Il pianeta connesso

La nuova dimensione della privacy

CONTRIBUTI

Atti del convegno - 28 gennaio 2015

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il pianeta connesso

La nuova dimensione della privacy

Atti del Convegno
28 gennaio 2015

www.garanteprivacy.it

In questo volume sono raccolti i contributi di studiosi ed esperti intervenuti al Convegno *Il pianeta connesso. La nuova dimensione della privacy*, organizzato dal Garante per la protezione dei dati personali in occasione della "Giornata europea della protezione dei dati personali" 2015.

Indice

Il pianeta connesso

Apertura dei lavori

Antonello Soro

Presidente del Garante per la protezione dei dati personali

Apertura dei lavori

Il pianeta connesso

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali

Abbiamo deciso di celebrare la *Giornata europea della protezione dei dati personali* promuovendo una riflessione sul futuro della privacy, sulle possibilità di accompagnare il progresso e l'innovazione con la tutela dei diritti fondamentali, in un tempo nel quale la continua evoluzione della tecnologia modifica con incredibile velocità i nostri modi di vivere.

Lo scenario che si dispiega davanti a noi non è più soltanto quello dello spazio globale dell'informazione.

È l'Internet di tutte le cose, con le sue molteplici applicazioni dalla domotica alle tecnologie indossabili sino alle città intelligenti, che attribuisce anche agli oggetti di uso comune un'identità "digitale" e li connette tra di loro.

È lo sviluppo esponenziale dei *big data*, alimentato dall'uso intensivo di tecniche di calcolo e algoritmi predittivi sempre più precisi ed applicati a volumi crescenti di dati.

È, in una parola, il pianeta connesso, nel quale si realizza compiutamente la continuità tra spazio fisico e spazio digitale, la nuova dimensione immateriale della nostra esistenza.

Gli orizzonti che si aprono sono vastissimi e, per molti aspetti, ancora non del tutto noti e prevedibili. L'unica certezza è la nuova e smisurata disponibilità di informazioni che potranno essere raccolte e scambiate ininterrottamente, spesso senza alcun intervento attivo o consapevole delle persone.

Il salto che ci attende non è solo quantitativo - per volume e varietà dei dati generati e sfruttati - ma qualitativo, dal momento che le nostre scelte saranno sempre più condizionate da apparecchiature intelligenti che assumeranno in modo automatico decisioni per conto nostro.

Rispetto all'attuale monitoraggio dei comportamenti degli utenti in Rete (analisi della navigazione, del contenuto delle email o dei social network) sarà possibile, in un futuro davvero prossimo, attingere direttamente ed in tempo reale anche a dati dinamici ed emotivi trasmessi dal nostro corpo, ben oltre la già sperimentata *sentiment analysis*.

Penso alle potenzialità delle tecnologie indossabili, dagli orologi intelligenti ai sensori a realtà aumentata.

La creazione di una rete di processi, dati e oggetti rischia di realizzare una totale riduzione dell'uomo a cosa: l'individuo considerato alla stregua di un semplice supporto connesso al mondo di Internet.

Il corpo come un oggetto da profilare in modo sempre più sofisticato per condizionare consumi, stili di vita, scelte individuali; e da sorvegliare per conoscere e conservare ogni aspetto anche quello più banale della quotidianità, realizzando un controllo sociale particolarmente invasivo che si estende, di fatto, alle nostre abitazioni, alla nostra fisicità.

Siamo noi stessi i primi ad innescare il processo, il più delle volte inconsapevoli delle conseguenze legate alla scia di informazioni personali che ogni attività o operazione compiuta lascia dietro di noi.

Forse dovremmo imparare a non affidarci con eccessiva superficialità alle lusinghe della tecnologia, abbagliati dai servizi e dalle opportunità che ci vengono offerte.

Sono convinto che di fronte alla complessità della società digitale, dobbiamo esorcizzare la tentazione neoluddista di un'opposizione ideologica nei confronti delle innovazioni e sfuggire da ogni inutile tecnofobia.

E tuttavia le innovazioni, che sono indispensabili per semplificare la vita e migliorare l'ambiente che ci circonda, devono essere governate per impedire che le esigenze del mercato e le logiche del profitto ci sottraggano i nostri spazi di intimità e di libertà e per evitare che i dati accumulati siano usati “contro di noi”.

In questi anni, abbiamo indirizzato la nostra attenzione ai

c.d. *"Over the Top"*, le multinazionali del web, monopolisti di un'economia digitale sempre più distante dai consueti canoni della competizione e della regolazione dei mercati, intermediari sempre più esclusivi tra produttori e consumatori, protagonisti influenti delle relazioni internazionali.

E nonostante l'evidente disparità di potere i Garanti europei, grazie anche alle recenti sentenze della Corte di Giustizia, hanno avviato un confronto che, ancora lontano dall'essere concluso, ha registrato la disponibilità dei giganti della Rete a misurarsi sul terreno di una protezione dei dati più rispettosa e attenta.

Mi riferisco ai vari rapporti sulla trasparenza pubblicati dopo lo scandalo Datagate, alla volontà di adeguarsi alla sentenza della Corte sul diritto a non apparire tra i risultati del motore di ricerca e, particolarmente rilevante per l'Autorità italiana, al riconoscimento del contenuto prescrittivo del nostro provvedimento in materia di privacy policy.

Probabilmente, anche al di là delle nostre ragioni, pesa la consapevolezza che il reiterarsi di comportamenti "scorretti", se non addirittura illeciti, rischia in primo luogo di compromettere seriamente la fiducia degli utenti e, di conseguenza, di riflettersi negativamente sui loro interessi economici.

Ma ora ci attende una nuova stagione e la sfida appare, se possibile, ancora più complessa.

E la difficoltà accresce il nostro convincimento che la protezione dei dati rappresenti la chiave attraverso la quale è possibile ricercare il più alto punto di equilibrio tra uomo e tecnica.

Nella società digitale, noi siamo i nostri dati: da questa semplice considerazione bisogna partire per ricercare nuove e più efficaci forme di tutela delle nostre libertà.

Seguire il percorso dei dati - presupposto indispensabile per assicurarne una effettiva protezione - diventa tuttavia sempre più complesso in realtà dove prevale l'asimmetria informativa e dove si assottiglia, fino a scomparire del tutto, la possibilità di mantenere il controllo sul flusso di informazioni che ci riguardano.

L'interazione automatica tra gli oggetti permette una continua raccolta e condivisione di informazioni, senza alcuna consapevolezza delle persone cui le stesse appartengono.

Del resto la catena dei soggetti che interagisce per implementare, distribuire e gestire le diverse innovazioni si moltiplica e si frammenta ininterrottamente: spesso gli sviluppatori che immettono nel mercato le infinite applicazioni - che quotidianamente scarichiamo sui nostri dispositivi - possono essere anche singoli individui e non coincidere con coloro che le distribuiscono né con chi archivia o detiene effettivamente i dati (di norma conservati in sistemi *cloud*).

Ma se da un lato la tecnologia offre nuove ed illimitate potenzialità di sviluppo, una raccolta massificata di dati ne aumenta in modo esponenziale la vulnerabilità con ripercussioni sempre più rilevanti per le nostre stesse vite.

I rischi non riguardano soltanto la sicurezza dei dispositivi, ma anche quella di tutti i collegamenti di comunicazione e delle infrastrutture.

Il bersaglio degli hacker sarà sempre più frequentemente questa rete di oggetti connessi, nell'ambito della quale i dispositivi mobili (come smartphone e tablet) saranno i vettori di accesso.

Penso all'accresciuta possibilità di creare blocchi sui sistemi informatici ai quali è legata la nostra vita quotidiana, dai pagamenti ai trasporti alla salute, proprio per effetto del moltiplicarsi di tali porte di ingresso e del loro continuo interagire.

La partita del *cybercrime* si giocherà essenzialmente su questo piano e per tale ragione il tema della sicurezza - intesa appunto come protezione dei dati - dovrebbe essere posto al centro non soltanto di un dibattito come quello di oggi, ma della stessa politica generale del Paese.

Le garanzie per rispondere a questa nuova sfida della modernità richiedono l'adozione di modelli tecnologici ritenuti sicuri.

L'ambizione delle Autorità di protezione dati è quella di ricercare un nuovo equilibrio tra fattibilità tecnica ed accettabilità

giuridica; di incorporare la tutela dei diritti nelle tecnologie e di responsabilizzare i titolari spingendoli verso l'adozione di nuovi modelli organizzativi di gestione e di controllo dei dati.

I concetti di *privacy by design*, *privacy by default*, valutazione dei rischi, *data breach* sono - ed il nuovo Regolamento segna in questo senso la direzione - la condizione affinché anche lo sviluppo dell'Internet delle cose sia attento ai dati, rispettoso delle persone e, soprattutto, sostenibile.

L'obiettivo è quello di arrivare ad un modello di sicurezza e di protezione dei dati perfettamente integrato in ogni dispositivo fin dalla progettazione e non aggiunto a posteriori, in quanto una volta esplosa la domanda dei consumatori sarà difficile ricondurre tutto entro un contesto di reale salvaguardia per i diritti individuali.

La protezione dei dati può rappresentare l'antidoto contro ogni possibile abuso, una risposta all'avanzare della società sorvegliata, il presupposto essenziale per garantire anche la sicurezza dei sistemi.

Le perplessità maggiori che si registrano da parte dei settori industriali partono dalla valutazione che, in materia di Internet o Things (IoT), considerato un mercato ancora immaturo, eventuali interventi, anche normativi rischiano di alzare barriere agli investimenti e di ostacolare l'innovazione ma, soprattutto, di essere inadeguati rispetto alla velocità dei cambiamenti.

Gli stessi settori si oppongono a soluzioni rigide astrattamente valide per ogni possibile scenario, ritenendo preferibili scelte flessibili ed approcci multidisciplinari.

Sarebbe allora utile, e questo Convegno è una buona occasione, un confronto costruttivo con tutti gli interlocutori interessati per individuare e promuovere soluzioni capaci di garantire una effettiva selettività della raccolta e, soprattutto, di verificare che il rispetto di specifiche misure di sicurezza sia bilanciato con l'efficienza dei diversi dispositivi ossia che non ne comprometta le funzionalità.

Mi riferisco, in particolare, al ruolo che possono avere le tecniche di anonimizzazione, la raccolta e l'utilizzo di dati aggregati

piuttosto che grezzi, l'adozione di tecniche sicure di trasmissione tra i diversi dispositivi o piattaforme, la possibilità di impostare ragionevoli tempi di conservazione ovvero prevedere sistemi automatici di cancellazione, la necessità di definire in modo chiaro tutti i soggetti che interagiscono nei diversi processi nonché i "luoghi" in cui i dati sono conservati.

E ancora, nella consapevolezza della dimensione globale dei fenomeni, occorre valutare se le soluzioni individuate, come ad esempio le certificazioni europee o internazionali, rappresentino un effettivo vantaggio competitivo per le aziende che le rispetteranno.

I Garanti europei in questo percorso potrebbero diventare, per gli operatori, interlocutori di riferimento: per assicurare che lo sviluppo della società digitale sia a vantaggio degli utenti e rispettosa dei loro diritti e per tentare di definire, anche con un approccio multidisciplinare, regole e principi condivisi.

Si tratta di stabilire un terreno comune di confronto, consapevoli che lo sviluppo del mercato digitale coinvolge anche altri rilevanti aspetti a partire dalla necessità di garantire una libera concorrenza e che sono urgenti interventi sugli attuali livelli di concentrazione dei mercati.

In questo senso si muove la Risoluzione del Parlamento Europeo del dicembre 2014, che chiede misure capaci di separare l'attività dei motori di ricerca dagli altri servizi offerti dai giganti della Rete.

In un mondo dove sempre più cose saranno connesse, e dove gli effetti della società digitale hanno una portata globale, diventa indispensabile che anche le nostre Autorità siano capaci di "connettersi" tra di loro, di fare "rete" per implementare sinergie, condividere esperienza e svolgere al meglio quel ruolo di garanzia che i Trattati (e la giurisprudenza della Corte di Giustizia) hanno loro espressamente attribuito.

Dobbiamo lavorare affinché la protezione dei dati assuma nel senso comune lo stesso ruolo di primo piano che le è stato già ampiamente riconosciuto in ambito giuridico.

I diritti nell'Infosfera

Sessione I

Juan Carlos De Martin
Politecnico di Torino

Antonio Spadaro
Direttore de "La Civiltà Cattolica"

Luca De Biase
"Nòva - Il Sole 24 Ore"

Moderatore **Augusta Iannini**
Vice Presidente del Garante
per la protezione dei dati personali

Sessione I

I diritti nell'Infosfera

Augusta Iannini

Ringrazio innanzitutto i relatori che ci accompagneranno in questa mattinata ed affrontiamo il tema della prima tavola rotonda, che ha un titolo impegnativo: *I diritti nell'Infosfera*. Infosfera è una parola che ha una metrica musicale ed anche intimista e che, invece, per contrapposizione, si associa ad uno spazio immenso, quello delle informazioni, quindi il cyberspazio, Internet, la telefonia digitale ma anche i mass media tradizionali. Per chi ha inventato questa parola, gli esseri umani sono organismi informazionali reciprocamente connessi in un ambiente che condividono, a loro volta, con altri organismi. Ogni persona, dunque, è costituita dalle proprie informazioni, si interconnette e genera contesti sociali multipli per differenti tipi di privacy.

Non dico una novità se sottolineo che i computer e gli smartphone ci hanno scaraventato in un "habitat" affollato di dati e plasmato da esperienze condivise. In questo mare di dati a noi piace vivere, ne apprezziamo i vantaggi ma spesso ne sottovalutiamo i rischi. Internet è una rete a strascico, dove il nostro "curriculum" professionale, di cui siamo orgogliosi, si mescola alle foto, ai commenti sui nostri profili dei social, di cui potremmo magari non essere più tanto fieri.

Questo è solo uno degli aspetti ma, di fronte a queste realtà, prodotte da informazioni che corrono molto più velocemente delle legislazioni e delle teorie sociali che vorrebbero regolamentarle, ha ancora senso parlare di tutela dei diritti fondamentali intesa in senso tradizionale? Oppure bisogna creare tutele diverse? O magari devono cambiare i parametri di riferimento nell'applicazione dei diritti fondamentali?

Abbiamo chiamato a districare questi problemi tre studiosi di differente formazione, vorrei introdurli: il dottor Luca De Biase, è un giornalista, scrittore italiano, fondatore e direttore di *Nòva - Il Sole 24 Ore*, editor di innovazione presso lo stesso quotidiano, responsabile del magazine digitale *Vita Nova*. Docente al Master di Comunicazione della Scienza all'Università di Padova, fa parte del tavolo permanente per l'innovazione e l'agenda digitale italiana. È autore di diversi libri, ricordo i più recenti: *Cambiare pagina per sopravvivere ai media della solitudine*, *I media civici: informazioni di mutuo soccorso*. È membro della Commissione sulle garanzie, i diritti e i doveri per l'uso di Internet alla Camera dei deputati, membro del Comitato scientifico per l'Agenda digitale in Emilia-Romagna. Tante altre cose le ho dimenticate, le ho omesse, ma sarò perdonata, spero!

Il professor Juan Carlos De Martin è un ingegnere, un accademico italiano, noto per la sua attività nell'ambito di Internet e società, insegna al Politecnico di Torino dove ha co-fondato e co-dirige il centro Nexa su Internet e società, è editorialista de *La Stampa* e di *Nòva - Il Sole 24 Ore*. Ha curato il libro *The digital public domain foundation for an open culture* e nel 2014 è stato nominato, anche lui, membro della Commissione di studio per i diritti in Internet istituita dal Presidente della Camera Laura Boldrini.

Padre Antonio Spadaro, è un gesuita, scrittore, critico letterario, teologo italiano, attuale direttore della rivista *La Civiltà cattolica*. Insegna *cyberteologia* presso la Pontificia Università Gregoriana, consultore del Pontificio Consiglio della cultura e di quello delle comunicazioni sociali. Collabora con numerose riviste di natura tecnico informatica ed è autore di numerosi articoli e volumi sulla Rete e in particolare *Cyberteologia: pensare il cristianesimo al tempo della Rete*, un libro che è stato tradotto in sette lingue e *Web 2.0: reti di relazioni*. E' autore della prima, lunga intervista giornalistica a Papa Francesco: *La mia porta è sempre aperta*.

Seguo l'ordine che è scritto nel programma e quindi sollecito il professor Juan Carlos De Martin al primo intervento e gli porgo una riflessione: in un suo articolo di qualche anno fa ho letto una frase che condivido con convinzione. Lei ha detto: *"Il web non è mai stato e non è una terra senza leggi"*. Forse, aggiungo io, è un po' complessa l'azionabilità di questi diritti nella Rete e comunque, al di là dei diritti esistenti, la Rete, con le sue peculiarità, sta facendo emergere nuovi o diversi diritti fondamentali. Non Le nascondo che mi incuriosisce molto sentir parlare di diritti un ingegnere e quindi Le porgo volentieri la parola.

Juan Carlos De Martin(1)

Ringrazio il Presidente Soro e la dottoressa Iannini. Sì, sono un ingegnere e avendo fatto parte della comunità Internet a partire dagli anni '80, provo a condividere con voi alcune riflessioni.

Fin dalla loro invenzione, prima Internet e poi il web sono stati raccontati utilizzando metafore (peraltro la stessa parola "web", ragnatela, è una metafora).

Inizialmente siamo stati noi, la comunità che ha fatto nascere questo spazio online, a proporre delle metafore, di solito legate alla cultura americana, metafore che hanno influenzato a lungo il pensiero sulla Rete.

Per esempio per molti anni si è parlato di "frontiera elettronica", pensando al grande mito americano della frontiera: uno spazio di possibilità illimitate, di grande libertà dell'individuo e di tenue presenza dei tradizionali poteri economici e politici.

Oppure si è parlato (lo ha fatto Howard Rheingold) di comunità virtuali, introducendo una parola ricca di storia come

(1) Questo testo è reso disponibile da Juan Carlos De Martin con licenza Creative Commons Attribuzione - Condividi allo stesso modo, *http://creativecommons.org/licenses/by/4.0/deed.it*. L'attribuzione va attribuita indicando il nome dell'autore e inserendo la URL del suo sito web, *http://demartin.polito.it*.

"comunità" all'interno dei discorsi sulla Rete. Le prime metafore sulla Rete, dunque, le hanno proposte i primi animatori di Internet.

Successivamente, tuttavia, con l'importanza crescente della Rete, anche altri hanno cominciato ad articolare narrative alternative con cui raccontare la Rete. E lo hanno fatto prendendo anche loro metafore di ispirazione americana, ma spesso volgendole nella loro accezione negativa. Di conseguenza troviamo, a partire dall'inizio del secolo, molti politici (anche italiani) che riprendono la metafora della frontiera elettronica dandole però un connotato negativo, ovvero, Internet come Far West, ovvero, Internet come terra senza legge, come terra dove i malfattori possono sostanzialmente fare ciò che vogliono rimanendo impuniti, dove il cittadino onesto vive nella paura di essere costantemente derubato, aggredito o peggio.

Questa metafora è stata usata forse nel momento istituzionalmente più alto nella primavera del 2011, quando il Presidente francese Sarkozy convocò un "eG8" dedicato a Internet. Da allora - almeno questa è la mia sensazione - mi sembra che questa metafora sia stata utilizzata sempre meno. Se confermato, è uno sviluppo positivo, dovuto innanzitutto al diffondersi della consapevolezza che, a differenza quanto veniva spesso detto in passato, le leggi valgono online esattamente quanto valgono offline, leggi come quella sulla diffamazione, sulla minaccia e tutte le altre fattispecie di reato. In altre parole, con le prime sentenze definitive per diffamazione su Facebook, con gli interventi frequenti e incisivi della Polizia postale, si sta diffondendo la consapevolezza che effettivamente siamo responsabili di tutto ciò che facciamo online, e che ciò vale per ciascuno di noi, semplici cittadini, come vale naturalmente per chi compie reati, ovvero, chi ruba, truffa, ecc..

Quindi in questa prima parte del mio intervento volevo semplicemente constatare con soddisfazione il fatto che la metafora negativa e, soprattutto, superficiale di Internet come Far West forse ha chiuso il suo ciclo vitale e che quindi possiamo iniziare a raccontare la Rete in altro modo.

Le metafore però sono seducenti e quindi mi è venuta voglia di continuare a giocare, se me lo permettete, con la metafora del West, provando a renderla un po' meno superficiale e un po' più aderente alla realtà. Quindi vi propongo un web immaginato non come cittadina da Far West alla Clint Eastwood (o alla Sarkozy), ma pur sempre come una cittadina di frontiera, con l'intento di provare a gettare un po' di luce su quanto sia cambiato il web in questi ultimi 10-15 anni.

Proviamo quindi a immaginare una cittadina di frontiera, ma stavolta, invece di un luogo senza legge, pensiamo a una cittadina dove lo sceriffo è presente e contrasta con discreto successo i malfattori; c'è, come sempre nella storia, una corsa agli armamenti tra ladri e forze dell'ordine, ma le leggi ci sono e sono fatte ragionevolmente rispettare.

Oltre a ciò, l'ipotetica cittadina della frontiera digitale che vi propongo di immaginare è caratterizzata da tre aspetti principali.

Innanzitutto, al posto dei tanti piccoli negozi di quando il web era giovane, ora la città ha dei grandi, sontuosi saloon. Questi saloon sono affascinanti, offrono servizi molto utili e sono, almeno per le loro funzionalità di base, gratuiti. Allo stesso tempo, però, pongono delle difficoltà. In particolare per entrare in uno di questi saloon non basta semplicemente spostare una di quelle porticine oscillanti a cui ci hanno abituato i film western, ma mi viene chiesto di leggere un lungo trattato - spesso più lungo dell'Amleto di Shakespeare - e di accettarlo prima di essere ammesso all'interno.

Si tratta in realtà di un contratto orientato a garantire moltissimi diritti al proprietario del saloon. In particolare, per la tecnologia innovativa usata da questi saloon, tutto quello che farò nel saloon sarà attentamente registrato, quindi ogni sguardo al pianista, ogni applauso, ogni ordine di bicchiere di whisky, ogni interazione con gli altri avventori. Il saloon avrà, quindi, il diritto di creare un dossier su di me, sulle mie abitudini e preferenze, e di venderlo (o cederlo) a terzi. Inoltre, il saloon - proprio come i saloon del Far West - si riserva il diritto discrezionale di cacciarmi fuori in

qualsiasi momento. Solo a queste condizioni posso accedere ai nuovi, scintillanti saloon.

Il secondo aspetto di questa cittadina è che il West - si sa - è polveroso e, quindi, l'acqua è particolarmente preziosa. Solo che chi porta l'acqua vuole decidere a chi arriva l'acqua e a chi no, quanta acqua arriva e a che prezzo. Sei, per esempio, un ricco venditore di pellicce e, anche grazie all'acqua, guadagni tanti dollari? Allora tu l'acqua la pagherai di più. Sei un saloon che vuole attrarre più clienti della concorrenza grazie a terme ricche d'acqua? Mettiamoci d'accordo e la tua acqua avrà condutture privilegiate. In questa cittadina, insomma, i proprietari degli acquedotti, essenziali per la vita di tutti (saloon, cittadini, sceriffo, sindaco, ecc.), vorrebbero tanto poter decidere arbitrariamente cosa fare della "loro" acqua.

La terza e ultima caratteristica che la cittadina ha acquisito in questi ultimi 15 anni è che in questa cittadina pullulano - come possiamo chiamarli? - degli "osservatori": i cittadini, in tutto ciò che fanno - quando vanno a fare la spesa, quando vanno a scuola, quando passano per strada, quando si mandano lettere, quando vanno ai saloon - sono osservati e registrati. Indiscriminatamente. Anche se sono preti, avvocati o giornalisti. E senza che nessuno controlli davvero gli "osservatori".

Questa immaginaria cittadina, vedete, non è banalmente il Far West, ma è comunque distopica. In particolare è una cittadina con *gravi problemi di tutela dei diritti dei cittadini*. Sempre restando in metafora (e trascurando molti altri aspetti che non posso per motivi di tempo): i diritti degli avventori dei saloon, il diritto all'acqua, il diritto di non venir spiati in maniera generalizzata e indiscriminata.

Uscendo di metafora e tornando a parlare direttamente di Internet, proprio ai diritti in Internet è dedicato il lavoro della commissione di studio istituita dalla Presidente della Camera Laura Boldrini nel luglio 2014. In questo momento - e fino a fine marzo 2015 - è in consultazione sul sito *Camera.civi.ci* la bozza di Dichiarazione di diritti in Internet che abbiamo pubblicato

nell'ottobre 2014. L'obiettivo primario della Dichiarazione è quello rendere espliciti i diritti di cui bisogna godere per poter vivere una vita civile e democratica in Internet.

Naturalmente non basta enunciare diritti per risolvere i problemi. Ma identificare con chiarezza i diritti è un presupposto importante per capire quale futuro vogliamo. Poi, è chiaro, ci si deve preoccupare, per esempio, delle case a cui l'acqua proprio non arriva o di chi, pur avendola, non può permettersi di pagarla. Tuttavia, lo ripeto, mi sembra importante interrogarci su quali siano i diritti, sia già esistenti, sia eventualmente nuovi, necessari per permettere una vita libera, uguale, solidale, dignitosa all'interno dello spazio digitale. E' quando abbiamo provato a fare con la dichiarazione dei diritti in Internet, a cui vi invito a contribuire per arricchirla e perfezionarla.

Tra i nuovi diritti, lasciate che vi citi i seguenti: il diritto di accesso alla Rete, senza la quale si è cittadini di serie B; il diritto alla neutralità della Rete, cioè che tutti possano utilizzare questa risorsa senza discriminazioni e senza interferenze; il diritti degli utenti delle grandi piattaforme, che sono così utili e così importanti per la nostra vita ma, proprio per questo, hanno bisogno di essere regolate; il diritto a un'educazione digitale. Il digitale, infatti, rispetto ad altri mezzi di comunicazione come la televisione o la radio, ha ancora più bisogno di utenti consapevoli, per cogliere appieno i benefici della Rete minimizzandone gli aspetti negativi.

Oltre ai nuovi diritti, riflettiamo poi brevemente sullo stato dei diritti preesistenti in questo nuovo spazio digitale, facendo, sempre per motivi di tempo, due soli esempi.

Il primo diritto su cui vi invito a riflettere è quello di espressione del nostro pensiero, il diritto che rende possibili tutti gli altri diritti. Grazie alla Rete il diritto di espressione del nostro pensiero è stato senza dubbio straordinariamente amplificato.

Tuttavia, qual è l'equivalente digitale di una manifestazione?

Attualmente una "manifestazione digitale", a seconda di come viene esattamente realizzata, rischia di essere illecita. Eppure in linea di principio tutti sono d'accordo che ciò che è lecito offline

dovrebbe essere lecito anche online. Il problema è che il quadro normativo, a volte risalente agli anni '80 del secolo scorso, è grossolano e va adattato ai tempi, tenendo specificamente presente i diritti dei cittadini e l'equivalenza offline-online. E' un processo che sta già avvenendo negli Stati Uniti, dove il *Computer Fraud and Abuse Act*, una legge federale, straordinariamente vaga, che è stata spesso utilizzata per perseguire a livello penale fatti che giudicheremmo, nel mondo fisico, legittimi, è sotto revisione (anche a seguito della tragica morte dell'attivista Aaron Swartz, ricercatore di Harvard, morto due anni fa anche in seguito ad un'indagine altamente controversa sul suo conto).

Il secondo diritto è quello di associazione. In Internet che cosa è un'associazione? I membri di una mailing list costituiscono un'associazione di fatto? E quelli di un gruppo Facebook? E se sono davvero associazioni, che tutele hanno? In un momento storico in cui i social network sono sempre più il veicolo di attività politiche, sociali e culturali porsi il problema della tutela delle attività associative mi sembra importante.

In conclusione, giocando con qualche metafora abbiamo provato a riflettere su quali siano i diritti necessari per assicurare alla Rete un futuro che non sia né il Far West digitale (mai davvero esistito) dell'ex Presidente Sarkozy, né la cittadina distopica dei saloon e delle spie (ahimè, fin troppo reale). I diritti che assicurino, per riprendere il titolo di questo convegno, un "pianeta connesso" ispirato a principi di libertà, solidarietà, dignità e eguaglianza. Grazie.

Augusta Iannini

Grazie professore per la Sua esposizione molto chiara: mi ha radicato nella convinzione che esistono dei diritti consolidati ma anche dei diritti nuovi ancora da definire che sono il diritto di accesso, il diritto alla neutralità della Rete etc. Naturalmente, come

sempre, non basta enunciare dei diritti, poi bisogna trovare i mezzi perché questi diritti possano essere soddisfatti in maniera semplice, in maniera diretta. Credo che questo poi sia l'approccio più complicato.

Passo la parola ora a Padre Antonio Spadaro, Direttore de *La Civiltà cattolica* e mi permetto di introdurre una tematica. Lei, nei Suoi interventi molto apprezzati, definisce la Rete: *"un ambiente comunicativo, informativo e formativo e non un mezzo da usare come un martello o un'antenna"*. Non uno strumento di comunicazione dunque, ma un vero e proprio ambiente, nel quale noi viviamo. L'esistenza digitale dunque, che però prescinde dalla presenza fisica, consentirebbe una forma di convivenza sociale che è una forma di reale partecipazione. Allora, come possiamo immaginare di essere cittadini a tutti gli effetti nell'Infosfera?

Antonio Spadaro

Grazie di questo invito, grazie al Presidente Soro, alla dottoressa Iannini e a voi qui presenti. Parto da una ovvietà, cioè che Internet ha cambiato il nostro modo di pensare e di vivere. Da questa semplice constatazione ho avviato anche la mia riflessione *cyberteologica*: un termine strano, ma significa semplicemente che, nel momento in cui la Rete cambia il mio modo di vivere e di pensare, cambia anche il mio modo di vivere e pensare la fede.

Questa direi che è un'ovvietà: la nostra esistenza di fatto è modificata dalla Rete, che ha un impatto forte sul nostro modo di vivere e pensare. Le tecnologie digitali, come diceva la dottoressa Iannini, non sono più dei *tools*, cioè degli strumenti completamente esterni al mio corpo e alla mia mente. La Rete non è uno strumento da usare e questa è una cosa che sembra ovvia, ma in realtà non lo è, perché ancora tutta la terminologia che usiamo per parlare della Rete è sostanzialmente di tipo strumentale.

La Rete non è uno strumento ma un ambiente nel quale noi

viviamo. Internet non è un insieme di cavi, di fili, di server, di computer, di tablet di smartphone eccetera, perché dire questo sarebbe, ad esempio, come identificare la realtà della famiglia con le pareti della casa in cui vive. Voi sapete che in inglese la parola casa si dice *house* e *home*. La famiglia che cos'è? La *house*? Le pareti della casa? No, ovviamente, sono le relazioni tra le persone, il focolare domestico, la *home*.

Dire che la Rete è uno strumento è come dire che la famiglia sono le mura di una casa. La Rete è una esperienza che si fa grazie agli strumenti tecnologici. La Rete è l'esperienza che facciamo grazie ai cavi, ai fili, ai modem eccetera, la Rete non è tubi, la Rete è persone.

Sarebbe errato identificare la realtà dell'esperienza di Internet con l'infrastruttura tecnologica che la rende possibile.

Che cosa è la Rete, dunque? Da buon gesuita io faccio l'*explicatio terminorum*, cioè devo capire il significato delle parole, altrimenti non ci intendiamo. Internet è innanzitutto un'esperienza umana, finché si ragiona in termini di strumenti noi saremo colpiti dalla bellezza assoluta di un iPhone 6 plus o di un Galaxy Note 4, ma non capiremo il significato antropologico di quella cosa lì. Resteremo colpiti, abbacinati dalla bellezza, di cui noi stessi ci stupiamo, degli oggetti che riusciamo a produrre, ma non capiremo nulla dell'esperienza che stiamo facendo.

Internet è uno spazio di esperienza che sempre di più sta diventando parte integrante in maniera fluida della vita quotidiana; anzi, Internet sta diventando e diventerà sempre di più invisibile e trasparente, in quanto comincia ad essere incorporato in tutto ciò con cui noi interagiamo. Sto ovviamente pensando all'Internet delle cose. La Rete in qualche modo non esiste, perché noi siamo già una rete, cioè noi siamo già un *hub* di connessioni, al di là del fatto che io abbia un cellulare o meno.

Poi, di fatto, lo strumento tecnologico mi aiuta a vivere in maniera diversa l'esperienza umana della connessione, che è un'esperienza che va al di là dei cellulari, degli smartphone e dei

computer. La vita stessa perciò è una rete che si esprime fisicamente e anche digitalmente.

Permettetemi di citare Benedetto XVI nel suo messaggio per la Giornata delle comunicazioni del 2011, quando disse: *"L'ambiente digitale* - è già interessante l'uso dell'espressione "ambiente digitale" - *non è un mondo parallelo, o puramente virtuale, ma è parte della realtà quotidiana"*. Con questa semplice frase di Benedetto XVI noi abbiamo archiviato una parola, la parola *virtuale*, che io non amo perché finta. Infatti la parola virtuale ha creato una schizofrenia nell'esistenza umana, di cui le prime vittime sono i giovani, perché siamo noi ad educarli, a formarli, quindi li educhiamo male, come degli schizofrenici, perché abbiamo detto loro che esiste la realtà reale e la realtà virtuale, che è tale perché non è reale.

Nel momento in cui Benedetto XVI dice che l'ambiente digitale non è un mondo puramente virtuale, sta dicendo che forse è il caso di parlare di ambiente *digitale*, non *virtuale*, che è altrettanto reale quanto l'ambiente fisico. La mediazione tecnologica non è affatto pura alienazione, questo è un altro problema che noi abbiamo ereditato dalla bomba atomica, perché nel momento in cui, con la seconda guerra mondiale, la tecnologia è stata percepita come una nemica dell'essere umano, noi abbiamo percepito la mediazione tecnologica come qualcosa di disumanizzante, mentre è frutto della libertà dell'uomo.

Voi sentite il vostro telefono di casa, quello analogico, come una minaccia? Oppure: se voi parlate con vostra mamma, i vostri fratelli, i vostri figli al telefono, sentite questa mediazione tecnologica come invasiva e terrificante, disumana? No, allora perché percepire e continuare a percepire la mediazione tecnologica come una minaccia?

Sempre Benedetto XVI scrive: *"I network diventano così sempre di più parte del tessuto stesso della società, un vero e proprio tessuto connettivo della nostra esperienza, della realtà del nostro rapporto con il territorio"*. La rete sociale non dà espressione a un insieme di individui, il web 1.0 diciamo così, ma è un insieme di

relazioni di individui, quindi il concetto chiave non è più la presenza in rete, ma la connessione. Se si è presenti ma non connessi, si è soli.

Qualcuno di voi è su Facebook? Sì, ecco: molti di voi. Avete mai postato una cosa su Facebook controllando, dopo 30 secondi, se qualcuno ha fatto "*I like*" o meno? E se voi avete postato una foto bellissima su Facebook e nessuno entro 30 secondi ha messo "*I like*", come vi sentite? È terribile. Questo avviene perché siete presenti ma non siete connessi, cioè nessuno vi vede. Questa è la percezione, l'esperienza della non comunicazione.

In Rete si sperimenta la prossimità, occorre dunque comprendere bene in che modo il concetto stesso di prossimo, così caro alla terminologia cristiana e così legato alla vicinanza spaziale, si evolva al tempo della Rete: chi è il mio prossimo al tempo della Rete? In questo momento siamo in streaming, qualcuno ci sta vedendo. Anzi, ci sono varie persone che sui vari network sociali stanno condividendo l'indirizzo web per seguire lo streaming online. Alcune persone ci stanno seguendo. Ecco, loro sono nostri prossimi, mentre magari altre persone, più vicine a noi, nella stanza accanto alla nostra sala, non lo sono. La Rete cambia il concetto di prossimo e questo, evidentemente, ha delle conseguenze di ordine politico. La Rete entra a far parte del concetto stesso di presenza, per cui se non sei connesso, socialmente parlando non ci sei. Se siamo connessi noi lasciamo tracce dovunque. Avviene già adesso, senza pensare al futuro: carta di credito, email, social network, Viacard e così via.

Il vero nucleo problematico della questione che ci stiamo ponendo, dal mio punto di vista, è proprio il concetto di presenza al tempo dei media digitali e dei social networks. Che cosa significa essere presenti gli uni agli altri? Che cosa significa essere presenti a un evento? Che cosa significa essere presente a una decisione? Che cosa significa, ad esempio, fare una manifestazione, come si può fare manifestazioni in Rete.

L'esistenza digitale appare configurarsi con uno statuto

ontologico incerto, prescinde dalla presenza fisica, ma offre una forma a volte anche molto vivida di presenza sociale che va evidentemente tutelata. L'esistenza digitale non è un semplice prodotto della coscienza, una proiezione, un'immagine della mente, ma non è neanche una *res exstensa*, cioè non è una realtà oggettiva ordinaria, anche perché esiste solo nell'accadere dell'interazione, nel momento in cui io interagisco. Le sfere esistenziali coinvolte nella presenza in Rete sono da indagare molto bene nel loro intreccio; questo per me è il nodo: che cosa significa essere presenti, oggi? Quando sei "presente?

Al di là delle definizioni e delle argomentazioni, il cuore della questione consiste nel fatto che una rigida distinzione duale tra naturale e artificiale, tra mente e corpo, tra *res cogitans* e *res extensa*, tra *esprit de finesse* e *esprit de geometrie*, non rende più ragione della realtà complessa che stiamo vivendo. Questo è un tema classico, noi stiamo vivendo questioni classiche.

Si apre davanti a noi oggi un mondo intermediario, ibrido, la cui ontologia andrebbe indagata meglio e così i diritti e i doveri ad essa connessi. Alla luce delle considerazioni sull'essere prossimo, come è possibile dunque immaginare il futuro della vita di una comunità civile al tempo della Rete? Il concetto di partecipazione - anche politica e anche ecclesiale - è strettamente legato a quello di presenza. Questo è un nodo, perché presenza connessa sembra essere l'opposto della privacy. In fondo tu "partecipi" quanto meno ti "tuteli" nella tua privacy.

Papa Francesco, lo scorso anno, ha affermato: *"Non abbiate timore di farvi cittadini dell'ambiente digitale"*. È interessante il fatto che il Pontefice abbia usato l'espressione *cittadini*, non ha detto semplicemente: *"non abbiate paura di entrare nella Rete"* o qualcosa di questo genere. Lui parla di essere cittadini, di cittadinanza digitale. Qui c'è un elemento di riflessione in più che andrebbe indagato meglio.

Le nuove tecnologie digitali hanno dato origine e stanno dando origine ad un vero e proprio nuovo spazio sociale, i cui

legami sono in grado di influire sulla cultura e sulla società: come essere cittadini al tempo della Rete? In un mondo sempre più fatto di informazioni - cioè in una Infosfera - da soggetti individuali intesi in senso classico, siamo diventati organismi informazionali interconnessi. Quindi organismi e informazioni, nodi di una Rete che vivono grazie alle informazioni di cui possono usufruire.

A questo punto dunque comprendiamo bene come l'accesso, cioè l'accesso alla Rete, stia diventando la nuova misura dei rapporti sociali: è un diritto indispensabile per essere cittadini. Non avere accesso significa essere scartati, che è un altro dei temi classici, fondamentali di Papa Francesco. La cultura della comunicazione per lui non può convivere con la cultura dello scarto: le due sono culture opposte, antitetiche. Il cablaggio delle reti ci permette di condividere in maniera globale le risorse che abbiamo, anche quelle intellettuali. Wikipedia, di fatto, è questo: ci permette con generosità di condividere le risorse, quindi di immaginarci nuove forme di partecipazione e di condivisione.

Inoltre, più in generale, il mondo dei media ha il potere di rendere visibile una maggioranza invisibile di esclusi, di relegati ai margini della strada, di dare voce ai loro diritti, trasmettendone i messaggi. Proprio qui entra in gioco la prossimità, cioè i media possono aiutarci ad avvertire il senso di solidarietà e il desiderio di lottare per i diritti umani, risvegliando la nostra consapevolezza contro la logica dello scarto.

I complessi e articolati meccanismi legati alla produzione sociale di conoscenza, supportati dalla Rete e dai social media, tematizzano questioni e istanze relative alla sfera pubblica che sono del tutto nuove. La Rete come luogo di partecipazione e di condivisione delle risorse, che permette di immaginarci forme di partecipazione alla vita sociale prima inimmaginabili.

A questo punto, se accettiamo questa visione, Internet diventa indispensabile per realizzare una serie di diritti umani, per contrastare le disuguaglianze, per accelerare lo sviluppo umano.

Quindi garantire l'accesso universale ad Internet deve essere una priorità. Dovrebbe forse già essere dichiarato un diritto costituzionale. Grazie.

Augusta Iannini

Grazie Padre Spadaro, mi pare di capire che il tema, a questo punto, sia quello di dare contenuti anche a questo diritto di accesso, come diritto da costruire e come un diritto fondamentale, che si porta però dietro anche tante altre considerazioni. È vero infatti che la Rete è partecipazione e condivisione ma all'interno di questa partecipazione e condivisione dobbiamo porci anche il tema dell'educazione alla Rete e all'utilizzo della Rete, diversamente avremmo una prospettiva un po' parziale.

Adesso passo la parola al dottor De Biase. Mi sembra di capire, dalle cose che ho letto e dalla sintesi di questi primi scambi, che l'Infosfera è un ambiente che si è riempito di informazioni, che si riempie tuttora di informazioni che si scambiano sulla Rete i soggetti che vivono in quest'ambiente, ma questi soggetti sono interconnessi tra loro. Invece, ai tempi all'informazione dell'epoca analogica, c'erano informatori e fruitori, quindi c'erano soggetti che si relazionavano in modo diverso. Se questo è vero, se questi soggetti portatori di informazione sono tutti interconnessi tra loro, bisogna anche riconsiderare il contenuto dei diritti della Rete e le loro forme di tutela?

Luca De Biase

Grazie. Buongiorno a tutti, molte cose intorno a questo concetto dell'Infosfera sono state dette. Ne ripeto una in modo radicale, semplicemente così: l'ambiente e il corpo umano si sono arricchiti di una nuova dimensione formata dall'informazione

scambiata, registrata, elaborata con strumenti digitali. Viviamo nell'ambiente, esistiamo con il nostro corpo, come sempre, ma questo ambiente è arricchito di informazioni e questo corpo è aumentato da una protesi alla quale nessuno rinuncia in nessun secondo della giornata e della notte: lo smartphone che ci connette costantemente all'ambiente ridefinito dalle informazioni.

La metafora che io propongo - visto che questo ci serve per arrivare alle conseguenze - è semplicemente l'ecosistema. Noi siamo nel nostro ecosistema, nella nostra città, nel nostro pianeta e questo ecosistema è arricchito da queste nuove possibilità. Che il telefono sia una protesi che si connette al sistema dello scambio, della registrazione e dell'elaborazione dell'informazione è un'esperienza di tutti, quasi ci manca un pezzo di corpo quando non ci funziona, se è finita la pila.

Addirittura - fatemelo dire con l'imprecisione di un non giurista - la Corte suprema degli Stati Uniti quando ha dovuto stabilire se la polizia poteva fare una perquisizione alle persone dentro al telefonino ha detto no, perché il telefonino è parte dell'anatomia umana. Fondamentalmente ci siamo resi conto di questa cosa, così come ci siamo resi conto che la città non potrà essere migliorata e ricostruita in modo più adatto alla nostra vita quotidiana senza tenere conto delle opportunità offerte dalla Rete e dal sistema dei fenomeni digitali che stiamo scoprendo. Non ha più senso la distinzione tra reale e virtuale, come ha detto giustamente Antonio: la realtà è questa e qui siamo. Inoltre, come ha detto Juan Carlos, non è un Far West perché le regole ci sono, caso mai, appunto, siamo di fronte a scelte decisive su come si fanno queste regole.

Abbiamo vissuto un periodo nel quale le regole specifiche per queste cose venivano fatte essenzialmente da chi costruiva la Rete, Lessig ha scritto un famoso libro che sottolineava come *code* sia la stessa parola sia quando si parla di software che quando si parla di legge. Effettivamente la legge di chi fa il software è il principale sistema con il quale ci regoliamo in Rete; quello che la piattaforma mi consente, mi suggerisce, mi stimola, mi incentiva a

fare è la regola principale che io seguo quando sto lavorando in Rete.

A fronte di quella regola mi posiziono, per cui tendenzialmente tutta questa vicenda della bizzarra disattenzione che le persone hanno nei confronti della privacy su Facebook, ad esempio, è dovuta al fatto che io penso di conoscere come funziona Facebook e quindi mi comporto in modo tale che condividerò delle informazioni che non mi importa se sono pubbliche o no. Prendo una strategia di relazione con la piattaforma che difende la mia privacy distinguendo il personaggio che sono su Facebook dalla mia persona reale, che io conosco e che mantengo privata attraverso la mia strategia di relazione con questa piattaforma. Quando Soro dice che noi siamo i nostri dati e quando si parla di organismi informazionali, la nostra reazione è del tipo: *"sì, sì, sarà, ma io sono io e i miei dati li posso in qualche modo controllare, così che non mi imbroglino"*.

Questo tipo di passaggio è abbastanza pericoloso e spiega la disattenzione che molti cittadini hanno nei confronti dei diritti in Rete, perché in qualche modo pensano di poter tenere sotto controllo, dal proprio punto di vista, la situazione. Siamo in un'epoca in cui questa digitalizzazione è ormai chiaramente un arricchimento dell'ecosistema nel quale si svolge la vita nostra, degli animali, delle piante e di tutto il resto. Ne abbiamo però una consapevolezza scarsa, ne tiriamo scarsamente fuori le conseguenze come più o meno avveniva nel concetto di ecosistema naturale nell'epoca del boom dell'industrializzazione.

Io penso che ci troviamo in una fase nella quale parliamo di ecosistema della Rete, di innovazione del digitale con le stesse forme di consapevolezza che avevamo all'inizio degli anni '70 in Italia per quanto riguardava l'ecosistema. Negli anni '60 parlare di ecosistema, di ecologia era roba da gente un po' fuori dal corso della storia che all'epoca era concentrata sull'industrializzazione: se c'erano delle esternalità negative tipo l'inquinamento, ci avremmo pensato in seguito. Adesso sono accadute alcune cose, disastri

ambientali, prese di consapevolezza, la ricerca di una qualità della vita che è diventata importante ed è stata connessa alla qualità dell'ambiente.

Poi un passaggio - secondo me clamoroso - nella nostra relazione con l'ecosistema naturale, cioè quando finalmente la singola persona ha capito che il suo gesto individuale influisce sul valore dell'ambiente nel suo insieme e la qualità dell'ambiente nel suo insieme influisce sulla sua felicità personale. Quando si è chiuso quel cerchio di consapevolezza per cui il mio gesto individuale conta per l'insieme e l'insieme conta per me, individuo.

Tutto questo percorso è durato sessant'anni per quanto riguarda la consapevolezza ambientale in senso naturale. Speriamo ce ne vogliano meno per la consapevolezza ambientale nell'ecosistema digitalizzato, arricchito dal digitale. Ma al momento siamo all'inizio del percorso: oggi si direbbe che, tutto sommato, la storia sia la digitalizzazione, che l'economia digitale indichi la direzione, non pensiamo alle esternalità negative culturali o altro, perché a quelle ci penseremo dopo.

Qualcuno comincia a pensarci, c'è una serie di iniziative, scopriremo che è una cosa importante per la qualità della vita e dell'ambiente tenere conto di questo approccio. Se l'Infosfera è un ecosistema, se la affrontiamo con la stessa qualità mentale, le cose nuove che stanno succedendo in questo momento e che penso accelereranno la presa di consapevolezza sono due.

Sono usciti anche in Italia dal *digital divide* molti dei nostri dirigenti istituzionali. Solo 15 anni fa, io penso, vi ricorderete tutti, tra i nostri politici e dirigenti delle istituzioni a parlare di Internet erano veramente pochi, a capirci qualcosa erano veramente pochissimi, chiusi fuori dalla Rete da un *digital divide* alla rovescia.

Adesso il discorso è molto diverso, il Parlamento è attento a queste cose, un gruppo di parlamentari si è aggregato numeroso intorno a queste questioni. Certamente - ho atteso a dire queste cose che tornasse Soro - il Garante della privacy è un'istituzione che è sempre stata avanti, da questo punto di vista, è *digital native*,

è nata all'epoca di Internet e sta portando avanti questa consapevolezza. Questo è il primo dato: c'è una maggiore attenzione, significativa e consapevole, nelle istituzioni.

Il secondo fatto è che due o tre conflitti globali si stanno svolgendo intorno alle questioni della Rete, se ci sarà o no neutralità, se l'educazione del futuro sarà digitale. Sono questioni epocali, dobbiamo cambiare il sistema dell'educazione, dell'istruzione, stiamo dicendo quanto e come deve essere utilizzata la Rete e Internet digitale per questo. Poi stiamo prendendo delle decisioni pazzesche, tipo: per la sicurezza dei nostri cittadini dobbiamo rinunciare alla privacy o viceversa, cosa sarà deciso di fronte a questo?

Sono dei crinali sui quali è talmente importante la decisione che si prende, che la consapevolezza è necessariamente destinata a crescere attorno a queste cose. L'ambiente digitale che conosciamo ormai è diventato prevalente nella nostra vita: Martin Hilbert, alla Annenberg School for Communication and Journalism della University of Southern dice che l'informazione registrata nel pianeta nel 2000 era per il 25% in digitale, nel 2013 era per il 98% in digitale. Tutto ciò non solo perché sono diminuiti i giornali di carta e i dischi in vinile, ma soprattutto perché è aumentata clamorosamente la quantità di informazioni che viene registrata in digitale.

Siamo in un ambiente digitalizzato per il 98% di quello che sappiamo: le conseguenze sono che la memorizzazione, l'elaborazione e la comunicazione sono molto più veloci, più facili, sfuggono più facilmente alla nostra coscienza abituata a tempi più lunghi e problemi più piccoli: ma ci adattiamo, impariamo, ed evidentemente stiamo prendendo consapevolezza di questo. Stiamo imparando a riconoscere che i conflitti fondamentali su *neutrality*, educazione, sicurezza o privacy portano a scelte decisive.

Come si approcceranno queste cose? Io suggerisco, tanto per farla breve, di prendere esempio da come abbiamo imparato a trattare l'ecosistema, è una cosa che ci aiuta perché è un sistema di interdipendenze: non si governa l'ecosistema prendendo un punto

di vista soltanto e l'ecosistema della Rete non è diverso. Quando prendiamo delle decisioni su questo dobbiamo prima fare una specie di valutazione di impatto digitale. Se facciamo di tutto solo a favore del copyright, sappiamo che distruggeremo il pubblico dominio, con tutte le conseguenze del caso. Se pensiamo che tutto sia sicurezza, distruggeremo la privacy, la libertà e l'espressione individuale.

Al fondo di tutto c'è una consapevolezza fondamentale, ecosistemica, che la Rete è un bene comune, come l'ambiente, come la natura, come gli oceani, che è capace di aggiustarsi in parte attraverso le sue intrinseche dinamiche innovative, a patto che sia neutrale, a patto che nessuno possa discriminare i dati. Se nessuno può discriminare i dati, da qualche parte c'è qualcuno che sta provando a portare all'attenzione di tutti l'innovazione che risolve il problema del quale stiamo parlando.

Se la Rete non è neutrale, decidono le grandi piattaforme, i grandi operatori o le istituzioni pubbliche. In quel caso il frutto dell'evoluzione è simile a una monocoltura nella quale l'ambiente è debole, fragile, poche variazioni possono distruggerlo o renderci la vita peggiore. L'ecosistema è ricco nella biodiversità, l'ecosistema digitale è ricco nell'infodiversità, la *net neutrality* è il diritto fondamentale e specifico della Rete che consente ai dati di non essere discriminati da nessuno e agli innovatori di provare a proporre la loro visione liberamente, come soluzione a quello che vedono nascere come problema in Rete.

Augusta Iannini

Io credo che ognuno dei relatori abbia lanciato dei messaggi che poi potranno essere coltivati con le successive tavole rotonde. Io non so se ognuno di loro vuole raccogliere, in un secondo velocissimo giro, degli spunti dagli interventi precedenti e, se del caso, perfezionare un po' il messaggio che avevano introdotto nel

precedente intervento. Velocemente, professor De Martin, su questo ecosistema.

Juan Carlos De Martin

Certo, rapidamente. Tra le molte cose che sarebbe interessante commentare, ne scelgo una, che ha enunciato Don Antonio Spadaro. Mi riferisco alla sua metafora della casa e sulla famiglia, di Internet che diventa sempre più invisibile. In realtà, nello specifico caso di Internet c'è un importante aspetto che va, a mio avviso, tenuto in conto.

È vero, infatti, che - nell'immagine di Don Spadaro - l'aspetto sostanziale è la famiglia, non la casa. Tuttavia, se le stanze sono piccole o grandi, se sedendomi sul divano ricevo una scossa, questo può avere un impatto molto forte sulla vita della famiglia. Nel caso di Internet, a differenza di altre infrastrutture di telecomunicazione, c'è una comunità di persone che dice: *"veramente la casa vorrei continuare a progettarla anche io"*. In altre parole, la casa non è data una volta per sempre, ma può assumere molte forme diverse. Mi sembra importante ricordarlo, anche da un punto di vista democratico.

Augusta Iannini

Padre Spadaro, la tecnologia vuole dare un messaggio? Come risponde?

Antonio Spadaro

Su questo sono assolutamente d'accordo, poi la potenza delle metafore ci aiuta a riflettere. Una volta la tecnologia era macchinosa,

cioè la macchina era "macchinosa", quindi l'accesso era pesante.

Vi ricordate i primi accessi a Internet attraverso il modem, la famosa scatoletta che emetteva un tipico e strano rumore? Dovevi sederti, accendere il computer, avviare il browser, avviare il modem, far partire una connessione. Tutto questo processo costituiva la pesantezza e la macchinosità della macchina. Invece adesso io sono già in Rete e sono qui, quindi non ho bisogno di accedere. La Rete è già nel mio cellulare, che è nella mia tasca. È questo che intendo dire come invisibilità e trasparenza, perché c'è un accesso che non mediato da un approccio liminare, quindi da soglie da attraversare. In questo consiste l'invisibilità dell'accesso.

Solo una parola in più sull'educazione, perché, Lei, appunto ha fatto questa affermazione, che è un argomento che non ho trattato, che richiederebbe una trattazione a parte. È un tema fondamentale. Qui c'è un problema, quello che abbiamo visto in questi anni, ovvero che l'educazione dei nativi digitali è stata curata da non nativi digitali, che hanno vissuto quella che definivo la schizofrenia tra il reale e il virtuale.

Io ho avuto una tappa della mia vita da educatore. La mia formazione, ovviamente, non è stata digitale, dato che ho 48 anni. Ne ho avuto una assolutamente logico-lineare-sequenziale. Mi rendevo conto però che il modo in cui i ragazzi nativi digitali mi parlavano della Rete era assolutamente incongruo, perché l'esperienza a cui facevano riferimento era quella che loro effettivamente avevano, ma il linguaggio per nominare l'esperienza era quello acquisito da persone che non avevano l'esperienza digitale.

In loro dunque era attiva una schizofrenia di linguaggio molto singolare. Così ho verificato che i giovani vivono in maniera corretta e coerente la loro presenza in Rete, ma nel momento in cui la tematizzano anche verbalmente, questa tematizzazione diventa incongrua.

Il tema dell'educazione diventa importante perché nel momento in cui il digitale diventa un ambiente, si struttura in

un ambiente, non hai bisogno solo e semplicemente di abituarti, ma - per usare sempre la metafora della casa già esposta precedentemente - devi "ad-domesticare" un ambiente, con tutte le connotazioni che l'addomesticare implica. Il processo educativo è uno dei nodi fondamentali per il nostro futuro.

Augusta Iannini

Dottor De Biase una domanda secca: in questa Infosfera, che è un ecosistema come Lei ce l'ha descritto, in cui tutti noi siamo immersi, a Suo giudizio c'è spazio per il bilanciamento di tanti interessi?

Luca De Biase

Questo è il punto, se il conflitto sarà frontale, ad esempio tra gli operatori telefonici che vogliono controllare la Rete abolendo la *net neutrality* e *the rest of us*, non ne usciremo, vincerà la lobby più forte, vincerà la lobby che riesce a prevalere. La governance della Rete richiede, come da molto tempo si dice, una logica *multi stakeholder*, che cosa voglia dire questo lo sanno di più gli studiosi della democrazia, che un giornalista che ci lavora ogni giorno. Stiamo parlando di livelli istituzionali e costituzionali complessi, seri, importanti, sui quali davvero ci dobbiamo impegnare per fare un salto costituzionale. Rispetto a questo il lavoro della Commissione presieduta dalla Presidente Boldrini alla Camera va sicuramente in questa direzione, parte dalla volontà di realizzare questo tipo di cose.

Rendiamoci conto che bisogna andare anche un pochino veloci, abbiamo parlato di organismi informazionali: la Deep knowledge ventures, una società di *ventures capital* di Hong Kong, ha cooptato nel Consiglio di amministrazione, con lo stesso

potere decisionale degli umani, un algoritmo chiamato Vital. È l'algoritmo di una macchina che impara dai dati che sono in Rete e prende delle decisioni, che nella finanza, noi sappiamo, sono molto spesso e sempre più spesso prese da algoritmi.

Non è da ridere questa cosa, è una realtà, noi prendiamo delle decisioni di sistema, fondamentali, sul mercato finanziario, che decidono del destino di generazioni come quelle che noi stiamo conoscendo in questo periodo. Sono sistemi decisionali dati in pasto a organismi informazionali chiamati algoritmi.

Se noi umani vogliamo continuare a dire qualcosa in questa Infosfera nella quale nuove specie stanno crescendo - lasciatemelo dire per gioco, ma è un po' così - sarà bene che facciamo velocemente un salto di consapevolezza e di regole costituzionali, cioè come decidiamo in maniera *multi stakeholder*, intorno a queste cose: se vince solo uno perderemo tutti.

Augusta Iannini

Bene, grazie e passiamo alla seconda tavola rotonda, la professoressa Califano e i suoi relatori sono invitati a salire sul palco, grazie.

IoT e protezione dei dati personali

Sessione II

Massimo Russo
Direttore di "Wired Italia"

Lella Mazzoli
Università degli studi di Urbino "Carlo Bo"

Roberto Baldoni
Università degli studi di Roma "La Sapienza"

Moderatore **Licia Califano**
Componente del Garante per la protezione dei dati personali

Sessione II

IoT e protezione dei dati personali

Licia Califano

In questa seconda sessione sposteremo l'attenzione su un tema di grande interesse, che definiremo, più nello specifico, "Internet delle cose". Occorre preliminarmente chiarire cosa si intende con questa espressione e quali sono le principali problematiche che questo tema porta con sé.

Che cosa si intende per Internet delle cose?

Al momento sono due i principali documenti che affrontano il problema dell'Internet delle cose in connessione con le esigenze di tutela della riservatezza e protezione dei dati personali: l'Opinione n. 8/2014 sui recenti sviluppi di Internet delle cose, adottata dal Working Party 29 nel settembre 2014 e la Dichiarazione di Mauritius, adottata il 14 ottobre 2014 nel corso della 36ma Conferenza internazionale delle Autorità per la protezione dei dati e la privacy di tutto il mondo.

In particolare il primo documento del WP 29 definisce con l'acronimo IoT ("Internet delle cose" dall'inglese *Internet of Things*) quelle tecnologie applicabili ad oggetti di uso quotidiano e comune che il gruppo Articolo 29 ha individuato in tre macro-categorie, peraltro indicative e non del tutto esaustive, visto il continuo incremento tecnologico.

In primo luogo pensiamo ai computer indossabili (i cd. *wearable computing*), per esempio abiti, accessori e altri dispositivi, occhiali indossabili dalle persone. In secondo luogo ci si riferisce al cd. *quantified self* ovvero sensori o ad altri dispositivi che sono utilizzati per misurazione di prestazioni o condizioni corporee,

per esempio i cronometri da polso che calcolano la distanza quando facciamo jogging o applicazioni e strumenti utilizzabili in campo sanitario.

Infine, vi è una terza categoria di oggetti che indichiamo come "domotica", cioè il frigorifero intelligente, la casa intelligente, gli allarmi antiincendio, le lavatrici collegate ad Internet.

Tali categorie di strumenti tecnologici trovano poi applicazione all'interno di differenti ambiti, dal trasporto privato (applicazioni di *infomobility*) alla sanità, con le applicazioni di *eHealth* volte a consentire il monitoraggio a distanza delle condizioni dei pazienti (telemedicina) lasciandoli vivere tranquillamente nel proprio ambiente domestico e familiare, fino a giungere ai cd. edifici intelligenti con applicazioni all'interno della casa per la gestione della stessa (*Smart Home)* e, più in generale, degli edifici residenziali, commerciali e industriali (*Smart Building*).

Si tratta di settori tecnologici in grande sviluppo, caratterizzati da un legame diretto, quasi fisico, con l'individuo che li utilizza e che, spesso inconsapevolmente, interscambia dati personali. Molto spesso l'individuo neanche sa che questi dispositivi funzionano non con particolari tecnologie ma semplicemente tramite un collegamento a Internet (quindi siamo nell'ambito delle comunicazioni elettroniche) oppure tramite l'utilizzo di tecnologie a medio raggio in radio frequenza (ovverosia Rfid e bluetooth).

Ora, non c'è dubbio che si tratta di strumenti che rappresentano una prospettiva importante di sviluppo e che quindi hanno anche delle influenze forti nell'ambito dello sviluppo economico del nostro Paese. È vero però, come si diceva, che l'individuo che li utilizza è spesso inconsapevole di ciò che in realtà rappresentano e di come, attraverso questi oggetti, si interscambiano dati personali.

L'Osservatorio *Internet of Things* della School of Management del Politecnico di Milano ci informa che nel 2013 in Italia sono stati 6 milioni gli oggetti interconnessi tramite rete cellulare, con un

aumento del 20 per cento in più rispetto all'anno precedente. E il fenomeno è in costante aumento e deve essere pertanto letto con differenti approcci e con differenti prospettive.

Tuttavia, in termini volutamente provocatori e dialettici, si potrebbe porre una domanda: "serve davvero Internet delle cose?"

Non c'è dubbio, infatti, che, da un certo punto di vista, l'IoT ci semplifichi la vita e che sia nato proprio per questo fine. Tuttavia non si possono nascondere i possibili abusi e i rischi innegabilmente connessi alla sicurezza e alla privacy, trattandosi di flussi di dati personali.

Trasferendo queste valutazioni volutamente provocatorie su un piano di analisi giuridica, occorre attribuire un nome a tali "preoccupazioni". Occorre infatti riflettere su una serie di questioni, individuate nella già citata Opinione del WP 29 quali il rischio di una asimmetria informativa, la possibilità che avvenga una profilazione dei soggetti che utilizzano IoT e, infine, la sicurezza dei dati personali.

Nel corso del convegno cercheremo, dunque, di sviluppare tali questioni, grazie al contributo dei relatori.

In primo luogo il dottor Massimo Russo, Direttore della rivista *Wired Italia*, che affronterà il tema dell'importanza della comunicazione e dell'approccio in grado di consentire all'utente una corretta informazione delle potenzialità ma anche dei rischi che sono insiti in ciò che chiamiamo e che abbiamo definito l'Internet delle cose. Questo in analogia con quanto mi pare essere lo spirito proprio della rivista che egli dirige, una finestra sempre aperta sui temi del progresso tecnologico che ha riproposto con successo in Italia il modello editoriale nato negli Stati Uniti anni fa.

Seguirà l'intervento della prof.ssa Lella Mazzoli, Professore ordinario di Sociologia dei processi culturali e comunicativi presso l'Università di Urbino "Carlo Bo", Direttore del Dipartimento di Scienze della comunicazione e discipline umanistiche nonché Direttore dell'Istituto per la formazione al giornalismo nel medesimo

Ateneo. Ha scritto tantissimi libri che non mi soffermo ad elencare, considerandoli noti e conosciuti.

Infine ascolteremo il contributo del Professor Roberto Baldoni, ordinario di Sistemi distribuiti presso la facoltà di Ingegneria dell'informazione dell'Università "la Sapienza" di Roma, dove peraltro dirige il Centro di ricerca in *Cyber Intelligence* e *Information security*. Il Prof. Baldoni definirà le caratteristiche del fenomeno dal punto di vista tecnologico e della sicurezza dei sistemi informatici.

Massimo Russo

Grazie. Buongiorno a tutti, grazie per avermi invitato. La tesi che sosterrò oggi con voi è che in realtà quel che sta succedendo con l'Internet delle cose non è qualcosa che ci obbliga a un semplice adeguamento delle normative, dei nostri stili di vita, a rivalutare rischi e opportunità. Serve un nuovo contratto sociale.

Il punto è che ci sono dei momenti della storia - e questo è uno di quelli - in cui l'accelerazione alla quale siamo sottoposti è tale che quel che esisteva fino a prima non funziona più. Gli strumenti ci sembrano improvvisamente inadeguati. Quel che stiamo vivendo oggi è paragonabile, nella storia della civiltà umana, solo alla prima e alla seconda rivoluzione industriale.

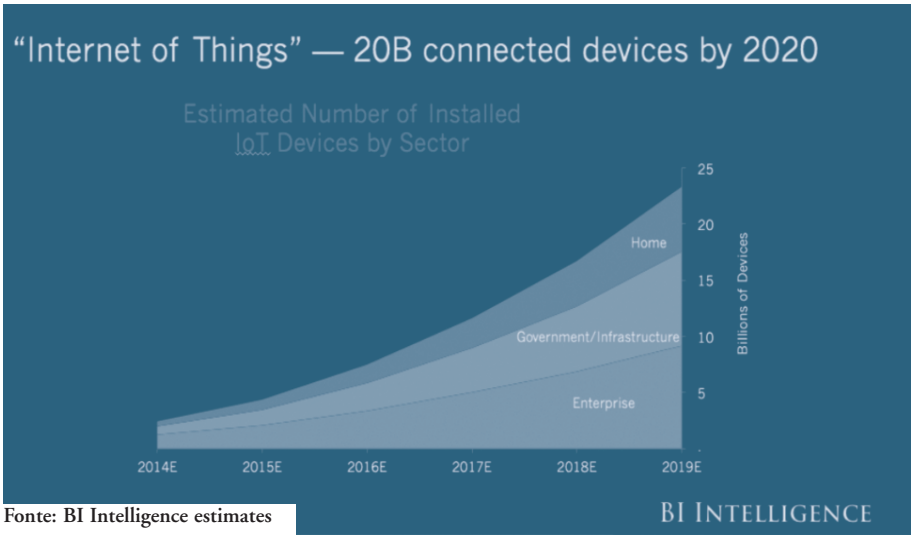
Di fronte a quel tipo di eventi, la reazione che avevamo era ed è, all'inizio, una reazione di sgomento, di paura, di visione del rischio più che delle opportunità. Indubbiamente le prime rivoluzioni industriali sono stati periodi che hanno portato trasformazioni e squilibri molto forti, rispetto ai quali, se oggi dovessimo dare un giudizio storico, certamente non potrebbe che essere positivo. Ci sono degli istanti - quello che stiamo vivendo oggi è uno di questi - in cui l'attitudine delle persone è la paura più che la comprensione.

Guardiamo questo video - le immagini dei fratelli Lumiere

dell'arrivo di un treno in stazione (*https://www.youtube.com/watch?v=-t1fztfz96A*) - e non ci suscita alcuna reazione. Oggi in questa sala, vedo qualche sorriso ma non vedo facce particolarmente preoccupate. Nel 1895, quando venne proiettato per la prima volta, provocò urla scomposte e la fuga dalla sala.

Ecco, quel tipo di urlo, quel tipo di panico è esattamente il momento che noi stiamo vivendo oggi e quell'urlo è oggi l'urlo che possiamo vedere in quest'altro video (*https://www.youtube.com/watch?v=t9Fxp3HK6DI*). È una macchina che si guida da sola, oggi da questo tipo di automobile sono stati percorsi centinaia di migliaia di chilometri, il video è del 2011. Sentite l'urlo? È l'urlo di panico di chi non vede le mani sul volante, di chi si trova di fronte a una distonia tra quel che gli comunicano i sensi e quel che ritiene possibile. Questo tipo di automobili, che oggi sono legali in alcuni Stati degli Stati Uniti e permettono ad esempio alle persone non vedenti di condurre una vita normale, di andare a fare la spesa, di tornare a casa, eccetera, sono possibili grazie a Internet delle cose e grazie ai sensori di cui stiamo parlando, combinati con una serie di altre cose, la più importante delle quali è l'intelligenza artificiale.

Quella che vediamo qui è una slide che ci racconta la crescita tumultuosa che stiamo vivendo.



Fonte: BI Intelligence estimates

Ci abbiamo messo quindici anni per collegare un miliardo e mezzo di computer alla Rete. Nel solo 2014 sono stati venduti circa un miliardo e mezzo di smartphone. In un anno abbiamo venduto, abbiamo immesso sul mercato lo stesso numero di dispositivi connessi che abbiamo impiegato quindici anni per installare, in precedenza.

Non solo, è anche una questione di potere di calcolo, di capacità di calcolo: noi tutti abbiamo in tasca oggetti come questo smartphone, che oggi hanno più potenza di calcolo di quanta ne disponesse il Governo degli Stati Uniti tra la fine degli anni '70 e l'inizio degli anni '80. Poi se li usiamo per giocare a Candy Crush piuttosto che per gestire il Governo federale di una superpotenza, ciò attiene a quel che noi facciamo delle cose, ma senza dubbio questo è un fattore che cambia completamente le cose.

Come diceva la professoressa Califano introducendo la nostra porzione di dibattito, ciò di cui stiamo parlando oggi è il frigo connesso con la lavatrice? È l'impianto elettrico di casa che ci permette di ridurre i consumi? È il tostapane che avvisa quando si guasta? È la possibilità di avere una serie di oggetti indossabili che ci monitorano, o non è, piuttosto, un totale cambiamento di paradigma?

Cambiamento di paradigma che è dato dall'incontro non solo di Internet, cioè della rete degli oggetti con il mondo reale, ma che è dato, in realtà, dalla combinazione di tre elementi. Il primo è Internet delle cose, il secondo, come dicevo qualche istante fa, è la possibilità di analizzare e di disporre di un'enorme quantità di informazioni, il big data, che si riversa su di noi. Chi detiene la capacità di analizzare queste informazioni oggi ha la chiave dell'economia e dello sviluppo.

Un esempio: ogni ora una catena di grande distribuzione come Walmart analizza le transazioni dei propri clienti, di quelli che vanno ad acquistare nei propri supermercati, e raccoglie 2,5 petabyte di dati, che è una cifra che detta così non significa nulla. Ci dice qualcosa però se consideriamo che si tratta di dieci volte

le informazioni contenute in tutti i libri nella Biblioteca del Congresso federale degli Stati Uniti. Ogni ora Walmart analizza 2,5 petabyte, cioè dieci volte la biblioteca del Congresso degli Stati Uniti, e ne trae conclusioni su condotte future.

Immaginate miliardi di sensori, 20 miliardi di sensori alla fine di questo decennio. Immaginate questa enorme quantità di dati, immaginate, ora, la capacità di analizzare questi dati, perché, come dice il fondatore del TED Saul Wurman, i *big data* di per sé sono una cosa stupida, serve il *big understanding*, la capacità di capirli. Questo *big understanding* oggi viene dato dall'intelligenza artificiale.

Prima Luca De Biase ricordava dell'algoritmo che è stato cooptato nel board di amministrazione di una società di *venture capital* di Hong Kong: l'intelligenza artificiale in questo momento è uno dei panorami che accelera più rapidamente dietro il finestrino del nostro treno.

Se noi mettiamo insieme l'Internet of Things, i *big data* e l'intelligenza artificiale è lì che tutto in qualche modo esplode.

C'è una società che è stata acquisita da Google all'inizio dell'anno scorso, che si occupa di intelligenza artificiale, si chiama Deepmind. Il video (*https://www.youtube.com/watch?v=EfGD2qveGdQ*) che ora vediamo proviene da una rara dimostrazione che c'è stata lo scorso anno, e racconta il processo di apprendimento di un algoritmo che si confronta con alcuni videogiochi: nella prima ora l'algoritmo perde, poi inizia a vincere. Qui siamo già dopo 240 minuti di auto istruzione e guardate, non solo vince sempre, ma trova una falla nel sistema e fa sì che l'avversario si autodistrugga, si distrugga da solo.

Stiamo parlando di macchine talmente efficienti che non solo sono in grado di svolgere al meglio i compiti che noi affidiamo loro, ma che sono anche in grado di apprendere e di individuare le falle nel sistema, in questo caso videogiochi e di perseguire l'obiettivo che è stato dato loro, anche al di là della stessa comprensione e conoscenza di chi ha messo in piedi questi algoritmi. Come dicono i ricercatori: *"it ruthlessly exploits the weaknesses of the system"*.

Immaginate questo tipo di algoritmi che auto apprendono, applicati non ai videogiochi, ma agli ambiti del nostro vivere: all'economia, alla finanza, in parte alla soluzione di problemi e alla gestione di sistemi complessi. Ci rendiamo conto di come in realtà Internet of things, i sensori, i *big data* e l'intelligenza artificiale siano già qui oggi e siano protagonisti di alcuni straordinari cambiamenti che ci chiederanno di ridefinire diritti e concetti fondamentali e segneranno la necessità della nascita di discipline come l'etica delle macchine.

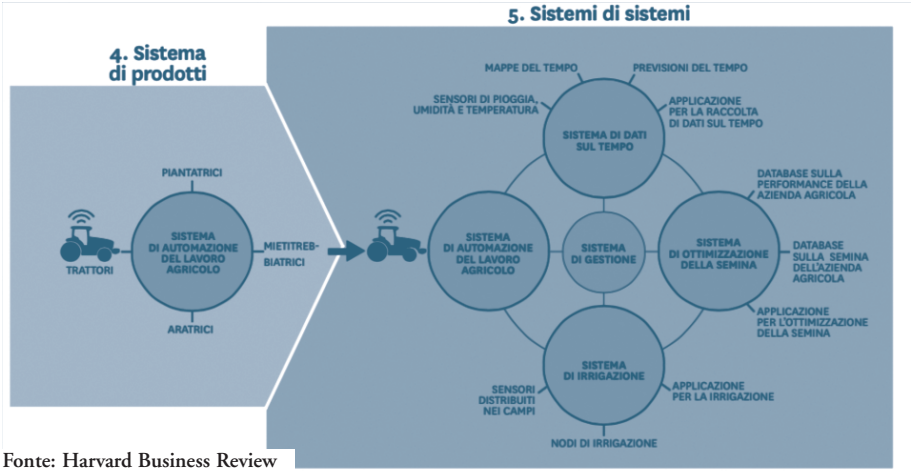
Ora, per definire l'Internet of Things, bisogna fare un passo indietro. Quando si parla di Internet of Things, si intendono tre cose. La prima è l'uno a uno, è un Internet delle cose molto semplice, proviamo a immaginarla, a rapportarla nella nostra vita quotidiana: è la nostra automobile che ha strumenti di auto diagnostica, la portiamo dal meccanico che la collega a un computer e rileva i dati. Questo è l'Internet of Things uno a uno.

Poi c'è l'Internet of Things *one to many*, da uno a molti, questo è quel che succede quando Tesla, che è un nuovo tipo di fabbricante di automobili, che oltre a vendere hardware gestisce informazione, avendo rilevato dai parametri delle proprie automobili quali sono le modalità più efficienti di utilizzo, come farebbe Apple rilasciando un aggiornamento, dalla propria centrale istruisce le automobili con un aggiornamento del proprio sistema operativo e le rende più efficienti. *One to many*: c'è un centro che istruisce molti sensori riceventi, sulla base di informazioni che a sua volta aveva ricevuto da essi, ed elaborato in precedenza.

Ma ancora non è questo, il tipo più potente di Internet delle cose. Il più esplosivo è sicuramente l'ultimo: *many to many*, il mondo di quei 20 miliardi di sensori che dialogano tra loro.

Quando tutto questo accade, in realtà è l'economia che ne viene totalmente scardinata, perché all'improvviso - qui vediamo un esempio tratto dall'*Harvard Business Review* - non parliamo solo di un prodotto intelligente, in questo caso un trattore, che può essere gestito attraverso computer da remoto, ma si tratta di un intero settore

industriale che entra in collisione, in competizione, in concorrenza con settori che prima erano molto diversi.



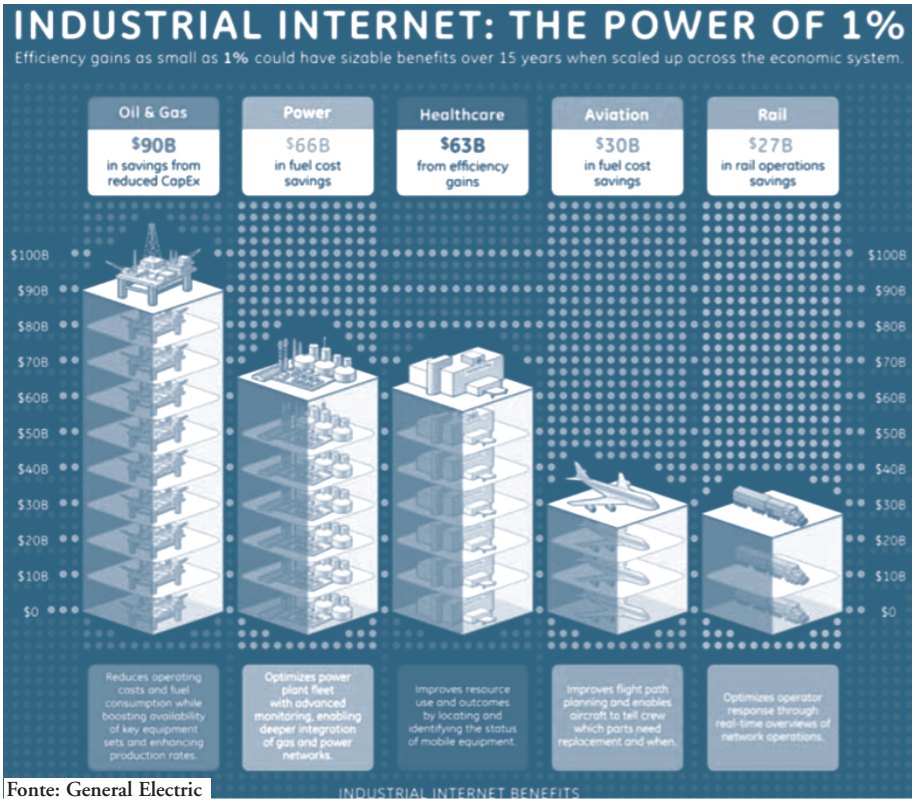
Fonte: Harvard Business Review

Quando il trattore entra a far parte di un sistema di automazione del lavoro agricolo, questo sistema di automazione del lavoro agricolo basato sull'informazione entra a sua volta in concorrenza, competizione e comunicazione con sistemi che prima erano in settori totalmente separati dell'economia: da società specializzate nella previsione del clima, ad aziende che producono sementi anche sulla base delle informazioni rilevate da milioni di trattori equipaggiati con sensori collegati alla Rete. Le aziende non producono più prodotti, o meglio, non producono solo prodotti, ma soprattutto gestiscono informazioni.

Ecco perché le catene del valore vengono completamente scardinate, ecco perché troviamo *Over the Top* - piattaforme digitali - che esercitano il loro ruolo economico in settori dove prima c'erano solo aziende industriali con un conto economico e una struttura assolutamente diversa, ecco perché tutto ciò è dirompente. Allora, se questa Internet of Things *many to many* è già presente, vediamo alcuni degli ambiti più interessanti in cui questa gestione delle informazioni - che poi diventa prodotto - sta esplicando i suoi risultati.

L'impresa italiana Selex sta installando in molte città americane, a cominciare da New York, un sistema (Di-boss) per la

gestione automatica degli edifici. Il sistema comporta ad esempio un'ottimizzazione e un risparmio significativo di energia, perché permette di ottimizzare sulla base delle necessità delle persone, di accendere e spegnere il riscaldamento nelle diverse aree sulla base della rilevazione di esseri umani. Certo, comporta forme più accentuate di controllo, perché significa, ad esempio, rilevare la presenza delle persone negli edifici e, se alle 17 tutti sono usciti dagli uffici, abbassare la temperatura di 4 o 5°.

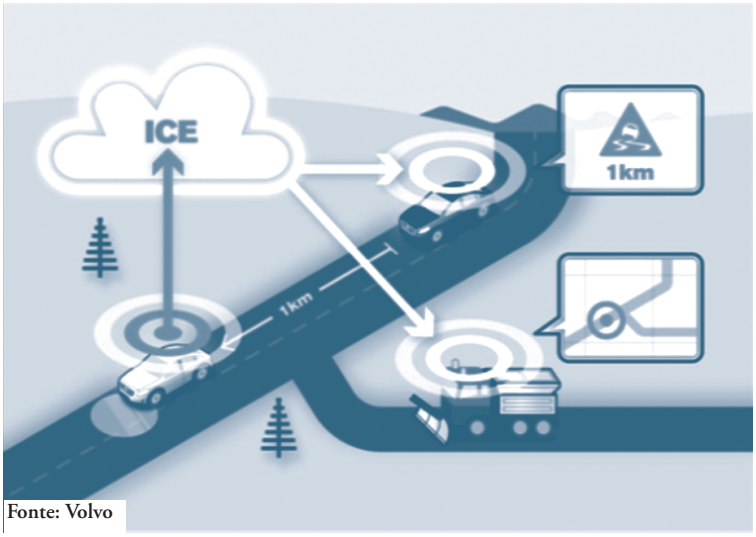


Fonte: General Electric

Questo è un altro esempio di Internet delle cose già oggi possibile: rappresenta i risparmi che General Electric ha stimato in diversi comparti industriali, grazie a Internet delle cose. Il miglioramento di efficienza marginale dell'1% può portare a diversi miliardi di dollari risparmio e di efficienza.

O, ancora, ecco un esempio di auto connessa, lo sta

sperimentando Volvo in Svezia. Vedete: la prima automobile ha dei rilevatori. Il fatto che ci sia ghiaccio sulla strada viene notificato allo spazzaneve e simultaneamente anche all'auto che segue un chilometro indietro. Quindi l'auto che segue in qualche modo modererà la velocità e avvertirà il proprio conducente del fatto che in quella zona c'è ghiaccio.



Fonte: Volvo

Ovviamente tutto ciò porta a un miglioramento significativo delle condizioni nelle quali viviamo, perché probabilmente permette di prevenire incidenti, di rendere più efficace la pulizia delle strade. Ma qual è il contratto sociale sulla base del quale ogni individuo sarà disponibile a condividere i propri dati sulla posizione con gli altri automobilisti, con le case fabbricanti di auto e con l'ente che gestisce le strade?

Ci sono diverse aziende americane che già lavorano su un'altra frontiera. Stanno progettando l'usabilità e la modalità con le quali si possono impiantare dei dispositivi sottopelle, che permettono di monitorare le nostre condizioni di salute, non solo, ma anche di prendere decisioni. Immaginiamoci, per un diabetico, che ci sia la possibilità di rilasciare insulina sulla base della misurazione continua della sua glicemia. Ci sono aziende che già oggi si pongono il problema di come debbano essere le interfacce

con le quali comanderemo, gestiremo, dialogheremo e chi dovrà avere accesso alle informazioni e sarà in grado di prendere le decisioni riguardo a tutto ciò.

Se questo è il panorama che abbiamo tracciato fino ad ora, secondo me si possono in qualche modo evidenziare delle linee guida, attraverso le quali affrontare questo cambio di paradigma.

AGENDA E LINEE GUIDA

1) Ridefinizione del concetto di privacy
2) Habeas data è il nuovo Habeas corpus
3) Un nuovo contratto sociale per la condivisione dei dati
4) Tutelare il criptaggio e l'anonimato
5) Proteggere il whistleblowing
6) Più che proibire, rendere accessibili le basi di dati secondo protocolli standard (open data pubblico e privato) e renderle interoperabili
7) Cambiare scala: regolamenti a livello europeo
8) Autorizzazioni flessibili: durata limitata nel tempo e nello spazio
9) < Leggi draconiane (già superate dai fatti) o allarmi generalizzati
10) > Coscienza critica

Da una parte è sicuramente necessario ridefinire il concetto di privacy, che non può più essere, in un'epoca come questa, *the right to be alone*, cioè il diritto di essere lasciati soli.

Certo, si può scegliere di essere lasciati soli, ma semplicemente non si farà più parte di questa società. In qualche modo la privacy va rinegoziata secondo linee diverse che non possono che essere linee di apertura, con la possibilità per il singolo di disponibilità dei dati che lo riguardano e di conoscenza di chi e come li sta utilizzando.

Faccio un altro esempio. Ancora discutiamo se sia corretto o meno archiviare tutti i nostri dati medici all'interno del fascicolo sanitario elettronico, per i presunti rischi che ciò comporta. Ma lo scenario è già cambiato. Attraverso la medicina predittiva, la

possibilità di accoppiare la raccolta del Dna di numerosi pazienti al *data mining* offre la *chance* di trovare la soluzione a numerose malattie.

In queste condizioni, chi rifiutasse di conferire alla ricerca il proprio materiale genetico - forse la parte più privata di noi stessi - starebbe esercitando un diritto o starebbe adottando un comportamento antisociale?

Se questa è la scala dei cambiamenti ritengo che le sentenze della Corte di Giustizia Europea come la *Costeja Gonzalez* sul diritto all'oblio (*C-131/12 Google Spain SL, Google Inc. / Agencia Española de Protección de Datos*), che è stata ricordata stamattina, in realtà non facciano che allontanarci, allontanare l'Europa, allontanare noi stessi dalle possibilità offerte da questo nuovo mondo.

Una parte rilevante del futuro di ognuno di noi in Rete, se vogliamo far parte di questo mondo, sarà la nostra reputazione.

La possibilità di gestire e manomettere la nostra reputazione come ci conviene, deindicizzando dati leciti dai motori di ricerca, anche se non siamo personaggi pubblici (qualsiasi cosa ciò possa significare oggi), è una cosa che mina le possibilità della *sharing economy*. Ci sono servizi, strumenti che oggi non sarebbero utilizzabili se ognuno di noi potesse gestire a piacimento la propria reputazione personale online. Pensiamo ad esempio ai servizi che permettono la condivisione degli alloggi, o ai servizi che permettono la condivisione dei trasporti, alle recensioni che riguardano servizi come alberghi o ristoranti o le nostre capacità professionali, per fare solo gli esempi più facili.

Se ciò è vero, bisogna riconoscere al tempo stesso che in quest'epoca l'*habeas data* è divenuto parte integrante dei diritti fondamentali, cioè dell'*habeas corpus*. È necessario un nuovo contratto sociale per la condivisione dei dati, il che significa che ognuno di noi dovrebbe avere consapevolezza dei dati su di sé che sono rilevati, ma anche che i dati, in qualche modo, dovrebbero essere a disposizione, dovrebbero essere aperti, non solo a chi li ha raccolti. Se le informazioni sono il petrolio

del XXI secolo, questo petrolio per la prima volta non è una risorsa scarsa, ma può servire sia alla piattaforma che lo ha estratto, sia ad altre piattaforme nuove entranti nell'area economica, nell'area culturale, nell'area della Rete.

Una parte integrante e significativa di un sistema che si viene a configurare in modo così aperto, però, è, dall'altra parte, la protezione rinforzata dell'anonimato e del criptaggio dei dati nelle comunicazioni personali. Si tratta di contrappesi essenziali. L'altro giorno il premier inglese David Cameron ha proposto di decrittare tutte le comunicazioni in rete, perché tanto chi è onesto non ha nulla da temere. Credo che questa sia una delle cose più pericolose che possano capitare. Dall'altra bisogna proteggere l'anonimato anche con i *whistleblower*, cioè proteggere chi, in qualsiasi momento, voglia rendere noto che le cose non stanno andando come dovrebbero, che c'è qualcuno che sta violando le norme.

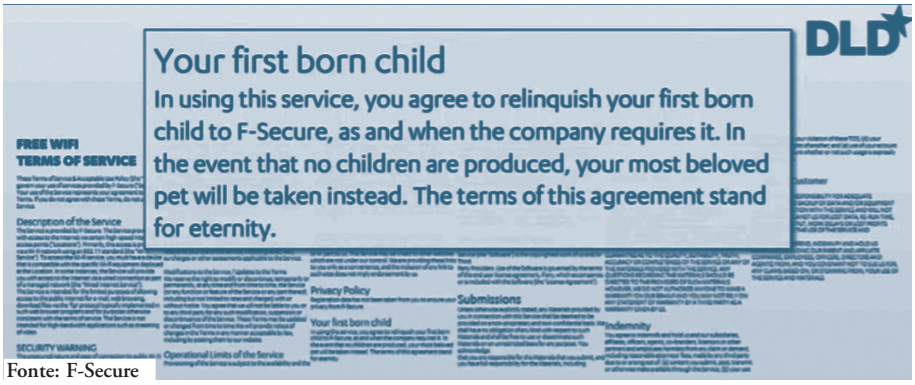
Infine credo sia ridicolo pensare ancora a normative sulla privacy che non siano di tipo continentale, dato che esistono 28 Authority per la privacy, sia pure coordinate a livello europeo, con regolamenti molto diversi. Provate a comparare quello che si dice in Irlanda con quello che si dice in Italia, ad esempio, e vi troverete di fronte a regole diverse, che impediscono la nascita di un mercato e di una società autenticamente continentali.

Sono possibili, da questo punto di vista, anche autorizzazioni all'uso dei dati flessibili nel tempo e nello spazio: ad esempio c'è il rischio di Ebola? Io sono stato nell'aeroporto dove c'è un malato di Ebola? È corretto che il Governo possa disporre dei dati del mio Gps? Sì, va bene, però discutiamo per quanto tempo e per quanti cittadini ciò sia applicabile. A che distanza dall'epicentro di ciò di cui stiamo parlando? Tempo e distanza possono essere parametri sui quali rinegoziare le autorizzazioni all'utilizzo dei nostri dati.

Infine vi lascio con una cosa divertente che ho visto qualche giorno fa. Io ho l'impressione che su tutto il tema della privacy ci sia moltissimo allarme e pochissima consapevolezza. Bisogna lavorare sulla coscienza critica. È stato pubblicato ieri un sondaggio

interessante della Mozilla Foundation che diceva che il 68% delle persone online in Italia è preoccupato che le società Internet sappiano troppo su di loro e la metà di chi naviga, il 54%, non si fida del fatto che il proprio diritto alla privacy sia rispettato online. In apparenza, dunque, grande allarme.

Ma ecco, guardate cosa è successo qualche tempo fa.



Fonte: F-Secure

Un'azienda che si chiama F-Secure ha aperto un *hotspot* gratuito a Londra, con la possibilità di collegarsi al *wi-fi*. Nei *terms and conditions*, cioè nei termini e nelle condizioni d'uso del servizio, ha aggiunto questo comma che diceva: *"Your first-born child" "Il tuo primo figlio"*. "Utilizzando questo servizio acconsenti a che la nostra azienda possa avere il tuo primo figlio; nel caso tu non abbia il primo figlio, ci rivarremo sul tuo animale domestico. I termini di questo servizio valgono per l'eternità".

Tutti hanno accettato e cliccato confermando *I agree* sui *terms and conditions* per avere il *wi-fi*. Tanto allarme da una parte, zero coscienza critica dall'altra.

Licia Califano

Quello prospettatoci da Massimo Russo è uno scenario estremamente complesso, dove, in realtà, la domanda di fondo parrebbe essere: "rincorriamo o cavalchiamo la modernità?".

Io, leggendo la biografia di Massimo Russo, vorrei fargli una domanda immediata.

Lei, nella sua biografia, dice: *"Pratico l'innovazione e coltivo il dubbio"*. È una frase che mi è piaciuta molto, perché effettivamente è un binomio che accomuna molti di noi. Ora, da questa relazione, emerge il profilo dell'innovazione, dell'importanza dell'innovazione. Le chiederei di metterci a parte anche della parte relativa al "dubbio" ovverosia a quelli che sono i principali profili problematici o critici dell'impiego di IoT.

Massimo Russo

Il dubbio è parte integrante della nostra vita quotidiana sulle scelte da intraprendere, però non impedisce di leggere il presente. Io leggo il presente e vedo che le cose di cui vi ho parlato oggi stanno già accadendo e accadranno, a prescindere da quanti di noi sono qui in questa sala oggi. Noi abbiamo una scelta: stare dentro la contemporaneità e in qualche modo tentare di governarla, oppure decidere di starne fuori. Ma ciò vuol dire aver rinunciato a far parte del proprio tempo.

Licia Califano

Sono assolutamente d'accordo, anzi, per il giurista e per la nostra Autorità evidentemente il problema è come la regola giuridica governa la realtà, che è in continuo cambiamento e come, in realtà, un'Autorità che nasce inizialmente con l'idea di una privacy come diritto ad essere lasciati soli (*right to be let alone*), già da tempo ha avuto un'evoluzione importante nella dinamica e nella prospettiva proprio della protezione del dato e quindi nella dimensione che Lei evocava.

La professoressa Lella Mazzoli interviene proprio nel

momento più opportuno come sociologa. A lei chiederei, piuttosto, proprio per aprire la prospettiva sociologica: "Rincorriamo o cavalchiamo la modernità? Il sentimento sociale prevalente è la curiosità o la paura?".

Lella Mazzoli

Internet of Things. L'intelligenza delle cose per la promozione della persona

Chiedere e chiedersi se nei confronti della tecnologia sia più forte il sentimento di curiosità o di paura è una questione che più volte ci poniamo, alla quale non sempre è facile dare risposta anche perchè la conoscenza che abbiamo della tecnologia non è sempre tale da permetterci interpretazioni corrette.

Partirò dal tema della conoscenza e della competenza per rispondere al quesito della professoressa Califano.

Interessanti indicazioni sono già arrivate, oltre che da Massimo Russo, anche dai relatori che ci hanno preceduti.

È la modernità e la contemporaneità a essere cariche di innovazione. Quella che è entrata nelle nostre vite è una innovazione potente e produce in noi sentimenti a volte contrapposti proprio per la sua forza e penetrazione.

Prenderò in esame la tecnologia oggetto del nostro panel: Internet delle Cose (Internet of Things, IoT da qui in avanti).

Do per accettato che oggetti che fanno cose che, se fossero fatte dagli uomini sarebbero intelligenti, sono oggetti intelligenti (possono agire, parlare, interagire). È questa la definizione che Marvin Minsky, John McCarthy *et alii* dettero di Intelligenza Artificiale (AI da qui in avanti) nel 1956 a Dartmouth(1).

(1) Cfr. McCarthy J, Minsky M.L., Rochester N., Shannon C.E. (1956), *A proposal for the Dartmouth summer research project on artificial intelligence*, in AI Magazine, volume 27, numero 4, 2006; Minsky M.L., Seymour P. (1972), *Artificial Intelligence*, University of Oregon Press; Minsky M.L. (1985), *La società della mente*, Adelphi, Milano, 1989.

Questi studiosi di AI prendono le mosse dagli studi di Alan Turing e dal suo test dell'imitazione(2). Gli studi di Turing hanno dato vita alla riflessione filosofica, sociologica e cognitivista e si sono sviluppati in un lungo periodo di analisi, relativamente al tema delle macchine pensanti e del loro impatto nei comportamenti dei soggetti umani(3). Sembrano date e definizioni lontane da noi ma, a mio parere, IoT non si allontana troppo da questi studi e da queste applicazioni. Infatti hanno caratteristiche molto vicine a quelle della AI con in più maggiori capacità per quanto riguarda la relazione e la socialità, ritrovabili, oggi, nel web non ancora compreso negli studi di AI.

Possiamo dire, dunque, che IoT è una evoluzione dell'uso della Rete e uno sviluppo della AI(4). Agli oggetti viene trasferita intelligenza, capacità, ma anche - forse qui sta la più importante innovazione - *relazione*. Più esattamente gli oggetti acquisiscono un ruolo attivo grazie al collegamento con la Rete.

Molteplici i campi di applicabilità. Tra questi:

- sanità: *eHealth* volta a consentire il monitoraggio a distanza delle condizioni dei pazienti (telemedicina), permettendo, in un numero di casi sempre maggiore, alle persone con patologie gravi o invalidanti, di poter continuare a vivere nel proprio ambiente domestico;
- handicap: per le persone con disabilità visive ad esempio l'Istituto Cavazza di Bologna(5) ha studiato e applicato nel tempo alcune sperimentazioni formative e di scrittura che oggi sono contenute in un museo tattile, il Museo Tolomeo, che permette di fare un'esperienza multi-

(2) Cfr. Touring A.M. (1950), *Computing machinery and intelligence*, in Mind, numero 59, pp. 433-460.
(3) Con alcuni collaboratori abbiamo sviluppato il suo pensiero anche per capire le relazioni attivate, fra le persone, attraverso i media sociali. Cfr. Mazzoli L., Giglietto F., *Social System: from simulation to observation*, in Agazzi E. (a cura di) The Legacy Of A.M. Turing, FrancoAngeli, Milano, 2013, pp. 139-148.
(4) Cfr. Cassimally H., McEwen A. (2014), *L'Internet delle cose*, Apogeo, Milano.
(5) Cfr. Istituto Cavazza di Bologna, www.cavazza.it.

sensoriale attraverso oggetti e tecnologie;

- edifici intelligenti: con applicazioni di domotica all'interno della casa (*Smart Home*) e degli edifici commerciali o industriali (*Smart Building*);
- *smart city*: dal gestire le priorità semaforiche sulla base del reale stato del traffico all'illuminazione stradale basata sul livello di luminosità, dal monitoraggio dei parametri ambientali alla raccolta dei rifiuti sulla base del livello di riempimento dei cassonetti;
- trasporto privato: applicazioni di *infomobility*, volte a fornire informazioni utili *real time*, come a esempio il calcolo del percorso più veloce sulla base del reale stato del traffico.

Parliamo, dunque, di oggetti che hanno un ruolo attivo - e partecipativo - vicino a quello che hanno le persone in Rete che chiamiamo comunemente *prosumer*(6) per il fatto che, contestualmente, sono produttori e consumatori di informazione, di critiche, di commenti, di relazioni.

Quanto meno questi oggetti promuovono le relazioni fra cose e persone o fra persone. Con questo voglio sottolineare il fatto che IoT significa far sì che un oggetto tradizionale (*in teoria ogni oggetto*), possa godere di quelle caratteristiche che normalmente hanno gli oggetti innovativi contenuti/nati per la Rete. Non nascono, cioè, nella e per la Rete ma ne acquistano le caratteristiche. Siamo al web 3.0, contraddistinto dal fatto che è un mondo aperto. Uno spazio all'interno del quale gli oggetti possono interagire con ciò che li circonda(7).

(6) Cfr. Toffler A. (1980), L*a terza ondata. I processi di democratizzazione alla fine del XX secolo*, Il Mulino, Bologna, 1998; Bartoletti R., Paltrinieri R. (2012), *Consumo e prosumerismo in rete: processi di creazione del valore*, Franco Angeli, Milano.

(7) Si rimanda qui al concetto di sistema chiuso e sistema aperto. Un sistema è chiuso quando non ha interazioni con l'ambiente, né entra né esce alcuna risorsa. Un sistema è aperto quando ha continui scambi circolari con l'ambiente, Indispensabili per la vitalità del sistema. Cfr. von Bertalanffy L. (1968), *La teoria dei sistemi aperti in fisica e biologia*, Franco Angeli, Milano, 1989; Mazzoli L. (2001), *L'impronta del sociale. La comunicazione tra teorie e tecnologie*, Franco Angeli, Milano.

Non lo fanno in modo *numerico* ma *intelligente* (secondo l'approccio di Minsky e Searle[8]). Lo fanno grazie a *sensori* e *attuattori*. Attraverso i sensori ricevono informazioni e le restituiscono all'ambiente producendo connessioni e interazioni. Queste connessioni e interazioni possono avvenire a distanza senza l'uso di tecnologie pesanti. Molto differenti, più friendly, rispetto ai primi esperimenti di realtà virtuale che utilizzavano oggetti piuttosto invasivi e innaturali[9].

Il rapporto fra sensori e attuatori può essere regolato da monitoraggio e controllo e vuol dire che, grazie ai sensori, è possibile monitorare il comportamento dell'oggetto e far arrivare l'informazione a chi è, a lui connesso. Ma è possibile, anche, comandare cose, oggetti, a distanza.

Interessanti alcuni dati dell'Osservatorio Internet of Things della School of Management del Politecnico di Milano[10]:

- nel primo semestre 2014 in Italia erano 6 milioni gli oggetti connessi tramite tecnologia cellulare (+20% rispetto al 2012);
- altro dato importante è che oltre il 70% delle connessioni deriva da 10 paesi, tra cui l'Italia (al terzo posto per numero di connessioni dopo Uk e Usa);
- tra le applicazioni più utilizzate in Italia nel 2014 ci sono le *Smart Car* (47%, 2 milioni di auto connesse), gli *Smart Metering* (i contatori intelligenti, 26%), le *Smart Home* (9%), le *Smart City* (2%)[11].

Il monitoraggio, fra gli altri interventi possibili, può anche

(8) Cfr. Searle J.R. (1980), *Minds, brains and programs*, in Behavioral and Brain Sciences, volume 3, issue 3, september 1980, pp. 417-424 .
(9) Si veda per tutti Rheingold H. (1992), *La realtà virtuale. I mondi artificiali generati dal computer e il loro potere di trasformare la realtà*, Baskerville, 1993.
(10) Cfr. l'articolo di Luigina Foglietti, *Internet delle cose: cresce in Italia il numero degli oggetti connessi*, in Wired.it, 25 febbraio 2014, [online] testo disponibile in: *http://www.wired.it/Internet/web/2014/02/25/Internet-delle-cose-oggetti-connessi-italia*.
(11) Fonte: Osservatorio Internet of Things della School of Mangement del Politecnico di Milano, *www.osservatori.net/Internet-of-things*.

determinare il controllo delle nostre azioni, dei nostri percorsi, delle nostre scelte.

Fin qui ho tratteggiato un quadro indicativo della evoluzione di questi oggetti ed evidenziato alcune loro applicazioni che vanno a modificare la nostra vita sociale. Vengo ora al tema centrale di questo incontro: la *privacy*

Quel che più a me interessa, per ciò che riguarda la protezione dei dati delle persone, sono gli aspetti sociali di IoT e il loro impatto sui dati personali. Mi interessa capire quanto siano importanti per la qualità della vita e per la sicurezza delle persone. Aspetti non in contrapposizione fra loro. Solo un esempio che ultimamente è apparso agli onori della cronaca. Le scarpe che riportano a casa persone colpite da patologie come l'Alzheimer o altro.

Fuor di dubbio che sensori e attuatori sono dei controllori capaci di monitorare e tracciare percorsi e di dare informazioni. A chi? È sempre pertinente il ricevente? C'è certezza della correttezza del trasferimento dei dati? Questi i quesiti.

Sotto il profilo sociale credo, che questa possibilità di "controllare" e "riportare a casa" persone in difficoltà sia piuttosto gratificante per una società complessa come la nostra, con seri problemi di welfare.

C'è certamente da verificare l'aspetto della sicurezza dei dati, ma di questo non mi occupo nè sotto il profilo tecnico nè legislativo e rimando a interventi più competenti che offriranno di sicuro linee guida necessarie per poter utilizzare al meglio queste opportunità. Tali per me, infatti, sono. Il controllo è uno degli elementi che fa funzionare un sistema e ne riduce la complessità ma può anche ridurre la libertà delle persone. Per Parsons era funzionale all'esistenza stessa del sistema(12).

In questo caso il controllo non è un meccanismo di chiusura per il funzionamento di un sistema, piuttosto è un meccanismo di

(12) Cfr. Parsons T. (1951), *Il sistema sociale*, Einaudi, Torino, 1995.

apertura verso l'ambiente (inteso come welfare, famiglia, benessere) che potrebbe migliorare la vita delle persone e, paradossalmente, la loro libertà. Ovvero la connessione tra gli oggetti e le persone possono qualificare la vita di relazione.

Sorge il problema della manipolazione delle informazioni. Chi garantisce che questi dati non siano utilizzati se non ai fini designati?

Un oggetto IoT produce dati che si riferiscono alle persone e alla possibilità del loro utilizzo. Ma questo non è un problema di oggi; in passato chi ha garantito sicurezza e privacy con i media precedenti a questi? Certo è che più un mezzo è potente, maggiori saranno i vantaggi, così come maggiori i rischi. Ma concettualmente non cambia, prima come ora resta il rischio di raggiungere informazioni non proprie.

Sono convinta che sia importante lavorare su standard tecnologici sicuri e affidabili, perché non possiamo pensare che una risorsa come questa vada persa per il solo pericolo di abusi e di sfruttamento. Il gruppo di lavoro *Article 29* si è espresso su questi rischi e possibilità(13). Fanno riflette le loro indicazioni per comprendere i vantaggi che garantiscono la privacy e la vita di qualità delle persone.

In conclusione evidenzio due aspetti, a sottolineare che i rischi, oltre che le opportunità, dipendono dalla conoscenza e dalle competenze che possono avere e sviluppare le persone.

1. Rischio di *asimmetria informativa*. Chi usa oggetti tecnologicamente avanzati, spesso non li conosce, non sa cosa e quali dati contengono, chi li riceve, chi li legge e utilizza ecc. Non tutti abbiamo cioè pari competenze perchè non abbiamo pari conoscenze.

(13) Article 29 è un gruppo di lavoro istituitosi il 16 settembre 2014 in seguito alla Direttiva 95/46/EC, del quale fanno parte i rappresentanti delle autorità nazionali di vigilanza, dell'European Data Protection Supervisor e della Commissione Europea. Il frutto di tale lavoro è raccolto nel parere n. 8/2014, atto con il quale si tenta di stilare una prima disciplina delle questioni giuridiche generate dall'utilizzo in crescente diffusione dei prodotti dell'IoT.

2. Il nostro Paese ha una *scarsa cultura digitale*. Anche su oggetti molto più diffusi di quelli di cui parliamo oggi, e che fanno parte della vita quotidiana. Occorre, credo, per ridurre il *divide* diffondere la conoscenza. Intervenire su abitudini e comportamenti. Diffondere la cultura digitale dovrebbe essere centrale nel trasferimento di conoscenze. Nel nostro Paese non è così - non sempre che io sappia - cui si aggiunge, arretratezza di infrastrutture tecnologiche avanzate e una loro differente distribuzione geografica, per cui ci troviamo, ancora oggi, a percorrere e a vivere territori ancora scoperti da connessione o con bande non sufficienti per comunicare.

Azzardo alcune riflessioni.

È possibile, in effetti, catturare informazioni sulle abitudini delle persone che utilizzano IoT e costruire su queste, percorsi per poi intervenire non correttamente.

Così come è possibile avere informazioni sullo stato di salute delle persone connesse via IoT (su questo tema, seppure non possa essere annoverato tra gli oggetti IoT, c'è il Fascicolo Sanitario Elettronico(14). Quanto conta avere le informazioni e i dati di salute su una tessera digitale? È sicurezza per la persona o è riduzione della privacy?).

Dipende dall'uso che se ne fa, dipende dalla protezione. Se i dati sono trasmessi a soggetti terzi possono facilmente essere utilizzati per tracciare percorsi, mode, uso di farmaci, vendita di prodotti. Se i dati restano di proprietà del cittadino, con garanzie di responsabilità legali e di privacy, sono una sicura opportunità.

Paure e preoccupazioni o curiosità, per riprendere la domanda di Licia Califano. Non ci sono risposte univoche.

(14) Cfr. Giglietto F., Mazzoli L. (2014), *Il fascicolo sanitario elettronico fra micro e macro, in Sociologia della comunicazione*, Franco Angeli, Milano, fascicolo 48, pp. 9-25. Questo articolo riporta i dati di una ricerca nazionale commissionata da Assinter Italia ed evidenzia, fra l'altro, le problematiche della relazione medico-paziente in presenza di tecnologie.

Anzi registriamo modifiche di posizione e di pensiero fra gli studiosi che parevano avere risposte certe. Per tutti cito gli autori del Cluetrain Manifesto. Doc Searls, David Weinberger *et alii*(15) che 15 anni fa sottolineavano la forza di Internet per la sua connessione aperta, decentrata e distribuita. Oggi si preoccupano dei *predoni* che approfittano dei nostri dati(16).

Posizioni che si modificano nel tempo, per la ricerca, per l'evoluzione del pensiero e delle filosofie. Queste evoluzioni (qualche volta involuzioni), a mio parere, non modificano il fatto che Internet è un ambiente in cui *noi* ci prendiamo cura (o ci dovremmo o ci dovrebbero permettere) di *noi* e *nel quale* attiviamo relazioni.

Recentemente è apparso un dato che mi pare interessante che evidenzia come il 44% delle persone pensa che la tecnologia abbia migliorato le relazioni, contro il 16% che pensa che siano peggiorate. Alla questione posta all'inizio non posso far altro che rispondere con un altro quesito. Siamo sicuri che alla connessione, con tutti i rischi di cui siamo consapevoli, preferiamo il controllo?

Proprio nella consapevolezza, conoscenza e cultura potrebbe risiedere la risposta. L'auspicio è che una formazione e informazione adeguate si occupino di questo e offrano risposte corrette ai cittadini permettendo a tutti di attivare scelte autentiche.

Licia Califano

Ringraziamo la professoressa Mazzoli per averci fornito nuovi e utili elementi di riflessione e passiamo la parola al professor Baldoni, il quale interverrà tramite un collegamento a distanza.

Da entrambi gli interventi che si sono succeduti mi sembra torni ancora più forte la domanda: "in che modo la regola giuridica

(15) Cfr. Levine F., Searls D., Locke C. & Weinberger D. (1999), *The Cluetrain Manifesto. The end of business as usual*, Fazi editore, Roma, 2000.
(16) Cfr. Levine F., Searls D., Locke C. & Weinberger D. (2015), *The New Clues,* [online] testo disponibile in: *https://medium.com/@nuovetesi/nuove-tesi-4a1def360351*.

deve saper governare il cambiamento?" O ancora: "quali garanzie, per governare i rischi, per la sicurezza dei dati personali, che evidentemente possono essere raccolti incrociati attraverso gli oggetti interconnessi?".

Se questa è la domanda, il tecnologo ci può rispondere, facendoci capire e raccontandoci i termini di una tecnologia sicura? Di una tecnologia che sappia confrontarsi con il giurista, da questo punto di vista e creare dunque uno strumento che ottimizza i profili che sono stati individuati questa mattina, con un ridimensionamento del rischio, che comunque resta evidentemente insito nell'uso di questi strumenti.

Lascio la parola al professor Roberto Baldoni.

Roberto Baldoni

Grazie a tutti i presenti, ringrazio il Presidente Soro per l'invito, mi scuso per non essere lì tra voi a causa di una improvvisa influenza, però ci tenevo ad essere presente a questo evento poiché include attori rilevanti e di diversa estrazione culturale in un settore, quello dell' Internet of Things (IoT), tra i più importanti del momento dal punto di vista tecnologico.

Ringrazio i tecnici che mi hanno permesso di realizzare questo collegamento in pochi minuti.

Avere persone di diversa estrazione culturale che discutono di sicurezza informatica e privacy è una ricchezza importante che noi di Sapienza abbiamo valorizzato da tempo attraverso la costituzione del Centro di ricerca di *Cyber Intelligence and Information Security*, primo in Italia a seguire questa linea multidisciplinare nell'*information security*. Questo perché, ad esempio, anche la migliore tecnologia non ha ragione d'essere senza una base giuridica che la renda legale ed utilizzabile.

Inizio questo intervento parlando dell'avvento ormai in atto dell' IoT.

Come descritto in questa slide l'Internet rappresenterà, di fatto, la seconda rivoluzione digitale dopo quella dei computer.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

È iniziata attraverso dei dispositivi, i nostri smartphone, nella slide vedete raffigurato uno smartphone di prima generazione e poi c'è stata, negli ultimi anni, una pletora di nuovi dispositivi che hanno reso sempre più ricco questo scenario *smart tv*, *iwatch*, *autonomous car*, impianti elettrici di seconda generazione, *smart glass* sono solo i primi prodotti di una lunga schiera che vedremo apparire nei prossimi anni e che "informatizzerà" il nostro stile di vita e tutti i settori merceologici.

Gli esperti di settore concordano sul fatto che la rivoluzione decollerà dal punto di vista economico a partire dal 2015. Quali sono i settori principali su cui è stato imperniato il concetto di IoT ad oggi?

Palazzi intelligenti, case intelligenti, automobili autonome, la sanità, l'agricoltura e i trasporti. Pensate che ci sono delle grandi industrie multinazionali informatiche, che si sono ristrutturate da anni, in modo che ogni laboratorio studi come realizzare applicazioni in uno di questi settori integrando l'informatica, ad esempio, nel monitoraggio strutturale degli edifici, nella irrigazione dei campi, nel risparmio energetico nelle case.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Per capire l'importanza del mercato dell'IoT focalizziamoci sull'area delle case intelligenti: Google ha acquisito nel gennaio 2014 Nest per 3.2 bilioni di dollari. Nest è una società che fabbrica termostati smart che apprendono come fissare la temperatura studiando le abitudini dei residenti. Si capisce quindi come Google pensi sia fondamentale nel prossimo futuro profilare gli utenti fuori dai browser e che il mercato delle *smart homes* sarà uno dei *main driver* di business del prossimo futuro.

Fonte: ABI Research, TechNavio, Pike Research, BI Intelligence Estimates

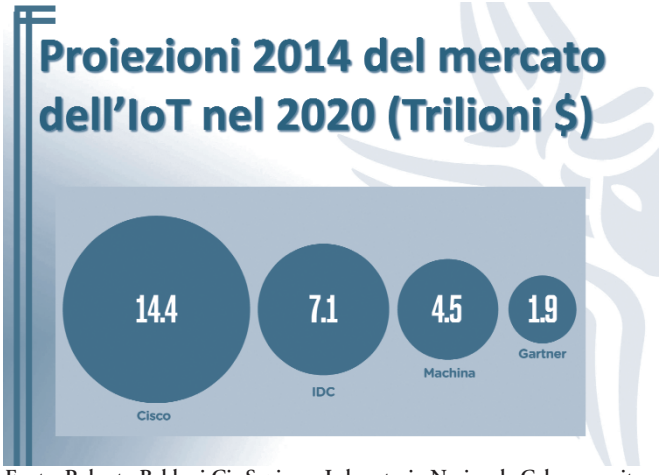
Questa ipotesi è confortata da diversi analisti che si aspettano per il 2020 dai 2 ai 20 bilioni di dispositivi connessi ad Internet e

con capacità computazionale dentro le nostre case (non considerando i classici PC e gli smartphone).

Gartner in particolare prevede 10 bilioni di unità intelligenti che saranno installate all'interno di tutti quei contesti che abbiamo discusso precedentemente.

Un numero di dispositivi veramente impressionante.

Questo corrisponde ad una proiezione di mercato per il 2020 che passa da 1.9 trilioni di dollari previsti da Gartner a 14.4 trilioni di dollari previsti da Cisco. È chiaro che se anche la verità si andrà a posizionare nel mezzo, questo rappresenterà un mercato dal quale l'Italia non può assolutamente stare fuori.



Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Come tutte le cose nuove, in particolare nel campo dell'informatica, il mercato parte proponendo prodotti che hanno *performance and beauty* come caratteristiche primarie, pensate agli smartphone, trascurando sicurezza e privacy.

Infatti sono di questi giorni notizie di gravi vulnerabilità riscontrate nel software delle smart TV e di attacchi verso altri dispositivi IoT.

Questi dispositivi sono facilmente attaccabili perché fondamentalmente hanno poche risorse fisiche - come memoria e capacità computazionale - rispetto ai calcolatori ed ai server classici che conosciamo.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

La scarsezza di risorse riscontrabile in questi dispositivi è anche dovuta alla loro economicità essendo orientati al mondo *consumer*. Rendere sicuri da attacchi informatici questi dispositivi una volta realizzati e messi sul mercato diventa praticamente impossibile.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Per dare un'idea di come questi dispositivi siano vulnerabili, nel 2008 la *botnet* Mariposa ha violato milioni di oggetti (non computer) che avevano un indirizzo IP. La cosa fu aiutata dal fatto che questi dispositivi usavano password molto deboli se non quelle di default dei produttori. Questo pone un problema di

consapevolezza della minaccia rispetto ai proprietari di questi dispositivi che dovrebbero proteggere i loro dispositivi almeno con password difficili da scoprire.

Il problema sicurezza da attacchi informatici non è ristretto ovviamente al solo settore dispositivi IoT.

Nel settore dei grandi sistemi informativi, la gravità del problema della sicurezza è stato recentemente sottolineato dalla pubblicazione del Cyber Security Report Italiano del 2014, che ha messo in luce i problemi ed il numero di attacchi a cui i sistemi informativi delle pubbliche amministrazioni sono soggetti.

Come detto, il mercato dell'IoT è una gigantesca opportunità economica anche se ci sono diversi fattori di incertezza che potrebbero attenuare questa opportunità.

Ad esempio il fatto che nell'IoT non esistono modelli di business predefiniti e standard riconosciuti.

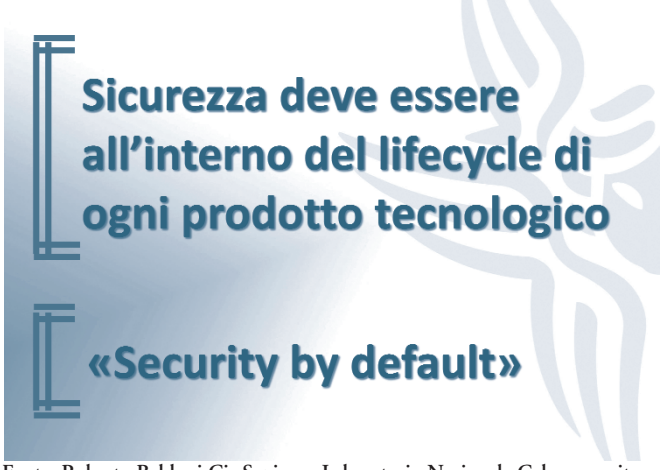
Tuttavia è ampiamente riconosciuto che una delle più importanti fonti di incertezza è rappresentata proprio dal livello di sicurezza e privacy che saremo in grado di assicurare a questi dispositivi.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Se riusciremo a fornire livelli adeguati di sicurezza, allora l'incertezza si trasformerà in un fattore di amplificazione dell'opportunità economica creando un circolo virtuoso.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Dobbiamo arrivare a quella che viene chiamata in gergo *security by default*, inserita all'interno della progettazione del dispositivo stesso. Proprio per evitare che questi dispositivi siano senza difese ed accessibili da chiunque abbia una minima capacità informatica.



Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

In questo scenario è fondamentale il ruolo del Governo, proprio perché l'opportunità economica è gigante e noi dobbiamo, come sistema paese, entrare all'interno di questo mercato, definendo una visione dell'IoT in Italia che includa sicurezza e privacy, specificando i settori dove l'Italia è interessata a competere

(ad esempio, agricoltura, case intelligenti, sanità), includendo possibili modelli di business che possano valorizzare aziende esistenti o crearne di nuove e realizzando in un ambente di cooperazione internazionale possibili standard.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Questo è un mercato tecnologico irrinunciabile per il nostro paese la cui nascita e crescita va pianificata e stimolata appropriatamente dal nostro governo.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Però sappiamo che noi italiani siamo piuttosto refrattari alla parola pianificazione che è alla base di ogni occasione economica. Ripeto, l'opportunità è gigante e l'Italia deve essere all'interno di questa opportunità per assicurarsi una prosperità economica e di sviluppo negli anni a venire. Vi do ora un esempio di cosa significa stimolare una crescita. Questo è un articolo uscito pochi mesi fa e riguarda la mia università: *Luci accese di notte in tutta la Sapienza: allarme sprechi*.

Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Il Governo e tutta la macchina della pubblica amministrazione italiana sono *in primis* fruitori di tecnologia, forse i più importanti clienti. Quindi la macchina statale può stimolare il mercato attraverso opportune politiche di innovazione: ad esempio realizzando un piano di risparmio energetico attraverso l'uso di tecnologia per tutti i palazzi della pubblica amministrazione. Considerate che ci sono studi del MIT che mostrano che, all'interno di un edificio pubblico, almeno il 30 o il 35% dell'elettricità che viene utilizzata è di fatto sprecata. Questo perché all'interno di un edificio pubblico nessuno realmente bada allo spreco!

Quindi sarebbe un piano di innovazione imponente che potrebbe dare spazio a molte aziende (anche italiane) che potrebbero crescere e irrobustirsi per andare poi a competere con nuovi prodotti/sistemi/soluzioni per il risparmio energetico sui mercati internazionali.

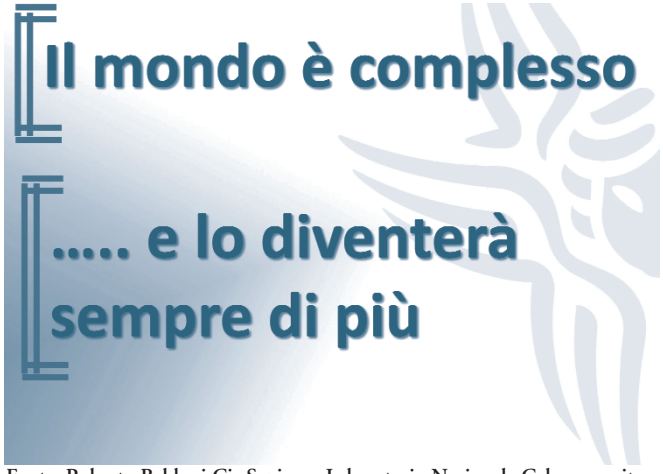
Allo stesso tempo dovremmo cercare di stimolare ricerca e formazione in IoT.

Se prendiamo ad esempio gli impianti elettrici di nuova generazione, è chiaro che avremo bisogno di formazione per quanto riguarda elettricisti e installatori.

Non soltanto dunque nuove tecnologie, nuove aziende nate dalla contaminazione con il mondo della ricerca, ma anche una formazione che guarda a come installare e posare certi dispositivi. Stesso discorso può valere per squadriglie di droni addestrati ad irrigare e curare grani estensioni di vitigni o altre colture.

Si potrebbero fare mille esempi di come il mondo cambierà a breve. Tutte queste azioni ed altre, che non cito per mancanza di tempo, significano pianificazione rispetto ad un obiettivo strategico di tipo industriale che si vuole perseguire come sistema Paese.

Sono giunto praticamente alla fine della mia presentazione. Vorrei chiudere dicendo ciò che spesso ricordo ai miei figli: *"il mondo è complesso, lo sarà sempre di più e noi dobbiamo attrezzarci per prevedere, capire e gestire questa complessità"*.

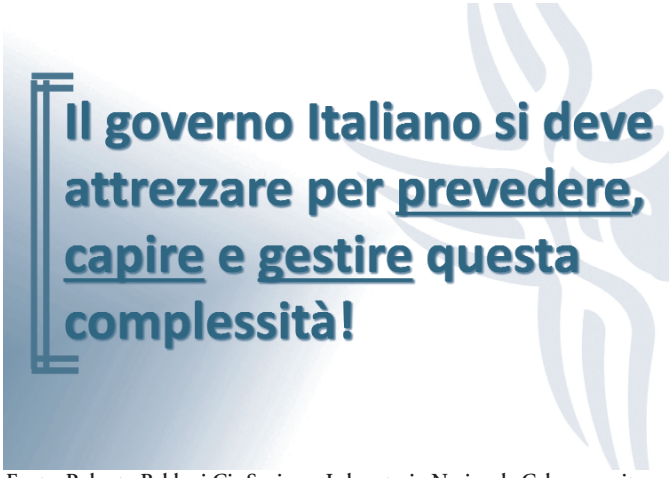


Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

Immaginate che quello che vediamo sotto i nostri occhi è solo l'inizio, sapete perfettamente delle problematiche che ci sono

oggi con l'utilizzo di droni, ma da qui a 20 anni avremo robot che entreranno nelle nostre case e ci aiuteranno nella vita di tutti i giorni.

A questo seguono problematiche di *security*, *safety* e *privacy* fortissime, per cui ci dobbiamo attrezzare come sistema paese per prevedere, capire e gestire questa complessità e trasformarla in opportunità economica e sviluppo.



Fonte: Roberto Baldoni Cis Sapienza Laboratorio Nazionale Cyber security

A questo punto mi chiedo se ad esempio in Italia una figura come il "Consigliere Tecnologico del Primo Ministro", presente in molte nazioni sviluppate, possa essere strategica per anticipare e preparare il governo a queste rivoluzioni.

Ci vogliono infatti alte competenze per cercare di prevedere che cosa accadrà anche solo a cinque anni e per cogliere al meglio come sistema paese le opportunità economiche che il futuro tecnologico ci offre. Con questo ho concluso.

Licia Califano

Ringrazio sentitamente, ancora una volta, i nostri illustri relatori e concludo osservando, in estrema sintesi, che, se Internet delle cose dal punto di vista sociologico rappresenta una nuova possibilità di apertura sociale e di relazione, esso è anche, e per certi

versi soprattutto, un'opportunità economica formidabile che va pianificata, capita e gestita. Non possiamo nasconderci che, come evidenziato nell'intervento del professor Baldoni, il problema della sicurezza esiste, è un problema sul quale si sta lavorando e che non va sottovalutato. Pertanto chiuderei questa sessione con una domanda di prospettiva, nel senso che è evidente che il tema che resta aperto è come coniugare correttamente sicurezza e privacy.

Ringrazio tutti e lascio la parola alla dottoressa Giovanna Bianchi Clerici.

Tecnologie indossabili e intelligenza aumentata

Sessione III

Giovanni Boccia Artieri
Università degli studi di Urbino "Carlo Bo"

Andrea Granelli
Presidente di "Kanso"

Federico Maggi
Politecnico di Milano

Moderatore **Giovanna Bianchi Clerici**
Componente del Garante per la protezione dei dati personali

Sessione III

Tecnologie indossabili e intelligenza aumentata

Giovanna Bianchi Clerici

Buongiorno a tutti, per l'ultima sessione dei nostri lavori, comincerei presentandovi i relatori ai quali chiederò - con molta cortesia e scusandomi - di essere piuttosto concisi nell'esposizione, perché molto è stato detto questa mattina, il tempo stringe e ci sono i ragazzi delle scuole che, graditissimi ospiti, devono però far rientro nei propri Istituti.

I nostri relatori sono: il professor Giovanni Boccia Artieri, Ordinario di Sociologia dei media digitali e Internet Studies all'Università di Urbino, vice direttore del centro LaRiCA (Laboratorio di Ricerca sulla Comunicazione Avanzata) presso il Dipartimento di Scienze della comunicazione. È anche coordinatore del corso di laurea in Informazione, media, pubblicità e autore di numerose pubblicazioni, tra le quali ricordiamo l'ultima, di quest'anno: *Gli effetti sociali del web*.

Il dottor Andrea Granelli è Presidente di Kanso, una società di consulenza specializzata in innovazione e *change management*. È stato in McKinsey, amministratore delegato di Tin.it, del laboratorio di ricerca del gruppo Telecom. Attualmente è membro del Comitato di valutazione del Cnr ed è anche Presidente dell'Associazione Archivio Storico Olivetti. Collabora con la Treccani.

Il giovanissimo professor Federico Maggi, ricercatore e professore per il corso di Computer Security presso il Politecnico di Milano, ha conseguito il dottorato di ricerca in California, Università di Santa Barbara, dedicandosi allo studio della rilevazione delle intrusioni informatiche. Si occupa principalmente di attività

legate al *cybercrime*, come la diffusione dei *malware* per i dispositivi mobili e tradizionali. È membro di comitati tecnico scientifici e, attualmente, sta lavorando per conto del Miur ad una ricerca proprio sui software infetti per i dispositivi mobili.

Oggi abbiamo il compito di soffermarci sul tema delle tecnologie indossabili e dell'intelligenza aumentata. Questo segmento dell'Internet delle cose (Internet of Things - IoT) attiene ai dispositivi miniaturizzati indossabili, che si integrano con il corpo della persona e sono concepiti per interagire costantemente con chi li indossa, agevolarlo nelle sue azioni e consentirgli di accedere in qualsiasi momento alle informazioni raccolte in Rete.

Si tratta, come è già stato ricordato, di sensori che raccolgono informazioni sulle persone stesse e sull'ambiente che li circonda, hanno proprietà di monitoraggio e sono comandati a distanza attraverso Internet. A differenza dei normali tablet e smartphone, i quali per essere usati devono essere tolti da una tasca o da una borsa e attivati, le tecnologie indossabili sono in perfetta simbiosi con il fruitore che potrà usarli, mentre cammina, guida e parla senza doversi interrompere per digitare un numero di telefono, o per scrivere un testo.

Possiamo parlare di "realtà aumentata" perché l'utilizzo diquesti dispositivi ci fa essere sempre connessi; proprio come se la Rete fosse parte dell'ambiente che concretamente percepiamo con i nostri sensi. I dispositivi più conosciuti sono i *Google Glass*, gli *smartwatch*, i braccialetti colorati. Proprio stanotte Apple ha annunciato che in primavera sarà sul mercato il loro *iWatch*.

Si tratta di oggetti che hanno avuto qualche problema di look, tant'è vero che sono stati chiamati famosi stilisti e designer per rivederne l'estetica. Alcuni sono particolarmente intriganti: gli anelli che consentono di far scorrere la musica o di muovere i personaggi di un videogioco. Tra questi ce n'è uno particolarmente interessante, l'*Air Type,* una tastiera con la quale scrivere, virtualmente, un testo. Ovviamente ciò implica che si conosca a memoria la disposizione dei tasti.

Ci soccorre però la possibilità di utilizzare nella scrittura la funzione "predizione" del testo.

I numeri di questo business del futuro sono stati detti, per cui non li ripeterei; partirei con il professor Artieri, che nei suoi studi affronta il tema delle interazioni. L'enorme diffusione di dispositivi indossabili porterà a condividere i dati con il vissuto delle persone. Tutto questo avrà ripercussioni nei nostri comportamenti sociali, non solo in Rete, ma anche nella vita quotidiana.

In particolare, La pregherei, se possibile, di soffermarsi su un tema che questa mattina non abbiamo ancora affrontato, ovvero il fenomeno del *quantified self*, che parrebbe la bizzarria di qualche anima candida: "misuro tutto", "misuro quindi esisto". In realtà può diventare un formidabile strumento di controllo sociale, perché potrebbe addirittura condizionare, per esempio nel caso della selezione di personale, l'assunzione delle persone.

Qualche anno fa in Giappone era di moda usare l'oroscopo per il *recruiting* poiché alcuni segni zodiacali erano ritenuti più affidabili rispetto ad altri. Rischiamo questo?

Giovanni Boccia Artieri

Social Internet of Everything: tecnologie indossabili e intelligenza connessa

1. Internet sparirà

Il futuro espanderà la relazione fra corpi ed informazioni, e lo farà secondo modi complessi: cose e processi saranno travolti e coinvolti nei diversi contesti sociali e di vita. E sono quei modi ciò che dovremmo imparare ad affrontare all'interno delle nostre culture di connessione. È l'Internet delle cose che avanza, e che si coniuga ad una dimensione di tecnologie *wearable*.

A dirla tutta, "Internet sparirà". Lo ha raccontato Eric Schmidt, presidente del consiglio di amministrazione di Google,

al World Economic Forum Annual Meeting 2015[1]: Internet sparirà perché *"sarà parte della nostra presenza per tutto il tempo"*.

Lo scenario che Schmidt prefigura è questo: "*There will be so many IP addresses… so many devices, sensors, things that you are wearing, things that you are interacting with that you won't even sense it"*.

Ha certamente in mente tra le altre cose il progetto *Phisical web*[2], uno standard aperto, promosso dal gruppo di Mountain View che mira a rendere possibile l'interazione con qualsiasi apparecchiatura semplicemente avvicinandosi ad essa, senza nessun bisogno di scaricare prima un'applicazione. Si tratta di micro interazioni che consentono un effetto "coda lunga"[3] in cui ogni cosa può offrire informazioni ed essere in connessione in modo utile: il collare di un animale domestico potrà chiamare il proprietario in caso di smarrimento; l'autobus informare sulla sua prossima fermata e i tempi di attesa; si potrà pagare il parchimetro avvicinando il proprio cellulare, ecc.

Non percepiremo quindi più l'infrastruttura che c'è dietro alle connessioni, e smetteremo persino di pensarci. Non saremo più immersi nell'Internet, ne saremo parte. Ma è proprio con questa invisibilità cognitiva e culturale che dovremo confrontarci nei prossimi anni, ragionando su Internet delle cose e *wearable technology*.

Certo, precisa Schmidt, la tendenza crescente a condividere dati e la possibilità di renderli disponibili all'uso dovranno avvalersi del permesso degli utenti. L'analisi di quei dati, in fondo, è finalizzata a migliorare le nostre vite.

In realtà, questa è la narrazione dominante, quella proposta dal mercato, poggiata sull'opacità dei processi e la tendenza diffusa

(1) Cfr. *http://www.hollywoodreporter.com/news/google-chairman-eric-schmidt-Internet-765989*

(2) *https://google.github.io/physical-web/*

(3) Cfr. Anderson C. (2006), *The Long Tail: Why the Future of Business is Selling Less of More, Hyperion*, New York; trad. it. (2007), *La coda lunga. Da un mercato di massa a una massa di mercati*, Codice, Torino.

alla condivisione dei dati. È anche con questa narrazione, allora, che ci dobbiamo confrontare per affrontare con maggiore consapevolezza la diffusione dei dispositivi indossabili. D'altra parte, visto che i dati personali sono il nuovo petrolio e il potere del XXI secolo si giocherà sul controllo dei (nostri) dati(4), occorre chiedersi chi siano oggi le "sette sorelle" digitali e se non siano molte meno.

2. Una rete sociale di oggetti e corpi

Dovremo imparare a sviluppare - e diffondere - una maggiore consapevolezza sulla necessità di prenderci cura dei dati e circa gli effetti che i dispositivi indossabili avranno sui comportamenti sociali e sulle nostre vite.

Anche in connessioni con gli altri, poiché i social network ci hanno abituato sempre di più a percepirci in uno stato di connessione continua tra noi, a prescindere dai vincoli spaziali e temporali(5). In particolare basta pensare alla crescita dell'uso in mobilità di tecnologie che mettono in relazione in modo crescente gli ambienti sociali e il loro rapporto con i dati immateriali.

Ma se per ora il confine comunicativo era tracciato rispetto a contenuti (tendenzialmente) rilasciati volontariamente da azioni dell'utente (fare un commento, mettere un like, decidere di geolocalizzarci in un luogo) il futuro espanderà la relazione fra noi, gli oggetti e le informazioni all'interno dei contesti sociali.

Lo scenario che si prospetta è fatto di 50 miliardi di oggetti che entro il 2020(6) saranno connessi a Internet. Oggetti che sono sì smartphone e tablet, ma anche parchimetri e strade, scaffali dei supermercati e bestiame: *la start up* olandese Sparked ha impiantato

(4) Cfr. Keen A. (2012),*Digital Vertigo: How Today's Online Social Revolution Is Dividing, Diminishing, and Disorienting Us*, St. Martin's Press, New York; trad. it. (2013), *Vertigine digitale. Fragilità e disorientamento da social media*, Egea, Milano.

(5) Cfr. Boccia Artieri G. (2012), *Stati di connessione. Pubblici, cittadini, consumatori nella (Social) Network Society*, FrancoAngeli, Milano.

(6) Cfr. *http://www.techeconomy.it/2014/01/08/cisco-2014-anno-di-svolta-per-lInternet-of-everything-vale-19-mila-miliardi-di-dollari/*

sensori nell'orecchio di una mucca in grado di inviare i parametri vitali e i movimenti del capo di bestiame via *wi-fi*.(7)

Si tratta di un primo passaggio culturale, quello all'Internet of Things, che vede l'interconnessione di dispositivi intelligenti capaci di comunicare dati in tempo reale in modo da modificare i processi: il sensore su uno scaffale comunica che i prodotti di una determinata marca sono finiti, quello sulla mucca che il momento del parto probabilmente si avvicina. Il nuovo paradigma ci richiede in questa prima fase di pensare la connessione tra cose come una realtà di riferimento e la sfida non sta tanto nel circondarci di oggetti intelligenti ma che questi sappiano relazionarsi tra loro.

Ma stiamo affrontando un'ulteriore evoluzione, come evidenzia la battuta di Marc Benioff(8), Ceo di salesforce.com: "Se sono su Facebook, perché la mia auto non è un mio *friend*?".

Il vero salto culturale lo abbiamo quindi se cominciamo a pensare a come questi oggetti si combinano non solo tra loro ma, in prospettiva più allargata, a reti sociali di persone e ai processi sociali, cioè secondo una cultura di Social Internet of Everythings (SIoE).

Si tratta di pensare come nella Rete delle nostre relazioni sociali connesse entrino una serie di oggetti con cui abbiamo rapporti quotidiani e a come ci metteremo in relazione attraverso loro.

In questo senso la nostra auto o la lavatrice o il nostro cane (i dati che rilasciano e li caratterizzano) come *friend* tra i *friend* (altre persone ma anche i loro oggetti), assieme, all'interno dei noti sei gradi di separazione e come parte di una comunità più estesa.

Questa realtà prospettata porta ad interrogarci anche sull'influenza che avrà questa rete di persone-e-cose connesse sui comportamenti sociali.

Questo salto evolutivo del rapporto tra noi e le tecnologie ci obbligherà ad abituarci a tenere sotto controllo vecchie variabili in

(7) Cfr. *http://www.ustelecom.org/blog/Internet-connected-cows-bananas-and-more*
(8) Cfr. *http://www.bloomberg.com/bw/articles/2014-01-10/salesforce-fans-get-the-benioff-bump*

modo nuovo, a fare diventare l'interazione con l'intelligenza negli oggetti parte della routine quotidiana, anche attraverso tecnologie indossabili.

3. Wearable technology: reattiva, immersiva, predittiva

La realtà delle tecnologie indossabili è in forte espansione perché sono mutate le condizioni di possibilità che la rendono realizzabile. Innanzitutto ci troviamo di fronte ad una variabile culturale data dalla legittimazione sociale delle tecnologie *wearable*: le persone hanno familiarizzato con l'esperienza di avere una tecnologia di connessione costantemente con sé, attraverso lo smartphone.

A questo va aggiunta una variabile tecnologica data dalla miniaturizzazione dei sensori che si unisce all'aumento di durata delle batterie e allo sviluppo molto veloce di tecnologie capaci di dialogare con gli smartphone che restano *hub* centrali per l'esperienza di connessione e alleati non sostitutivi delle tecnologie indossabili.

Una terza caratteristica è rappresentata dal collasso del confine tra uomo e computer che viene vissuto come condizione sempre più naturale sottolineata dall'espansione di interfacce a facile interazione corporea (gestuali, vocali, tattili).

Ci sono almeno tre dimensioni lungo cui si sviluppa la *wearable technology* con precise implicazioni sia in termini di comportamenti, sia di sicurezza per ciascun livello:

1. *dimensione reattiva*: gli accessori *wearable* come estensione del corpo, dotati per esempio di sensori capaci di interpretare il movimento. Oltre a raccogliere dati, consentono di relazionarsi all'ambiente circostante;
2. *dimensione immersiva*: ha a che fare con la capacità di approcciare alla realtà con logica "aumentata", come accade per esempio con gli occhiali indossabili. Pensiamo ai *Google Glass* messi negli ultimi tempi un po' da parte ma che probabilmente ricompariranno nel mercato di largo consumo dell'*eyewear;*
3. *dimensione predittiva*: svariate tipologie di strumenti

collezionano dati sui comportamenti degli utenti, per poi analizzarli e costruire modelli di previsione di quegli stessi comportamenti.

Quest'ultima dimensione in particolare rappresenta la frontiera della nuova generazione di *wearable*, come accade nel *mobile health*.

In questo settore stiamo assistendo ad un'evoluzione simile a quella subita dalle previsioni meteorologiche: siamo passati dal monitoraggio con i barometri a sofisticati sistemi di previsione computazionali. Samsung sta lavorando su un prototipo di dispositivo indossabile in ambito medico chiamato Edsap(9) che monitora - raccogliendo nel tempo i dati ed applicando specifici algoritmi - i livelli di ansia, lo stress, la qualità del sonno.

Leggendo le onde cerebrali riesce a rilevare in anticipo i principali segnali di un ictus, avvertendo così per tempo la persona che indossa il device.

Siamo solo agli inizi di una realtà in completa trasformazione, come sottolinea David Bonilla, vice presidente di Oracle ed *executive dean* al College of Information Systems and Technology dell'Università di Phoenix(10): "*Le tecnologie indossabili che stiamo vedendo sul mercato ora sono le prime goffe versioni di quello che sta arrivando […] In futuro, il tuo SmartWatch accederà istantaneamente ai registri medici, a informazioni sulla dieta per poi sincronizzarli con sensori nel supermercato e nel centro commerciale per lo shopping e fornire in tempo reale consigli sulla salute. Le scarpe intelligenti e le camicie biometriche ricorderanno che è necessario raddrizzare la postura, idratarsi, correre e camminare in modo corretto per proteggere la schiena e le ginocchia. Una benda intelligente dirà ai diabetici quando la glicemia si sta abbassando. E la tecnologia aptica vi darà l'intimità a distanza*".

(9) *http://global.samsungtomorrow.com/c-lab-engineers-developing-wearable-health-sensor-for-stroke-detection/*
(10) *http://www.latimes.com/health/la-he-future-wearables-20150124-column.html#page=1*

4. Privacy ed effetto "piccolo fratello"

In questo scenario i dispositivi del *quantified self* e computer sempre più *wearable* da diventare impercettibili nell'uso (anche se spesso visibili) metteranno in relazione mole di dati comportamentali e dei vissuti: medie dei nostri battiti cardiaci, nei corridoi dell'ufficio e sotto sforzo durante una corsa, e quantità e tipologia di caffè bevuti, con possibili *alert* automatici alla rete di *friend* aziendali che alla macchinetta distributrice del piano domotico ci sanzioneranno socialmente per l'eccesso di caffeina ingerita in relazione alla nostra tachicardia. Esempio risibile, ma che dobbiamo pensare esteso ai diversi ambiti della vita quotidiana nei quali rilasciamo e rilasceremo sempre più dati che verranno riorganizzati all'interno di un database relazionale con altri dati delle nostre reti sociali di uomini/oggetti. Dispositivi e oggetti, corpi e reti sociali, saranno sempre più interconnessi attraverso un design dell'esistenza come flussi continui di dati da mettere in relazione.

Le conseguenze di questo sviluppo hanno a che fare con il controllo in fatto di sicurezza e privacy(11) e riguarderanno presto ambiti che al momento non sempre sembrano evidenti. Pensiamo, per esempio, alle *terze parti*, quelle con cui accettiamo - spesso inconsapevolmente - di condividere dati personali su salute e comportamenti ogni qual volta accettiamo le licenze d'uso del nostro strumento indossabile. Non è detto che queste terze parti abbiano standard di protezione dei dati equivalenti a quelli garantiti dall'azienda che ha fabbricato e da cui abbiamo acquistato il *device*.

Oppure pensiamo all'effetto "piccolo fratello" che si crea quando con i nostri strumenti indossabili memorizziamo e rendiamo a quel punto condivisibili dati relativi ad altre persone(12):

(11) Cfr. Mann S., Nolan J., Wellman B. (2013), *"Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments"*, Surveillance & Society, vol. 1, n. 3.

(12) Pensiamo al caso di Sarah Slocum che nel mese di febbraio 2014 è stata aggredita dagli avventori in un bar a San Francisco in cui era entrata indossando Google Glass. Cfr. *http://www.sfgate.com/news/article/Google-Glass-attack-offers-a-new-lens-on-privacy-5267616.php*

la de-privatizzazione del mondo si associa così ad una sua messa in visibilità costante attraverso l'abitudine ad essere *always on*.

In tal senso, come società, ci troveremo a ripensare i problemi all'interno della cultura della SIoE in un mix tra bisogni dell'individuo e bisogni della società, in un equilibrio problematico tra deriva orwelliana e condivisione partecipata.

5. Prendersi cura del dato

Diventerà discriminante curarci sempre più di come i nostri dati (del corpo e dei nostri oggetti ed ambienti quotidiani) si lasciano trattare come informazioni e di come verranno messi in relazione, per non tacere dei rischi corrispondenti(13).

Da una parte, quindi, dovremo far crescere la cultura della privacy in una realtà connessa dove trasparenza e visibilità rappresentano un valore.

Occorrerà sviluppare maggiore consapevolezza degli utenti connessi e delle possibilità di gestione circa: il diritto a controllare quanto su di sé viene comunicato, il diritto all'inviolabilità personale e il diritto di definire e gestire divulgazione ed occultamento delle informazioni personali, decidendo cosa condividere e quando.

Dall'altra dovremo essere consapevoli di come nello stato di interconnessione ogni nodo rappresenta un potenziale vettore di attacco per l'intero sistema: nella social IoE hackerare i dati non avrà solo a che fare con una manipolazione e distruzione di informazioni ma con una manipolazione e distruzione fisica del mondo(14).

Di qui nuove sfide, come ad esempio quella per i produttori di operare attraverso principi di *security by design* che garantiscano un adattamento online alle minacce da parte dei dispositivi connessi.

(13) Cfr. Perera C., Ranjan R., Wang L., Khan S., Zomaya A. (2015), *"Privacy of Big Data in the Internet of Things Era"*, IEEE IT Professional Magazine, PrePrint Special Issue Internet of Anything

(14) Cf. Haynes P., Campbell T. A. (2013), *"Hacking the Internet of Everything"*, Scientific Amarican, August 1, *http://www.scientificamerican.com/article/hacking-Internet-of-everything/*

La prospettiva della social IoE ci pone di fronte alla prospettiva di un mutamento di paradigma che non è solo di tipo tecnologico ma che richiede di essere supportato da una cultura adatta: una cultura della connessione che sappia dare risposte in termini di cultura del dato, degli oggetti intelligenti e della sicurezza.

L'Internet di ogni cosa è, quindi, prima di tutto, una narrazione sociale da cominciare ad immaginare, per governare il cambiamento in modo consapevole.

E dovremo imparare a sviluppare - e diffondere - una maggiore consapevolezza sulla necessità di prenderci cura dei dati e degli effetti che i dispositivi indossabili avranno sui comportamenti sociali e sulle nostre vite.

Dovremmo invece capire subito che il tema della cura dei dati non va trattato come un tema riservato ad addetti ai lavori o agli esperti della privacy. Perché quello della cura dei dati è ora un tema pubblico.

Giovanna Bianchi Clerici

Grazie professore, Lei ci conferma che siamo sempre più sul versante della protezione dei dati e non più della "privacy" come è sempre stata intesa, in senso anglosassone.

Con il dottor Granelli, esperto di tecnologie indossabili che riguardano il settore sanitario, vorrei rimanere in questo ambito, con un richiamo alle opportunità e ai rischi che questi dispositivi (salvavita, braccialetti per la misurazione dei parametri vitali, monitoraggio delle attività sportive) comportano.

Se ne avesse voglia vorrei anche affrontare il tema dell' "uomo potenziato", a cui so che si è interessato. C'è un signore, Pistorius, che è un po' l'emblema di quello che abbiamo visto fino ad ora, ma il futuro, con l'immissione di chip sottopelle e altre diavolerie del genere, farà sì che avremo a che fare con un uomo che sarà costantemente online, con tutto quello che ne conseguirà.

Andrea Granelli

Ringrazio la dottoressa Bianchi Clerici e il Presidente Soro per questo invito. Il tema posto è naturalmente molto ampio; provo a rispondere alle Sue domande ripartendo dallo *status quaestionis* di questo convegno.

Ritengo che il cuore del problema non sia tanto raccontare le infinite e affascinanti (e talvolta inquietanti) applicazioni del futuro che verrà - producendo lunghe liste di innovazioni - quanto piuttosto domandarsi quali sono le implicazioni di quest'alluvione tecnologica per noi oggi, per noi cittadini, per noi imprenditori e soprattutto per le Istituzioni che ci rappresentano? In particolare per quelle Istituzioni che devono provare a normare qualcosa che forse non è normabile a priori.

Ad esempio - parlando di *eHealth*, e cioè di applicazione del digitale alla salute dei cittadini - non è sufficiente descrivere le meraviglie che possono (e potranno) fare i sistemi di monitoraggio continuo, il loro impatto sulla vita (e il costo sociale) dei lungodegenti, le implicazioni sui costi sanitari derivanti dall'uso su larga scala della sensoristica in grado di misurare in tempo reale lo stato di salute degli anziani, evitando che vadano a fare visite di controllo periodico e avvertendo loro, le famiglie e il medico curante solo quando alcuni parametri superano la soglia della normalità.

Siamo certamente di fronte ad un futuro potenzialmente molto affascinante, dove le tecnologie digitali - lo abbiamo visto in molte delle presentazioni di stamattina - ci fanno capire chiaramente il loro contributo migliorativo. Quando si introduce anche il tema dei rischi, si tende a dire che sì, certo, c'è anche qualche rischio, ma i rischi ci sono sempre stati nell'innovazione; tutto sommato, basta un po' di consapevolezza, sapere che è normale, senza soffermarsi troppo sulle "antipatiche" situazioni problematiche.

Oggi abbiamo usato questa parola "consapevolezza" molte volte, ma che cosa vuol dire davvero essere consapevoli del digitale? Quali competenze ci servono? È un fatto semplicemente di

conoscenza tecnica? E' sufficiente aumentare il numero di parole inglesi del nostro vocabolario per essere consapevoli delle trasformazioni che queste tecnologie introdurranno nella nostra vita? Siamo in grado di prevedere queste trasformazioni anche nelle loro componenti più problematiche, per loro natura oscure?

Guardiamo negli ultimi anni quanti fallimenti di previsione ci sono stati. Siamo riusciti a prevedere ben poco. Io credo che questo sia un problema di carattere generale, che forse richiede di essere un poco più saggi e magari guardare anche un po' indietro, alla storia, a ciò che si è già manifestato e attingere non solo dalla conoscenza tecnica, ma anche da saperi più umanistici e sapienziali.

È spesso alla sapienza che i grandi filosofi - pensiamo ad Heidegger o a Nietzsche - ad un certo punto della loro vita ritornano: ai presocratici, ai filosofi antichi, ai testi fondativi delle grandi religioni, perché forse nel loro pensiero, ci può essere quella sapienza che ci aiuta a meglio contrastare rischi e timori per le nuove tecnologie; non basta infatti la pura citazione di parole tecniche, cosa che sembra ci dia molta sicurezza sul fatto che dominiamo la materia.

Vorrei allora porre sostanzialmente due questioni. La prima è che è molto difficile separare il concetto di tecnologie indossabili da quello di Internet of Things: diciamo che è il digitale che si declina in tanti modi e che sta "invadendo" un po' tutti campi della nostra vita. Il digitale è infatti sempre più composto di oggetti, di intelligenza, di connessione e quindi la sfida, per noi, è cercare di immaginare (è forse più efficace l'espressione inglese - *to envision*) tutto ciò che queste innovazioni vorranno dire per la nostra vita.

Tra l'altro preferisco usare l'espressione *Internet dentro le cose,* più che *Internet delle cose*, perché la dimensione rivoluzionaria non è tanto il collegamento degli oggetti in Rete (e fra di loro), quanto il mettere intelligenza e connettività dentro le cose, ma anche nell'ambiente in cui viviamo e addirittura dentro il nostro corpo. E questa possibilità tecnologica apre anche un grande tema ontologico.

Questa possibilità di mettere dentro gli oggetti queste capacità fa sì che questi oggetti siano in grado di elaborare moltissime informazioni, e quindi possano decidere in maniera quasi autonomia e inoltre possano raccogliere e memorizzare informazioni che possono anche condividere con altri oggetti intelligenti. Infine questi oggetti possono connettersi tra di loro. Si possono quindi avere organismi elementari - oggetti elementari come i mattoncini del Lego - che però messi insieme creano oggetti complessi e quindi comportamenti complessi.

Questo è un altro filone di indagine molto affascinante e articolato: comportamenti automatizzati che nascono da processi collettivi dove non è facilmente prevedibile il comportamento risultante semplicemente conoscendo il comportamento dei singoli oggetti elementari che compongono dinamicamente l'aggregato.

Detto in altro modo, la semplice lettura dei programmi che determinano il comportamento dei singoli oggetti, dei piccoli robot, non ci dice quasi nulla su come si comporteranno quando si aggregheranno in oggetti collettivi. Siamo di fronte ad un universo complesso, e quindi anche molto difficile da prevedere.

Da questo punto di vista certamente una caratteristica interessante è che con queste tecnologie si aprono straordinari spazi applicativi: possiamo fare tantissime cose.

A questo punto vorrei affrontare un punto specifico, che tocca il tema della privacy, e che entra pertanto nell'ambito di competenza dei giuristi. Io non sono un giurista, e quindi vedo le cosa "dall'esterno" del loro ambito. Ho però avuto la fortuna occuparmi di innovazione digitale in prima persona. Ho infatti partecipato alla nascita di Internet in Italia fin dalla sua prima fase pionieristica: prima come braccio destro del fondatore di Video On Line Nicola Grauso, e poi creando tin.it, di cui ho fatto l'amministratore delegato; infine ho fatto il capo della ricerca di Telecom per molti anni, gestendo circa un migliaio di ricercatori. Mi sono quindi posto anche problemi pratici: ad esempio come tradurre idee innovative in soluzioni pratiche e utili, oppure come e verso

quale direzione indirizzare gli sviluppi del software. Ciò che rende diverso il digitale dall'ennesima innovazione tecnologica - potremmo pensare all'energia, ai materiali, alla micromeccatronica - è il fatto che il digitale davvero apre infiniti spazi di applicabilità.

Questo problema di avere infinite possibili applicazioni pone sostanzialmente un grande tema etico: quando è stata inventata la leva, l'utente aveva grossomodo un solo modo per usarla ed era quindi chiaro quello che poteva essere fatto con questa innovazione. Per il digitale, invece, è tutta un'altra storia. Anche le applicazioni più semplici possono essere usate in tanti modi. Questa dimensione dell'uso multiplo apre pertanto uno spazio etico: ci sono infatti usi "buoni" e usi "cattivi". Come facciamo a discriminarli, a discernere fra un uso corretto e un uso pericoloso? Certo questo non è un primato del digitale; si è già visto più volte nella storia della tecnica.

Pensiamo all'energia atomica: può curare il tumore o distruggere - con le sue reazioni - intere città; la stessa pistola può proteggere un indifeso o uccidere persone ignare. Nel caso del digitale, però, il potenziale di applicabilità è massimo, visto che si aprono infinite possibilità applicative, e quindi il tema etico del "corretto" utilizzo assume un ruolo centrale.

Questo è il primo punto che vorrei sottolineare: oggi c'è un'eccessiva enfasi sull'alfabetizzazione digitale: anche il Governo e le forze politiche usano questa espressione, tra l'altro per me oscena: alfabetizzare, insegnare l'abc del digitale. Solo che generalmente si alfabetizzano gli analfabeti; quando sento la parola alfabetizzare, penso che il destinatario sia una persona ignorante. Io parlo, invece, di cultura digitale: non si tratta tanto di imparare a usare uno strumento, si tratta di capirne le implicazioni, gli effetti collaterali, le precondizioni, i modelli economici sottesi.

Serve una competenza più profonda; il tema però non viene affrontato con chiarezza, perché chi guida e orienta i temi legati al digitale è un sistema economico potentissimo - anzi un vero proprio mondo, un mondo guidato dall'offerta. Facciamo un semplice calcolo: le prime 13 aziende americane che si occupano di digitale -

solo le prime 13 (ce ne sono molte di più in America) - valgono tre volte la Borsa italiana, tre volte la nostra economia. E stiamo contando solo quelle 13 aziende; non abbiamo considerato né l'Europa (pensiamo al mondo delle telecomunicazioni o il mondo del software) né l'Oriente.

Quel numero rappresenta dunque una piccola parte dell'economia digitale: basta pensare a quanto vale Samsung o alla "neonata" Ali Baba - il sito di e-commerce cinese che si è quotato recentemente e vale, già oggi, un terzo della Borsa italiana. Questo settore economico sta anche esercitando un potere culturale, una sorta di pensiero unico che sostanzialmente dice: "*Il digitale è cosa buona e giusta; più ne hai meglio è, se qualcosa non funziona, la prossima versione lo risolverà*".

Ritengo dunque necessario reinserire - anche nel mondo digitale - il pensiero critico; quello autentico auspicato da Cartesio: il dubbio sistematico. Cartesio riteneva necessario il dubbio sistematico non tanto per generare scetticismo, ma per costruire il metodo scientifico su basi solide e verificabili. Vedo, da osservatore del mondo digitale, che non c'è più senso critico. Il fenomeno digitale viene - come abbiamo detto all'inizio - sempre descritto con elencazioni infinite delle meraviglie della tecnica, promesse straordinarie di cose che cambieranno. Ma se non inseriamo in questi ragionamenti anche il senso critico, se non incominciamo a riflettere sui crescenti lati oscuri, se non ci domandiamo quali saranno le implicazioni sociali e umane derivanti dall'adozione diffusa di alcune tecnologie.

Per questi motivi la questione etica è importante, perché siamo di fronte - come utenti - a molte opzioni di utilizzo. La questione è dunque non solo il come insegnare a usare una determinata soluzione digitale, ma il come insegnare quello che i gesuiti chiamano il discernimento, e cioè la capacità di capire quado un utilizzo è corretto ("buono") e quando è invece scorretto ("cattivo"). Mi viene in mente, a questo proposito, una riflessione di un famoso intellettuale di metà Novecento, Paul Goodman:

"Dipenda o no dalla nuova ricerca scientifica - diceva -, *la tecnologia è un ramo della filosofia morale non della scienza, perché è legato alle scelte"*.

Allora, di questo tema si parla troppo poco; il rapporto tra etica e tecnologia non è questione secondaria rispetto alla costruzione di una competenza digitale. L'intenzionalità nell'uso di una specifica soluzione digitale deve essere compresa e ciò dipende anche dai metodi di design adottati. Si parla sempre più frequentemente di *affordance*, come caratteristica di un oggetto ben progettato: l'*affordance* è la proprietà di un oggetto di "suggerire" in maniera naturale (senza l'uso di manuali) le "corrette" modalità di utilizzo.

Questo concetto va bene per gli oggetti fisici, ma l'*affordance* di un'applicazione cosa significa?

Basta guardare come la gente usa oggi la posta elettronica. Ci sono decine e decine di pratiche di uso completamente diverse, alcune delle quali particolarmente problematiche. Infatti un certo modo di usare la posta elettronica sta intossicando le aziende. Alcune aziende stanno addirittura togliendo la posta elettronica; hanno infatti stimato che questo sistema di comunicazione digitale - se mal utilizzato - può assorbire fino al 20% del tempo dei manager, un giorno la settimana. E questo tempo è sempre più spesso utilizzato per leggere e/o rispondere a mail inutili. Se ne parla però molto poco, quasi in maniera carbonara, perché se qualcuno dice: *"Sono un po' a disagio con la posta elettronica"*, viene preso per analfabeta, gli si dice che non è al passo coi tempi, che è obsoleto. Per questi motivi se ne parla poco.

A me è capitato, avendo scritto un libro che si intitola *Il lato oscuro del digitale* ed essendo non solo un esperto ma soprattutto un appassionato di digitale, di osservare che - alla fine della presentazione del libro - i partecipanti - come se si fossero presi coraggio - iniziavano a parlare dei problemi, dei timori, delle disillusioni: c'è chi parlava appunto dell'incubo della posta elettronica, chi metteva in dubbio la qualità delle informazioni che

si trovano in Rete, chi metteva in luce i problemi della sicurezza informatica, chi infine si preoccupava dei propri figli e - ad esempio - del crescente fenomeno del bullismo online. Tutto ciò affiorava quasi naturalmente, ma ciò accadeva perché il tema del digitale era stato affrontato anche dal punto di vista critico. Se non parliamo diffusamente e approfonditamente anche delle dimensioni problematiche, come possiamo costruire un percorso anche normativo alla diffusione e uso del digitale?

C'è poi un secondo aspetto di cui vorrei parlare - e riprendo la domanda della dottoressa Bianchi Clerici sul cosiddetto "uomo aumentato". Questo è un altro tema molto delicato che va analizzato con cura e con competenza.

La *National Science Foundation*, il grande organismo di ricerca americano guidato dallo Stato, ha lanciato agli inizi del 2000 un gigantesco progetto sull'uomo "potenziato": *Converging Technologies for Improving Human Performance*; il suo obiettivo è sviluppare nuove tecnologie in grado di potenziare l'uomo e di contrastarne le innate (e crescenti con l'invecchiamento della popolazione) fragilità.

Questo progetto - e si può solo pallidamente immaginare la quantità di risorse, dirette e indirette, che sta trascinando dietro di sé - si riassume con un acronimo che ne esprime la potenza e l'ampiezza: *NBIC = Nanotechnology, Biotechnology, Information Technology and Cognitive Science*. L'obiettivo è lavorare su tutte queste dimensioni tecnologiche per trovare soluzioni tecnologiche in grado di migliorare l'uomo.

L'idea che c'è dietro è che l'uomo sia una creatura che noi stessi - gli uomini - possiamo plasmare a nostro piacimento e che noi sappiamo cosa sia buono e cosa sia cattivo. Questo tema dell'"uomo potenziato" - di cui gli oggetti indossabili, la sensoristica e l'Internet dentro le cose sono componenti strumentali - comporta un grandissimo problema etico e giuridico, e cioè il fatto che effettivamente gli uomini non siano tutti uguali. Infatti cominciano a emergere "sottogruppi" di umani molto differenti fra loro che

possono/vogliono vantare specifici diritti. Ci sono già fatti concreti. Ad esempio il caso di Pistorius è emblematico: una persona con un forte handicap che - grazie alle nuove tecnologie - ha potuto disporre di protesi ("semplicemente" meccaniche) che lo hanno talmente potenziato che gli è stato ad un certo punto impedito di partecipare alle Olimpiadi dei "normali", perché era più veloce degli altri.

I pochi che si occupano di etica della tecnologia, incominciano a domandarsi: se si incomincia a rendere possibile la nascita di uomini "aumentati", loro pretenderanno diritti a scapito delle persone normali, e allora dove andremo a finire? Questo è un primo filone etico dove ciò che viene potenziato non è tanto e solo l'intelligenza o il carattere (grazie all'uso di ansiolitici, psicofarmaci, ecc.), ma l'uomo nel suo complesso, nella sua durata di vita, nella sua capacità posizionarsi e di capire gli altri.

Il secondo filone è stato toccato anche recentemente: i diritti dei "quasi umani". In Argentina l'orango Sandra che stava da quasi trent'anni nello zoo di Buenos Aires ha ottenuto l'*habeas corpus*. I giudici che hanno concesso la sua "liberazione" hanno accettato la tesi che l'animale provasse sensazioni quasi umane e quindi - per l'*habeas corpus* - non poteva essere tenuto in prigione contro la sua volontà senza aver commesso un crimine. La cosa ha fatto grande scalpore e se ne parlerà nel prossimo futuro.

Abbiamo, dunque, da una parte l'uomo che diventa "superuomo" - *übermensch* (oltre-uomo), se usiamo la famosa espressione di Nietzsche - e dall'altro l'emergenza di "quasi-uomini", che in quanto esseri che provano sentimenti "quasi umani" vantano anch'essi dei diritti da tutelare.

Infine - ed è la ciliegina - c'è il mondo delle tecnologie che vuole costruire macchine autonome - robot, androidi, droni - che si muovono e decidono senza l'ausilio diretto dell'uomo ma solo con algoritmi (oggi scritti dall'uomo, ma domani chissà) e dati prelevati dal contesto in cui operano. Parliamo ad esempio della *Google Car:* se fa un incidente di chi è la colpa? Chi è il responsabile dell'incidente di una macchina che si guida da sola?

Non si possono ovviamente usare le regole che valgono per un frullatore che ci ferisce.

Io credo, pertanto, che affrontare con maggiore profondità questa dimensione problematica ed etica sia necessario per prefigurare il futuro e usare gli strumenti legislativi per provare a orientare sia l'evoluzione tecnologica sia i processi di adozione verso un futuro migliore. Dobbiamo dunque incominciare a chiederci davvero che cosa significhi "aumentare" l'uomo? Che tipo di forzatura umana e sociale viene posta in essere con il fatto che poi sarà necessario tutelare ANCHE gli uomini aumentati? E poi, chi ha il diritto di essere aumentato? Nasceranno nuove forme di discriminazione?

Credo che questo genere di riflessioni, che oggi sono lontane dal dibattito tecnologico corrente - che si concentra sui processi di alfabetizzazione digitale, sulla costruzione delle rete *ultra-broadband*, su come le aziende si devono relazionare digitalmente con la Pubblica Amministrazione (fatturazione elettronica, identità digitale, ecc.), su chi debba controllare la Rete Telecom - debbano (ri)acquisire centralità.

È come se noi fossimo incantati dalla tecnologia, un po' come capitò a Pinocchio quando entrò nel paese dei balocchi. Se uno si rilegge - tra l'altro, Marisa Marraffino l'ha fatto in un suo libro - il famoso pezzo di Collodi senza conoscere la fonte del brano, pensa che sia una descrizione di Facebook: *"Questo paese non somigliava a nessun altro paese del mondo* […].*Nelle strade, un'allegria, un chiasso, uno strillìo da levar di cervello! Pinocchio, Lucignolo e tutti gli altri ragazzi si ficcarono subito in mezzo alla gran baraonda, e in pochi minuti, come è facile immaginarselo, diventarono gli amici di tutti. Chi più felice, chi più contento di loro?"*

Sembra lontano ma è un tema molto vicino. Quanti giovani incominciano a dire: *"Io ho 550 amici"* (quelli registrati su Facebook). Come possiamo pensare (o lasciar loro pensare) che quella sia vera amicizia!

Forse non ce ne accorgiamo ma anche i nostri figli si stanno

abituando a questi termini e - *nomen omen* - il concetto "operativo" di amicizia viene oggi definito da Facebook.

Una breve riflessione conclusiva: oramai non possiamo tirarci fuori da questi temi, come faceva notare correttamente il direttore di *Wired* Massimo Russo; siamo parte di un flusso più grande che ci determina. Forse non possiamo orientarlo ma possiamo educare i comportamenti nostri e dei nostri figli, possiamo aguzzare il nostro senso critico e soprattutto possiamo ridurre la nostra passività inconsapevole.

Dobbiamo avere il coraggio di capire, di non smettere di farci domande "tendenziose", di domandarci: ma perché è così? Non potrebbe essere in un altro modo? Che significato c'è dietro? Che gruppo di potere c'è dietro? Questa gratuità - tutto è sempre più gratuito - che prezzo mi chiede di pagare davvero?

Possiamo anche decidere di accettare consapevolmente l'utilizzo di applicazioni digitali "problematiche", che ci prendono i dati personali, che ci monitorano, che riducono le nostre capacità cognitive, siamo adulti. Ma quanta gente, ad esempio i nostri figli, lo fa senza consapevolezza?

Io credo che molti di questi aspetti, che nascono nei piccoli comportamenti digitali quotidiani - e non sono influenzati dalle grandi battaglie per la libertà lanciate ad esempio dai movimenti hacker - ci richiedono di prendere della pause, di guardare il mezzo digitale con occhi un po' più critici, di ri-flettere sul nostro "essere digitali".

Naturalmente perché ciò sia possibile ed efficace, dobbiamo avere un certo dominio della materia; non basta una semplice infarinatura digitale. Però è importante la "postura" che teniamo verso il mondo digitale; non di perenne sospettosità e neppure di cieca fiducia e adorazione ma di passione unita a quel costruttivo dubbio sistematico che ci suggeriva Cartesio.

Un'ultima nota conclusiva: solamente un anno fa sono usciti i primi articoli su *The Economist* critici anche sugli impatti che la rivoluzione digitale porterà dal punto di vista occupazionale.

Un recente rapporto dell'università di Oxford (*The Economist*, editoriale *The Effect of today's technology on tomorrow's jobs will be immense - and no country is ready for it*, 18 gennaio 2014) ha fatto il calcolo che nel prossimo ventennio quasi il 50% dei lavori che oggi vengono fatti saranno svolti da software, computer, androidi, droni. La domanda che dobbiamo porci è: quel 50% dove andrà a finire?

Ciò che stupisce è che di questa questione si discute pochissimo, anche da quelle parti sociali che dovrebbero essere più vicine ai lavoratori. Oltretutto proprio nel mondo del software si sta sviluppando il fenomeno del caporalato.

Sembra che il mondo sia talmente innamorato di questo potere magico del digitale che non senta l'esigenza di porsi neanche quei problemi che sono già oggi facilmente leggibili.

Giovanna Bianchi Clerici

Grazie dottor Granelli in particolare per quest'ultima riflessione. Platone temeva che la scrittura avrebbe ucciso la capacità di ricordare degli esseri umani. La storia ci ha invece dimostrato che, nel flusso dei cambiamenti, l'importante è cercare di governarli il più possibile.

Il dottor Maggi è un esperto di sicurezza, veramente una cosa assai complicata. Le chiederei semplicemente di tenere come barra di riferimento nella Sua esposizione un problema che per il Garante è centrale, ovverosia come si può tutelare al massimo la sicurezza dei dati, affinché non finiscano nelle mani di malintenzionati che intendano usarli per cose illecite.

Inoltre, Le chiederei - questo più da cittadina che non da esponente di un'Autorità - come si può garantire la sicurezza dei dati anche nei confronti di entità come i Governi o le imprese che li potrebbero voler utilizzare per scopi magari non illeciti, ma neppure troppo nobili. Prego.

Federico Maggi

Grazie al Garante per l'invito e grazie per lo spunto. L'essere ultimo in una giornata come questa ha il lato negativo che la maggior parte degli aspetti che riguardano le applicazioni di che cosa si può fare, di bene o di male, con Internet of Things sono già state dette. Quindi andrò un po' rapidamente sulle prime slide(1) che mi ero preparato.

La prima riporta una citazione del 2008 ed è stata presa da un rapporto del *National Intelligence Council*, e dice che gli individui, le aziende, e i governi sono impreparati per quello che può succedere nel futuro, quando collegheremo degli oggetti che fino a ieri non erano mai stati collegati ad Internet. Il primo spunto che vorrei dare al pubblico e al resto dei relatori è: siamo preparati oggi? Oggi abbiamo visto una giornata in cui gli spunti applicativi sono stati infiniti, c'è soltanto la nostra fantasia, la fantasia di chi progetta, come limite.

Avevo pensato di parlarvi dell'Internet of Things attraverso tre fattori, di cui il primo doveva essere quello tecnologico, ma non avevo pensato di dover spendere troppo tempo per parlare di un altro fattore, ossia del ruolo dei media. Invece vorrei spenderci qualche minuto. Secondo l'inventore di *Ethernet*, per i non tecnici è il protocollo che fa funzionare la scheda di rete quando si collega al cavo, quindi non proprio l'ultimo arrivato, Robert Metcalfe, il ruolo dei media ha fatto la maggior parte del fenomeno di Internet of Things.

Io sono d'accordo con lui non perché è Robert Metcalfe, ma perché l'abbiamo visto, se guardiamo davvero con ottimo critico tutta l'aura magica che c'è intorno all'intelligenza artificiale, ai *wearable computer*, ai tessuti intelligenti e tutto quanto, sotto c'è comunque un microprocessore e del codice che esegue. È una tecnologia che esiste da sempre e quello che succede è che,

(1) Le slide illustrate sono disponibili all'indirizzo: *http://s.maggi.cc/iotsec2015*

indipendentemente da quello che ci facciamo girare sopra, indipendentemente dal calcolo che noi facciamo, si tratta di codice creato da esseri umani. Questo, nonostante tutto, non è cambiato.

Quindi è bene evitare di confondere codice creato da esseri umani, che implementa un algoritmo matematico, con qualcosa di senziente.

L'intelligenza artificiale non è senziente, non è ancora senziente, quindi non può essere una minaccia, non può essere un aggressore, non può essere un programma che trova una falla in un sistema e gioca al videogioco barando. Quello è - mi dispiace dirlo - un programma che ha trovato il "massimo di una funzione", è un programma che ha trovato il modo migliore per giocare. Bisogna stare un po' attenti a leggere sempre con occhio critico e rivolgersi quanto più possibile ai tecnici quando si interpreta la facciata che i media ci stanno facendo vedere dell'Internet of Things.

Io dovevo parlarvi di sicurezza, quindi adesso, dopo aver saltato un po' delle slide introduttive, vi parlerò di sicurezza. Vado subito al punto: mi riallaccio ad una parola utilizzata dal dottor Granelli. Se non serve alfabetizzazione tecnologica - affermazione su cui sono abbastanza d'accordo - serve alfabetizzazione di sicurezza. La risposta alla Sua prima domanda, dottoressa Clerici, è che serve alfabetizzazione di sicurezza.

Fare alfabetizzazione di sicurezza significa insegnare da subito a chi programma, a chi programmerà, ai programmatori del futuro, i nostri figli, i nostri studenti per me, a programmare in modo sicuro. La risposta non è, dal mio punto di vista, normativa, o meglio, ovviamente le norme hanno un grosso peso, ma dal mio punto di vista di tecnico la risposta è: educare i programmatori del futuro a creare software che siano quanto più immuni da attacchi. Questo, chiaramente, capirete che non è facile, nel senso che in un modo o nell'altro, ne siamo testimoni tutti i giorni, basta aprire un giornale neanche tanto tecnologico e gli attacchi ci sono in quantità, un giorno sì e l'altro pure.

Secondo me la risposta parte dai banchi di scuola, anche della

scuola superiore, perché nella scuola superiore si impara a programmare in C, ad esempio, che è un linguaggio di programmazione che rischia di sparire. Alcuni studenti al mio corso di sicurezza quando vedono un listato di programma in C dicono: aiuto, C, non me lo ricordo più.

Non possiamo permetterci il lusso di parlare di tecnologie che possono fare qualunque cosa la nostra fantasia possa immaginare, se prima non abbiamo risolto il problema della sicurezza, ma non sull'Internet of Things, su qualunque sistema, quindi su questo computer, sul palmare, sui nostri sistemi che già conosciamo bene. Infatti c'è troppa incertezza già lì, dunque non possiamo costruire delle automobili che si guidano da sole, se l'autostrada su cui vanno non è per niente sicura.

Fare sicurezza significa gestire un rischio. Qui ho messo solo due delle variabili che gli esperti di sicurezza normalmente vedono.

C'è una terza variabile che è quella della minaccia. Comunque, il rischio - che è l'oggetto che un esperto di sicurezza deve cercare di minimizzare - è direttamente proporzionale al numero di minacce, al numero di asset, o di dispositivi, di superfici attaccabili, chiamateli come volete e di vulnerabilità. La minaccia è qualcosa che non possiamo controllare, non possiamo chiedere agli aggressori di smetterla di attaccare i nostri dispositivi, possiamo controllare il numero dei dispositivi e il numero di vulnerabilità.

Ora, il numero di dispositivi, converrete con me, non possiamo farlo che salire, nel senso che un presupposto, un requisito dell'Internet of Things è proprio quello di avere quanti più dispositivi possibile, in ogni angolo del pianeta, affinché monitorino qualsiasi cosa, affinché implementino questo concetto di collezione di dati come una *commodity*. C'è una slide che non ho qui ma che ho visto qualche giorno fa, dove c'è un pozzo di petrolio che sputa fuori dati. L'estrazione del petrolio è una *commodity*, possiamo prenderlo come assodato, l'estrazione di dati è diventata una *commodity*. Quindi, non possiamo abbassare la quantità di dispositivi, ma possiamo controllare la quantità di vulnerabilità e lo

facciamo con alfabetizzazione di sicurezza dei nostri futuri programmatori.

Questa slide è ripresa da una presentazione fatta durante le feste, il 25 e il 27 dicembre, presentata al *Chaos Computing Congress*. Riguarda un censimento che è stato fatto sui dispositivi che rispondevano sulla porta 80 - per i non tecnici *http* - ossia i dispositivi che rispondevano se interrogati su Internet. È stata fatta una scansione dell'intero spazio Internet. Sono stati isolati poi quelli che riguardavano dispositivi associabili alle tecnologie Internet of Things, che è la fetta di sinistra. Ora, di questa fetta di sinistra i due ricercatori di Check Point hanno controllato se ci fossero vulnerabilità, quale tipo di software girava, eccetera (c'erano tecnologie diverse, erano sistemi diversi, loro hanno ironicamente messo un tostapane, ma c'era di tutto lì dietro).

Comunque, prima di controllare se ci fossero delle vulnerabilità non note, hanno guardato qual era la versione del sistema operativo (anche se è scorretto chiamarlo sistema operativo), che girava su questi dispositivi *embedded*. Il 98,4% avevano la stessa versione dello stesso sistema, RomPager versione 4.7 mi pare. È una versione che è stata creata nel 2002. Il 98% dei dispositivi che hanno risposto sulla porta 80, che sono stati catalogati come associabili a una tecnologia Internet of Things, avevano tutti la stessa versione dello stesso sistema e, grande notizia, le stesse tre vulnerabilità.

Erano tutti identici, software datato, non aggiornato - perché di Rom Pager ne sono state fatte ulteriori versioni. Sono passati 13 anni dal 2002! In questo lasso di tempo i possessori di tali dispositivi o non avevano la possibilità di aggiornare, o non hanno voluto aggiornare, o il produttore non ha rilasciato aggiornamenti in quella zona.

Qui mi riallaccio a un discorso che fatto nella precedente sessione sul ruolo delle Telco: qual è il ruolo di un service provider che è, di fatto, chi offre connettività a questi dispositivi? Secondo Schneider, che è abbastanza noto a chi fa sicurezza, il ruolo degli

Internet service provider è quello di essere i *carrier* di questi aggiornamenti. Chi meglio dell'Internet provider sarà in grado di offrire dispositivi gestiti e continuamente aggiornati quando c'è un aggiornamento di sicurezza?

Ovviamente offrire aggiornamenti di sicurezza non è una cosa facile, perché richiede tempo e soprattutto richiede denaro. Se un dispositivo deve costare sempre meno, perché devo produrne sempre di più e devo portare il cliente a comprare l'ultima versione, che non è molto diversa dalla precedente, tecnicamente, ma ha qualche funzione in più, allora mi disinteresso degli aggiornamenti e propongo un nuovo prodotto hardware diverso dai precedenti: magari ha ancora lo stesso software, magari ha ancora le stesse vulnerabilità, se non altre.

Vorrei aprire una parentesi sul tipo di vulnerabilità che sono state trovate. Per chi si occupa di sicurezza, anche se non sono esattamente identiche, le tre vulnerabilità trovate erano tutte riconducibili alla classe dei *buffer overflow*, ossia vulnerabilità causate da una gestione della memoria non corretta. Il programmatore ha introdotto degli errori, non volontariamente si spera, che possono essere sfruttati da un aggressore per far girare il codice che vuole su questi dispositivi, quindi far sbattere la macchina contro un muro, resettare la connessione di un router piuttosto che altro, a vostra fantasia.

I pochi capelli che mi sono rimasti sono dovuti al fatto che quando ho visto quali erano le vulnerabilità che c'erano, ho riconosciuto le stesse vulnerabilità che insegniamo i nostri studenti a evitare quando programmano. Verso la fine del corso di *computer security* ci sono un paio di lezioni, tre belle orette divertenti, in cui si parla di come riconoscere e come evitare i *buffer overflow.* Le stesse vulnerabilità che qui sono state trovate in un software datato 2002.

Voglio concludere, perché oggi è stato toccato un punto che riguarda il fatto che non solo l'ambiente fisico è adesso collegato a un sistema digitale, ma anche il sistema digitale è collegato

attivamente, con degli attuatori - è stata utilizzata questa parola - all'ambiente fisico a sua volta. La cosa interessante non è che questi due mondi sono collegati, ma il fatto che il legame è a doppio filo.

Se io devo regolare, per fare un esempio banale, la temperatura in una stanza, ho bisogno di leggere la temperatura e di attuare un'azione per regolare la temperatura stessa. Ora, la regolazione della temperatura è un esempio molto semplice, ma provate a generalizzarlo sui casi applicativi che abbiamo visto oggi.

Prendiamo un attuatore, progettato dall'azienda X, che agisce secondo quello che il programma progettato dall'azienda Y fa, in base alla lettura fatta da un sensore prodotto dall'azienda Z. Cosa succede se questi tre componenti - che presi singolarmente magari sono anche sicuri - se il mondo fisico risponde in modo inatteso? In fisica questo fenomeno si chiama risonanza, ossia un circolo vizioso tra due sistemi, di cui uno è controllato e l'altro risponde amplificando gli effetti del controllo.

Questa è, potenzialmente, una classe di vulnerabilità che forse non conoscevamo. Visto che le marche dei dispositivi, le aziende che li producono sono tutte diverse, è possibile interfacciarli: è proprio uno dei presupposti! Trasparenza, "interfacciabilità", apertura. Pertanto non è da escludere il fatto che questi dispositivi siano effettivamente di produttori diversi.

Di riservatezza dei dati personali in realtà non avevo pensato di occuparmi molto durante la mia presentazione, ma ho una mia piccola slide sull'argomento. Anche se la TV che c'è sulla slide è vecchia, si riferisce ad un caso molto nuovo, il caso LG, non so se qualcuno ne ha letto, è passato abbastanza in sordina, devo dire. Successe ad un certo punto che, dopo aver comprato una delle ultime Smart TV della LG, i possessori si videro arrivare un messaggio che diceva: aggiorna questo dispositivo, perché è arrivata l'ultima versione che ti permetterà di utilizzare servizi di Smart TV. I servizi però c'erano anche prima.

Quando io sono uscito dal negozio, nessuno mi ha detto che se volevo utilizzare questa tv dovevo aderire a questa nuova privacy

policy, a questi termini di servizio. Succede che nella nuova versione del software si richiede: se tu vuoi utilizzare ancora qualcosa a cui ti sei abituato, qualcosa che era diventato un servizio utile per te, dovrai aderire a questa *privacy policy*. Non lo devi fare, ma se vuoi continuare a utilizzare il tuo prodotto com'era prima, come funzionava prima, lo devi fare.

Va bene, io posso dire no, non lo faccio, perdo i servizi di *Smart TV*. Fa niente, perché nella seconda riga della *policy* c'era scritto che, nonostante tu dica di no, io continuerò a raccogliere dati. Ed è scritto nei termini di servizio! Continuerò a raccogliere dati - va bene, anonimizzati, d'accordo - per imparare le tue abitudini televisive, per suggerirti un programma o una pubblicità, magari su qualcosa che comprerai o che ti voglio far comprare.

Un altro aspetto interessante di questa storia è che non c'era e non c'è tutt'oggi - si tratta di più di un anno fa - una versione scaricabile, leggibile, dei termini di servizio. Il produttore ha fatto di tutto non per nascondere, ma per rendere non disponibile alla massa, tranne che ai possessori della TV, la *privacy policy*, nel senso che i termini di servizio si potevano leggere soltanto dal televisore. Il fatto che io li abbia trascritti è perché qualcuno si è messo di buzzo buono e li ha trascritti come un amanuense, su un documento che poi ha reso disponibile in Rete. Sul sito del produttore però questo non c'è scritto.

Per concludere, riguardo a quali sono le soluzioni e le direzioni, la soluzione, che non è tale ma è quello a cui vogliamo auspicare, è quella, come tecnici e docenti, di accrescere una alfabetizzazione riguardo alla sicurezza il prima possibile. Quindi non solo nel quarto anno di ingegneria informatica, o al quarto anno di scienza dell'informazione, ma anche nella scuola in cui si inizia a programmare.

Poi servono tecnologie un po' più nuove, perché abbiamo visto che le tecnologie che ci sono fino ad ora, almeno sotto la lente di ingrandimento di un tecnico, sono le stesse tecnologie, sono solo più piccole e costano meno, ma sostanzialmente sempre del

codice C gira. Quello che serve sono tecnologie veramente nuove e innovative dal punto di vista della sicurezza e della riservatezza dei dati.

Ad esempio nella specifica di Bluetooth 4.2, il protocollo senza fili che si può utilizzare per scambiare foto tra cellulare e computer e viceversa, è inclusa una novità che rende possibile scrivere programmi che non possono essere tracciati. Mi spiego meglio. Il dispositivo, quando viene spostato da un ambiente all'altro e si collega con più dispositivi diversi, mantiene il suo indirizzo, l'indirizzo della scheda di rete, chiamiamolo così anche se Bluetooth in realtà non si chiama scheda di rete. Quello che è stato introdotto in Bluetooth 4.2 è la possibilità di mascherare, in termini ultra semplificati, questo indirizzo, ossia di non renderlo tracciabile a ulteriori dispositivi che si collegheranno con lo stesso dispositivo. Ad esempio se io ho collegato questo palmare a una rete, a un altro dispositivo Bluetooth, non solo lo stesso dispositivo Bluetooth non potrà riconoscermi tra un po' di tempo, ma un altro dispositivo Bluetooth non potrà parlare con quello a cui mi sono collegato e dire: è lo stesso dispositivo? Non lo potrà sapere.

Con questo concludo lasciando, per chi fosse interessato, un riferimento alla versione "verbosa" di tutta questa presentazione, con la parte che ho saltato e tutti i riferimenti bibliografici e tecnici: *http://s.maggi.cc/iotsec2015*.

Grazie.

Giovanna Bianchi Clerici

Grazie. Io sarò tra coloro che cercheranno di capire tutta la versione. Sono grata ai relatori che hanno partecipato a questa sessione e vorrei dare la parola, per le conclusioni, al Vice Presidente della Camera, Onorevole Marina Sereni, che ringrazio particolarmente perché è stata presente dall'inizio alla fine del convegno.

Il pianeta connesso

Chiusura dei lavori

Marina Sereni

Vice Presidente della Camera dei Deputati

Chiusura dei lavori

Il pianeta connesso

Intervento di Marina Sereni, Vice Presidente della Camera dei Deputati

Voglio ringraziare il Presidente Soro e tutta l'Autorità per l'invito. Non posso certo tirare le conclusioni di un dibattito estremamente ricco e complesso che ho ascoltato con grande interesse. Ho trovato molto stimolanti tutte le relazioni e credo che il materiale di questa giornata di lavoro meriti di essere riletto e approfondito.

Credo di poter dire però che questo convegno ha dato a tutti noi - parlamentari, studenti, esperti qui presenti - molti spunti di riflessione e di lavoro per il futuro, ognuno nel suo campo.

Sono emersi dei punti che mi pare siano di base e condivisi.

In primo luogo intanto la dimensione che Internet ha assunto nella società e nella vita di tutti noi, una dimensione che non possiamo più relegare al tema dei nuovi media, perché riguarda la totalità della nostra vita. Nella prima sessione sono state usate alcune metafore: la casa e la famiglia, la cittadina di frontiera, l'ecosistema. Tutte metafore che ci riportano all'ambiente in cui noi viviamo e alla quotidianità che ognuno di noi affronta nelle sue molteplici attività.

Il secondo elemento: siamo di fronte a mutamenti molto veloci. In pochissimo tempo, la Rete è diventata il più grande spazio pubblico dei nostri tempi. Credo abbia ragione Padre Spadaro quando stamattina diceva che è diventato un insostituibile strumento di conoscenza e di esercizio dei diritti. Questo tratto, nonostante tutti i rischi, le preoccupazioni e le criticità che abbiamo giustamente sottolineato, credo debba essere mantenuto. Internet è diventato un vero e proprio ponte tra persone e culture lontane, tra chi poteva essere escluso fino a poco tempo fa totalmente e invece oggi può partecipare, può essere protagonista, quindi una fonte di sviluppo, di crescita non solo culturale ma anche economica.

Nel vostro dibattito, in molte relazioni, la dimensione economica della Rete, di ciò che può accadere nello sviluppo di Internet è stata non a caso molto evidente.

Naturalmente tanto più Internet si diffondeva e assumeva le dimensioni di cui voi ci avete parlato, tanto più abbiamo tutti avvertito - come diceva prima il dottor Granelli, qualcuno vergognandosi di dirlo, - l'esigenza che questa potenzialità, questo sviluppo non si trasformasse in un luogo di arbitrio, in un luogo in cui i diritti, la dignità delle persone potessero essere calpestati, comunque potessero soccombere in nome di un indeterminato concetto di libertà della Rete, o di magnifica e progressiva sorte delle tecnologie.

Da qui la necessità di una riflessione. Magari lo stiamo facendo troppo lentamente, è verissima la contraddizione di cui ci parlava il prof. Russo stamattina - parliamo di qualcosa che sembra il futuro e invece ci siamo immersi dentro - però intanto abbiamo cominciato.

Quindi, ancorché con questa percezione, con questa distonia, credo dobbiamo avere la consapevolezza che stiamo facendo un lavoro importante, che l'Authority sta facendo un lavoro importante per cercare di riportare tutti ad una riflessione sul rischio che questo spazio, da spazio di libertà e di conoscenza possa, invece, diventare qualcos'altro. Possa essere uno spazio in cui i princìpi fondamentali si affievoliscono fino ad annullarsi, se non ci impegniamo a definire dei princìpi certi e chiari per evitare che prevalgano magari gli interessi più forti.

Prima qualcuno ha citato le Sette Sorelle. Ci siamo guardati con il Presidente Soro e la dottoressa Iannini e ci siamo chiesti: ma saranno sette? Ci arriviamo a sette? Ecco, proprio perché i grandi protagonisti nella Rete sono pochi c'è un lavoro da fare per evitare che l'assenza di princìpi certi e chiari possa far prevalere gli interessi più forti dell'economia, della politica, della comunicazione di fronte, invece, all'interesse generale, all'interesse degli individui e delle comunità.

In questo delicato contesto tutti quanti abbiamo letto con interesse la pronuncia della Corte di giustizia del 13 maggio 2014, che ci richiama ad un bilanciamento di interessi diversi, contrapposti, per evitare, appunto, che gli interessi economici prevalgano sulle libertà individuali. Quella sentenza che tutti hanno definito la "sentenza Google", ci dice che l'interferenza con il diritto della persona alla protezione dei dati non può essere giustificata meramente dall'interesse economico del motore di ricerca.

Quella stessa pronuncia della Corte riconosce che il diritto degli individui di richiedere ai motori di ricerca la rimozione dei collegamenti alle informazioni personali che li riguardano, allorquando siano imprecise, inadeguate, non pertinenti o eccessive in rapporto alle finalità per le quali sono state trattate e al tempo trascorso, deve essere affermato. Noi ci siamo dovuti misurare con questo tema, perché il Presidente Soro ce lo ha chiesto. Come Camera dei Deputati abbiamo assunto una specifica disciplina in materia di diritto all'oblio in sede di Ufficio di Presidenza e abbiamo misurato nel nostro piccolo, che però non è piccolissimo, il tema che poco fa il professor Artieri citava, dicendo che la trasparenza e la privacy debbono poter andare insieme.

Abbiamo dovuto costruire una disciplina in merito ad alcune istanze che sono pervenute concretamente alla Camera dei Deputati, aventi per oggetto "*Dati personali contenuti in atti parlamentari*" e abbiamo dovuto trovare una disciplina, che a me pare un passo importante ed equilibrato, per bilanciare la tutela del singolo - quindi rispondere a quei singoli - e il principio costituzionalmente riconosciuto di pubblicità dei lavori parlamentari. Siamo dentro un campo molto delicato, molto complesso, l'Ufficio di Presidenza ci ha lavorato e ha costruito una risposta.

Come qui è stato citato non ci siamo fermati a questo aspetto, abbiamo tentato di fare un lavoro, c'è qui Anna Masera che con la Presidente Boldrini ha guidato questo sforzo, questa esperienza che io considero molto positivamente. Abbiamo provato a vedere, dal punto di vista di un Parlamento, se possiamo mettere

insieme, in maniera multidisciplinare, delle competenze diverse, alcune delle quali sono state qui con noi stamattina, in una Commissione per i diritti e i doveri in Internet. Abbiamo voluto intanto cominciare a declinare il tema dei diritti, cercando di definire quali sono i diritti che possiamo immaginare di dover garantire nella Rete, quali sono i diritti degli utenti.

Mi piace ricordare, tra i vari diritti - alcuni ne sono stati qui citati nelle relazioni di stamattina, non li riprendo - che ce n'è uno specifico legato all'educazione degli utenti, a un uso consapevole della Rete e all'esercizio di questi propri diritti. Questo è un tema che trasversalmente molti di voi hanno toccato, e che io personalmente considero fondamentale. Poco fa Artieri diceva: imparare a prenderci cura dei nostri dati. Russo concludeva la sua relazione facendo l'esempio di chi ha cliccato sul primo figlio nato uguale al cane, ecc.. Maggi poco fa è tornato su questo aspetto a proposito della sicurezza.

Il tema è gigantesco, e penso che abbia fatto bene la Commissione per i diritti e i doveri in Internet, nella bozza di Carta dei diritti, a indicare questo - oltre ad altri se volete più scontati e più ovvi - come uno dei terreni su cui continuare a lavorare. La Carta dei diritti in Internet non prelude a una legge, non sarebbe compito della Commissione farlo, ovviamente ci sono proposte di legge anche al Senato, c'è qui la collega del Senato che si sta occupando di *cyberbullismo*. Ci sono proposte di legge alla Camera che riguardano l'educazione digitale, ci sono delle iniziative di singoli parlamentari.

Questa Commissione è emanazione della Presidenza della Camera, ha un altro compito, ha elaborato una bozza di Carta dei diritti in Internet che, come detto, non prelude alla scrittura di una legge, per ora, ma indica un percorso. La chiave sta nel tema dei bilanciamento dei diversi interessi in gioco, applicabili alla dimensione non solo nazionale, naturalmente, ma universale e comunque sovranazionale.

L'8 dicembre questa Commissione ha varato la bozza che alcuni di voi conosceranno, questa bozza di Dichiarazione per i

diritti in Internet, la cui finalità è quella di far sì che la libertà, l'uguaglianza e la diversità delle persone siano garantite anche nella Rete, attraverso il rispetto di alcuni princìpi su aspetti fondamentali: il diritto di accesso, la neutralità della Rete, la tutela dei dati personali e della loro identità e inviolabilità, il diritto all'anonimato e all'oblio, le garanzie sulle piattaforme e, appunto, l'educazione anche all'uso corretto di Internet in sicurezza.

Il testo è stato reso disponibile alla consultazione pubblica sulla piattaforma dei media civici e la raccolta dei contributi avrebbe dovuto avere durata di quattro mesi e finire a fine febbraio, poi è stata prorogata fino alla fine di marzo. Sottolineo questo aspetto perché vedo qui non solo tanti esperti, che avranno sicuramente dei suggerimenti da dare, ma anche tanti giovani, tanti ragazzi che su questo stanno studiando, si stanno formando e credo che possa essere interessante avere suggerimenti da tutti voi.

Nel frattempo abbiamo aperto un canale con altri parlamenti, e anche questo lo considero un dato importante. Mi risulta, non so se sono in errore, che noi siamo il primo Parlamento a tentare questa strada; su questa base abbiamo interpellato i parlamenti di altri Paesi per chiedere anche a loro eventuali suggerimenti e riflessioni. Tutto ciò per avvicinare un momento in cui si possa elaborare una analoga Carta andando oltre i confini del nostro Paese, guardando all'Europa e magari ad una dimensione più globale come quella delle Nazioni Unite.

Naturalmente non sono entrata nel merito delle innumerevoli, direi infinite sollecitazioni delle vostre relazioni, non sarei stata in grado di farlo e non mi compete. Voglio però davvero ringraziare l'Authority e tutti i relatori perché è stata una mattinata di grande interesse, molto formativa e anche di grande stimolo. Ogni tanto, anche alla vigilia dell'elezione del nuovo Capo dello Stato, c'è bisogno di questo.

Grazie e buona giornata.