RIVISTA DI SCIENZE DELL'EDUCAZIONE

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM
ANNO LVI • MAGGIO/AGOSTO 2018

DOSSIER
GIOVANI DONNE:
ASPIRAZIONI RISORSE
FRAGILITÀ'

2018/2

RSE

POSTE ITALIANE SPA - SPED. IN ABB. POSTALE D.L. 353/2003 (CONV. IN L. 27/02/2004 N. 46) ART. 1, COMMA 1 E 3, C/RM/04/2014

RIVISTA DI SCIENZE DELL'EDUCAZIONE

PUBBLICAZIONE QUADRIMESTRALE
EDITA DALLA PONTIFICIA
FACOLTÀ DI SCIENZE DELL'EDUCAZIONE
"AUXILIUM" DI ROMA

DIREZIONE
Via Cremolino 141
00166 Roma

Tel. 06.6157201
Fax 06.615720248

E-mail
rivista@pfse-auxilium.org
coordinatore.rse@pfse-auxilium.org

Sito internet
http://rivista.pfse-auxilium.org/

Informativa GDPR 2016/679
I dati personali non saranno oggetto di comunicazioni o diffusione a terzi. Per essi Lei potrà richiedere, in qualsiasi momento, accesso, modifiche, aggiornamenti, integrazioni o cancellazione, rivolgendosi al responsabile dei dati presso l'amministrazione della rivista.

ASSOCIATA
ALLA UNIONE STAMPA
PERIODICA
ITALIANA

Aut. Tribunale di Roma
31.01.1979 n. 17526

Progetto grafico impaginazione
e stampa
EMMECIPI SRL

ISSN 0393-3849

RIVISTA DI SCIENZE DELL'EDUCAZIONE

ANNO LVI NUMERO 2 • MAGGIO/AGOSTO 2018

Poste Italiane Spa
Sped. in abb. postale d.l. 353/2003
(conv. in L. 27/02/2004 n. 46) art. 1, comma 2 e 3, C/RM/04/2014

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM

SOMMARIO

DOSSIER

GIOVANI DONNE: ASPIRAZIONI, RISORSE, FRAGILITÀ

Young women: aspirations, resources, fragility

SISTEMA PREVENTIVO OGGI

ALTRI STUDI

ORIENTAMENTI BIBLIOGRAFICI

RIVISTA DI SCIENZE DELL'EDUCAZIONE

PONTIFICIA FACOLTÀ DI SCIENZE DELL'EDUCAZIONE AUXILIUM

ALTRI STUDI

RSE

PRIVACY E COMPORTAMENTI ECONOMICI

PRIVACY AND ECONOMIC BEHAVIOR

ALESSANDRA SMERILLI[1]

Introduzione

La *privacy* sta assumendo sempre più rilievo nei nostri giorni. Più aumentano le connessioni e le condivisioni in Rete, più ci si domanda dove vanno a finire le tracce che lasciamo *online*. E attorno ai nostri dati sta crescendo un mercato che è diventato il più grande al mondo. Le nostre informazioni hanno un grande valore economico. Quanto valgono? Come vengono utilizzate? Chi se ne avvantaggia? Quanto siamo consapevoli del "valore" delle nostre informazioni?

In questo articolo e in quelli che seguono, quali contributi della Tavola rotonda *Il continente nascosto: dati e persona nel cyberspazio interconnesso*, che ha aperto presso la Facoltà di Scienze dell'Educazione "Auxilium" di Roma il Corso interdisciplinare 2017-2018 dal titolo *Al principio la Rete. Vivere ed educare in una società connessa*, cercheremo di considerare l'aspetto della *privacy* e della diffusione delle informazioni in Rete da vari punti vista: sociale, psicologico, economico.[2] Gli Autori lavorano nel campo della sicurezza informatica e, proprio per questo, forniscono una panoramica ragionata, e a volte provocatoria, dei rischi che si corrono in Rete.

Da tutti i contributi emerge come sia la persona a fare la differenza e che, dal mondo della Rete non bisogna proteggersi, ma occorre saperlo abitare consapevolmente.

Ci sembra interessante, dunque, iniziare questa rassegna con un contributo introduttivo che si concentra in particolare sugli aspetti socio-economici.

1. La privacy

La *privacy* è un concetto difficile da spiegare. Le prime definizioni risalgono al 1890: essa è stata descritta come protezione dello spazio personale di un individuo e del suo diritto a essere lasciato solo[3], oppure come controllo e salvaguardia delle informazioni personali.[4] Essa è legata alla dignità, autonomia e libertà umana.[5]

Si potrebbe pensare che la *privacy* sia l'opposto della condivisione (*sha-*

ring); in realtà essa rappresenta il controllo sulla condivisione.
Come individui e consumatori ci muoviamo costantemente tra i confini del privato, condiviso o pubblico, e le decisioni che prendiamo circa questi confini determinano costi e benefici, tangibili e intangibili. L'economia della *privacy* è quel ramo della scienza economica che studia i *trade-offs* associati al bilanciamento della sfera pubblica e privata, tra soggetti, organizzazioni e governi.
L'analisi economica dei dati e della *privacy* cerca di studiare i costi e i benefici associati con le informazioni (soprattutto quelle personali), per i soggetti che usano i dati, per i possessori di dati, per la società nel suo complesso.
I progressi velocissimi in questo campo mostrano tutto il loro potenziale e la capacità di aumentare sia i benefici sia i danni per l'economia e per le persone.
L'elaborazione dei dati personali può aiutare ad accrescere il *welfare*, abbassare i costi di ricerca, ridurre le inefficienze economiche, ma nello stesso tempo può diventare causa di perdite, di disuguaglianze economiche, di sbilanciamento di poteri tra chi controlla i dati e chi è controllato.
Viene spontaneo domandarsi: perché la *privacy* è una questione economica? Oggi relativamente pochi possessori di dati (e di tracce che si lasciano *online*) sono nella posizione di controllare e collegare comportamenti di miliardi di persone. L'enorme ammontare di dati che vengono quotidianamente raccolti hanno un grande valore economico. La scienza economica cerca allora di studiare i costi e i benefici, per persone e organizzazioni, derivanti dalla condivisione dei dati e dal controllo sulla condivisione.

2. L'economia della privacy

Quando si parla di *privacy* e di economia della *privacy* bisogna chiedersi cosa è il mercato della *privacy* o, meglio, quali sono i mercati. Infatti si possono distinguere tre differenti mercati.
Il primo è rappresentato da transazioni che hanno una rilevanza, dal punto di vista della *privacy*, nel mercato dei beni ordinari: mentre si comprano beni o servizi, si rivelano informazioni personali. È il caso, per esempio, delle carte di fedeltà dei supermercati, per i viaggi, ecc. Si acquistano beni e servizi e tramite le carte le transazioni vengono registrate. La nostra storia di acquisti, insieme a quella di tutti gli altri possessori di carta, è uno strumento utile per le aziende, così come le transazioni effettuate attraverso una carta di credito.
C'è poi il mercato dei dati personali: un esempio è dato da *infomediari* che commerciano dati tra di loro, oppure l'offerta di servizi gratuiti in cambio di dati (es. *social networks*): qui anche se il prezzo è zero, il consumatore sta effettivamente comprando un servizio in cambio di dati. Un'iscrizione a *Facebook*, o *Instagram*, è un contratto in cui il *social network* concede la possibilità dell'utilizzo e dello scambio di informazioni, in cambio

RIASSUNTO

L'articolo offre la chiave di lettura e di interpretazione degli articoli che, nella sezione "Altri studi", riportano gli interventi tenuti durante la Tavola rotonda del 21 ottobre 2017 alla Facoltà "Auxilium", con la quale si è aperto il Corso interdisciplinare 2017-2018 sul tema: *Al principio, la Rete. Vivere ed educare in una società connessa*.

L'Autrice approfondisce il tema dalla prospettiva socio-economica, in particolare riferendosi all'economia della *privacy,* quel ramo della scienza economica che studia i *trade-offs* associati al bilanciamento della sfera pubblica e privata, tra soggetti, organizzazioni e governi.

Parole chiave

Economia della *privacy*, paradosso della *privacy*, asimmetria informativa, razionalità limitata.

SUMMARY

The article offers the key to reading and interpreting some articles in the section "Other Articles" which are talks given during the Round Table of October 21, 2017 at the "Auxilium" Faculty. It was part of the opening of the Interdisciplinary Course for 2017-2018, on the theme: *In the beginning, the Network. Living and educating in a connected society*.

The Author presents an in-depth

della cessione dei propri dati personali e della tracciatura delle proprie attività.

Infine esiste il vero e proprio mercato della *privacy*: i consumatori acquistano prodotti e servizi per maneggiare e proteggere i loro dati personali, come strumenti per proteggere le comunicazioni.

Vista nel suo insieme, l'attività di condivisione dei dati, e il mercato che ne deriva, a volte migliora il *welfare*, inteso come benessere di una collettività, a volte lo peggiora.

Da una parte esistono benefici attesi che possono emergere dalla messa a disposizione dei dati, sia per i possessori dei dati, sia per i soggetti, così come esistono costi opportunità quando i dati non sono condivisi. D'altra parte, possono emergere benefici anche dal proteggere i dati ed esistono costi quando viene violata la *privacy*, soprattutto quando è una violazione in ambito privato che ha risvolti nella sfera pubblica e lavorativa dei soggetti. Ma proteggere i dati ha anch'esso un costo.

I benefici della condivisione possono essere, per esempio:

- la conoscenza delle preferenze dei consumatori che permette di realizzare migliori prodotti e di diminuire i costi di pubblicità;
- il miglioramento dei servizi delle imprese basato sull'osservazione dei comportamenti osservati;
- i progressi che possono derivare in

study on the theme from a socio-economic perspective with particular reference to the economy of *privacy,* a branch of the economic sciences that studies the *trade-offs* associated with balancing the public and private spheres, between subjects, organizations and governments.
Key Words
Economy of *privacy*, paradox of *privacy*, informational asymmetry, limited relationality.

RESUMEN

El artículo ofrece la clave de lectura e interpretación de los artículos que, en la sección "Otros estudios", informan sobre las intervenciones realizadas durante la Mesa Redonda, el 21 de octubre de 2017 en la Facultad "Auxilium", con la cual se abrió el curso interdisciplinar de 2017-2018 sobre el tema: *Al principio, la red. Vivir y educar en una sociedad conectada*.
La Autora profundiza el tema desde la perspectiva socio-económica, refiriéndose en particular a la economía de la *privacy*, esa rama de la ciencia económica que estudia los *trade-offs* asociados con el equilibrio de la esfera pública y privada, entre sujetos, organizaciones y gobiernos.
Palabras clave
Economía de la *privacy*, paradoja de la *privacy*, asimetría informativa, racionalidad limitada.

campo medico dalla condivisione di dati su pazienti di tutto il mondo;

- la vita ordinaria e sociale può giovarsi dell'uso di applicazioni *social* per il traffico, la frequenza dei mezzi pubblici, ecc.

3. Alcune dimensioni economiche della *privacy*

3.1. Privacy, pubblicità e commercio elettronico

Il commercio elettronico è uno degli esempi più comuni di come le imprese utilizzano i tantissimi dati che collezionano dagli utenti e consumatori.
Nel 2012 sono stati spesi 36,6 miliardi di dollari in pubblicità digitale, nel 2015 si è passati a 52,8 miliardi. La raccolta di dati sui consumatori permette di personalizzare la pubblicità, e l'uso della pubblicità sui mezzi digitali permette di misurarne la sua efficacia meglio che con altri mezzi: l'utente è tracciabile, le sue mosse sono osservate. A proposito di *social networks*, un ricercatore della *Stanford University*, Michal Kosinski, ha creato uno strumento che analizzando *post* e *like* su *Facebook* riesce a dare un profilo completo della personalità dell'utente.[6]
Alla Rete non interessa il mio nome e cognome, basta sapere dove e quando navigo per raggiungermi con pubblicità e offerte dedicate.
Per identificare e prevenire frodi nei pagamenti *online*, *Paypal* ha sviluppato un sistema per controllare i pa-

gamenti e correlarli a dati personali dei clienti, quali indirizzi IP, informazioni sul *browser*, ed altri dati tecnici. Questo ha portato a un miglioramento del *trust* (fiducia) negli scambi commerciali online.[7]

3.2. Privacy e discriminazioni di prezzo

Il fatto che i nostri comportamenti sono tracciati permette alle imprese di personalizzare le offerte che ci rivolgono, e quindi di fare discriminazione di prezzo (prezzi diversi per diversi utenti): si stima che i prezzi di prodotti identici possono variare dal 10 al 30% in base alla localizzazione e alle preferenze rivelate da diversi utenti *online*. Questo avviene per esempio con i biglietti aerei: persone diverse, che fanno ricerche da computer diversi (cioè diversi indirizzi IP), possono ottenere prezzi differenti per diversi viaggi. I prezzi si avvicineranno per ognuno alla propria disponibilità a pagare, grazie alla storia degli acquisti precedenti.

3.3. Altre forme di discriminazione

La tracciabilità dei dati e dei profili può dare tante opportunità, ma nello stesso tempo è un potente strumento di discriminazione.

Immaginiamo un mondo in cui le imprese siano in grado di predire le future condizioni di salute dei possibili lavoratori che stanno selezionando, a partire da una manciata di dati estratti dai profili *social*… e quindi immaginiamo che le decisioni sulle assunzioni si basino anche su queste previsioni, nella totale inconsapevolezza dei candidati.

Prendiamo un altro caso: *Airbnb* è il più grande operatore al mondo per affitti di stanze o appartamenti. Nel sito di *Airbnb* il profilo del proprietario è visibile *online*. È stato dimostrato che nella città di New York i proprietari non afro-americani riescono ad affittare in media al 12% in più rispetto agli afroamericani per appartamenti equivalenti.

3.4. Privacy e salute

La digitalizzazione della medicina sta ottenendo enormi progressi in quella che, per esempio, è la telemedicina e lo scambio di informazioni importanti a livello mondiale: visite che si possono effettuare senza spostarsi, consulti tra medici a distanza, e anche operazioni chirurgiche effettuate a distanza. I costi sanitari a carico del Servizio Nazionale possono diminuire drasticamente attraverso la digitalizzazione. Ma a livello istituzionale, per esempio, due ospedali tedeschi hanno già avuto intrusioni da parte di *hacker* che hanno sequestrato tutte le cartelle cliniche, riconsegnate in cambio di un riscatto.

Anche il campo della genetica è interessato da questioni relative alla condivisione dei dati e alla *privacy*: raccogliere dati a livello mondiale può favorire la sconfitta di malattie rare. Ma quanto valgono quei dati per le compagnie di assicurazione? Perché negli Stati Uniti le compagnie di assicurazione o altre imprese (di fatto collegate) offrono la mappatura del DNA a prezzi molto scontati?

E se iniziassimo a parlare del mercato del credito, comprenderemmo perché *Google* vuole diventare una banca.

4. Il paradosso della *privacy*

In un Rapporto del 2015, il *Pew Research Center* afferma che il 93% degli americani sostiene che controllare le informazioni personali è molto importante, ma solo il 9% ritiene nella pratica di effettuare un buon controllo delle proprie informazioni.[8] E se la maggioranza dichiara di avere bisogno di *privacy*, nello stesso tempo la quasi totalità dei consumatori rimangono avidi utilizzatori di strumenti e tecnologie che condividono le loro informazioni con sconosciuti.

La apparente dicotomia tra attitudini alla *privacy*, intenzioni e comportamenti è chiamata *paradosso della privacy*. Dai dati empirici e sperimentali sembra che, normalmente, i soggetti attribuiscono un valore molto alto alla propria *privacy*, ma sistematicamente attuano comportamenti non in linea con le loro preferenze dichiarate. Da uno studio che illustra questo paradosso, risulta che i partecipanti ad un esperimento, classificati secondo le proprie preferenze per la *privacy* attraverso un questionario, compivano sistematicamente scelte di rivelazione di dati personali, indipendentemente da quanto precedentemente dichiarato.[9]

Per esempio, il 66% degli americani dichiara di non sopportare le pubblicità fatte su misura, ma la quasi totalità usa strumenti che permettono di far questo.

Dal punto di vista reputazionale, il paradosso della *privacy* evidenzia la vulnerabilità delle persone, che molte volte si ritrovano con conseguenze non previste, e indelebili, dei propri comportamenti sulla Rete.

I danni economici di un problema reputazionale derivante da condivisione non sempre consapevole di dati possono essere anche ingenti. Pensiamo al caso di un giovane che si presenta a colloqui di lavoro e sistematicamente non viene selezionato a causa di foto imbarazzanti in Rete oppure di post controversi su *Facebook*.

Per non parlare di persone affermate nel proprio lavoro, o nella vita pubblica, che in pochi istanti rovinano la propria immagine, ritrovandosi in balia dei *social media*.

4.1. Le cause

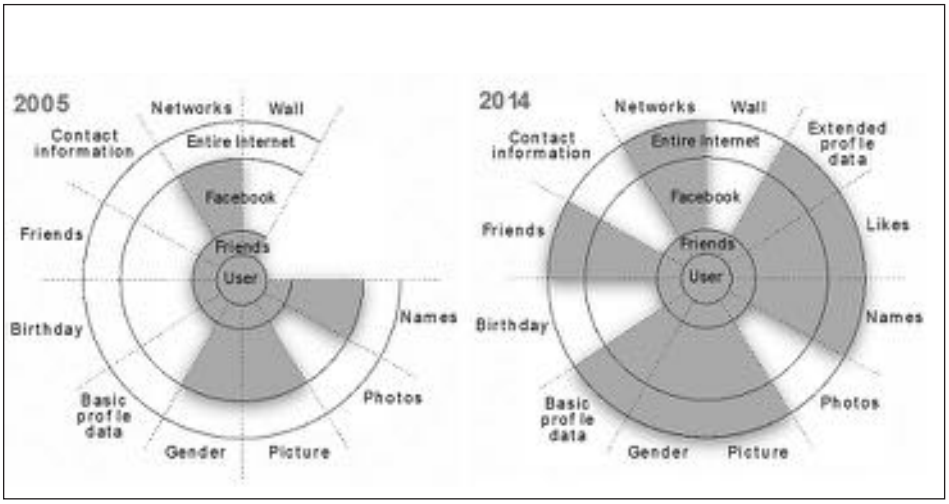
La prima causa del paradosso della *privacy* è l'*asimmetria informativa* che esiste tra chi raccoglie dati e chi li condivide: molti soggetti non sono consapevoli di quanto le loro informazioni siano raccolte e condivise e non conoscono gli strumenti di protezione, che pure esistono.

Molti atti di condivisione, quindi, vengono fatti nell'ignoranza di dove andranno a finire le informazioni condivise e di chi le utilizzerà. I risultati di alcuni esperimenti confermano che la poca conoscenza di alcuni fenomeni è una causa della condivisione di dati personali senza averne la consapevolezza.

In uno studio su acquisti *online*, i soggetti potevano acquistare, a prezzi

differenti da diversi rivenditori. Normalmente, a parità di altre cose essi sceglievano di acquistare dai rivenditori più economici. In una versione dove venivano fornite informazioni sui diversi livelli di protezione della *privacy* e dei dati delle carte per acquistare dai diversi rivenditori, i soggetti erano disposti a pagare di più per comprare da rivenditori più affidabili dal punto di vista della *privacy*. Un'altra causa, molto legata alla prima, è quella della cosiddetta *razionalità limitata*: come esseri umani non sempre riusciamo a fare scelte razionali prevedendo tutte le possibili conseguenze delle nostre azioni. La limitazione della razionalità si esprime anche attraverso i cosiddetti *bias* cognitivi, che sono errori di valutazione ricorrenti nella popolazione. Tra essi i più importanti sono i seguenti:

- *bias dello status quo*: le persone, generalmente, a parità di altre condizioni, se trovano moduli con opzioni precompilate e item già *cliccati*, preferiscono lasciarli come sono, se non contrari alle proprie preferenze. Cliccare su *item*, o togliere un *click* è più costoso, in termini di impegno e di tempo, rispetto a lasciare il tutto come è. È il motivo per cui in molti Stati, per esempio, l'opzione della donazione di organi in caso di morte è quella considerata di *default* e se le persone non sono d'accordo con questa scelta devono comunicarlo. In questo caso il *bias* dello *status quo* permette di avere una percentuale più alta di donatori di organi. Se, infatti, l'opzione di *default* fosse quella di non donare, molte persone, semplicemente per non doversi fermare a leggere e selezionare l'opzione, non darebbero il consenso alla donazione degli organi. I *default settings* sono dunque un importante strumento per influenzare le decisioni di rivelare o meno le proprie informazioni. I *social networks*, e il mondo della Rete più in generale, fanno leva su questa forma di ra-



zionalità limitata. Per esempio, dal 2005 al 2014 è aumentata notevolmente l'area dei *default settings* su *Facebook* circa le condivisioni, come mostra la Figura 1.[10]

- *present bias*: rivelare le proprie informazioni può avere una gratificazione immediata, per esempio intangibile (i *likes* degli amici ad un aggiornamento di stato), o tangibile (uno sconto). Il costo è spesso incerto, e generalmente non immediato (la foto su Facebook di baldoria con gli amici … e il futuro datore di lavoro, lo sconto oggi e le informazioni per ricevere prezzi su misura la prossima volta). È stato dimostrato che il *present bias* può condizionare le persone con attitudini più restrittive circa la *privacy* a condividere informazioni personali in cambio di gratificazioni immediate. Quando arriva un'offerta immediata di uno sconto su un biglietto aereo o su un acquisto *online* che si sta effettuando, e per accedere all'offerta bisogna rispondere a diverse domande anche abbastanza personali, si è tutti tentati di ottenere al più presto l'offerta. In quel momento bisognerebbe pensare che i nostri dati valgono molto di più dell'offerta proposta.[11]

4.2. Le valutazioni e il contesto

A causa dell'asimmetria informativa e dei *bias* cognitivi e comportamentali, che generano mancanza di consapevolezza sugli effetti della condivisione dei propri dati, è difficile valutare il reale valore dell'informazione. Molto spesso, sempre nella nostra inconsapevolezza, i nostri dati sono svenduti alle compagnie pubblicitarie.

Per comprendere quanto i consumatori sottovalutino l'importanza economica delle proprie informazioni, è stato stimato che le società di comunicazione e pubblicità vendono elementi della storia della navigazione da parte degli utenti a 0,0005 dollari a persona. E invece dalle interviste, i consumatori dichiarano che pagherebbero $2,28 per nascondere la storia della loro navigazione, $4,05 per nascondere la lista dei contatti, $1,19 per la posizione, $1,75 per l'identificazione del numero di telefono, $3,58 per il contenuto dei loro messaggi di testo, $2,12 per eliminare la pubblicità. Gli esperimenti dimostrano, tuttavia, che le valutazioni dipendono molto dai contesti. Quando c'è molta incertezza sulle proprie preferenze e sul valore delle proprie azioni, le persone cercano indizi nel contesto per comprendere come sia meglio comportarsi. Per questo motivo i contesti possono essere manipolati da chi vuole raccogliere informazioni, in modo da invitare le persone a condividere i propri dati.

In un esperimento realizzato nella Carnegie Mellon, un gruppo di circa 200 studenti è stato sottoposto a un questionario sui propri comportamenti.[12] Alcune domande si soffermavano su comportamenti considerati non corretti, del tipo: «hai mai sbirciato la posta elettronica di un tuo collega o di un tuo amico?». Gli studenti sono stati suddivisi in sotto-

campioni casuali e di uguale numerosità. Le domande erano uguali per tutti, ma nei tre gruppi variava l'interfaccia grafica dello schermo: un gruppo aveva un'interfaccia neutra, un gruppo si trovava davanti ad una pagina professionale con il logo dell'Università, mentre il terzo gruppo vedeva l'immagine di un diavoletto e la scritta «How BAD are you?». L'esperimento ha dimostrato che il terzo gruppo ha dato un numero maggiore di risposte positive a domande su comportamenti poco corretti, rispetto agli altri due gruppi. Il contesto dunque è molto importante per spingere le persone a rivelare i propri dati e le proprie informazioni.

Conclusione

Il tema della *privacy* e dei suoi risvolti economici nell'era dell'informazione è di grande attualità.

Di fronte al grande valore delle informazioni personali i cittadini e i consumatori sembrano non avere piena consapevolezza dell'importanza dei loro atti di condivisione e/o di protezione: il paradosso della *privacy* è proprio l'espressione di questa mancanza di consapevolezza. In molti credono che una buona regolamentazione possa essere la soluzione di tanti problemi. In realtà, per quanto una regolamentazione possa essere ben fatta ed efficace, l'evoluzione tecnologica in questo campo è velocissima, e una norma dovrebbe cambiare in continuazione per stare al passo con i cambiamenti.

Una buona normativa è una condizione necessaria, ma non sufficiente alla protezione della propria *privacy*, dei dati personali e della reputazione. Molto più efficace risulterebbe un'educazione e una formazione su questi temi fin dai primi anni di scuola, in modo da accrescere l'informazione e la consapevolezza rispetto ai comportamenti in Rete.

Infine, se è vero che quando non si paga per un prodotto vuol dire che il prodotto siamo noi, è pur vero anche che il mercato siamo noi, e siamo noi a decidere cosa vendere o acquistare. Bisogna solo dotarsi del bagaglio tecnologico e di informazioni necessarie a fare scelte informate e consapevoli.

NOTE

[1] Docente di Economia politica alla Pontificia Facoltà di Scienze dell'Educazione "Auxilium".

[2] È possibile rivedere e riascoltare i contributi del Corso interdisciplinare 2017-2018 accedendo al canale YouTube della Facoltà "Au-

xilium": https://www.youtube.com/watch?v=TQkxxmMMryg&list=PLC9QdYdBY_1uy9cD3T6LG_Kf7FksjUMzU (24-05-2018).

[3] Cf Warren Samuel D. - Brandeis Louis D., *The right to privacy*, in *Harvard Law Review* 4(1890)5, 193-203.

[4] Cf Westin Alan, *Privacy and Freedom*, New York, Atheneum Publishers 1967.

[5] Cf Schoeman Ferdinand David, *Privacy and social freedom*, Cambridge, University Press 1992.

[6] Cf *Apply Magic Sauce*, in https://applymagicsauce.com/ (25-05-2018).

[7] Cf Andrade Pedro Less - Hemerly Jess - Recalde Gabriel - Ryan Patrick, *From Big Data to Big Social and Economic Opportunities: Which Policies Will Lead to Leveraging Data-Driven Innovation's Potential?*, in Bilbao-Osorio Beñat - Dutta Soumitra - Lanvin Bruno (Edd.), *The Global Information Technology Report 2014*. *Rewards and Risks of Big Data,* Geneva, World Economic Forum and INSEAD 2014.

[8] Cf Madden Mary - Rainie Lee, *Americans' attitudes about privacy, security and surveillance*, in *Pew Research Center Internet and Technology* (20-05-2015), in http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (25-05-2018).

[9] Cf Spiekermann Sarah - Grossklags Jens - Berendt Bettina, *E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior.* Third ACM Conference on Electronic Commerce, Tampa 2001, 38-47.

[10] Cf Acquisti Alessandro - Brandimarte Laura - Loewenstein George, *Privacy and human behavior in the age of information*, in *Science* 347(2015)6221, 509-514.

[11] Cf Acquisti Alessandro, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*. Fifth ACM Conference on Electronic Commerce, New York 2004, 21-29.

[12] Cf John Leslie K. - Acquisti Alessandro - Loewenstein George, *Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information*, in *Journal of Consumer Research* 37(2011)5, 858-873.

IL CONTINENTE NASCOSTO: DATI E PERSONA NEL CYBERSPAZIO INTERCONNESSO

HIDDEN CONTINENT: DATA AND PERSONS INTERCONNECTED IN CYBERSPACE

CLAUDIO PANAIOTTI[1]

Non ho scritto articoli, tantomeno libri sugli argomenti che andremo a trattare ma ho letto chi, molto meglio e più approfonditamente di me, ha stimolato la mia curiosità e le mie riflessioni attraverso idee e provocazioni.
Vorrei dare avvio al mio intervento, partendo da una citazione di Larry Andrews divenuta famosa ed applicata al mondo della Rete: «Se non state pagando per qualcosa, significa che non siete il cliente; siete il prodotto venduto».
Il sapere, che un tempo si identificava con la conoscenza del passato, viene oggi identificato con la capacità di prevedere il futuro. A partire da questa logica, i dati, il cui trattamento come vedremo è fondamentale per tali attività predittive, vengono ad occupare il centro del palcoscenico. Oggi, tutte quelle informazioni digitali che sono state raccolte possono essere sfruttate con modalità innovative per realizzare nuovi scopi e liberare nuove forme di valore.
Se è vero che la conoscenza è di per sé una grande forma di potere, allora detenere dati, processarli e riutilizzarli equivale a gestire un enorme potere. I dati sono, per la società dell'informazione, quello che era il petrolio per l'economia industriale: principale fonte di ricchezza, alimentano servizi ed imprese, ma potrebbero anche far aumentare le diseguaglianze. I dati digitali non somigliano a nessuna risorsa del passato ed hanno una caratteristica diversa da altre materie prime: quella di poter essere riutilizzati più volte, aggregati e disaggregati in diversi *dataset* senza perdere (alcuni entro certi limiti temporali) la loro caratteristica di produrre valore. Cambiano le regole dei mercati e impongono cambiamenti etici e giuridici e, sul loro sfruttamento, si combatteranno infinite battaglie.
D'altronde la posta in gioco è enorme. La società di ricerche di mercato IDC *(International Data Corporation)*[2] prevede che nel 2025 "l'universo digitale" (i dati che ogni anno sono creati e copiati) raggiungerà i 180 *zettabyte* (180 seguito da 21 zeri). E siamo sempre noi, con i nostri com-

portamenti quotidiani a fornire gratuitamente questa materia prima.
Anche la qualità dei dati è cambiata. Non sono più semplici raccolte di nomi ed altre informazioni personali come l'età, il sesso e il reddito. La nuova economia si basa soprattutto sull'analisi in tempo reale di flussi rapidi di dati spesso non strutturati (i cosiddetti *Big Data*): i milioni di video e di foto generati dagli utenti dei *social network*, le informazioni prodotte dai pendolari mentre vanno al lavoro. Dai treni alle turbine eoliche, dalle tavolette dei water ai tostapane, tutti gli apparecchi e i terminali generano dati. Il mondo sarà invaso dai sensori ed ovunque andremo lasceremo una traccia digitale anche senza essere collegati a Internet.
Come sostiene Paul Sonderegger, responsabile della strategia *Big Data* di *Oracle*, i dati saranno l'esternalità suprema: qualsiasi cosa facciamo produrrà dei dati.
All'inizio *Facebook* e *Google* usavano i dati sugli utenti per indirizzare meglio la pubblicità. Negli ultimi anni, invece, hanno scoperto che i dati possono trasformarsi in una molteplicità di servizi di intelligenza artificiale potenzialmente redditizi, tra cui, a solo titolo di esempio, la traduzione (*Google,* grazie al lavoro di noi utenti, ha praticamente gratis in casa il correttore ortografico più completo al mondo, disponibile praticamente in tutte le lingue vive ed il sistema continua a migliorarsi attraverso un effetto secondario del nostro uso quotidiano del motore di ricerca riutilizzando i miliardi di *query* che gestisce ogni giorno), oppure il riconoscimento facciale e la valutazione dei tratti della personalità sulla base di come un utente interagisce. Ognuno di questi servizi può essere rivenduto ad altre aziende.
Tutti vogliono sfruttare un potentissimo motore economico chiamato *data-network*: si usano i dati per attirare nuovi utenti, che a loro volta generano nuovi dati, che aiutano a migliorare i servizi, che attirano altri utenti; ed i grandi operatori attingono dai giacimenti più ricchi. Più gli utenti pubblicano commenti, mettono *like* o interagiscono su *Facebook,* più l'azienda di Mark Zuckerberg impara altre cose su quegli utenti. *Facebook* fa testare alcuni dei suoi algoritmi ai propri utenti per esempio quando caricano e *taggano* le foto degli amici ed è così che i suoi computer oggi riescono a riconoscere centinaia di milioni di persone con una precisione del 98%.
Allo stato attuale i consumatori e i colossi di Internet sono stretti in uno scomodo abbraccio: gli utenti non sanno quanto valgono i loro dati, ma stanno anche mostrando i sintomi della cosiddetta "impotenza appresa": i termini e le condizioni dei servizi spesso sono impenetrabili e gli utenti non possono fare altro che accettarli (ad esempio, le *app* per gli *smartphone* si chiudono immediatamente se non si clicca su "accetto"). Da parte loro, le aziende sono diventate dipendenti dalla "droga" dei dati e non hanno interesse a modificare il patto con gli utenti. Pagare per i dati e svi-

RIASSUNTO

L'Autore riflette, a partire dal social network *Facebook*, come sia importante aumentare i nostri livelli di consapevolezza sulle opportunità, ma soprattutto sui pericoli insiti nell'era digitale dove, al di là degli aspetti tecnologici e dei presidi automatici di sicurezza, deve essere il fattore umano a riacquisire la necessaria centralità.

È la persona il cardine attorno a cui riformulare un processo di comunicazione attiva per la tutela di noi stessi.

Parole chiave

Big data, cybersicurezza, world wide web, Facebook, Google, fake news.

SUMMARY

Beginning from the social network *Facebook*, the Author reflects on how important it is to increase our level of understanding the opportunities and, above all, the dangers of the digital world where, beyond the technological aspects and automatic security settings, the human

luppare sistemi costosi per tracciare le transazioni renderebbe la raffinazione dei dati molto meno redditizia.
Le grandi aziende tecnologiche hanno accumulato troppo potere e sono in grado di identificare in tempi brevissimi i loro concorrenti potenzialmente pericolosi e, grazie alle loro enormi risorse finanziarie, possono comprare le start-up che minacciano il loro dominio del mercato.
Le autorità *antitrust* dovranno affinare i loro strumenti per l'era digitale. La Commissione Europea, in base alla normativa vigente, non ha impedito la fusione di *Facebook* con *WhatsApp,* ma non ha tenuto conto che *Facebook* stava comprando un pericoloso rivale. Solo successivamente, a seguito della fusione degli archivi, la Commissione ha minacciato sanzioni per presunto abuso di posizione dominante.
Se i dati personali sono venduti o condivisi possono essere facilmente divulgati e per questo motivo l'Unione Europea vuole rafforzare il controllo sui privati che detengono dati, anche se sarà difficile fare rispettare regole in un mondo in cui i flussi di dati si mescolano e si incrociano tra loro.
Almeno per quanto riguarda i dati personali, il modello attuale è sostanzialmente insostenibile e mano a mano che il valore dei dati aumenta e che l'economia intorno ai dati diventa più importante, le "raffinerie" di informazioni digitali intascano tutti i profitti.
Eric Posner, docente di diritto presso la *Law School* della *University of Chicago* (USA) e Glen Weyl*,* Principal Researcher alla *Microsoft Research* New England, evidenziano ad esempio come, in ultima analisi, i servizi di intelligenza artificiale non sono prodotti dagli algoritmi bensì dalle persone che generano la materia prima. Essi stanno lavorando ad un sistema per misurare il valore del contributo

factor must take central role. The person is the center around which the reformulation of an active communication process must take place to protect ourselves.
Key words
Big data, cybersecurity, world wide web, Facebook, Google, fake news.

RESUMEN

El Autor reflexiona, a partir de la red social Facebook, en torno a qué tan importante es aumentar nuestros niveles de concienciación sobre las oportunidades, pero más que todo sobre los peligros inherentes a la era digital donde, más allá de los aspectos tecnológicos y los dispositivos de seguridad automáticos, debe ser el factor humano el que readquiere la centralidad necesaria. La persona es el eje alrededor del cual reformular un proceso de comunicación activa para la protección de nosotros mismos.
Palabras clave
Ciberseguridad, red mundial, Facebook, Google, noticias falsas.

individuale ai dati, con l'obiettivo di garantire uno scambio più equo. Il problema, afferma Weyl (ma potremmo anche dire "Microsoft…", per intenderci!) è far capire alle persone che i loro dati hanno un valore e che hanno diritto ad un compenso.

Da anni il mondo è segnato dalle guerre per il controllo del petrolio e pochi si preoccupano di una guerra per i dati anche se l'economia dei dati ha lo stesso potenziale di conflittualità.

La merce sei tu è il titolo di un articolo di John Lancaster, scrittore e giornalista britannico del quale riporto alcuni stralci: «*Facebook* dice di voler mettere in contatto le persone, ma in realtà è la più grande azienda di sorveglianza della storia dell'umanità e i suoi clienti sono gli inserzionisti pubblicitari.

Alla fine di giugno del 2017 Mark Zuckerberg ha annunciato che *Facebook* era arrivato a due miliardi di utenti mensili attivi. In parole povere, a maggio due miliardi di persone in tutto il mondo avevano usato *Facebook*. È difficile rendersi conto dell'enormità di questo risultato. Tenete presente che *thefacebook*, come si chiamava all'inizio, era stato lanciato nel 2004 solo per gli studenti di Harvard. Non ci sono imprese umane, nuove tecnologie, nuovi servizi pubblici o privati che siano stati universalmente adottati così in fretta. La velocità con cui si è diffuso *Facebook* supera di gran lunga quella di Internet, per non parlare di tecnologie antiche come la televisione, il cinema o la radio. Un'altra cosa incredibile è che più *Facebook* cresce, più i suoi utenti ne dipendono. Al contrario di quanto ci si aspetterebbe, la maggiore diffusione non corrisponde a un livello di coinvolgimento più basso, a dispetto degli altri strumenti citati pri-

ma. Nel lontano ottobre 2012, quando Facebook ha superato il miliardo di iscritti, il 55% degli utenti lo usava tutti i giorni. Oggi che gli iscritti sono due miliardi, la percentuale è salita al 66%. Il principale concorrente di *Facebook* in termini di utenti registrati è *YouTube*, di proprietà dell'arcinemica *Alphabet* (l'Azienda che prima si chiamava *Google*) con 1,5 miliardi di utenti. Al terzo, quarto e sesto posto ci sono *WhatsApp* con 1,2 miliardi, *Messenger* con 1,2 miliardi e *Instagram* con 700 milioni di utenti. Questi ultimi tre servizi, o *app* o come si voglia chiamarli, hanno una cosa in comune: appartengono tutti a *Facebook* che è la quinta società al mondo per un valore in borsa pari a 445 miliardi di dollari».[3]

La *mission* di *Facebook* era "rendere il mondo più aperto e connesso". Leggendola, chi non usa *Facebook* potrebbe chiedersi: perché? Essere connessi viene presentato come un fine in sé, come una cosa intrinsecamente e automaticamente positiva. Ma è cosi? Flaubert, parafrasando Julian Barnes, uno scrittore britannico, guardava con scetticismo alla ferrovia pensando che avrebbe semplicemente permesso a più gente di spostarsi, incontrarsi ed essere stupida. Non c'è bisogno di essere misantropi come Flaubert per pensare la stessa cosa di *Facebook*. Per esempio, è opinione diffusa che questa piattaforma abbia avuto un ruolo cruciale nella elezione del Presidente degli Stati Uniti, Donald Trump. Come questo abbia giovato all'umanità non è chiaro…

Zuckerberg sa benissimo come funziona la testa delle persone ed ha una particolare consapevolezza delle dinamiche sociali legate alla popolarità ed allo stato sociale: ad Harvard ha studiato per prendere una doppia specializzazione in informatica e in psicologia…

Analogamente, il suo primo finanziatore, Peter Thiel, miliardario della Silicon Valley, laureato in filosofia a Stanford, si era avvicinato alle idee del filosofo franco-statunitense René Girard, autore di un influente saggio intitolato *Delle cose nascoste sin dalla fondazione del mondo*. Il pensiero di Girard ruota intorno al concetto di "desiderio mimetico". L'uomo nasce con il desiderio di nutrirsi e di ripararsi: una volta soddisfatte queste necessità fondamentali comincia a guardare ciò che fanno (e vogliono) gli altri e li imita. Nella sintesi di Thiel "l'imitazione è alla radice di ogni comportamento". L'uomo non sa cosa vuole o chi è, non ha valori e convinzioni; ha solo l'istinto di copiare e fare confronti. L'uomo è la creatura che non sa cosa desiderare e che guarda gli altri per decidere. Desideriamo ciò che desiderano gli altri perché imitiamo i loro desideri. Thiel, dunque, ha sposato la causa di Zuckerberg con grande entusiasmo perché ha visto in *Facebook* il primo business tipicamente *girardiano* fondato sul bisogno di copiare gli altri. *Facebook* così, come altri *social*

media, ci arricchisce in termini di democrazia?
Dipende… È implicita nella sua natura la tendenza intrinseca a frammentare gli utenti in gruppi di persone che la pensano allo stesso modo. L'obiettivo di "connettere" le persone, in pratica, significa metterle in contatto con chi è d'accordo con loro. È impossibile dimostrare sino a che punto queste bolle in cui ci chiudiamo siano pericolose per la società, ma è abbastanza chiaro che hanno un impatto molto forte su un tessuto politico sempre più frammentato.
Altro problema è quello rappresentato dalle *fake news,* bufale e post verità diffusissime nella comunicazione in Rete (ma non solo!), che però indicano una realtà resa possibile dal passaggio del dibattito pubblico da una agorà a bunker ideologici chiusi.
All'aria aperta le *fake news* possono essere combattute e smascherate; su Facebook (o altri *social media* o nei media in generale), se non si fa parte della comunità in cui vengono raccontate, è impossibile sapere anche solo che sono state messe in circolazione e *Facebook* non ha alcun interesse economico a dire la verità.
Quindi, se ai nostri giorni è vero che "se una merce è gratis allora la merce sei tu", nessuna azienda incarna questo assioma meglio di *Facebook*.
La filosofa tedesca Hannah Arendt, scomparsa nel 1975, scriveva che in una società dove ogni cosa diventa opinabile, ognuno è forse *libero* di dire ciò che vuole, ma nessuno viene realmente ascoltato e si registra, di conseguenza, "una desolante equivalenza tra chi denuncia un comportamento e chi lo nega senza alcuna differenza". Cosicché la scomparsa della verità, e dunque della realtà, viene fatta passare come il "trionfo della discussione pubblica". In definitiva, quando la verità è ridotta a mera opinione assistiamo al venir meno del confine esistente tra verità ed opinione e, di riflesso, tra i fatti e le opinioni, per cui "una società in cui ogni affermazione equivale alle altre e può imporsi esclusivamente attraverso la persuasione o la violenza, può rendere impotenti quanto una rigida censura".
In tutto ciò i clienti di *Facebook* non sono gli utenti, ma gli inserzionisti pubblicitari che usano il *social network* e sfruttano la sua capacità di indirizzare gli annunci ad un pubblico ricettivo.
Perché a *Facebook* (o *altri social media*) dovrebbe importare se le notizie che fa circolare sono false? Quello che gli interessa è far arrivare il messaggio alle persone giuste, non il contenuto.
Auguriamoci solo che Facebook non sposi una causa… qualunque essa sia!
Le grandi società che detengono i nostri dati sanno tutto quello che c'è da sapere su di noi, il nostro nome, l'indirizzo, il nostro reddito, il livello di istruzione, lo stato civile, i gusti, le opinioni politiche, le prefe-

renze sessuali, le nostre letture preferite come i gusti musicali, chi frequentiamo, le nostre immagini, i luoghi dove siamo stati e dove andremo… e cosi via per ogni nostra manifestazione. Più tutti i posti dove abbiamo pagato con una carta di credito e, ovviamente, cosa abbiamo acquistato e *Facebook* riesce a risalire all'identità degli utenti attraverso il codice identificativo del telefono.
Questo significa che, più ancora della pubblicità, il vero *business* di *Facebook* è la sorveglianza. Di fatto *Facebook* è la più grande azienda di sorveglianza della storia dell'umanità.
Certo non è l'unica; la detenzione e l'utilizzo dei cosiddetti *Big Data* aprono enormi prospettive positive, ma per contro dobbiamo essere consapevoli che la posta in gioco è più alta di quanto non si creda comunemente.
Il pericolo di non governare i *Big Data* nel rispetto (difficilissimo, forse impossibile) della *privacy* o di farsi ingannare dal significato dei dati, va molto al di là di bazzecole come la pubblicità mirata su Internet.
Ricordando la scena di apertura del film *Minority Report*, diretto da Steven Spielberg e scritto dalla fantasia predittiva di Philip K. Dick, con l'avvento dei *Big Data* emerge un problema ancora più grave: l'utilizzo delle previsioni per giudicarci o penalizzarci attraverso l'analisi delle nostre propensioni. Ovvero la possibilità di usare le previsioni sui nostri comportamenti per giudicarci e punirci ancora prima delle nostre azioni.
Fantascienza? Non si direbbe, tenendo conto di quante società del settore utilizzano le tracce digitali che lasciamo nella Rete e che vengono raccolte, memorizzate ed elaborate per verificare la nostra affidabilità economica, sociale o verificare l'opportunità di offrirci un posto di lavoro in ragione di uno *screening* accuratissimo, ma del quale non siamo a conoscenza ed i cui criteri potrebbero essere assai discutibili sotto il profilo etico.
Anche ciò che riteniamo essere nostre idee e comportamenti possono essere (sono) fortemente influenzati e manipolati da chi conosce quasi tutto di noi (il "quasi" è un inno alla speranza!).
In chiusura, vorrei accennare a un parassita delle formiche. Il suo nome è *Dicrocoelium dendriticum.* È un maestro del controllo della mente. Si tratta di un piccolo parassita che trascorre la sua vita adulta nel fegato degli erbivori. Niente di terribilmente insolito, ma perché un parassita (nella nostra società della Rete ne contiamo parecchi!) sia un organismo di successo deve affinare certi comportamenti. Quando l'adulto depone le uova, queste finiscono nell'intestino crasso ad esempio di una pecora ospite ed eliminate. Fine della stirpe? Assolutamente no! Le lumache, che si cibano anche del prodotto di scarto delle pecore, assumono un bel po' di uova che si sviluppano e vengono eliminate con la secrezione della bava. Come tor-

nare dentro una pecora visto che quest'ultima non mangia lumache? Presto detto: ci pensano le formiche che assumono la secrezione delle lumache consentendo al nostro simpatico verme di insinuarsi nel sistema nervoso della formica ed assumere il controllo del suo cervello (se così possiamo chiamarlo).

Durante il giorno la formica si comporta in modo normale ma, quando tramonta il sole, sente l'irrefrenabile esigenza suicida di arrampicarsi in cima ad un filo d'erba serrandolo con le mandibole, attendendo il giorno successivo per riassumere il controllo delle sue azioni e ripetere il tutto. La formica non sa perché ogni sera salga in cima ad un filo d'erba e neppure sa cosa attendersi… forse pensa di aver deciso di farlo e basta. In realtà. il comportamento è deciso totalmente dal parassita che la costringe ad un comportamento innaturale che segnerà la sua fine; ovvero quella di essere mangiata insieme al filo d'erba da una pecora di passaggio. Per tutto il tempo, è probabile, che la formica ignori beatamente di essere condizionata da uno straordinario manipolatore.

Online questa strategia ha grande successo: ci sono innumerevoli operazioni che cercano di farci salire sul proverbiale filo d'erba. Molti di noi sono già in cima, fieramente aggrappati e convinti di trovarsi lassù perché *lo vogliono*… Riflettiamoci insieme…

Bibliografia di riferimento

CALIGIURI Mario*, Cyber Intelligence. Tra libertà e sicurezza*, Roma, Donzelli Libri 2016.

GIRARD René, *Delle cose nascoste sin dalla fondazione del mondo. Ricerche con Jean-Michel Oughourlian e Guy Lefort* [Des choses cachées depuis la fondation du monde, Paris, Grasset 1978], tr. it. di Rolando Damiani, = Saggi. Nuova serie, Milano, Adelphi 1996.

LANCHESTER John, *You Are the Product*, in *London Review of Books*, 39(2017)16, 3-10.

MAYER-SCHÖNBERGER Viktor - CUKIER Kenneth N., *Big data*. *Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà* [Big Data: A Revolution That Will Transform How We Live, Work, and Think, Boston, Eamon Dolan/Mariner Books 2014], = Saggi, Milano, Garzanti 2013.

SEIFE Charles*, Le menzogne del Web. Internet e il lato sbagliato dell'informazione*, Torino, Bollati Boringhieri 2015.

The world's most valuable resource is no longer oil, but data, in *Economist.com* (May 6th 2017), in https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource (30-04-2018).

NOTE

[1] Capo del Servizio Sistemi Informatici del Segretariato Generale della Presidenza della Repubblica italiana. Il testo è la relazione che il Dott. Panaiotti ha tenuto il 21 ottobre 2017 all'interno del Corso interdisciplinare 2017-2018 alla Facoltà di Scienze dell'Educazione "Auxilium" di Roma. Si è voluto mantenere il tono orale dell'intervento, che è stato rivisto dall'Autore.

[2] Fondata nel 1964, IDC (*International Data Corporation*) è la prima società mondiale specializzata in ricerche di mercato, servizi di consulenza e organizzazione di eventi nei settori ICT e dell'innovazione digitale. Oltre 1.000 analisti in 50 Paesi del mondo mettono a disposizione a livello globale, regionale e locale la loro esperienza e capacità per assistere il mercato della domanda e dell'offerta nella definizione delle proprie strategie tecnologiche e di business a supporto della competitività e della crescita aziendale. Ogni anno IDC conduce oltre 300.000 interviste, pubblica 5.000 report di ricerca e influenza più di 10.000 CIO ai propri eventi. La filiale italiana di IDC, costituita nel 1986, integra la visione strategica sviluppata dal gruppo a livello mondiale con le proprie competenze sul mercato ICT locale. Presso la sede di Milano lavorano più di 40 specialisti, suddivisi in quattro aree (Ricerca e Consulenza italiana, IDC *Insights*, *Industry Solutions* ed *EU Government Consulting*) e nella divisione dedicata agli eventi. Cf http://idcitalia.com/home (30-04-2018).

[3] Lanchester John, *You Are the Product*, in *London Review of Books* 39(2017)16, 3.

IL VALORE DELLE INFORMAZIONI NELLA SOCIETÀ POST-INDUSTRIALE

THE VALUE OF INFORMATION IN A POST-INDUSTRIAL SOCIETY

CORRADO GIUSTOZZI[1]

La società nella quale viviamo viene comunemente definita "società dell'informazione", a sottolineare come sia l'informazione, e non più il possesso di beni materiali, a costituirne il valore. Secondo la definizione che ne dà Wikipedia «Il termine società dell'informazione è usato da alcuni sociologi per indicare l'attuale società post-industriale, spesso a seguito della terza rivoluzione industriale. Ciò che più spiccatamente la caratterizza è il prevalere di un bene immateriale come l'informazione rispetto all'industria, il settore dell'economia che è stato trainante per tutto il XX secolo, e più in generale dei servizi o terziario».[2]

Questa definizione fa dunque esplicito riferimento ai profondi mutamenti paradigmatici introdotti nel mondo del lavoro e dell'economia già a partire dagli Anni Sessanta dello scorso secolo, grazie anche al progresso delle tecnologie dell'informazione e della comunicazione, e trasmette una visione della società nella quale la risorsa strategica prevalente non è più quella materiale e produttiva in senso tradizionale, bensì quella relativa agli aspetti tecnologici, informativi, comunicativi. Nella "società dell'informazione" l'economia si fonda sempre più sulla produzione di servizi basati sulla manipolazione e l'elaborazione delle informazioni, ed il valore di un'impresa non sta più tanto nei suoi *asset* materiali bensì nella conoscenza che gestisce, considerata come vera e propria risorsa strategica. Non per nulla l'informazione viene anche definita da alcuni come "il petrolio del terzo millennio", a significare proprio che essa costituisce la preziosa materia prima che alimenta le attività immateriali dell'economia post-industriale.

1. Il valore economico dell'informazione

Essendo oramai definiti e citati da alcuni decenni, questi concetti sono divenuti tanto noti e famosi nell'immaginario collettivo da apparire oggi frusti e ovvii, veri e propri luoghi comuni, se non addirittura solo vuoti slogan. Eppure, paradossalmente,

RIASSUNTO

Il detto degli antichi che "L'informazione è potere" è lo spunto scelto dall'Autore per riflettere e affermare che oggi l'informazione è valore, un valore economico addirittura superiore a quello che fino a pochi anni fa era di esclusivo appannaggio dei più grandi gruppi industriali tradizionali. E le informazioni personali lo sono ancora di più, in quanto consentono di ricavare valore dal comportamento e dalle attitudini dei singoli, sia al fine di sviluppare prodotti e servizi legittimi sia per attuare azioni illegittime o veri e propri crimini. È il nostro comportamento, come sempre, a fare la differenza: e la conoscenza dei meccanismi oscuri della Rete è il primo passo per non rimanervi intrappolati.

Parole chiave

Dati, informazioni, economia, società in rete, *deep web.*

SUMMARY

The ancient saying that "Information is power" is the point chosen by the Author to reflect and affirm that today, too, information has value, an economic value that is even superior to what, until a few years ago, was belonging exclusively to the large traditional industrial groups. Personal information is even more valuable in that it allows one to recover value from the behavior and atti-

mai come ai nostri giorni riflettono la vera essenza della società nella quale viviamo, nella quale il potere economico è sempre più nelle mani di aziende che hanno fatto la propria fortuna non possedendo o producendo alcunché di materiale, e addirittura fanno degli *asset* industriali quasi un disvalore.

"L'informazione è potere", lo sapevano anche gli antichi: ma oggi l'informazione è valore, un valore economico addirittura superiore a quello che fino a pochi anni fa era di esclusivo appannaggio dei più grandi gruppi industriali tradizionali.

Può dunque apparire curioso scoprire, ad esempio, che al giorno d'oggi la più grande azienda di taxi al mondo non possieda neppure un'automobile: si tratta ovviamente di *Uber*, che come noto basa il proprio *business* esclusivamente sulla mediazione fra chi necessita di un passaggio e chi è disponibile ad offrirlo con la propria autovettura. Ma la cosa più sorprendente è che il valore attualmente attribuito a questa azienda (circa 68 miliardi di dollari nel febbraio 2018)[3] è di oltre quindici volte superiore rispetto a quello attribuito ad *Hertz*, la quale tuttavia possiede un parco di oltre 700.000 veicoli nel mondo e dispone di 9.700 sedi, praticamente in tutti i Paesi del pianeta.[4]

Analogamente sappiamo tutti che il *social media* più popolare al mondo, ovvero *Facebook*, non crea autono-

tudes of individuals, both to develop legitimate products and services as well as to carry out illegitimate actions, even crimes. It is always our behavior that makes the difference: knowledge of the obscure mechanisms of the Newtork is the first thing needed to avoid being trapped.
Key words
Data, information, economy, society, networked, *deep web.*

RESUMEN

El dicho de los antiguos que "la información es poder" es el punto elegido por el Autor para reflexionar y afirmar que hoy la información es un valor, un valor económico, incluso superior a lo que hasta hace pocos años eran prerrogativa exclusiva de la mayoría de los más grandes grupos industriales tradicionales. Y las informaciones personales lo son aún más, en cuanto permiten destacar el valor del comportamiento y de las actitudes de las personas, tanto para desarrollar productos y servicios legítimos, como para implementar acciones ilegítimas o verdaderos crímenes. Nuestro comportamiento, como siempre, es el que hace la diferencia: y el conocimiento de los mecanismos oscuros de la Red es el primer paso para no quedar atrapados ahí.
Palabras clave
Datos, informaciones, economía, sociedad en red, *deep web* [red profunda].

mamente alcun contenuto. È tuttavia piuttosto sconvolgente scoprire che il valore attribuito a quest'azienda (circa 480 miliardi di dollari) è di circa centocinquanta volte superiore a quello attribuito al quotidiano *New York Times*, che tuttavia impiega oltre 1.300 giornalisti per produrre i propri contenuti editoriali.[5]

E ancora, può meravigliare il fatto che il maggior fornitore al mondo di ospitalità non possieda neppure una stanza. Il soggetto in questione è *Airbnb*, che opera come intermediario tra chi cerca camere o appartamenti in affitto per breve tempo e privati interessati ad offrire in affitto propri spazi extra. Ebbene, il valore attribuito a questa azienda (circa 31 miliardi di dollari)[6] è di circa sei miliardi di dollari superiore a quello dell'intera catena Hilton,[7] che però possiede oltre 850.000 stanze in 5.200 alberghi in 105 Paesi del mondo.

Ed infine, tutti conosciamo *Amazon*: è la più grande azienda di commercio al dettaglio al mondo, eppure non possiede neppure un negozio; tuttavia il suo valore (stimato in oltre 500 miliardi di dollari)[8] è oltre il doppio di quello attribuito a Walmart,[9] che però possiede 12.000 negozi in 28 Paesi, impiega oltre due milioni di lavoratori, ed è in assoluto la prima azienda privata al mondo sia per volume di fatturato che per numero di dipendenti. Queste riflessioni ci fanno toccare con mano come realmente il para-

digma che regola i rapporti di potere nella società contemporanea sia profondamente mutato rispetto al passato, e l'informazione non sia più solo un bene astratto ma abbia assunto un valore concreto e monetizzabile, addirittura superiore a quello dei tradizionali *asset* industriali. E la nostra economia si fonda su tale valore molto più di quanto a prima vista si possa pensare.

2. Gli impatti non proporzionali della manipolazione dell'informazione

Se l'informazione è il nuovo valore della nostra società rimane purtuttavia un bene immateriale e, come tale, manipolabile assai più facilmente e con conseguenze assai più rilevanti rispetto alle possibilità consentite nella società industriale tradizionale. Si può ben dire che gli impatti derivanti da una attenta manipolazione di informazioni strategiche non siano proporzionali al costo della manipolazione stessa: ossia si possono ottenere effetti devastanti anche con sforzi relativamente contenuti. Ciò rende del tutto asimmetrico il rapporto di forze tra chi ha interesse a perturbare lo *status quo*, ad esempio la situazione del mercato, e chi invece lo tutela. Nel mondo dell'informazione "liquida", l'attaccante è sempre in vantaggio.

Un esempio eclatante di quanto sproporzionati possano essere gli effetti di manipolazioni apparentemente piccole si è avuto il 23 aprile 2013, quando qualcuno riuscì a compromettere l'account *Twitter* della famosa agenzia di stampa *Associated Press* e potè inviare un *tweet* fasullo. Il messaggio diceva semplicemente: «Notizia straordinaria: due esplosioni alla Casa Bianca, Barack Obama è ferito».[10] Ovviamente il messaggio scatenò la preoccupazione del mondo intero, solo però per lo spazio di un paio di minuti: quanto è bastato perché la notizia venisse smentita dalle altre agenzie e dai diretti interessati, riportando rapidamente il mondo alla normalità. Probabilmente non si trattò di nulla più che un'azione goliardica, resa possibile dalla banale compromissione di un account minore quale quello di *Twitter*, considerato evidentemente poco rilevante nel grande business dell'*Associated Press* e quindi verosimilmente protetto con poca cautela.

Nulla di fatto, si potrebbe pensare: la società dell'informazione ha reagito alla velocità della luce, ristabilendo in un attimo la verità dei fatti e riportando la calma negli osservatori e nel pubblico senza alcuna conseguenza apparente. Peccato che in quei minuti anche la Borsa di New York abbia reagito alla velocità della luce, subendo un crollo verticale di circa duecento punti: una destabilizzazione che non si era vista neppure in occasione dell'attacco alle Torri Gemelle. Come il proverbiale battito di ali di una farfalla in Brasile, che può provocare uno tsunami in Indonesia, così una piccola password violata ed un messaggio spurio di una cinquantina di caratteri hanno provocato un terremoto nella principale Borsa della nazione economicamente più solida

al mondo. Il tutto è durato solo pochi minuti, certo: un tempo breve, ma sicuramente sufficiente a qualcuno che avesse voluto o potuto sfruttare la situazione a proprio vantaggio, diventando milionario con poco sforzo.

3. L'informazione e il ciberspazio

Quando nel 1982 William Gibson[11] inventò il concetto di *cyberspace,* egli stesso non aveva la benché minima idea di cosa potesse realmente essere: d'altronde a quell'epoca Internet era ancora molto al di là da venire, e lui non possedeva neppure un computer personale. Così nella sua mente il *cyberspace* prese forma come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici... Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano [...]».[12] Insomma, un mondo "altro" fatto di informazione pura ed accessibile mediante tecniche di realtà virtuale.

Oggi viviamo in una realtà più incredibile di quella immaginata dalla fantascienza di trent'anni fa, e non ci facciamo nemmeno caso. Eppure interagiamo quotidianamente con una Rete planetaria, Internet, che non solo è onnipresente ed ubiqua, ma è addirittura considerata un bene primario ed un diritto fondamentale; abbiamo tutti in tasca un dispositivo, lo *smartphone*, che unisce in sé funzioni di telefono, calcolatore, macchina fotografica, navigatore, lettore musicale, assistente personale... e ci offre l'accesso istantaneo a qualsiasi essere umano ed a qualsiasi informazione o servizio presenti sul pianeta; e di conseguenza gran parte della nostra vita sociale e di relazione è oramai tecnomediata e si svolge nel, o attraverso il, ciberspazio.

Una conseguenza di ciò è che la quasi totalità delle informazioni e dei dati che quotidianamente produciamo, consultiamo o manipoliamo, sia riguardanti noi stessi che gli altri, nascono o finiscono, direttamente o indirettamente, in Rete. Non solo: come tanti Pollicino cibernetici, nei nostri spostamenti virtuali attraverso le maglie del ciberspazio lasciamo dietro di noi, consapevolmente o inconsapevolmente, tante lunghe scie di briciole digitali. Sono le tracce delle nostre interazioni con le persone, le cose e i sistemi con cui abbiamo avuto a che fare: si trovano nei posti più disparati, e spesso ne ignoriamo addirittura l'esistenza. Ma ogni sito che visitiamo, ogni messaggio che inviamo o riceviamo, ogni servizio di cui usufruiamo, ogni acquisto che facciamo, ogni spostamento che effettuiamo... in breve ogni azione che compiamo, ma anche la nostra sola presenza, lasciano da qualche parte il segno della loro interazione tanto con il mondo fisico quanto con quello digitale, che sono oramai compene-

trati ed integrati in questa nuova forma di realtà che è il nostro ciberspazio di tutti i giorni.

Di solito ciò è inevitabile e innocuo; molto spesso, peraltro, siamo noi stessi a disseminare spontaneamente informazioni su di noi e le nostre attività, ad esempio condividendole tramite i *social network* o gli strumenti di *microblogging*. È sicuramente intrigante e divertente interagire con gli altri in questo modo, e le generazioni più giovani lo fanno oramai costantemente come espressione della propria personalità o nuova forma di socializzazione. Non molti però sono consapevoli dei potenziali rischi, e sanno come comportarsi correttamente in modo da non correre rischi spiacevoli e soprattutto inutili.

Il fatto è che anche queste informazioni su di noi, apparentemente innocue, hanno un valore per qualcuno o addirittura si prestano ad essere sfruttate per scopi imprevisti quando non illeciti o addirittura criminosi. Possono ad esempio essere usate per tracciare le nostre abitudini, le nostre preferenze, i nostri comportamenti: nel migliore dei casi ciò ha il solo scopo di consentire alle aziende ed organizzazioni con cui interagiamo di fornirci servizi migliori, più mirati sulle nostre esigenze, e quindi più utili ed efficaci; più spesso serve a costruire il nostro profilo di consumatore, per proporci acquisti di beni o servizi tarati ad esempio sui nostri gusti, le nostre aspettative inespresse e la nostra capacità di spesa inferita; talvolta invece serve a giocare slealmente, ad esempio per stabilire il prezzo al quale venderci un prodotto o servizio, personalizzandolo al massimo rialzo stabilito accettabile in funzione dell'analisi dei nostri indicatori comportamentali.[13]

Anche i dati anonimi e aggregati, da questo punto di vista, hanno un loro preciso ed elevato valore economico. Conoscere ad esempio gli spostamenti medi o i percorsi automobilistici più usuali della popolazione di un certo quartiere, forniti abitualmente dai navigatori o dai GPS dei nostri *smartphone*, potrebbe ad esempio aiutare un'amministrazione cittadina illuminata ad ottimizzare i servizi di gestione del traffico o a pianificare meglio i trasporti pubblici su base locale; ma viceversa, conoscere i dati di attività fisica e gli indicatori dei principali parametri corporei della popolazione di una certa zona, anch'essi abitualmente forniti dagli *smartwatch* e dalle comuni applicazioni per il *fitness* ed il *jogging*, potrebbe consentire a qualche operatore senza scrupoli di differenziare su base territoriale il prezzo dei farmaci o delle polizze sanitarie per massimizzare slealmente i propri profitti.

Più semplicemente, per un operatore commerciale poter sapere che un determinato soggetto attua certi comportamenti in Rete (legge certe notizie, visita certi siti, effettua certe ricerche, compra certi prodotti, mette "mi piace" a certe pagine, ...) costituisce un enorme valore perché gli consente ad esempio di sviluppare campagne specifiche di *marketing* tagliate su misura per quel soggetto... anche ignorandone completamente l'iden-

tità! È infatti sufficiente poter attribuire con ragionevole approssimazione tali azioni ad un medesimo soggetto, pur non conoscendone le reali generalità,[14] per poter attuare i comportamenti commerciali desiderati. E magari vendere o scambiare con altri operatori le informazioni raccolte, in modo da incrociarle e completarle con quelle provenienti da altre fonti e costruire profili comportamentali sempre più precisi, e sempre riferiti a soggetti perfettamente sconosciuti.

Il paradosso insito in queste situazioni è che i dati personali anonimi o aggregati non vengono percepiti come critici dagli interessati e non sono neppure soggetti a tutela da parte della normativa sulla *privacy*; essi hanno tuttavia un loro preciso valore di mercato, e sono ancora più appetibili agli operatori rispetto ai dati personali di soggetti identificabili proprio in quanto, non ricadendo sotto la protezione della legge, non espongono ad alcun tipo di vincolo o sanzione chi dovesse utilizzarli per scopi di profilazione.

4. Il valore e i rischi dell'identità digitale

Infine bisogna sottolineare che in Rete noi non siamo ciò che siamo, ma siamo ciò che dimostriamo di essere. La nostra identità digitale non è altro che una copia di credenziali tramite le quali un sistema automatico può riconoscerci, consentendogli così di mettere a nostra disposizione le risorse che ci competono o di erogarci i servizi cui abbiamo diritto: ma chiunque conosca tali credenziali possiede di fatto la nostra identità e può dunque spacciarsi per noi, ottenendo indebiti benefici e soprattutto addossandoci la responsabilità se non addirittura la colpa delle sue azioni.

Proprio per questo, anche le informazioni relative alle identità personali hanno un valore materiale: si comprano e si vendono al mercato nero, nel cosiddetto *dark web*, ed esistono precisi listini i cui valori dipendono dal tipo di credenziale offerta e dal potenziale profitto che potrebbe ricavarne l'acquirente.

Un recente *survey* ha mostrato che le informazioni più a buon mercato sono i numeri di carte di credito, che vanno dai 5-8 dollari l'una se accompagnate dal solo codice CVV/CVV2 ai 15 dollari se fornite assieme al numero di conto corrente cui sono collegate, per arrivare intorno ai 30 dollari se corredate di tutti i dati anagrafici del titolare. Le credenziali di accesso ai servizi di pagamento *online* valgono di più, in funzione dei limiti di spesa e del saldo ad esse associati: si va da 20-50 dollari per *account* aventi saldi fino a 1.000 dollari, via via a salire fino ad arrivare a 200-300 dollari per saldi compresi fra 5.000 e 8.000 dollari.[15]

La nostra identità digitale è dunque il nostro bene più prezioso nel ciberspazio, e dovremmo tutelarla con la massima cura per evitare di incorrere in incidenti e problemi dalle conseguenze potenzialmente anche gravi. Eppure sono poche le persone che attuano anche le più semplici misure di tipo comportamentale per

proteggersi contro il rischio di compromissione delle credenziali che ci identificano in Rete.
Tutte le statistiche sono infatti da sempre concordi nel confermare che la principale fonte di incidenti informatici, sia nella sfera privata che in quella professionale, è dovuta ad una scorretta o trascurata gestione delle *password* da parte degli utenti. Adoperare una *password* banale, semplice da indovinare o da scoprire per tentativi, oppure non custodirla adeguatamente, è come lasciare la porta o la finestra di casa aperte o al massimo nascondere la chiave d'ingresso sotto lo zerbino.
Eppure non è difficile adottare una corretta igiene preventiva nella gestione delle *password*. Le regole sono semplici: sceglierle sufficientemente complicate da non poter essere facilmente indovinate, non scriverle o almeno conservarle in un luogo protetto, cambiarle frequentemente; e soprattutto non adoperare mai la stessa *password* su sistemi o account differenti, ma avere tutte *password* diverse, una per ciascun servizio. Questa diversificazione è fondamentale per limitare i danni in caso di guai: serve infatti ad evitare che, qualora un malintenzionato dovesse malauguratamente scoprire una *password*, si ritrovi automaticamente in mano in un colpo solo *tutte* le identità della propria vittima.
Certo, nel momento in cui siamo costretti a possedere ed impiegare decine di credenziali diverse (perché ogni sistema o servizio ha la sua) è difficile potersi ricordare a memoria tutte le *password*, ma occorre resistere alla tentazione di scriversele o peggio di sceglierle tutte uguali. Esistono *software* e applicazioni, anche gratuite, che fungono da "portachiavi" e consentono di memorizzare in modo sicuro su un PC o uno *smartphone* decine e decine di *password*: utilizzare uno di questi prodotti è la soluzione migliore per non correre rischi.

5. Il nostro comportamento fa la differenza

Così come per la gestione delle *password*, esistono semplici norme che ci aiutano a tenere un sano e sicuro comportamento anche negli altri aspetti della nostra vita nel ciberspazio. La parola d'ordine è sempre *consapevolezza*: conoscere i problemi ed i rischi ci aiuta a prevenirli adottando linee di condotta adeguate, proprio come facciamo nel mondo reale.
Evitare la tecnologia perché si è sfiduciosi o peggio ancora spaventati da essa è un errore, tanto quanto lo è il considerarla automaticamente perfetta adoperandola in modo acritico ed incosciente. Il problema non è la tecnologia in sé, ma l'uso che noi e gli altri ne facciamo. La tecnologia dell'informazione è oramai una parte inevitabile della nostra società e della nostra vita quotidiana: e rifiutandoci di usarla, per timore o insicurezza, ci priviamo di una enorme serie di vantaggi e comodità senza realmente diminuire i nostri potenziali rischi.
Le informazioni sono il petrolio della nostra società, e fanno gola a tanti operatori. Le informazioni personali

ancora di più, in quanto consentono di ricavare valore dal comportamento e dalle attitudini dei singoli, sia al fine di sviluppare prodotti e servizi legittimi sia per attuare azioni illegittime o veri e propri crimini. È il nostro comportamento, come sempre, a fare la differenza: e la conoscenza dei meccanismi oscuri della Rete è il primo passo per non rimanervi intrappolati.

NOTE

[1] Esperto di sicurezza cibernetica dell'Agenzia per l'Italia Digitale per lo sviluppo del CERT-PA, e componente il *Permanent Stakeholders' Group* dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione (ENISA).

[2] *Società dell'informazione*, in *Wikipedia. L'enciclopedia libera* (10 aprile 2018), in //it.wikipedia.org/w/index.php?title=Societ%C3%A0_dell%27informazione&oldid=96169994 (09-06-2018).

[3] Cf Somerville Heather, *SoftBank is now Uber's largest shareholder as deal closes*, in https://www.reuters.com/article/us-uber-softbank-tender/softbank-is-now-ubers-largest-shareholder-as-deal-closes-idUSKBN1F72WL (09-06-2018).

[4] Cf Reuters, *Hertz Global Holdings Inc (HTZ)*, in https://www.reuters.com/finance/stocks/companyProfile/HTZ (09-06-2018).

[5] Cf *Here's Why Facebook Just Gained $21 Billion in Value*, in http://fortune.com/2018/04/10/heres-why-facebook-just-gained-21-billion-in-value (09-06-2018).

[6] Cf Lauren Thomas, *Airbnb just closed a $1 billion round and became profitable in 2016*, in *CNBC* (09-03-2017), in https://www.cnbc.com/2017/03/09/airbnb-closes-1-billion-round-31-billion-valuation-profitable.html (09-06-2018).

[7] Cf *Hilton Worldwide Holdings*, in http://fortune.com/fortune500/hilton-worldwide-holdings (09-06-2018).

[8] Cf Egan Matt, *Facebook and Amazon hit $500 billion milestone*, in *CNN Money* (27-07-2017) in http://money.cnn.com/2017/07/27/investing/facebook-amazon-500-billion-bezos-zuckerberg/index.html (09-06-2018).

[9] Cf La Monica Paul R., *Amazon is worth almost twice as much as Walmart*, in *CNN Money* (04-04-2017), in http://money.cnn.com/2017/04/04/investing/amazon-stock-900-alltime-high/index.html (09-06-2018).

[10] Cf *«Attacco alla Casa Bianca, Obama ferito» La Borsa crolla, ma era un falso tweet*, in *Corriere.it* (23-03-2013), in https://www.corriere.it/esteri/13_aprile_23/usa-falso-tweet-attentato-obama_ae320698-ac40-11e2-b753-2de04ad0a16e.shtml (09-06-2018).

[11] Scrittore di fantascienza statunitense naturalizzato canadese, considerato il principale esponente della corrente letteraria *cyberpunk*.

[12] Il termine, comparso per la prima volta nel racconto di William Gibson, *Burning Chrome*, pubblicato in *Omni Magazine* nel 1982, è stato reso famoso dal romanzo, scritto dallo stesso autore, *Neuromancer*, pubblicato nel 1984.

[13] Cf Berberi Leonard, *Biglietti aerei, il prezzo dipende da un algoritmo: se compri da tablet (o dal centro città) costano di più*, in *Corriere.it* (27-20-2017), in https://www.corriere.it/cronache/17_ottobre_28/voli-se-algoritmo-ti-alza-19135ce6-bb50-11e7-8ef5-94a13146dc45.shtml (09-06-2018).

[14] Cosa che si fa ad esempio mediante i cosiddetti *cookie*, piccoli pezzi di informazione che vengono depositati nei nostri *browser* dai siti che visitiamo, al fine di tracciarne le attività di navigazione.

[15] Cf *How Much is Your Identity Worth … on the Black Market?*, in *Identity Theft Resource Center*, in https://www.idtheftcenter.org/Identity-Theft/how-much-is-your-identity-worth-on-the-black-market.html (09-06-2018).

IL FATTORE UMANO NELLA SICUREZZA INFORMATICA: IL RUOLO CHIAVE DELLA CONSAPEVOLEZZA

THE HUMAN FACTOR IN INFORMATION SECURITY: THE KEY ROLE OF UNDERSTANDING

ISABELLA CORRADINI[1]

Lo scenario digitale nel quale ci si muove è in continua evoluzione, considerato che i temi dell'Intelligenza Artificiale e dell'Internet delle Cose (*Internet of Things*, IoT) avranno uno spazio e un'attenzione sempre maggiori.
Le tecnologie digitali pervadono la vita di tutti e non possono essere considerate (almeno non più) come qualcosa di esterno all'individuo. Sarebbe in proposito opportuno evitare l'uso del termine virtuale quando si fa riferimento ai comportamenti in Rete, dal momento che le azioni sono reali al pari delle conseguenze prodotte.
La persona, ovvero il fattore umano, si muove in un continente complesso e articolato che apre almeno a tre considerazioni.
La prima è che tutti (o quasi), indipendentemente dall'età, ci troviamo immersi in una realtà che comporta tanti vantaggi ma, al contempo, espone a diversi rischi, da quelli relativi alla profilazione mediante i *Big Data*, alla gestione in sicurezza dell'identità digitale. Se è vero che le nuove generazioni saranno sempre più digitali, non per questo potranno considerarsi esenti da tali rischi.
La seconda è che la possibilità di avere tutto il mondo in tasca grazie ad uno *smartphone* rende sempre meno marcati i confini tra contesto privato e lavorativo, tranne quelli che, con molta fatica, l'essere umano riesce a mantenere.
Infine, questo scenario risulta essere molto articolato per lo sviluppo dell'IoT, dove si assiste alla fusione tra mondo fisico e virtuale. Le previsioni indicano che saranno miliardi gli oggetti dotati di sensori connessi in Rete che andranno ad influenzare diversi settori del quotidiano, dal commercio al sistema bancario, alla vita privata dell'individuo. Nel frattempo si parla già dell'Internet di tutte le cose (*Internet of Everything*, IoE).
Tuttavia, nonostante i benefici di queste tecnologie digitali, già da tempo gli esperti di sicurezza Information Technology (IT) hanno allertato sui rischi dell'IoT: la connessione tra i due mondi, infatti, e la mole di dati prodotti, costituiscono

un'attrattiva per i cybercriminali, a fronte anche di un'oggettiva impossibilità di garantire la sicurezza di tutti i dispositivi interconnessi.
Spesso, purtroppo, nel delineare le strategie di intervento, si sottovaluta l'importanza del fattore umano che, invece, se informato e formato in modo adeguato, può costituire l'elemento vincente della sicurezza di ogni organizzazione.
Il presente articolo si focalizza sull'importanza del fattore umano nella sicurezza informatica (*cybersecurity*) e sulla necessità di adottare comportamenti consapevoli nell'uso delle tecnologie digitali. Esse, infatti, non sono né buone né cattive: la differenza consiste nell'uso che ne fanno le persone.

1. Comportamenti rischiosi ed ingegneria sociale

Diversi rapporti pubblicati annualmente sulla sicurezza informatica[2] sottolineano come l'anello debole della *cybersecurity* sia rappresentato dal fattore umano. Il Rapporto 2018 sulle violazioni dei dati (*data breach*) pubblicato da Verizon,[3] ad esempio, evidenzia la necessità di continuare ad investire su programmi di formazione nelle aziende, dal momento che l'essere umano è tra le principali vulnerabilità sfruttate dai cybercriminali. Basta, infatti, che un dipendente di un'azienda cada nel tranello di una mail *phishing* per compromettere la sicurezza aziendale.
Il *phishing* è un tipo di frode *online* che consiste nell'invio di una mail esca agli utenti - generalmente fingendosi organizzazioni riconosciute - con lo scopo di indurre la vittima a fornire informazioni sensibili, come numeri di carta di credito, password, ecc. Combinando il carattere di urgenza con la naturale curiosità umana, l'utente, soprattutto in condizioni di fretta o di distrazione, viene indotto ad aprire link o allegati malevoli: nel più fortunato dei casi si tratta solo di spam, negli altri invece si scarica un malware[4] che infetta il sistema operativo. Talvolta queste mail sono molto più mirate, vale a dire che, invece di essere inviate ad una moltitudine di persone come accade nel caso del *phishing*, sono recapitate a target specifici (utenti e aziende). In questo caso si parla di messaggi di *spear phishing* e la difficoltà a riconoscerli sta nel fatto che sembrano provenire da un indirizzo conosciuto.
Nei messaggi, inoltre, si fa spesso riferimento a dettagli personali dell'utente, come ad esempio un compleanno, un acquisto effettuato di recente. Ovviamente, dietro queste attività mirate c'è spesso uno studio delle abitudini e del comportamento del soggetto target, per far sì che egli possa essere attratto dalla familiarità delle parole contenute nella mail e compiere delle azioni ad esclusivo vantaggio dell'ingegnere sociale.
Gli esempi descritti, infatti, rientrano nel campo dell'ingegneria sociale *(social engineering)* che, in sintesi, mira a sfruttare le relazioni umane per ottenere informazioni. Si tratta di una forma di *hacking* cognitivo (*cognitive hacking*),[5] ovvero un tipo di attacco

RIASSUNTO

Il presente articolo si focalizza sull'importanza del fattore umano nella sicurezza informatica (*cybersecurity*) e sulla necessità di adottare comportamenti consapevoli nell'uso delle tecnologie digitali. Esse, infatti, non sono né buone né cattive: la differenza consiste nell'uso che ne fanno le persone.

Parole chiave

Cybersecurity, ingegneria sociale, fattore umano, tecnologie digitali, *cybercrimine*, consapevolezza.

SUMMARY

The present article focuses on the importance of the human factor in information security (*cybersecurity*) and on the necessity of adopting behavior that is aware of the use of digital technology. In fact, it is neither good or bad: the difference consists in the use people make of it.

Key words

Cybersecurity, social engineering, human factor, digital technology, *cybercrime*, awareness.

RESUMEN

El presente artículo se refiere a la importancia del factor humano en la seguridad informática (*cybersecurity*) y a la necesidad de adoptar comportamientos conscientes en el uso de las tecnologías digitales. Estas no son, en sí mismas, ni buenas ni malas: la diferencia consiste en el uso que de ellas hacen las personas.

Palabras clave

Seguridad informática, ingeniería social, factor humano, tecnologías digitales, *crimen informático*, consciencia.

non tecnologico la cui riuscita è legata specificamente al cambiamento del comportamento degli utenti, indotto manipolandone la percezione. L'ingegnere sociale non ha necessariamente competenze informatiche: il suo *modus operandi* è basato soprattutto sulle sue capacità di creare empatia e di trasformare la sfiducia dell'interlocutore in fiducia.[6]

La riuscita di queste tecniche si basa sull'applicazione di principi psicologici noti nell'ambito della psicologia sociale[7] e sulle euristiche, vale a dire strategie cognitive mediante le quali le persone elaborano giudizi, prendono decisioni, senza impegnare troppe risorse mentali.

Non di rado, infatti, l'elaborazione delle informazioni avviene senza prendere in considerazione tutti i fattori della situazione. Così, ad esempio, la familiarità, la simpatia, il bisogno di aiuto diventano leve strategiche che sulle quali l'ingegnere sociale può agire nel suo esclusivo interesse. Oltre al *phishing* e alle tecniche di ingegneria sociale, ci sono poi altri

comportamenti umani che possono compromettere la sicurezza dei propri dati e di quelli dell'organizzazione nella quale si lavora. Se, ad esempio, si usano account personali invece di quelli aziendali, va da sé che si pongono questioni di sicurezza, oltre che di credibilità. Non è un caso che le aziende stanno adottando politiche sempre più stringenti riguardo l'utilizzo di dispositivi e account rigorosamente aziendali, proprio perché ad essi sono dedicate specifiche protezioni da parte dei settori IT.

C'è poi il tema della gestione delle *password*, un vero e proprio lavoro cognitivo e non certo banale, dal momento che bisogna sceglierle "robuste" e aggiornarle. E nemmeno replicarle nei molti account che si possiedono. Secondo i rapporti diffusi annualmente da Keeper Security,[8] dall'analisi di milioni di stringhe diventate pubbliche a causa di violazioni di dati (*data breach*) la *password* più diffusa continua ad essere "123456".

Nel corso degli anni, l'elenco delle *password* utilizzate più di frequente non sembra avere avuto grandi cambiamenti. Sebbene gli esperti di sicurezza segnalino come la gestione delle *password* sia un'attività di vitale importanza per la sicurezza informatica, non tutti dedicano tempo e risorse (anche cognitive) a tale compito.

2. Ossessione della condivisione e impatti sociali

Il *web* è disseminato di ami, come le mail di *phishing,* e di tracce: queste sono rappresentate da tutte le informazioni che si lasciano in Rete, che si tratti di un acquisto fatto o di notizie postate su un profilo *social*. Queste tracce raccontano di noi, di chi siamo, di cosa facciamo, di cosa preferiamo. Basti pensare alla localizzazione delle mappe di *Google* o ai *like* lasciati sui vari *social media*. Tutte queste informazioni contribuiscono alla creazione di veri e propri profili reputazionali, utilizzati con l'obiettivo di indirizzare mirate attività di marketing, che saranno sempre più gestite in modo automatico grazie ai continui progressi delle tecniche di Intelligenza Artificiale.[9]

Sotto il profilo della sicurezza, è evidente che il problema sta nei dati che si immettono e si condividono in Rete. In particolare, si osserva come ormai sui *social* viene pubblicato di tutto, dalla scelta delle vacanze ai dettagli della propria vita personale, senza porsi il problema che il pubblico della Rete, pur essendo invisibile, può essere particolarmente numeroso e con interessi diversi. C'è dunque anche chi vi trova lo strumento privilegiato per la realizzazione di attività illecite e criminose. Si pensi, ad esempio, al fenomeno della pedopornografia online, che sfrutta le foto di minori diffuse via *web*. Il desiderio di condividere i momenti felici della nascita e dei primi anni dei propri figli, purtroppo rischia di trasformarsi in un problema serio per la *privacy* e la sicurezza dei minori.

Senza contare che la condivisione di foto e video in Rete può costituire una vera e propria ossessione, al

punto che è stato coniato il termine di *sharenting.*[10]

Il problema riguarda non solo le generazioni di giovani, ma anche di adulti. Si è ormai talmente immersi nel vasto universo dei *social media* che perfino l'evento reale viene vissuto in differita: non sono pochi coloro che, invece di godersi appieno le emozioni di un concerto o di una cena tra amici, preferiscono passare il tempo a documentare tutto l'evento con *post* e *tweet*.

Catturati dal proprio *smartphone* non ci si accorge più dell'"altro"; non mancano casi di cronaca in cui, invece di prestare aiuto a persone in difficoltà, si è preferito continuare a fotografare e filmare per poi avere lo *scoop* da mettere in Rete.

Il punto focale sul quale riflettere è il paradosso del rapporto che si è instaurato con le tecnologie digitali: da un lato esse hanno cambiato il modo di lavorare e creato nuove opportunità di comunicare e socializzare; dall'altro, soprattutto per i più giovani, sembra invece che ad essere preferita sia la relazione *online* piuttosto che quella *offline* (di persona). Inoltre, va osservato che un "legame emotivo" troppo stretto con il proprio dispositivo può condurre a stati di malessere: la ricchezza degli stimoli prodotti da uno *smartphone*, infatti, può essere così assorbente da soffrirne quando si è impossibilitati ad usarlo, condizione nota con il nome di nomofobia.[11]

Tali considerazioni non devono condurre ad una demonizzazione delle tecnologie digitali, perché sono comunque portatrici di vantaggi, ma occorre essere consapevoli dei rischi ai quali un loro uso sconsiderato può esporre. Rischi che vanno ben oltre la sicurezza informatica e che riguardano prima di tutto il benessere dell'individuo e la salvaguardia delle relazioni umane.

3. Educare alla consapevolezza

Dal momento che i cittadini sono utilizzatori delle tecnologie digitali sia nel privato che in ambito lavorativo, va da sé che il tema della sicurezza informatica non può essere considerato di esclusivo interesse per i soli specialisti del campo.[12]

Le minacce evolvono, le tecnologie pure ed il problema va affrontato con un approccio olistico, se si vogliono ottenere risultati efficaci.

Di conseguenza, a parte il contributo delle soluzioni tecnologiche, indispensabili ma non risolutive, occorre adoperarsi seriamente per lo sviluppo di una cultura della sicurezza volta ad incrementare la sensibilità verso una maggiore conoscenza delle minacce informatiche: una maggiore confidenza con l'ambiente *online*, infatti, permette di comprenderne i pericoli e gestirli di conseguenza. Sviluppare la cultura della sicurezza richiede però di intervenire in modo differenziato a seconda dei destinatari, con la progettazione di attività che vanno dalla sensibilizzazione alla formazione e l'impiego di strumenti e metodologie didattiche specifici.

Nella pratica quotidiana si assiste

spesso all'utilizzo di parole sicuramente attrattive, come quella di *awareness* per indicare la consapevolezza, ma che poi devono tradursi in efficaci programmi di intervento. Ad esempio, per quanto riguarda l'ingegneria sociale, è fondamentale che le persone acquisiscano consapevolezza delle tecniche usate dai cybercriminali e sviluppino la capacità di elaborare dei punti di attenzione.[13]

In un'ottica più estesa, dal momento che l'approccio alle tecnologie digitali è sempre più precoce, è bene cominciare fin dalla scuola il percorso di educazione al loro uso consapevole. Allo scopo è possibile sviluppare progetti e programmi volti a favorire un'adeguata conoscenza del mondo digitale con cui bambini e ragazzi interagiscono.

In questa direzione si muovono alcuni interessanti progetti, tra i quali "Programma il Futuro",[14] iniziativa promossa dal MIUR (Ministero dell'Istruzione, Università e Ricerca) e realizzata dal CINI (Consorzio Interuniversitario Nazionale per l'Informatica) che ha lo scopo di diffondere lo sviluppo del *pensiero computazionale* attraverso la programmazione (*coding*) in un contesto di gioco.

Il Progetto permette di sviluppare consapevolezza sugli aspetti più scientifici e culturali dell'informatica, il cosiddetto pensiero computazionale.[15] Il messaggio di fondo, infatti, è che bisogna imparare a diventare un consumatore consapevole e responsabile delle tecnologie. In altre parole: non usare il tuo telefono solo per giocarci, programmalo!

Recentemente, per rispondere alle esigenze formative degli insegnanti, nel Progetto è stata avviata un'area didattica dedicata all'uso consapevole delle tecnologie digitali.

Una recente indagine, infatti, che ha coinvolto gli insegnanti partecipanti all'iniziativa, ha fatto emergere tre importanti aspetti:[16] il ruolo svolto da genitori e insegnanti nel favorire l'uso consapevole delle tecnologie digitali; la scarsa consapevolezza dei rischi ai quali gli studenti sono esposti (bullismo, molestie, truffe, ecc.); la necessità di promuovere iniziative formative per rafforzare la conoscenza ed il senso di responsabilità legate al loro uso.

Lavorare sulla consapevolezza è quindi necessario non solo per rispondere ai bisogni di sicurezza, ma anche perché permette di far comprendere e sfruttare appieno le tante opportunità offerte dalle tecnologie digitali, alle quali non bisogna rinunciare.

Conclusione

Lo scenario digitale è in continua evoluzione ed occorre essere in grado di cogliere tutti i benefici possibili e gestire i rischi che ne derivano.

La sicurezza informatica non può funzionare delegando alle sole tecnologie il ruolo di risolutore. Ne sono testimonianza i risultati dei vari rapporti sulla sicurezza che indicano come gli incidenti e gli attacchi informatici, con vittime più o meno illustri, siano in costante aumento e sempre più specializzati. Nell'ottica di una stra-

tegia olistica non può essere assolutamente trascurato il fattore umano, soprattutto alla luce dello sviluppo dell'Internet delle cose e dei progressi dell'Intelligenza Artificiale.
Qualunque tecnologia, infatti, anche la più avanzata, rischia di essere inefficace in mano a persone non consapevoli dei rischi e delle minacce.

NOTE

[1] Psicologa sociale esperta di fattore umano nella sicurezza, *safety, security* e *cybersecurity*, e di comunicazione aziendale. È presidente e direttore scientifico di *Themis*, Centro ricerche socio-psicologiche e criminologico-forensi e co-fondatore (con il Prof. Enrico Nardelli) del *Link&Think Research Lab*, focalizzato sugli aspetti socio-tecnici delle tecnologie dell'informazione e dell'educazione informatica (pensiero computazionale). Già docente di Psicologia sociale e di psicologia del comportamento criminale presso l'Università degli Studi dell'Aquila, insegna in corsi specialistici e master universitari, tra i quali il Master in Intelligence Economica ed il corso di perfezionamento in Security Manager presso l'Università di Roma Tor Vergata. Coordina le attività di monitoraggio, di comunicazione e dell'area "uso consapevole delle tecnologie digitali" di Programma il Futuro, progetto realizzato dal Consorzio Interuniversitario Nazionale per l'Informatica (CINI) per conto del Ministero dell'Università e della Ricerca (MIUR) con l'obiettivo di diffondere la cultura informatica nelle scuole. Autrice di numerose pubblicazioni nazionali e internazionali, cura una collana sul tema della reputazione per la casa editrice Franco Angeli.

[2] Si vedano, ad esempio, i Rapporti del CLUSIT (Associazione Italiana per la Sicurezza Informatica) in https://clusit.it/rapporto-clusit/ (22-04-2018).

[3] Cf 2018 Data Breach Investigations Report (DBIR), in https://www.verizonenterprise.com /resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf, 1-8 (22-04-2018). Nel rapporto sono stati analizzati più di 53.000 attacchi e oltre 2.000 violazioni in 65 Paesi.

[4] *Malware* indica un programma in grado di produrre danni al Pc di chi lo utilizza. In questa categoria rientra anche il *ransomware*, che impedisce alla vittima di accedere al sistema del computer se non procede al pagamento di un riscatto (*ransom*). L'attacco si diffonde soprattutto via mail, mediante un allegato (es. un documento, un'immagine).

[5] Cf Cybenko George - Giani Annarita - Thompson Paul, *Cognitive hacking: A battle for the mind,* in *Computer* 35(2002)8, 50-56.

[6] Cf Corradini Isabella - Franchina Luisa, *Ingegneria sociale: aspetti umani e tecnologici*, Roma, Edizioni Themis 2016.

[7] In particolare ci si riferisce ai sei principi di cui parla lo psicologo sociale Robert Cialdini che, applicati spesso in modo automatico ed inconscio, guidano le azioni umane. I sei principi sono: reciprocità, coerenza, simpatia, autorità, scarsità e riprova sociale. Si veda, ad esempio, Cialdini Robert B., *Le armi della persuasione. Come e perché si finisce col dire di sì*, Milano, Giunti 2005.

[8] Keeper Security è una società creatrice di software per la gestione delle password. Cf https://keepersecurity.com/it_IT/ (22-04-2018).

[9] Cf Corradini Isabella (a cura di), *Internet delle cose. Dati, sicurezza e reputazione*, Milano, Franco Angeli 2017.

[10] Termine nato dalla combinazione di *parenting* e *sharing*. Indica l'uso abituale dei *social media* da parte di genitori per condividere immagini e notizie sui propri figli, dalla nascita ai primi passi, ai compleanni, ecc. È stato introdotto nel dizionario inglese Collins. Cf https://www.collinsdictionary.com/it/dizionario/inglese/sharenting (22-04-2018).

[11] Forma di dipendenza, caratterizzata dalla paura incontrollata di rimanere sconnessi dal proprio cellulare. Il neologismo, abbreviativo di *no-mobile-phone*, è apparso nel 2008 a se-

guito di una ricerca condotta nel Regno Unito dall'Ente di ricerca YouGov.

[12] Cf Corradini Isabella, *Le buone pratiche nella cybersecurity: fattore umano ed awareness*, in *ICT Security Magazine* (2015) n.127, in https://www.ictsecuritymagazine.com/articoli/le-buone-pratiche-nella-cybersecurity-fattore-umano-ed-awareness/ (22-04-2018).

[13] Cf Id., *Human factors in hybrid threats: the need for an integrated view*, in CESMA Working Group on Hybrid Threats (Ed.), *Hybrid Cyber Warfare and the evolution of aerospace power: risks and opportunities*, I Quaderni del Cesma, Roma, Associazione Arma Aeronautica 2017, 85-96.

[14] Cf il Sito del Progetto *Programma il Futuro,* in http://www.programmailfuturo.it (22-04-2018).

[15] Sul tema si veda, ad esempio, Lodi Michael - Martini Simone - Nardelli Enrico, *Abbiamo davvero bisogno del pensiero computazionale*?, in *Mondo Digitale* (novembre 2017), in http://mondodigitale.aicanet.net/2017-5/articoli/MD72_02_abbiamo_davvero_bisogno_del_pensiero_computazionale.pdf, 1-15 (22-04-2018).

[16] Gli esiti dell'indagine, realizzata dal Centro Ricerche Themis, sono basati sull'analisi di 2.422 risposte di insegnanti di ogni ordine e scuola, con una larga rappresentanza della primaria (59% dei partecipanti). Pur avendo di fatto rilevato le percezioni degli insegnanti, va comunque osservato che molti docenti hanno una lunga esperienza di insegnamento (l'87% ha più di 10 anni di esperienza) e sono pertanto in grado di valutare e riportare in modo affidabile la situazione che vivono con i propri studenti. L'indagine è scaricabile al link https://themiscrime.com/it/attivita/ricerche/item/271-indagine-themis-sull-uso-consapevole-delle-tecnologie-digitali (22-04-2018).