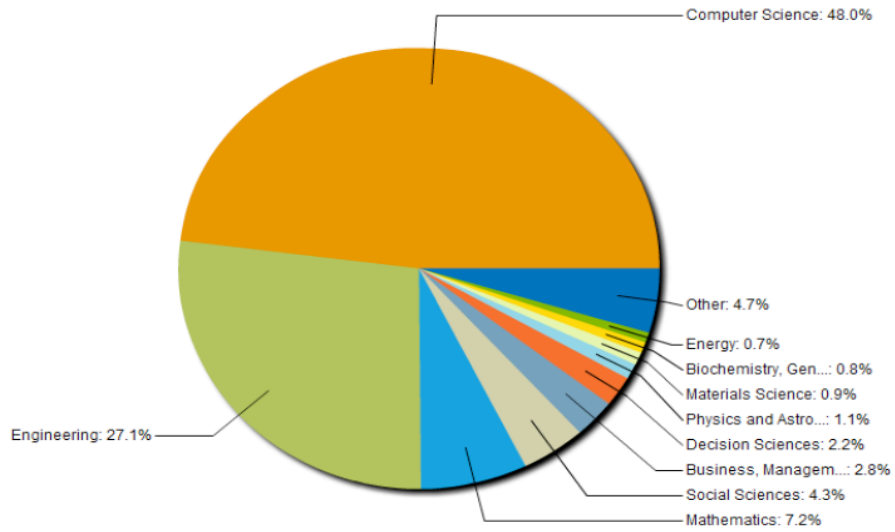
23. La Cina sta facendo la parte del leone, come mostra la fig. X, in processo che vede presenti anche discipline economiche e giuridiche nonché le scienze sociali (fig. X).

Figura X  
Internet of Things in Publications (database Scopus, 2003-2013)



Fonte: Kimmo Ahola Tekes, 2013

Figura X  
Internet of Things in Publications (database Scopus, query by Subject Area)



Fonte: Kimmo Ahola Tekes, 2013

24. Si tende oggi a definire “*smart*” un ambiente connesso che è già predisposto alla *Internet of Things*. Si parla dunque di:

- a. *Smart cities (smart environments, smart spaces, smart living, smart planet);*
- b. *Smart grids (smart meters, smart energy)*
- c. *Smart transport*
- d. *Smart buildings*
- e. *Smart health*
- f. *Smart education*
- g. *Smart materials*
- h. *Smart technologies*
- i. *Smart phones*

Figura X  
Internet of Things



Fonte:

25. La sfida è dunque quella di connettere a un'unica infrastruttura, una Internet evoluta, reti di comunicazione sui più diversi protocolli, rendendole efficienti, interoperabili, strategiche.