IAI
Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

Internet of things, big data e privacy: la triade del futuro

di Sabrina Palanza

ABSTRACT

Questo saggio analizza uno degli ambiti di ricerca in continua espansione negli ultimi anni, quello dell'Internet delle cose (*Internet of Things*, IoT), che studia come rendere gli oggetti di uso quotidiano "intelligenti", facendoli interagire tra loro e con gli utenti, sviluppando in senso evolutivo le capacità intrinseche della rete. Grazie alla rapidità dei progressi tecnologici, infatti, gli oggetti più comuni, impiegati in diversi settori quali la logistica, la mobilità, la salute ecc., si stanno rivelando gli apripista di un gran numero di nuove applicazioni che permetteranno di migliorare la qualità della vita e di avere più informazioni riguardo all'ambiente in cui questi oggetti si trovano. Il primo capitolo si concentra sulla definizione e sulla diffusione dell'IoT, offrendo una rapida panoramica sulle componenti degli oggetti *smart*. Il secondo capitolo si sofferma sulla relazione esistente e sempre più forte tra il mondo degli oggetti intelligenti e i dati, i metadati e i *big data*, nonché sul processo di raccolta dei dati e nello specifico sul *data mining* e il *business analytics*, cercando di evidenziarne eventuali pro e contro. Nel terzo capitolo si discute delle possibili ripercussioni del fenomeno dell'IoT sulla privacy del singolo utente cercando, a tal proposito, di dare una definizione del concetto di privacy e di descrivere la sua evoluzione; analizzando le problematiche dei dispositivi attualmente disponibili sul mercato; e illustrando come queste ripercussioni potrebbero trovare parziale soluzione nel concetto di *privacy by design*.

Privacy | *Sicurezza* | *Unione europea* | *Italia*

keywords

ISSN 2280-6164

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

Internet of things, big data e privacy: la triade del futuro

di Sabrina Palanza*

1. Dall'Internet of Things all'Internet of Everything

1.1 Una definizione di Internet delle cose

Internet delle cose (*Internet of Things*, IoT) è un neologismo riferito all'estensione di internet al mondo degli oggetti e dei luoghi concreti. Questo concetto è stato introdotto nel 1999 da Kevin Ashton, ricercatore britannico del Mit (Massachusetts Institute of Technology), che teorizzò per primo un mondo di sensori, distribuiti ovunque, direttamente collegati alla rete internet. Tra i primi progetti sperimentali occorre ricordare la piattaforma Cense (*Central Nervous System of the Earth*), perfezionata nei laboratori Hewlett Packard nel 2009, il cui obiettivo era quello di fornire una nuova visione del mondo, in un certo senso più reale, utilizzando sensori intelligenti in grado di rilevare ogni tipo di variazione ambientale dalla pressione alla temperatura, passando per le correnti marine e atmosferiche.

Da quel momento in poi, la crescita inarrestabile della tecnologia wireless e satellitare ha fatto sì che si arrivasse a progettare oggetti sempre più connessi, in grado di trasferire in rete una mole considerevole di informazioni e dati. Non sono dunque, come tradizionalmente si potrebbe pensare, solo computer o tablet ad essere connessi alla rete, ma "cose", che divenendo "*smart*" riescono a fornire alle persone applicazioni facili da usare in ogni circostanza. Ad esempio il polsino sportivo da indossare durante il jogging quotidiano, con schermo luminoso e facile da leggere mentre si è in movimento, collegato direttamente alla rete con dispositivi Gps (*Global Positioning System*), che fornisce informazioni sui chilometri corsi e il percorso fatto. Il concetto di internet "delle cose" implica infatti l'assenza di computer potenti e non "portabili", sostituiti da oggetti di uso quotidiano meno potenti.

* Sabrina Palanza ha conseguito una laurea magistrale in Relazioni internazionali presso l'Università di Perugia.

· Documento preparato per l'Istituto Affari Internazionali (IAI), ottobre 2016.

La presenza negli oggetti di sensori connessi alla rete (e agli altri oggetti *smart*) permette un trasferimento di dati supportato dalle caratteristiche principali dell'oggetto. L'oggetto infatti riceve input che dall'ambiente esterno comunicano i dati acquisiti ad un server il quale, dopo un'elaborazione degli stessi, formula "comandi" da inviare all'oggetto smart facendo sì che risponda con degli output[1] (volti, per esempio, al perfezionamento del servizio svolto dall'oggetto). Centrale, quindi, appare il ruolo della condivisione dei "dati", il carburante per la produzione successiva di informazioni. I dati singolarmente non risultano particolarmente significativi, ma se analizzati in grandi volumi possono portare alla delineazione di modelli e tendenze, ad esempio comportamentali, che sommandosi ad altre fonti di informazioni producono poi la conoscenza.

Nel mondo dell'IoT i dati aumentano continuamente, innescando una serie di progressi importanti anche da un punto di vista economico. Non a caso, infatti, l'economista Jeremy Rifkin[2] parla ormai da tempo di "terza rivoluzione industriale" riferendosi all'era digitale, un'epoca che porta con sé la presenza sulle piattaforme dell'IoT di dati che incidono significativamente sulla "catena del valore" (*value chain*), in quanto attraverso lo studio delle informazioni presenti si potranno andare a creare applicazioni in grado di aumentare l'efficienza aggregata. Questa condivisione di informazioni, del tutto gratuita, sta sviluppando la cosiddetta *sharing economy*, che potrebbe avere conseguenze inaspettate per la crescita dei Paesi in via di sviluppo, fornendo loro quel "bagaglio di informazioni" finalizzato alla risoluzione di alcuni dei problemi che si trovano ad affrontare.

Se da un lato la maggior parte degli esperti in tecnologia ed economisti ritengono che l'IoT sia un passo verso un mondo migliore più interattivo, sociologi ed esperti di diritto rimangono invece più scettici, rilevando alcune problematiche legate alla sicurezza e alla privacy. Numerosi studi dimostrano che attacchi hacker potrebbero prendere il controllo dei dispositivi senza che l'utente se ne accorga, o che qualcuno potrebbe ricostruire le abitudini alimentari dei consumatori analizzando il flusso di dati provenienti dal frigorifero, così come una semplice lavatrice potrebbe divenire la "complice" di criminali comunicando loro l'assenza dei padroni di casa[3]. Tutto ciò viene agevolato, inoltre, dal fatto che spesso gli utenti hanno un unico contratto con lo stesso fornitore di servizi internet, telefono e televisore, trasferendo così nelle mani di un unico soggetto un'ingente quantità di informazioni. Quali sono quindi le insidie dietro questo fenomeno? Un *cyber* criminale, per esempio, potrebbe trasformare i dispositivi *smart* in oggetti in grado di eseguire delle azioni a comando, tra cui inviare i dati memorizzati verso soggetti terzi non autorizzati, attivare webcam integrate per spiare il proprietario dell'oggetto e inoltrare messaggi di spam.

[1] Adrian McEwen e Hakim Cassimally, *L'Internet delle cose*, Milano, Apogeo, 2014.

[2] Jeremy Rifkin è docente alla Wharton School of Finance and Commerce e presidente della Foundation on Economic Trends di Washington.

[3] Carlo Focarelli, *La privacy. Proteggere i dati personali oggi*, Bologna, Il Mulino, 2015, p. 26-27.

© 2016 IAI ISSN 2280-6164 DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

Ma l'adozione di massa degli strumenti digitali e della connettività fra oggetti apre anche scenari molto più estesi, come il controllo e la selezione delle informazioni che vengono fornite agli utenti tramite gli attuali canali comunicativi. Delineando profili specifici dell'individuo grazie ai dati raccolti sulle sue abitudini o preferenze politiche, si potrebbero infatti "filtrare" le informazioni da fornirgli, influenzandone i comportamenti futuri. Le grandi imprese, interessate alla massimizzazione dei loro profitti, potrebbero decidere di acquistare dati personali e sensibili dai produttori di software (o di componenti presenti negli oggetti *smart*) senza informare l'utente, per delineare le tendenze del mercato e modificare di conseguenza la produzione. Questi sono solo alcuni dei rischi ai quali gli sviluppatori di dispositivi informatici ma anche e soprattutto gli esperti di diritto sono tenuti a trovare una risposta, e lo devono fare rapidamente, considerando la repentina crescita del settore in esame.

1.2 Ideare l'Internet delle cose

Progetto e realizzazione sono le due parole chiave quando si parla di Internet delle cose. Sinonimi per i più, assumono una valenza significativa per Alexandra Deschamps-Sonsino, imprenditrice leader nel campo dell'IoT, che ricorda l'importanza di questa distinzione considerando il gran numero di persone coinvolte in questo settore – artisti che collaborano con i designer per le installazioni e nel rendere l'oggetto "bello", ingegneri che lavorano alla realizzazione dei prodotti, sviluppatori dei software, hacker che immaginano prototipi[4]. A questo elenco di figure, che per semplificazione sono classificate con il termine "costruttore", vanno aggiunti tutti coloro che successivamente si occupano della raccolta, dell'elaborazione e dell'archiviazione dei dati – dalla pubblica amministrazione alle aziende private, passando per i gestori dei social network fino ai grandi motori di ricerca come Google che, cogliendo la portata innovativa dell'IoT, stanno investendo su un processo di standardizzazione per definire dispositivi di misurazione che permetteranno agli utenti di monitorare i loro consumi domestici attraverso le *smart grid*.

Appare evidente come il mondo dell'IoT sia un "patchwork" di soggetti, in cui Internet gioca il ruolo di filo conduttore e allo stesso tempo di campanello d'allarme, mostrando come la necessità di una regolamentazione riguardante il flusso continuo dei dati sia ormai impellente.

[4] Adrian McEwen e Hakim Cassimally, *L'Internet delle cose*, cit., p. 12.

ISSN 2280-6164

1.3 La tecnologia dell'Internet delle cose

Sensori, tag Rfid[5], attuatori, *smart code*[6] sono gli "arti" del sistema dell'IoT che nel momento in cui vengono applicati agli oggetti trasmettono e ricevono informazioni, utilizzando come piattaforma di scambio il web. É diventato talmente economico produrre microchip da inserire nei dispositivi che un registratore di cassa può eseguire Windows così come un frigorifero può lavorare con OS X di Apple, e se a ciò si aggiungono sensori che rilevano l'importo contenuto in cassa o i prodotti mancanti del freezer la "magia" dell'Internet delle cose si avvera.

Analizzando nel dettaglio l'architettura di rete dell'IoT, si può parlare di tre livelli[7]:

- l'interfaccia con il mondo fisico, composto da nodi di sensore (tag) che interagendo con l'ambiente forniscono un codice identificativo, acquisendo informazioni e trasmettendo con meccanismi di rete wireless le informazioni al secondo livello;
- mediazione, ovvero il secondo livello, di cui fanno parte i tag Rfid, che raccolgono le informazioni del primo livello e li trasmettono al terzo;
- centro di controllo, il terzo ed ultimo livello, con sistemi che acquisiscono le informazioni, le memorizzano e le rielaborano.

Un ulteriore elemento da tenere in considerazione a proposito della tecnologia dell'IoT è lo sviluppo delle piattaforme online. Il web 2.0 ha infatti sviluppato uno stile di programmazione che utilizza le Api (*Application Programming Interface*) per interagire con altri programmi e non solo altri utenti, sfruttando così appieno i servizi offerti.

1.4 La diffusione dell'Internet delle cose

Ad oggi, sono connessi ad internet circa 1,5 miliardi di pc e 1 miliardo di cellulari, e da qui a dieci anni si prevedono 100 miliardi di dispositivi connessi alla rete. Questa cifra, occorre però ricordare, viene stimata considerando la capacità attuale della tecnologia, e quindi appare chiaro che un'ulteriore improvvisa crescita nel settore tecnologico aumenterà ancor di più le cifre. Anche in Italia attualmente ci si attende una crescita, in particolare nei settori riguardanti: *smart car*, dotate di box

[5] Con tag Rfid (*Radio Frequency Identification*), viene indicata in telecomunicazioni ed elettronica la tecnologia utilizzata per l'identificazione e memorizzazione automatica di dati provenienti dall'ambiente esterno, attraverso particolari etichette elettroniche (tag), che utilizzano la radiofrequenza per tale identificazione e per comunicare a distanza con i dispositivi fissi o portatili. Tracciando l'oggetto, lo si può collegare all'acquirente mettendone a rischio la privacy.

[6] Gli *smart code*, come i codici QR, sono codici a barre bidimensionali, che vengono impiegati per memorizzare informazioni utili (per esempio relative all'oggetto sui cui sono posti) destinate ad essere lette tramite smartphone o altri strumenti tecnologici.

[7] Osservatorio Internet of Things, *Internet of Things: come migliorerà la nostra vita e le nostre aziende*, studio per Econocom, 2013; "Internet of things, il presente e il futuro delle tecnologie", in *Digital 4 Executive*, 31 agosto 2016, http://www.digital4.biz/executive/approfondimenti/internet-of-things-il-presente-e-il-futuro-delle-tecnologie_4367215861.htm.

ISSN 2280-6164

Gps/Gprs per la localizzazione del veicolo e la registrazione dei parametri a scopo assicurativo; *smart home*, con il 46 per cento dei proprietari di casa intenzionati ad acquistare prodotti per il risparmio energetico e la sicurezza; *smart city*, in quanto la maggior parte dei comuni italiani, negli ultimi tre anni, ha ideato almeno un progetto basato sulla tecnologia dell'IoT[8]. Ulteriore esempio di interesse nel settore è il fatto che l'Università Sapienza di Roma sia alla guida del progetto internazionale "Sunrise", che ha come scopo ultimo quello di trasformare gli oceani in autostrade digitali dove opereranno dispositivi connessi con comunicazioni acustiche ed ottiche per condurre operazioni come lo sminamento, la localizzazione di persone scomparse e la ricerca di giacimenti di idrocarburi. In questa prospettive l'*Internet of Things*, nella sua continua evoluzione, potrebbe diventare "l'*Internet of Underwater Things*"[9].

Quello italiano è solo un esempio della "forza centrifuga" di diffusione di questo fenomeno. Per raggiungere un buon grado di competitività, ovviamente, sono anche necessari investimenti da parte delle istituzioni, come nel caso della Commissione europea che nell'ottobre 2015 ha deciso di investire 16 miliardi di euro nella ricerca e nell'innovazione per i successivi due anni. Il piano rientra nell'ambito del programma Horizon 2020 e intende favorire lo sviluppo delle *smart cities*, il *digital single market* e l'IoT[10].

1.5 Verso l'Internet of Everything

Secondo studi condotti da Cisco[11] nel 2013, l'IoT starebbe per subire un'ulteriore evoluzione, passando dalla connessione tra dispositivi ad un tentativo di connessione di tutto ciò che esiste. Per questo si inizia a parlare di *Internet of Everything* (IoE)[12]. L'IoE andrebbe a connettere non solo i dispositivi ma anche le persone, i dati e i vari processi, utilizzando una rete intelligente in grado di ascoltare, apprendere e dare nuove informazioni, con attenzione ad una maggiore sicurezza rispetto quella attuale. Riguarderà ogni settore della vita quotidiana, dal lavoro all'attività fisica, passando per il commercio e il sistema bancario assicurativo. Avendo margine d'azione in tutti questi settori, secondo Cisco, anche le potenzialità economiche di tale attuazione dell'IoT saranno maggiori, apportando un notevole sviluppo negli

[8] Marco Minghetti, "Internet of things, l'anno della svolta", in *Nòva 100*, 14 aprile 2015, http://marcominghetti.nova100.ilsole24ore.com/?p=7608.

[9] Patrizia Licata, "Internet of things negli oceani: l'Italia capofila con un software ad hoc", in *Corriere delle Comunicazioni*, 28 luglio 2015, http://www.corrierecomunicazioni.it/tlc/35668_internet-of-things-negli-oceani-l-italia-capofila-con-un-software-ad-hoc.htm.

[10] Commissione europea, *La Commissione investe 16 miliardi di euro in finanziamenti a favore della ricerca e dell'innovazione nei prossimi due anni*, 13 ottobre 2015, http://europa.eu/rapid/press-release_IP-15-5831_it.htm.

[11] Cisco è una delle aziende leader nella fornitura di apparati di networking ed è stata fondata in California nel 1984 da un gruppo di ricercatori della Standford University.

[12] Cisco Consulting Services, *The Internet of Everything: A $19 Trillion Opportunity*, gennaio 2014, http://www.cisco.com/web/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf.

ISSN 2280-6164

investimenti pubblici, nell'utilizzo dei capitali finanziari e nella ricerca, favorendo un risparmio nelle spese pubbliche. L'IoT sembrerebbe avere già in sé tutti gli strumenti per favorire la nascita, non troppo lontana, dell'IoE. Ad ogni modo questo rapido sviluppo tecnologico evidenzia il lento iter legislativo per regolamentare un tale flusso di dati in continuo aumento. Si potrebbe parlare, a tal proposito, di un internet a due velocità: quello tecnologico e quello giuridico.

2. L'Internet delle cose e i dati

2.1 L'Internet delle cose genera big data: i concetti di "dato" e "metadato" e come si arriva ai megadati

Come un'automobile necessita di benzina per funzionare, così l'IoT necessita di dati per alimentarsi e migliorarsi. Due ambiti diversi ma connessi che combinati producono una sorta di "superpotere" nelle mani di soggetti pubblici e aziende. Soprattutto per queste ultime, l'informazione da sempre ha rappresentato una risorsa economica e saper analizzare i dati raccolti dagli oggetti *smart* appare essere una vera e propria sfida da cogliere senza esitazione alle porte dell'economia 2.0. Il *data mining* si afferma come uno dei settori più strategici per le aziende che operano nel contesto contemporaneo, le quali, autonomamente o grazie all'aiuto di esperti, possono incrociare dati avendo l'utente come unità di analisi per scoprire opportunità di investimenti economici enormi. Ma cosa sono i dati e come si arriva ai megadati (*big data*) è argomento tutt'ora dibattuto.

Un problema trasversale che interessa gli esperti di diritto e non solo, è quanto concerne la definizione di "dato" e di "dato personale". Infatti, oggigiorno, ci sono norme che si applicano per i "dati" e norme che si applicano per i "dati personali" e più specificatamente per i "dati sensibili". Altro problema che fa discutere è se rientrino nei "dati" anche i cosiddetti "metadati", ovvero quelle informazioni che associate ad una pagina web, o anche ad una parte di essa, riescono a descriverne il contenuto e il contesto di riferimento[13].

Seguendo le linee guida Ocse del 1980, rivedute nel 2013[14], sono da definirsi come "dati personali" tutte quelle informazioni relative ad un determinato individuo[15] e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, il suo stato di salute, ecc. A questa definizione, ripresa anche dalla Direttiva 95/46/CE del 1995[16], segue quella di "dato sensibile" riportata anche dal Codice in

[13] Carlo Focarelli, *La privacy*, cit., p. 28.

[14] Garante per la protezione dei dati personali, *Linee guida Privacy Ocse riviste*, 9 settembre 2013, http://www.garanteprivacy.it/garante/doc.jsp?ID=2629667.

[15] Ocse, *The OECD Privacy Framework*, settembre 2013, p. 52, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

[16] Articolo 2a della Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche

ISSN 2280-6164

materia di protezione dei dati personali italiano, ovvero quei dati che possono rivelare l'origine etnica e razziale di una persona, le sue convinzioni religiose, politiche, l'adesione a partiti politici, lo stato di salute e la natura sessuale[17].

Con l'evoluzione tecnologica, inoltre, altre tipologie di dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche e quelli che consentono la geolocalizzazione, ovvero quei dati che vengono prodotti quotidianamente dagli utenti con l'utilizzo di oggetti *smart*. A tal proposito, il gruppo di esperti Ocse ha suggerito che il termine "dati personali" venga inteso in chiave evolutiva, considerando anche quelle informazioni che, se connesse ad altri dati sull'individuo, possono produrre effetti su di esso, sottolineando l'importanza del modo in cui i dati vengono utilizzati[18]. Questa interpretazione della definizione di "dato personale" è significativa nel momento in cui si parla di "metadati", ovvero quei dati che descrivono in modo strutturato le proprietà dei dati presenti in una pagina web, descrivendone, per esempio, il contenuto e la locazione. Basti pensare ad una libreria digitale contenente diversi dati/oggetti: è proprio grazie ai metadati che è possibile scoprire chi ha creato il dato in analisi, chi lo possiede, quando è stato creato, ecc.

Indubbiamente, i metadati risultano essere una grande risorsa, ad esempio per le scienze sociali in quanto se opportunamente interrogati possono arricchire i risultati di una ricerca, ma allo stesso tempo costituiscono un problema per i promotori della privacy, che li considerano, se non opportunamente regolamentati, un'invasione della sfera personale dell'individuo. Inoltre, con il repentino sviluppo della tecnologia dell'IoT, e la conseguente velocità e quantità di dati raccolti dai sensori posti nei vari oggetti *smart*, si inizia a ritenere che le norme vigenti (riguardanti gli *small data*[19]) non siano più sufficienti in un mondo in cui qualunque informazione può trasformarsi in un dato, o meglio in *big data*, attraverso il processo della datizzazione[20]. In un parere del 2015 del Garante europeo della protezione dei dati è presente una calzante definizione di *big data*: "the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions"[21].

con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:31995L0046.

[17] Articolo 4, comma 1, lettera d del Codice in materia di protezione dei dati personali, Decreto legislativo n. 196 del 30 giugno 2003, http://garanteprivacy.it/garante/doc.jsp?ID=1311248.

[18] Ocse, *The OECD Privacy Framework*, cit., p. 50.

[19] Per small data si intendono quei dati in un formato altamente strutturato (per esempio la password di un sistema operativo) e in un volume ridotto facilmente gestibile (per esempio gli orari dei treni, i risultati di una partita, ecc.) e tutto ciò che può essere rapidamente disponibile nella vita quotidiana dell'individuo, fornendo una soluzione mirata a domande specifiche. Le caratteristiche di questi dati, quindi sono: volumi ridotti, rapidi tempi di risposta e decentralizzazione dei dati, con la creazione di banche dati autonome, da usare per scopi specifici.

[20] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. A Revolution That Will Transform How We Live, Work and Think*, London, John Murray, 2013, p. 78.

[21] European Data Protection Supervisor, *Meeting the Challenges of Big Data* (Opinion 7/2015), 19 novembre 2015, p. 7, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/

© 2016 IAI ISSN 2280-6164 DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

2.2 Gli attori in gioco e la proprietà dei dati

Quando si parla di "dati", come ricorda il Garante italiano per la privacy[22], si possono giuridicamente identificare quattro attori principali:

- l'interessato, ovvero la persona fisica cui si riferiscono i dati personali;
- il titolare, ossia la persona fisica, l'azienda, l'ente pubblico ecc. cui spettano le decisioni sugli scopi e sulle modalità del trattamento dei dati, e gli strumenti da utilizzare;
- il responsabile, che può essere una persona fisica, una società, un ente pubblico o un'associazione a cui il titolare affida compiti specifici per il trattamento e controllo dei dati;
- l'incaricato, ovvero colui che per conto del titolare elabora o utilizza, con determinate finalità, i dati, seguendo le direttive del titolare.

I problemi principali dovuti all'"emorragia" di dati prodotta dall'IoT sono due. Da un lato quello legato alla protezione dei dati che, se usati abusivamente, possono divenire oltre che una risorsa economica per le aziende anche un'arma contro l'utente stesso (si pensi agli attacchi hacker, ai furti d'identità online, ecc.). Dall'altro, quello di stabilire e definire con chiarezza i ruoli di coloro che vengono a contatto con i dati stessi.

2.3 La raccolta dei dati

Per dare un'idea di quanto valgono i nostri dati, la Federal Trade Commission ha pubblicato nel 2014 un rapporto che rivela le cifre di un'industria poco conosciuta: quella dei *data broker*, ovvero coloro che raccolgono informazioni personali sul consumatore attingendo da fonti più o meno pubbliche, rivendendo queste informazioni alle società commerciali[23]. Questo studio ha dimostrato che nel 2012 nove di queste aziende "di raccolta" dati hanno ricavato 426 milioni di dollari vendendo le informazioni raccolte, per tre scopi principali: marketing, riduzione dei rischi e ricerca di persone. I dati finalizzati al marketing, per ovvi motivi, sono i più redditizi, ma il lo studio ha evidenziato come anche i dati riguardanti lo stato di salute della persona (comprendenti anche la propensione a cercare online informazioni su malattie e farmaci) siano redditizi.

Il dibattito tradizionale sulla privacy è molto acceso quando si parla della monetizzazione dei dati, soprattutto quando è la privacy stessa che diviene risorsa economica e quando sono gli utenti stessi a cederla in cambio di servizi gratuiti.

Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf.

[22] Garante per la protezione dei dati personali, *Cosa intendiamo per dati personali?*, http://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali.

[23] Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability*, maggio 2014, https://www.ftc.gov/node/311771. Si veda anche l'infografica compilata dalla Kenan-Flagler Business School, *The Business of Data Brokers*, 19 febbraio 2015, https://onlinemba.unc.edu/blog/data-brokers-infographic.

ISSN 2280-6164

Certo è che, nei dibattiti sulla protezione dei dati personali, uno dei cardini su cui non si transige è il "requisito di avviso e consenso" alla raccolta dei dati, ossia il principio per cui l'utente deve essere avvisato che i suoi dati saranno raccolti. Ciò è ormai previsto dalle norme giuridiche esistenti, ma secondo alcuni giuristi perde di significato nel momento in cui si parla di *big data*[24]. Infatti, per loro natura, questa evoluzione dei dati non è significativa nel momento della raccolta, che può avvenire da più oggetti *smart* contemporaneamente attraverso i Rfid, bensì quando i *big data* vengono analizzati ed archiviati nella loro immensa varietà, velocità e volume.

Purtroppo attualmente la messa in sicurezza dei *big data* appare secondaria, soprattutto quando sull'altro piatto della bilancia si trova la "sicurezza nazionale". Molti governi, grazie alla raccolta indiscriminata di dati, sostengono infatti di riuscire a prevenire gli attacchi terroristici o a identificarne i responsabili, come è accaduto poco dopo l'attentato alla Maratona di Boston del 2013, quando i colpevoli sono stati identificati utilizzando le "tracce digitali" lasciate dagli attentatori sui social network (Facebook) che avevano precedentemente utilizzato. La sfida è di prevenire tempestivamente le minacce servendosi dei *big data* e di tecniche specifiche di analisi, che prendono il nome di *big data style analysis*, destinate a sostituire gli attuali sistemi Siem (*Security Incident and Event Management*)[25].

Parlando di raccolta dati, risulta quindi in ultima analisi esserci un problema di "bilanciamenti": tra sicurezza e rischio di ipercontrollo (statale e non), tra servizi offerti dalle aziende e cessione della nostra privacy, tra diritto e libero mercato.

2.4 Data mining: concetto superato dal business analytics

"*Data mining*" è il termine con il quale si identificano tutte le tecniche e le metodologie finalizzate all'estrazione di sapere e conoscenza partendo da una vasta mole di dati, e al successivo utilizzo di questo sapere per scopi scientifici, industriali ecc. Oggigiorno, gran parte delle aziende sono impegnate nell'attuazione del *data mining*, considerandolo un investimento a lungo termine. Ed è proprio l'immensa mole di dati che ormai le aziende si trovano a dover gestire che ha portato allo sviluppo del *business analytics*. Gli strumenti di quest'ultima metodologia di analisi possono aiutare le aziende ad identificare rapidamente le informazioni importanti (soprattutto per soddisfare l'utente, evitando così di chiedergli dati che poi non sarebbero utilizzati), permettendo così una maggiore trasparenza aziendale e una maggiore condivisione della conoscenza internamente alle aziende stesse[26]. Considerando questo nuovo elemento, non solo dal punto di vista economico-

[24] Carlo Focarelli, *La privacy*, cit., p. 70.

[25] Peter Wood, "How to Tackle Big Data from Security Point of View", in *Computer Weekly*, marzo 2013, http://bit.ly/1G0wgcI.

[26] Ecos, Dedagroup e Gartner Group, "Big data: riconoscerli, gestirli, analizzarli", in *Dedagroup Highlights*, n. 1 (febbraio 2012), http://www.ecos2k.it/allegati/BigData.pdf.

ISSN 2280-6164

aziendale ma più in generale, si parla di *big data analytics*, che si stima andrà a influenzare lo sviluppo dei software che si occupano di sicurezza, analisi, ecc. Ad oggi, ad ogni modo, è il *data mining* a gestire l'afflusso di dati, e questo sottolinea come le norme attuali e vigenti siano ancora troppo ancorate ai vecchi *small data*, e non sembrano ancora in procinto di occuparsi di questo ulteriore passo in avanti fatto dalla tecnologia.

Un esempio di gap tra tecnologia e diritto è rilevabile analizzando le linee guida Ocse del 1980 (rivedute nel 2013). Al paragrafo 8 si parla di "principio di qualità", secondo il quale i dati raccolti dovrebbero essere rilevanti rispetto ai fini per i quali vanno usati, e in base a questo, aggiornati[27]. Di conseguenza, anche per quanto attiene la "trasparenza" nell'utilizzo dei dati raccolti da parte delle grandi aziende, è rinvenibile una lacuna dal punto di vista giuridico, come viene ricordato nel parere del Garante europeo della protezione dei dati dello scorso novembre, nel quale si fa appello alle imprese affinché adottino *privacy policies* maggiormente tutelanti i diritti del singolo individuo[28]. È evidente che, senza considerare l'evoluzione verso il *big data analytics* ma fermandosi al *data mining*, il sistema giuridico attuale sembra essere molto lontano dall'attuale scenario tecnologico, nel quale avviene ancora una raccolta indiscriminata di dati, e questo gap sembra destinato ad aumentare già nei prossimi mesi.

2.5 Pro e contro dei big data

Subito dopo lo scandalo del Datagate del giugno 2013, causato dalle rivelazioni dell'ex tecnico informatico della Cia Edward Snowden, l'opinione pubblica internazionale ha iniziato a vedere con sospetto la raccolta dei dati, ed i cittadini hanno cominciato a rendersi maggiormente conto dei pericoli e delle insidie prodotte da ogni loro singola azione che, volente o nolente, produce tracce digitali: dal pagamento degli acquisti con la carta di credito al telepass, all'uso quotidiano di telefoni, tablet ecc.

La tracciabilità, d'altro canto, come sottolineato anche da un rapporto dell'Ocse del 2013[29], è incrementata dallo sviluppo tecnologico e se ben regolata da norme attinenti e puntuali può facilitare e accrescere la sicurezza sul luogo di lavoro, nei luoghi pubblici e anche nelle abitazioni, migliorare la funzionalità dei trasporti pubblici, della sanità, della pubblica amministrazione, e sostanzialmente dare nuovo stimolo e impulso all'innovazione[30].

[27] Ocse, *The OECD Privacy Framework*, cit., p. 56.

[28] Si veda il punto 1.2. European Data Protection Supervisor, *Meeting the Challenges of Big Data*, cit., p. 8-9.

[29] Ocse, "Exploring Data-Driven Innovation as a new Source of Growth. Mapping the Policy Issues Raised by 'Big Data'", in *OECD Digital Economy Papers*, n. 222 (18 giugno 2013), http://dx.doi.org/10.1787/5k47zw3fcp43-en.

[30] Carlo Focarelli, *La privacy*, cit., p. 49.

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016 ISSN 2280-6164

Da un punto di vista giuridico è possibile notare come lo sviluppo di delicati meccanismi di analisi basati su *big data* e algoritmi, creati da alcune università americane, fa sì che si possano prevedere in anticipo le sentenze emesse dalla Corte suprema degli Stati Uniti. Il primo modello, lanciato nel 2004 dal team guidato da Theodore W. Ruger, docente della University of Pennsylvania, è riuscito a prevedere con esattezza il 75 per cento delle sentenze dei giudici togati basandosi sulle precedenti sentenze emesse, ossia attingendo e scandagliando automaticamente le basi di dati che raccolgono sentenze, commenti e dispositivi vari, essendo questi predisposti alla consultazione e condivisione, e dunque utilizzando il meccanismo degli "open data"[31]. Strumenti del genere a favore della prevedibilità e trasparenza delle procedure giuridiche sarebbe utili anche in Paesi, come l'Italia, rinomati per la lentezza del sistema giudiziario e burocratico. Non a caso nell'aprile 2015 è stata lanciata una piattaforma, chiamata "JurisWiki", che rende gratuitamente consultabili online tutte le sentenze e le banche dati giuridiche italiane[32].

Restando nella sfera del diritto e focalizzandosi sull'esercizio dei diritti politici, le criticità non si esauriscono qui. Infatti internet e i dati cominciano ad essere utilizzati come un pozzo dal quale attingere informazioni sui potenziali elettori così da far pervenire loro messaggi di propaganda politica mirati, come è accaduto negli Stati Uniti durante le ultime elezioni. Alcuni analisti hanno provato come i messaggi politici "personalizzati", creati grazie alle tracce digitali rinvenibili in profili Facebook, e-mail, siti visualizzati, ecc. accuratamente studiati dallo staff di Barack Obama, hanno contribuito a far sì che il presidente in carica venisse riconfermato nonostante all'inizio della campagna elettorale i sondaggi lo dessero nettamente in svantaggio rispetto ai suoi avversari[33]. L'applicazione delle classiche tecniche di marketing utilizzate dalle grandi imprese multinazionali sta diventando comune nel mondo della politica, andando ad influenzare la scelta politica degli elettori.

Tutto ciò ha spinto l'Ue, in particolar modo la Commissione europea, ad intraprendere il lungo percorso di sostituzione della Direttiva 95/46/CE, col fine di creare un'unica normativa applicabile in tutto il territorio e possibilmente esportabile, così da arginare gli effetti di quegli ordinamenti statali, come quello statunitense, che tendono a vedere la protezione dei dati più in base a modelli commerciali, tralasciando l'aspetto dei diritti fondamentali. Nonostante gli sforzi comunitari il testo del Regolamento (UE) 2016/679[34], frutto degli ultimi tre anni di lavoro, sembra non aver centrato *in toto* l'obiettivo propostosi, ovvero quello di regolamentare il fenomeno della proliferazione dei *big data*.

[31] Per maggiori informazioni si veda il sito del progetto "Supreme Court Forecasting Project 2002", http://wusct.wustl.edu.

[32] Simone Aliprandi, "JurisWiki ha già vinto: la Cassazione sta oscurando tutte le sentenze. Sarà un caso?", in *CheFuturo!*, 21 maggio 2015, http://www.chefuturo.it/?p=44113.

[33] Stefano Lucchini e Raffaello Matarazzo, *La lezione di Obama. Come vincere le elezioni nell'era della politica 2.0*, Milano, Baldini e Castoldi, 2014, p. 75-96.

[34] Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32016R0679.

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016
ISSN 2280-6164

3. La privacy nell'era dell'Internet delle cose

3.1 Le origini del concetto di privacy e la sua evoluzione

Dato il quadro di riferimento fornito, occorre concentrarsi più approfonditamente sul diritto alla privacy e il diritto alla protezione dei dati. Solitamente, i due concetti tendono ad essere considerati un *unicum*, mentre in realtà vi sono solo alcune intersezioni tra loro. Quella che comunemente viene chiamata privacy è infatti il diritto alla riservatezza delle informazioni personali e della propria vita privata, mentre la privacy in sé è un concetto molto più ampio, che coinvolge indubbiamente la protezione dei dati ma non solo[35].

L'istituto della privacy nasce nell'ordinamento statunitense come il diritto a "essere lasciato solo" (*to be let alone*) nel 1890, grazie ad un saggio pubblicato precedentemente da due giovani avvocati americani. Con lo sviluppo tecnologico successivo alla Seconda guerra mondiale, la nozione di diritto alla privacy ha preso forma in molte legislazioni nazionali[36], lasciando spazio ad una nozione più ampia di privacy, incentrata soprattutto sull'individuo, di pari passo con il riconoscimento dei diritti dell'uomo. Ad esempio, in Europa tale principio è stato recepito dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, che prevede il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza (art. 8)[37]. Con il progresso tecnologico, questo fondamentale concetto è stato riportato ed attuato in vari trattati, come nella Carta dei diritti fondamentali dell'Ue[38], che all'art. 8 recita:

> 1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

3.2 Privacy e sicurezza

Da una parte vi è quindi il diritto fondamentale alla privacy, comprendente anche il diritto alla protezione dei dati in assenza del quale risulta difficile immaginare un mondo in cui sia davvero possibile avere libertà di movimento, espressione

[35] Carlo Focarelli, *La privacy*, cit., p. 36.

[36] Ian J. Lloyd, *Information Tecnology Law*, 6. ed., Oxford, Oxford University Press, 2011, p. 47-48.

[37] Convenzione europea per i diritti dell'uomo, 4 novembre 1950, http://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention.

[38] Carta dei diritti fondamentali dell'Unione europea, 26 ottobre 2012, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ITA.

ISSN 2280-6164

e associazione. Dall'altra vi è la spinta a scambiare le proprie libertà con una maggiore sicurezza, in un mondo pieno di insidie come quello contemporaneo, segnato dal terrorismo e da attacchi quotidiani fuori e dentro il *cyberspazio*. Dal continuo bisogno di difendersi da una serie di minacce nascono la maggior parte dei problemi legati ad un equo bilanciamento di questi due aspetti.

Spesso si tende infatti ad ignorare il rischio di politiche nazionali aggressive e della sorveglianza di massa, facilitata dallo sviluppo tecnologico e dall'interconnessione degli oggetti analogici, perché negli ultimi anni è cresciuta la percezione del doversi proteggere, *in primis* dal terrorismo. Dopo l'11 settembre 2001, per esempio, la National Security Agency (Nsa) americana ha ripetutamente ribadito che, al fine di evitare una situazione analoga a quella già verificatasi, occorreva un'attività di sorveglianza continua, applicando la tecnica del *data mining* ad ogni singolo oggetto utilizzato nella vita quotidiana[39]. Il cittadino americano ha accettato di rendere accessibile al proprio stato e/o ad agenzie private una mole consistente di dati più o meno personali, senza considerare se il *data mining* e la sorveglianza di massa potessero essere strumenti adeguati per contrastare i terroristi[40]. Tutto ciò è stato legalmente possibile sia perché gli stessi cittadini americani hanno dato il loro consenso affinché questo controllo potesse avvenire, sia perché le norme vigenti in America, coadiuvate da una diversa politica interna/estera rispetto a quella europea, sembrano propendere, di fatto, a privilegiare la sicurezza nazionale sopra ogni altro aspetto. Solo nel 2015, come conseguenza del Datagate e delle informazioni rivelate da Snowden, il Senato statunitense ha avvertito l'esigenza di approvare il cosiddetto "Freedom Act"[41], che secondo alcuni dovrebbe limitare la sorveglianza di massa portata avanti dalla Nsa, ma che secondo altri risulta essere un provvedimento troppo blando e non funzionale alla continua crescita tecnologica.

Ad ogni modo, a riprova della diversa impostazione europea rispetto a quella americana, occorre ricordare che, proprio per fronteggiare il continuo sviluppo dell'IoT, il Gruppo di lavoro ex Art 29, che riunisce i rappresentanti delle Autorità garanti europee per la privacy, ha espresso nel 2014 un parere ufficiale su privacy e sicurezza nell'IoT[42] contenente linee guida che produttori di IoT e piattaforme IoT, sviluppatori e parti terze devono applicare nel rispetto nella normativa vigente nell'Ue (norme sul trattamento dei dati contenute nelle direttive europee 95/46 e 2002/58). La strada intrapresa solo negli ultimi anni in Europa sembra ruotare attorno a principi diversi da quelli americani. É una strada che privilegia la tutela dei dati personali piuttosto che la sicurezza, che tende a lavorare a bozze di progetti

[39] Bruce Schneier, *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, New York/London, W.W. Norton, 2015, p. 135-137.

[40] Ibidem, p. 139-140.

[41] The USA Freedom Act, 2 giugno 2015, http://judiciary.house.gov/index.cfm/usa-freedom-act.

[42] Article 29 Working Party, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221), 16 settembre 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf.

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016 ISSN 2280-6164

di "Internet Bill of Rights" per tutelare l'individuo online piuttosto che ad attuare politiche sulla sorveglianza di massa. Benché indubbiamente la sicurezza è, e sarà sempre, un importante elemento da prendere in considerazione nel processo legislativo, nel vecchio continente la privacy, alla luce della crescita tecnologica, sta assumendo un valore diverso, nuovo e più definito.

3.3 Problematiche relative ai dispositivi IoT in commercio

Secondo uno studio sull'IoT condotto nel 2015 da Hewlett Packard, circa l'80 per cento dei dispostivi attualmente in commercio presenta carenze dal punto di vista della privacy[43]. Alcune delle problematiche evidenziate riguardano la mancata richiesta di password complesse, la mancanza di collegamenti crittografati per consumare meno energia e prolungare la durata delle batterie, e la vulnerabilità dei software. I maggiori rischi per la privacy, e quindi anche per la sicurezza dei dati dell'individuo, secondo questo studio sono:

- il mancato controllo da parte dell'utente sul flusso dei dati generati dal dispositivo IoT in uso in quel momento, a causa di un'attivazione improvvisa oppure perché gli oggetti, comunicando tra loro, si attivano autonomamente;
- il possibile rilevamento da parte dei dispositivi di dati personali riguardanti terze parti che non hanno prestato il loro consenso affinché ciò avvenisse;
- la generale mancata applicazione delle norme vigenti ai dati anonimi.

Il problema però consiste nel fatto che l'anonimato è alquanto difficile da mantenere in un sistema in cui l'identificazione del profilo dell'individuo è quasi automatica. Infatti la proliferazione non regolamentata di numerosi singoli dati anonimi porta di fatto alla delineazione del profilo del singolo. I dati anonimi, secondo lo studio, in realtà non possono essere considerati davvero tali, in quanto la somma di essi svela dettagli dell'utente cui si riferiscono.

Come già accennato nel precedente paragrafo, a tal proposito il Gruppo di lavoro ex Art 29 ha pubblicato un parere ufficiale su privacy e sicurezza nell'IoT[44] in cui si distingue fra tre diverse tipologie di dispositivi IoT: i *wearables* (indossabili), i *quantified self* ovvero quei dispositivi che permettono di avere dati relativi a attività/orario/abitudini quotidiane della persona, e i dispositivi *home automation*, tipo frigoriferi e lampade. Questa distinzione dovrebbe essere utilizzata dai produttori di IoT per sviluppare un approccio proattivo, e non reattivo, che riesca ad anticipare possibili invasioni della sfera della privacy della persona, già nella fase della progettazione del prodotto, ovvero quella che nella proposta del nuovo regolamento europeo viene definita *privacy by design*. Secondo il Gruppo di lavoro ex Art 29, le imprese che rispetteranno queste linee guida godranno di una maggiore fiducia da parte degli utenti, che si materializzerà in un aumento dei profitti.

[43] Hewlett Packard, *Internet of Things Research Study. 2015 Report*, ottobre 2015, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[44] Article 29 Working Party, *Statement on Statement of the WP29...*, cit.

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

In realtà, la questione appare più complessa, in quanto non è facile dire quanto l'utente sia consapevole delle eventuali insidie poste dalla proliferazione intrusiva cui andrà incontro, e soprattutto dell'approccio dominante dell'IoT che prevede, ad oggi, una raccolta continua ed indiscriminata di dati (anche senza uno scopo) benché si stia ormai uscendo dalla fase *start-up* e la raccolta indiscriminata condannata dai difensori della privacy sembri, secondo alcuni, perdere di significato.

3.4 Diritto alla protezione dei dati: Privacy Enhancing Technologies (Pet)

Pet è l'acronimo di *Privacy Enhancing Technologies*, ovvero tutte quelle tecnologie per il miglioramento della privacy, già da tempo immesse nel mercato, finalizzate alla protezione dei dati confidenziali senza interrompere la divulgazione di informazioni necessarie per gli scambi commerciali, le transazioni finanziarie, ecc. La Commissione europea ha più volte fatto riferimento a queste tecnologie, soprattutto in relazione all'applicazione della Direttiva europea 95/46, sostenendo che il loro utilizzo risulta essere un buon compromesso nell'attuazione degli strumenti giuridici esistenti e potrebbe aiutare a ridurre la raccolta e l'uso di dati personali[45]. Del resto, un riferimento a questo importante concetto è contenuto anche nell'art. 3 del Codice italiano in materia di protezione dei dati personali, rubricato "Principio di necessità nel trattamento dei dati", che recita:

> I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità"[46].

Molto conosciuti, parlando di Pet, sono dei plug-in creati per i browser che controllano e bloccano i siti internet che cercano di tracciare e capire l'utilizzo della rete stessa da parte degli utenti[47]. La necessità di mantenere l'anonimato online è stata ulteriormente accresciuta dall'avvento dei *big data* e quindi dall'evoluzione dei dispositivi della famiglia dell'IoT. Tale necessità stata rimessa alla sfera giuridica statuale più che a quella europea, benché ogni stato resti comunque vincolato al rispetto dei principi e delle garanzie relative alle libertà fondamentali sancite dalla Convenzione europea sui diritti dell'uomo e dalla Carta dei diritti fondamentali dell'Ue (nonostante non si parli esplicitamente di un "diritto all'anonimato"). A tal proposito, l'allora Commissario europeo per la Giustizia, la libertà e la sicurezza

[45] Commissione europea, *Promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET)* (COM/2007/228), 2 maggio 2007, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52007DC0228.

[46] Codice in materia di protezione dei dati personali, cit.

[47] Alcuni di questi plug-in sono: Lightbeam, Privacy Badger, Disconnect e FlashBlock.

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

Jacques Barrot durante un'interrogazione parlamentare del 3 aprile 2009 affermò che:

> The fundamental right to protection of personal data is enshrined in Article 8 of the EU Charter. Whilst there is no explicit right to electronic anonymity as such under Community law, the Data Protection Directive 95/46/CE, is to require that personal data must be processed fairly and lawfully, including the data minimisation principle. This principle may be furthered by the use of anonymous data wherever possible. Confidentiality of communications and related traffic data is protected by the directive on privacy and electronic communications 2002/58/EC. The data minimisation principle, leading to anonymity, may also be achieved by the use of Privacy Enhancing Technologies (PETs). However Member States may adopt measures to restrict the scope of these principles which are necessary to safeguard important public interests such as national security or law enforcement, including combating terrorism or fighting cybercrime[48].

3.5 Dal Rfid al Nfc

Appurato che con l'IoT vi è una perdita di controllo sui dati, dovuta anche ad un'asimmetria informativa a sfavore dell'utente, occorre capire la causa di ciò. Il primo sviluppo legato all'IoT che ha già trovato ampio riscontro nel mercato è da ricondursi ai Rfid (*Radio-Frequency Identification*). È proprio questa una delle maggiori preoccupazioni per gli esperti di privacy, ovvero che il Rfid delinei un profilo dell'utente molto dettagliato, dal conto in banca agli spostamenti che compie, passando per le sue preferenze e scelte di mercato. Anticipando la tecnologia, in un certo senso, il Garante per la Privacy in Italia aveva ribadito già nel 2005 l'importanza di ridurre la raccolta dei dati e lo stretto nesso con la finalità del loro trattamento, e quindi il principio di liceità e finalità dei dati, e l'importanza di fornire al consumatore etichette dettagliate sulle caratteristiche dei Rfid[49].

Riguardo all'accesa discussione sui Rfid iniziata negli ultimi anni, merita menzione l'approvazione da parte del Comitato europeo di normazione (Cen) di un nuovo standard che prevede che siano gli stessi produttori di Rfid, già nella fase di costruzione del sensore, a prevedere che impatto questo avrà nella protezione dei dati. Si tratta sostanzialmente di una forma di *privacy by design* dei Rfid, che secondo alcuni verrà disciplinata più approfonditamente dopo il 2018, anno in cui il nuovo Regolamento europeo in materia di protezione dei dati personali diventerà effettivamente applicabile in via diretta in tutti i Paesi Ue.

[48] European Parliament, *Answer given by Mr Barrot on behalf of the Commission*, 3 aprile 2009, http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-0897&language=EN.

[49] Garante per la protezione dei dati personali, *"Etichette intelligenti" (RFID): Il Garante individua le garanzie per il loro uso*, 9 marzo 2005, http://www.garanteprivacy.it/garante/doc.jsp?ID=1109493.

ISSN 2280-6164

Ma parlando di "strumenti per comunicare", il Regolamento, come formulato, sembra non occuparsi di un altro elemento, che nell'ultimo anno ha preso sempre più piede grazie alla diffusione degli smartphone, ovvero il Nfc (*Near Field Communication*) meglio conosciuto come "comunicazione in prossimità". Grazie a questa nuova tecnologia, che consente una comunicazione bidirezionale, l'IoT sta facendo un ulteriore passo avanti, cambiando ancora di più il modo di interagire con il mondo circostante. Basti pensare che lo smatphone dotato di Nfc potrebbe autonomamente passare in "modalità silenziosa" al nostro ingresso sul posto di lavoro solo attraverso la lettura del tag Nfc presente sulla nostra scrivania. Da un punto di vista tecnologico tutto ciò risulta essere indubbiamente un grande passo avanti, ma rappresenta anche un problema per i giuristi che sono sempre più preoccupati della sorte dei dati.

Un documento che può essere considerato una buona "piattaforma di riflessione" è il sopracitato parere n. 8 del 16 settembre 2014 del Gruppo di lavoro ex Art 29[50], che quantomeno individua gli sviluppi della tecnologia dell'IoT (riconoscendone l'invasività) e la necessità di rendere anonime alcune informazioni, pur considerando quelle situazioni in cui la re-identificazione dei dati sarà necessaria. Da questa consapevolezza e conoscenza della materia in questione, ci si aspettano proposte di norme più all'avanguardia e soprattutto più puntuali nel risolvere il problema del trasferimento e della conseguente protezione dei dati. Servono insomma norme che non tralascino gli importanti sviluppi tecnologici degli ultimi mesi, a maggior ragione considerando che il nuovo Regolamento europeo, pubblicato nel maggio 2016 sulla Gazzetta ufficiale dell'Unione europea[51], risulta essere già "vecchio" alla luce dello sviluppo dei sensori Nfc e dunque della previsione di crescita del fenomeno dei *big data*.

3.6 Crittazione

Nonostante i cultori della privacy parlino da tempo della sua "morte"[52], soprattutto per mano della tecnologia Rfid e Nfc, occorre ricordare – parlando di Pet – uno dei più vecchi metodi di difesa dei dati personali a cui gli utenti, in attesa di un miglioramento e piena attuazione della legislazione vigente, possono far ricorso, ovvero la "crittazione". Tenuta inizialmente segreta negli Stati Uniti durante gli anni '80, la crittazione risulta essere un metodo molto efficace, trasparente e semplice da usare per proteggere i propri dati.

Sono attualmente disponibili programmi di crittazione per chat come Off-the-Record o Cryptocat, o per proteggere la voce su Internet (per es. quando si usano programmi come Skype) come Silent Circle, TorFone, RedPhone o Blackphone,

[50] Article 29 Working Party, *Statement on Statement of the WP29*..., cit.

[51] Regolamento (UE) 2016/679 del 27 aprile 2016, cit.

[52] Evgeny Morozov, "The Dangers of Sharing", in *The New York Times*, 12 gennaio 2012, http://nyti.ms/1lhC82X.

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016
ISSN 2280-6164

e per quanto riguarda la posta elettronica anche Google sta iniziando ad offrire programmi di crittazione per i propri utenti. Occorre però ricordare che Google cripta la connessione a Gmail in automatico, e incripta le e-mail mentre si trovano nel suo server e restano lì: in tal modo Google processa le e-mail e ha una copia delle chiavi per accedere ai file criptati. Va notato che la maggior parte dei metadati non possono essere criptati. Infatti, criptando il contenuto della nostra e-mail non possiamo criptare il destinatario e il mittente, dunque queste informazioni rimangono possibili obiettivi di occhi indiscreti. Infine, occorre ricordare il protocollo Tls (*Transport Layer Security*) che, come il suo predecessore Ssl (*Secure Sockets Layer*), incripta parte della nostra navigazione web ovvero ciò che accade automaticamente quando navigando in internet appare la scritta "https" al posto di "http". Questo meccanismo, però, non è predisposto per tutti i siti web, e per questo motivo sono state creati alcuni plug-in per i browser Chrome e Firefox, come HTTPS Everywhere, che aumentano la sicurezza della navigazione e risultano essere strumenti efficaci[53].

La crittazione, inoltre, non risolve i problemi di carattere giuridico legati alla privacy (ad esempio quello del consenso alla diffusione dei dati personali). In primo luogo, infatti, l'utilizzo dei dati crittati non può essere unilaterale, ossia chi riceve un messaggio crittato da un altro utente deve anche accettarlo in questa forma. Dopodiché i dati, una volta de-crittati, sono però destinati a sfuggire nuovamente al controllo di chi li ha inviati, e ciò comporta dei rischi per la privacy del mittente. Per il momento una risposta a questi problemi è stata data, ancora una volta, dalla tecnologia con lo sviluppo delle "funzioni hash", ovvero la trasformazione di un testo in un codice alfanumerico di varia lunghezza. Ma come è già stato detto, la tecnologia è in continuo divenire, e sicuramente anche quest'ultima funzione sarà destinata a divenire obsoleta a breve, mentre la necessità di una regolamentazione della protezione dei dati è destinata a rimanere attuale per molto tempo.

3.7 Programmi pro-privacy

La tecnologia, negli ultimi anni, ha comunque cercato di sanare il problema della privacy online e della protezione dei dati, anche attraverso i cosiddetti "programmi pro-privacy" – rigorosamente (quanto meno in Italia) in regola con il Codice della privacy e il diritto di autore dei programmi installati su pc[54]. Uno dei più famosi esempi di programmi pro-privacy attualmente disponibili è Tor (*The Onion Router*)[55], un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo di *onion routing*. Tor protegge gli utenti dall'analisi del traffico attraverso una rete di router, gestiti da volontari, che permettono il traffico anonimo in uscita e la realizzazione di servizi anonimi nascosti. Come Tor, ci sono anche altri *proxies* usati come strumenti di protezione e anonimato e possono

[53] Bruce Schneier, *Data and Goliath*, cit., p. 215-217.
[54] Codice in materia di protezione dei dati personali, cit.
[55] Bruce Schneier, *Data and Goliath*, cit., p. 216.

ISSN 2280-6164

essere utilizzati per evadere la sorveglianza e la censura. Il loro funzionamento è relativamente semplice: i dati che appartengono ad una qualsiasi comunicazione non transitano direttamente dal client al server, ma passano attraverso i server Tor che agiscono da router costruendo un circuito virtuale crittografato a strati (*onion router*). Ci sono inoltre molte accortezze sia tecnologiche sia riguardanti le abitudini quotidiane che possono essere adottate, come spegnere il servizio di localizzazione dello smartphone quando non è necessario usarlo, evitare di pubblicare dettagli su siti pubblici, imparare a dire "no" quando viene chiesto di lasciare il nostro numero telefonico nei negozi per avere informazioni sui prodotti, eccetera[56].

3.8 Privacy by design

La *privacy by design* (PbD) è un concetto sviluppatosi negli anni '90, che riguarda il principio di incorporazione della privacy a partire dall'ideazione di un qualsiasi progetto (strutturale o concettuale) col fine di preservare la riservatezza dei dati personali circolanti nelle reti di larga scala[57]. La PbD è strutturata in uno schema che prevede tre grandi linee di azione (tecnologia dell'informazione, pratiche commerciali responsabili e progettazione delle strutture) e sette principi operativi, ossia:

1. l'essere proattivo e non reattivo, prevenire e non correggere: ovvero anticipare e prevenire gli eventi invasivi della privacy prima che essi accadano;
2. privacy come impostazione di default, ovvero cercare di realizzare il massimo livello di privacy assicurando che i dati personali siano automaticamente protetti in qualunque sistema *information technology* o di pratica commerciale;
3. privacy incorporata nella progettazione, ovvero la privacy è incorporata nel sistema *ab origine* senza diminuirne le funzionalità;
4. massima funzionalità in un calcolo non a somma zero: la privacy non viene vista come valore opposto alla sicurezza, ma si cerca di realizzarli entrambi;
5. sicurezza fino alla fine: ovvero la piena protezione del ciclo vitale dei dati, dal primo dato acquisito fino all'ultimo che verrà distrutto;
6. visibilità e trasparenza, ovvero mantenere la trasparenza sul processo sia per gli utenti che per i fornitori;
7. rispetto per la privacy dell'utente, che diviene centrale per i progettisti e per gli operatori[58].

La PbD ha molti risvolti pratici attuali, considerando che lo sviluppo industriale coinvolge sempre l'utente finale, il consumatore. Basti pensare agli investimenti che le aziende fanno sulla privacy, considerata come un valore aggiunto e non

[56] Ibidem, p. 158.

[57] Nicola Fabiano, "Privacy by design: l'evoluzione della privacy", in *Secsolution*, 6 aprile 2011, http://www.secsolution.com/notizia.asp?id=6597.

[58] Ann Cavoukian, *Privacy by Design. I 7 principi fondazionali*, febbraio 2011. Allegato a Nicola Fabiano, *Il futuro della privacy: dalla Privacy by Design ad uno standard*, presentazione al convegno "La privacy che verrà", Firenze, 5 aprile 2014, http://e-privacy.winstonsmith.org/e-privacy-XV.html#i14.

ISSN 2280-6164

un costo improduttivo[59]. In ambito europeo, come detto in precedenza, si è già proceduto alla revisione della normativa sulla privacy (Direttiva 95/46/CE)[60] per armonizzare tra loro gli strumenti normativi degli Stati membri in relazione a vari aspetti, tra cui appunto la PbD. L'importanza di questo concetto viene anche ribadita nel parere del Garante europeo della protezione dei dati, secondo cui:

> Technology and privacy-friendly engineering can play a key role in ensuring that transparency and user control, as outlined above, will become a reality. Laws, regulations, contractual terms, internal procedures, and privacy policies, while important, will not suffice on their own. Individuals need to be offered new, innovative ways to be informed about what happens to their data, and to exercise control over their data[61].

Il quadro normativo europeo e quello internazionale sono in continua evoluzione, così come il concetto di privacy e le tecnologie a supporto della stessa. L'attuale normativa europea, comunque, dispone già l'utilizzo di misure tecniche che richiamano le Pet, che restano infatti una base solida su cui sviluppare il più evoluto concetto di PbD. Uno sviluppo che tutti i più irriducibili sostenitori della privacy sperano vedersi concretizzare a seguito della corretta applicazione (e di una lettura in chiave "evolutiva") di quanto previsto dal nuovo Regolamento europeo, che sarà definitivamente applicabile in via diretta in tutti i Paesi Ue a partire dal 25 maggio 2018, data entro la quale dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento.

Conclusioni

In questo saggio si è cercato di illustrare come lo sviluppo della tecnologia wireless e satellitare abbia permesso la nascita del fenomeno dell'IoT e di come quest'ultimo sarà in grado di cambiare profondamente la vita quotidiana dell'uomo. Il "carburante" del fenomeno, come si è visto, sono i dati che vengono raccolti continuamente e indiscriminatamente dagli oggetti *smart*, ossia oggetti "comuni" dotati di sensori connessi alla rete e con altri oggetti *smart*. Nonostante gli evidenti vantaggi apportati da questa tecnologia, sono stati sottolineati i possibili rischi derivanti dalla diffusione di massa di questi oggetti "intelligenti" (furti d'identità, vendita dei dati per fini economici, ecc.). Rischi che fondamentalmente provengono proprio dai dati raccolti, che di per sé risultano essere pressoché innocui ma che tramite processi di analisi come la datizzazione (*data mining*) e il *big data analytics*, diventano una minaccia per la sicurezza e la privacy dell'individuo. La privacy – di cui si parla sempre più dopo il Datagate del 2013 – e il relativo diritto alla privacy appaiono argomenti strettamente connessi alla raccolta e alla rielaborazione dei dati. L'importanza di questi temi, inoltre, è stata percepita non solo dai giuristi, ma

[59] Bruce Schneier, *Data and Goliath*, cit., cit., p. 206.
[60] Direttiva 95/46/CE del 24 ottobre 1995, cit.
[61] European Data Protection Supervisor, *Meeting the Challenges of Big Data*, cit., p. 14.

ISSN 2280-6164

anche dagli stessi produttori di software e dagli informatici, come dimostra la vasta gamma di tecnologie per il miglioramento della privacy (Pet) e la cosiddetta *privacy by design* (PbD). Dal canto loro, i giuristi chiedono norme di carattere vincolante che identifichino "diritti e doveri" dei diversi attori coinvolti nel processo produttivo degli oggetti *smart*. Il diritto, infatti, è chiamato già da ora a dare una risposta innovativa e, paradossalmente, più originale del fenomeno stesso che va a regolare, per poter porre le corrette basi giuridiche (siano esse, inizialmente, di carattere europeo e poi, eventualmente e gradualmente, mondiale) che permetteranno un approccio "*smart*" al fenomeno in analisi. Ricordando, sempre, la regola generale secondo cui un *corpus* di regole vale nella misura in cui effettivamente è applicato da chi lo deve applicare.

Aggiornato 6 ottobre 2016

ISSN 2280-6164

Riferimenti

Simone Aliprandi, "JurisWiki ha già vinto: la Cassazione sta oscurando tutte le sentenze. Sarà un caso?", in *CheFuturo!*, 21 maggio 2015, http://www.chefuturo.it/?p=44113

Article 29 Working Party, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (WP 221), 16 settembre 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Ann Cavoukian, *Privacy by Design. I 7 principi fondazionali*, febbraio 2011. Allegato a Nicola Fabiano, *Il futuro della privacy: dalla Privacy by Design ad uno standard*, presentazione al convegno "La privacy che verrà", Firenze, 5 aprile 2014, http://e-privacy.winstonsmith.org/e-privacy-XV.html#i14

Cisco Consulting Services, *The Internet of Everything: A $19 Trillion Opportunity*, gennaio 2014, http://www.cisco.com/web/services/portfolio/consulting-services/documents/consulting-services-capturing-ioe-value-aag.pdf

Commissione europea, *Promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata* (PET) (COM/2007/228), 2 maggio 2007, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:52007DC0228

Ecos, Dedagroup e Gartner Group, "Big data: riconoscerli, gestirli, analizzarli", in *Dedagroup Highlights*, n. 1 (febbraio 2012), http://www.ecos2k.it/allegati/BigData.pdf

European Data Protection Supervisor, *Meeting the Challenges of Big Data* (Opinion 7/2015), 19 novembre 2015, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf

European Parliament, *Answer given by Mr Barrot on behalf of the Commission*, 3 aprile 2009, http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2009-0897&language=EN

Nicola Fabiano, "Privacy by design: l'evoluzione della privacy", in *Secsolution*, 6 aprile 2011, http://www.secsolution.com/notizia.asp?id=6597

Federal Trade Commission, *Data Brokers. A Call for Transparency and Accountability*, maggio 2014, https://www.ftc.gov/node/311771

Carlo Focarelli, *La privacy. Proteggere i dati personali oggi*, Bologna, Il Mulino, 2015

ISSN 2280-6164

Hewlett Packard, *Internet of Things Research Study. 2015 Report*, ottobre 2015, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

Italia, *Codice in materia di protezione dei dati personali*, Decreto legislativo n. 196 del 30 giugno 2003, http://garanteprivacy.it/garante/doc.jsp?ID=1311248

Kenan-Flagler Business School, *The Business of Data Brokers*, 19 febbraio 2015, https://onlinemba.unc.edu/blog/data-brokers-infographic

Patrizia Licata, "Internet of things negli oceani: l'Italia capofila con un software ad hoc", in *Corriere delle Comunicazioni*, 28 luglio 2015, http://www.corrierecomunicazioni.it/tlc/35668_internet-of-things-negli-oceani-l-italia-capofila-con-un-software-ad-hoc.htm

Ian J. Lloyd, *Information Tecnology Law*, 6. ed., Oxford, Oxford University Press, 2011

Stefano Lucchini e Raffaello Matarazzo, *La lezione di Obama. Come vincere le elezioni nell'era della politica 2.0*, Milano, Baldini e Castoldi, 2014

Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data. A Revolution That Will Transform How We Live, Work and Think*, London, John Murray, 2013

Adrian McEwen e Hakim Cassimally, *L'Internet delle cose*, Milano, Apogeo, 2014

Marco Minghetti, "Internet of things, l'anno della svolta", in *Nòva 100*, 14 aprile 2015, http://marcominghetti.nova100.ilsole24ore.com/?p=7608

Evgeny Morozov, "The Dangers of Sharing", in *The New York Times*, 12 gennaio 2012, http://nyti.ms/1lhC82X

Ocse, "Exploring Data-Driven Innovation as a new Source of Growth. Mapping the Policy Issues Raised by 'Big Data'", in *OECD Digital Economy Papers*, n. 222 (18 giugno 2013), http://dx.doi.org/10.1787/5k47zw3fcp43-en

Ocse, *The OECD Privacy Framework*, settembre 2013, http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

Osservatorio Internet of Things, *Internet of Things: come migliorerà la nostra vita e le nostre aziende*, Econocom, 2013

Bruce Schneier, *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, New York/London, W.W. Norton, 2015

Unione europea, *Carta dei diritti fondamentali dell'Unione europea*, 26 ottobre 2012, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ITA

ISSN 2280-6164

Unione europea, *Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:31995L0046

Unione europea, *Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, http://eur-lex.europa.eu/legal-content/it/TXT/?uri=celex:32016R0679

Usa, *Freedom Act*, 2 giugno 2015, http://judiciary.house.gov/index.cfm/usa-freedom-act

Peter Wood, "How to Tackle Big Data from Security Point of View", in *Computer Weekly*, marzo 2013, http://bit.ly/1G0wgcI

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 16 | 12 - OTTOBRE 2016

Istituto Affari Internazionali (IAI)

L'Istituto Affari Internazionali (IAI), fondato nel 1965 su iniziativa di Altiero Spinelli, svolge studi nel campo della politica estera, dell'economia e della sicurezza internazionali. Ente senza scopo di lucro, lo IAI mira a promuovere la conoscenza dei problemi attraverso ricerche, conferenze e pubblicazioni. A questo scopo collabora con istituti, università, fondazioni di altri paesi, partecipando a diverse reti internazionali. I principali settori di ricerca sono le istituzioni e le politiche dell'Unione europea, la politica estera taliana, le tendenze dell'economia globale e i processi di internazionalizzazione dell'Italia, il Mediterraneo e il Medio Oriente, l'economia e la politica della difesa, i rapporti transatlantici. Lo IAI pubblica una rivista trimestrale in lingua inglese (The International Spectator), una online in italiano (AffarInternazionali), due collane monografiche (Quaderni IAI e IAI Research Papers) e altre collane di paper legati alla ricerca dell'istituto.

Via Angelo Brunetti, 9 - I-00186 Roma
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Ultimi DOCUMENTI IAI

16 | 12 Sabrina Palanza, *Internet of things, big data e privacy: la triade del futuro*

16 | 11 Andrea Dessì, *Re-Ordering the Middle East? Peoples, Borders and States in Flux*

16 | 10 Roberto Aliboni, *La politica libica dell'Italia*

16 | 09 Ettore Greco, *L'eredità del passato, le sfide del futuro. L'Istituto Affari Internazionali e il "metodo" Spinelli*

16 | 08E Alessandro Marrone and Ester Sabatino, *2016 NATO Summit: What Agenda for Italy*

16 | 08 Alessandro Marrone e Ester Sabatino, *Vertice Nato 2016: quale agenda per l'Italia*

16 | 07 Beatrice Valentina Ortalizio, *Last Call for the Denuclearisation of the Korean Peninsula. How to Tackle North Korea's Nuclear Threat*

16 | 06 Bernardo Venturi, *Somali Perspectives: Security, Elections, and the Federalisation Process*

16 | 05 Bernardo Venturi and Miryam Magro, *The EU and the Global Development Framework. A Strategic Approach to the 2030 Agenda*

16 | 04 Fabrizio Saccomanni, *L'Italia e la riforma della governance economica europea*