Università degli Studi di Torino

Dipartimento di Giurisprudenza

Corso di Laurea Magistrale a Ciclo Unico in Giurisprudenza

LA TUTELA GIURIDICA DEI "*BIG DATA*" TRA PROPRIETÀ E ACCESSO

Relatori

Prof. Marco Ricolfi

Prof. Ugo Pagallo

Candidato

Tommaso Fia

Ai miei nonni: Beppe, Lucia, Marina e Nicola

INDICE

INTRODUZIONE

A partire dal secondo dopoguerra, le tecnologie dell'informazione e della comunicazione (*Information and Communication Technologies*, ICTs) hanno assunto una fondamentale rilevanza per il benessere dei singoli cittadini e delle organizzazioni umane. Lo sviluppo di sistemi di raccolta e archiviazione di dati sempre più efficienti ha favorito la nascita dell'economia dell'informazione, in cui i soggetti economici hanno adottato modelli di *business* basati sullo scambio di dati e informazioni[1].

A causa dei recenti progressi tecnologici, oggi il benessere delle società dei Paesi sviluppati non solo inerisce alle ICTs, ma dipende da queste: secondo alcune stime, almeno il 70% del prodotto interno lordo (PIL) di taluni Paesi sviluppati (quali il Canada, la Francia, la Germania, l'Italia, il Giappone, il Regno Unito e gli Stati Uniti d'America) dipende da beni intangibili[2]. Uno dei principali fattori che ha determinato il passaggio a una società dipendente dalle informazioni è lo sviluppo di tecnologie di sfruttamento dei dati sempre più complesse ed efficienti. Oggi, le imprese e le autorità pubbliche sono in grado di raccogliere ingenti quantità di dati in tempo reale, e, come mai in precedenza, conducono attività di raccolta, archiviazione, analisi e riutilizzo di quantità di dati umanamente incalcolabili mediante procedure altamente automatizzate (quali, ad esempio, algoritmi e sistemi di *machine learning*). L'accesso ai dati è divenuto un *asset* prezioso e strategico[3]. A tali *trends* tecnologici si fa riferimento col nome di *Big Data*. Nel presente lavoro, si cercherà di analizzare le questioni giuridiche ed economiche legate all'accesso ai *Big Data* da parte di diversi *stakeholders*, quali imprese e autorità del settore pubblico. Come si vedrà, taluni limiti all'accesso ostano alla fruizione di tali utilità da parte di una pluralità di attori economici[4].

Il primo capitolo è dedicato al fenomeno dei *Big Data* nella realtà

---

[1] J. RIFKIN, *L'era dell'accesso, La rivoluzione della new economy*, Mondadori, 2000.
[2] L. FLORIDI, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014, 4.
[3] D.L. RUBINFELD – M.S. GAL, *Access Barriers to Big Data*, in 59 *Arizona Law Review*, 2017, 342.
[4] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 339 ss.

economica. In particolare, si approfondirà il ruolo dei *Big Data* e delle tecnologie correlate (vale a dire l'Internet delle Cose e il *Cloud Computing*) negli odierni scenari economici (c.d. *data-driven innovation*, DDI).

Nel secondo capitolo ci si dilungherà sulle fasi della catena di valore dei *Big Data* (raccolta, archiviazione, analisi e utilizzo dei dati), cui corrispondono diversi sottomercati dei *Big Data*, e sui soggetti che conducono attività di sfruttamento economico di tali utilità nei diversi anelli della catena del valore (ad esempio, le piattaforme digitali e le autorità del settore pubblico). In tali sottomercati sono presenti barriere all'ingresso di diversa natura (tecnologica, giuridica ecc.) che limitano l'accesso al patrimonio digitale e determinano l'insorgere di vantaggi competitivi in capo a pochi soggetti. Fra i limiti all'accesso ai dati, se ne possono individuare principalmente due di carattere giuridico: da un lato, il diritto alla *privacy* informazionale (negli Stati Uniti) e la protezione dei dati personali (nell'Unione europea), e, dall'altro, le questioni di appartenenza riguardanti i dati non personali (*data ownership*), oggetto di recenti dibattiti nel versante europeo.

Nel terzo capitolo, si prenderanno in considerazione le questioni inerenti alla *privacy* informazionale e alla tutela dei dati personali rispettivamente nei versanti americano ed europeo. Dopo aver presentato a grandi linee i due modelli di protezione giuridica, ci si soffermerà sui problemi determinati dal trattamento di ingenti quantità di dati personali e, quindi, sulle risposte operative di ciascun ordinamento. Il primo mostra notevoli ristrettezze rispetto alle nuove sfide imposte dai *Big Data*, dal momento che le questioni relative alla *privacy* informazionale sono demandate prevalentemente a codici di autocondotta delle imprese, su cui vigila la Federal Trade Commission (FTC). Nel versante europeo invece esiste una disciplina normativa dettagliata a tutela dei dati personali, recentemente innovata dal Regolamento Generale sulla Protezione dei Dati (Regolamento (UE) 2016/679, *General Data Protection Regulation*, o "GDPR"). In tale atto normativo, il legislatore ha introdotto limiti sostanziali al trattamento dei dati personali. Fra questi, ci si concentrerà sui limiti più stringenti alla raccolta e all'uso dei dati (ad esempio, il diritto alla portabilità dei dati e il diritto alla cancellazione). Poi, si riserveranno trattazioni a parte alla questione della c.d. proprietarizzazione dei dati personali, ai recenti sviluppi in materia della c.d. *group privacy*, determinati

dall'utilizzo di tecniche di *data analytics*, e alla necessità di considerare le esternalità negative determinate dagli algoritmi.

Nel quarto e ultimo capitolo, si passeranno in rassegna i recenti dibattiti in materia di proprietarizzazione dei dati non personali, cioè non riferibili ad alcuna persona fisica, quali la quasi totalità dei dati raccolti dai sensori degli oggetti dell'Internet delle Cose nei contesti industriali. A tal proposito, la letteratura giuridico-economica parla di *data ownership*. Dal momento che la tutela accordata dai regimi di esclusiva esistenti (diritto d'autore, diritto *sui* generis sui database, segreto commerciale, tutela brevettuale, proprietà fisica) non è adeguata alla tutela di *datasets* di grandi dimensioni, secondo alcuni commentatori occorre configurare un nuovo diritto esclusivo su tali utilità. Nondimeno, sarà necessario capire se un nuovo strumento di privativa sia giustificato a livello economico, giacché la produzione di dati non personali sembra non aver bisogno di un ulteriore incentivo giuridico. Allo stato attuale delle cose, poche piattaforme digitali (quali *Google*, *Facebook*, *Amazon* e *Apple*) hanno il controllo di fatto su ingenti quantità di dati, scambiate ricorrendo allo strumento del contratto. Occorrerà capire, in ultima istanza, quali sono i campi del diritto più appropriati per garantire la condivisione delle risorse digitali fra un numero più elevato di agenti economici.

CAPITOLO PRIMO.
IL FENOMENO DEI *BIG DATA* NELLA REALTÀ ECONOMICA

Abstract

A partire dagli anni Novanta del secolo scorso, lo sviluppo notevole delle tecnologie dell'informazione e della comunicazione (ICTs) ha comportato il passaggio all'economia dell'informazione, in cui il valore di scambio delle merci è dato dal contenuto di conoscenza che esse posseggono. In seguito, dagli anni Dieci del Duemila, la diffusione delle tecnologie dei Big Data*, del* Cloud Computing *e dell'Internet delle Cose ha comportato un sostanziale aumento dell'efficienza delle attività condotte dagli agenti economici che, a vario titolo, sono ricorsi allo sfruttamento di tali ricavati tecnologici.*

1. Le informazioni come input fondamentale dell'economia digitale

A partire dagli anni Novanta del secolo scorso, lo sviluppo delle tecnologie dell'informazione e della comunicazione (*Information and Communication Technologies*, ICTs) ha avuto un impatto notevole sulle attività umane, influenzandone il progresso sociale, economico e culturale. Gli studiosi dell'economia hanno descritto il cambiamento del paradigma economico facendo riferimento principalmente a due espressioni, che condividono certi contenuti.

In prima istanza, alcuni hanno parlato di economia digitale[5] (o *new economy*), focalizzando l'attenzione sull'utilizzo massiccio, esteso a ogni settore, delle tecnologie informatiche e digitali. In particolare, l'economia digitale «*involves acquisition, processing and transformation, and distribution of information. Its three major components are the hardware (primarily computers) that processes information, the communications systems that acquire and distribute information, and the software that, with human help, serves to manage the systems*»[6].

In secundis, altri autori hanno focalizzato l'attenzione sulla nozione di economia dell'informazione (o economia informazionale). Come ha affermato Manuel Castells in una serie di saggi di grande successo[7], l'età dell'informazione è dominata da una forma di capitalismo "informazionale", in cui i modelli di *business* seguiti dalle imprese sono incentrati principalmente sull'innovazione tecnologica e sullo scambio di dati e informazioni. L'economia dell'informazione ha un carattere globale, nel senso che i suoi «*core components have the institutional, organizational, and technological capacity to work as a unit in real time, or in chosen time, on a planetary scale*»[8]. Occorre tenere presenti due connotati di tale modello. In

---

[5] Il termine "economia digitale" è stato coniato da Don Tapscott in un suo fortunato saggio. Vedasi D. TAPSCOTT, *The Digital Economy: Promise and Peril In The Age of Networked Intelligence*, McGraw-Hill, 1994.

[6] W.D. NORDHAUS, *Productivity growth and the new economy*, Brookings Papers on Economic Activity, 2002, 221 ss.

[7] Si fa riferimento alla celebre trilogia *The Information Age*, dedicata all'economia, alla società e alla cultura dell'età dell'informazione. Si vedano M. CASTELLS, *The Information Age: Economy, Society and Culture. Volume I: The Rise of the Network Society*, Wiley Blackwell, 2010; M. CASTELLS, *The Information Age: Economy, Society and Culture. Volume II: The Power of Identity*, Wiley Blackwell, 2009; M. CASTELLS, *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*, Wiley Blackwell, 2010.

[8] M. CASTELLS, *The Information Age: Economy, Society and Culture. Volume I: The Rise of the Network Society*, *op. cit.*, 202.

primo luogo, nel nuovo scenario economico, beni intangibili quali dati e informazioni assumono un'importanza fondamentale, poiché il controllo dell'accesso a queste risorse è divenuto la forma privilegiata di capitalizzazione di tali utilità[9]: il valore di scambio delle merci è dato dal contenuto di conoscenza che queste contengono[10], e dipende dalla capacità di limitarne la diffusione mediante determinati strumenti giuridici (le privative intellettuali[11]). In secondo luogo, si è verificato un graduale spostamento «*dalla vendita di beni alla vendita dell'accesso ai servizi resi da tali beni*»[12].

A partire dal secondo decennio del Duemila, l'economia dell'informazione ha raggiunto uno stadio più evoluto grazie alla diffusione delle tecnologie dei *Big Data*, per le quali si può procedere alla «*datizzazione di tutto quanto*»[13]. Oggi, autorità pubbliche e compagnie private acquisiscono, archiviano, sottopongono a procedimenti di analisi e riusano enormi quantità di dati personali e non personali per diverse finalità.

Occorre chiarificare maggiormente il concetto di *Big Data* e, in seguito, passare all'analisi di tecnologie strettamente connesse (l'Internet delle Cose e il *Cloud Computing*) e dell'impatto economico-sociale delle attività di sfruttamento dei *Big Data* (*data-driven innovation*, DDI).

---

[9] A. GORZ, *L'immateriale: Conoscenza, Valore e Capitale*, Bollati Boringhieri, 2003, 23. Si rimanda anche al fondamentale J. RIFKIN, *L'era dell'accesso, La rivoluzione della new economy*, Mondadori, 2000.

[10] Si rimanda a D. FORAY, *L'economia della conoscenza*, Il Mulino, 2006.

[11] E. RULLANI, *Le capitalisme cognitif: du déjà vu?*, in 2 *Multitudes*, 2000, 87 ss.

[12] N. LUCCHI, *Tecnologie dell'informazione e della comunicazione*, in M. DURANTE e U. PAGALLO (CUR.), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, 2012, 7.

[13] V. MAYER-SCHÖNBERGER – K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013, 130. «*Datizzare un fenomeno significa convertirlo in forma quantitativa, in modo da poterlo tabulare e analizzare*» (V. MAYER-SCHÖNBERGER – K. CUKIER, *op. cit.*, 109). L'autore approfondisce i casi della datizzazione delle parole, della posizione e delle interazioni. Il fenomeno della datizzazione su larga scala pone seri problemi epistemologici: secondo quanto affermato da Chris Anderson nel 2008 sulla rivista *Wired*, il diluvio dei dati rende il metodo scientifico obsoleto. Com'è stato opportunamente dimostrato in un recente lavoro, tale approccio induttivo ingenuo ed estremo è da evitare, giacché «*there is as yet no evidence data alone can bring about scientifically meaningful advance*» (H. HOSNI – A. VULPIANI, *Forecasting in Light of Big Data*, in *Philosophy & Technology*, 2017, 11).

2. Big Data*. Aspetti definitori, rapporto con le tecnologie dell'Internet delle Cose e del* Cloud Computing *e innovazione* data-driven

Nel gergo degli informatici, la "legge di Moore" indica che ogni diciotto mesi raddoppia la potenza dei calcolatori (calcolata sulla base del numero dei *transistors* nei circuiti integrati).

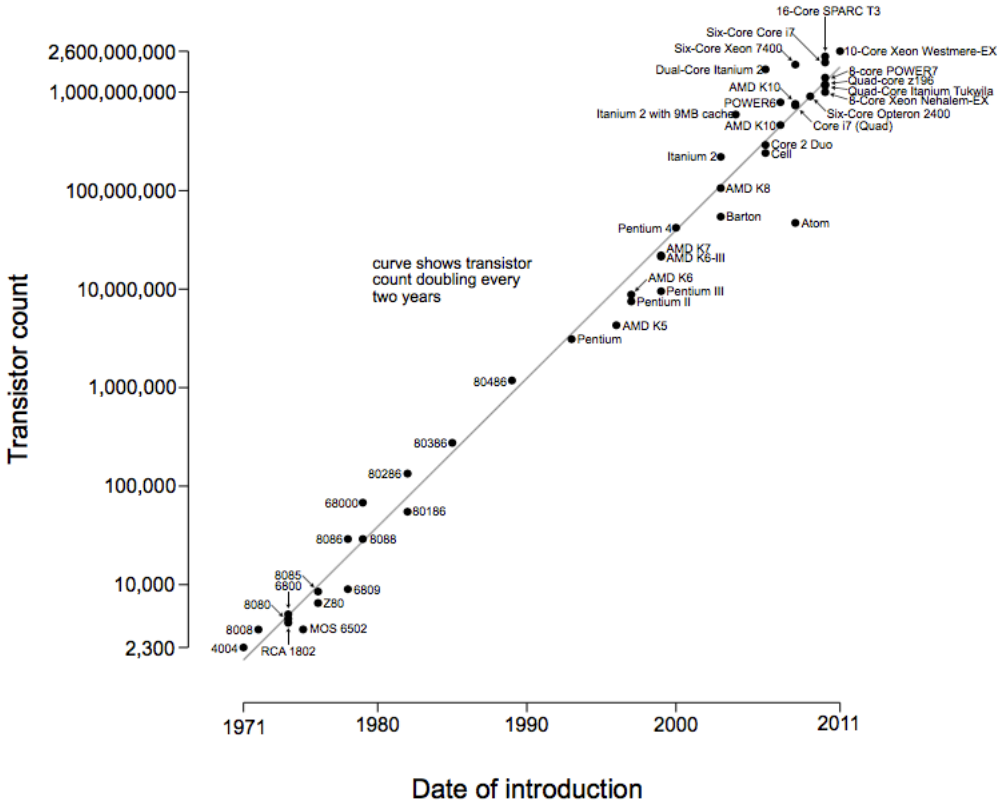

Figura 1. La Legge di Moore. Fonte: *Wikipedia.en* (http://en.wikipedia.org/wiki/Moore%27s_law, ultimo accesso 19 settembre 2017).

La crescita vertiginosa della capacità computazionale dei dispositivi elettronici comporta un aumento esponenziale della produzione di dati. Oggi esistono «*much more data than humanity has ever seen in its entire history*»[14]. Ogni giorno, infatti, sono prodotti più di 2,5 *exabytes* (EB, cioè un trilione di *bytes*, o 10^{18} *bytes*) di dati, e, nel 2015, il totale dei dati generati su scala globale si aggirava intorno

[14] L. FLORIDI, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014, 12.

agli 8 *zettabytes* (ZB, cioè un triliardo di *bytes*, o 10^{21} *bytes*[15]). In futuro, tali grandezze sono destinate a crescere in modo esponenziale.

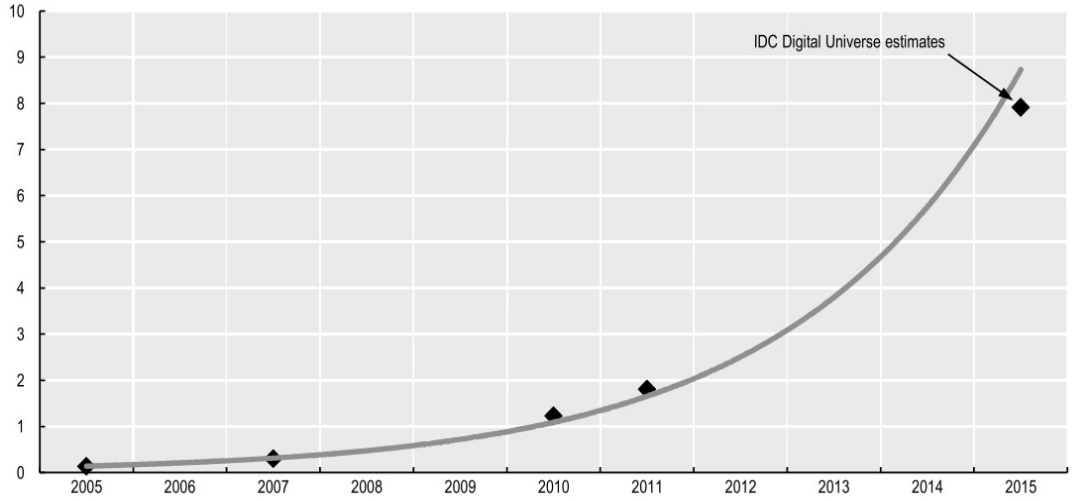

Figura 2. La quantità stimata di dati archiviati nel mondo. Fonte: OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, 2015.

Le cifre menzionate pocanzi attestano che l'umanità sta vivendo l'inizio di una rivoluzione guidata dai dati. A partire dall'ultimo decennio, numerosi soggetti economici (quali imprese e autorità del settore pubblico), a vario titolo, raccolgono quantità di dati incalcolabili alla mente umana in formato digitale, sia su *Internet* sia mediante sensori che registrano le attività della realtà delle cose fisiche[16]. A tali entità ci si riferisce con l'espressione *Big Data*. A differenza dei *datasets* tradizionali, i *Big Data* comprendono principalmente dati non strutturati che postulano l'utilizzo di procedimenti automatizzati di analisi (quali gli algoritmi e i sistemi di intelligenza artificiale) al fine di ricavare informazioni di valore. Le ingenti risorse digitali, inoltre, possono essere (ri)usate in un ampio ventaglio di contesti economici.

Taluni attenti studiosi hanno notato che, da quando il termine *Big Data* è entrato nel c.d. *hype cycle*, esso è stato accostato a molteplici nozioni a seconda della prospettiva adottata. L'ampia pluralità di definizioni, che denota un certo

[15] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being,* 2015, 20.
[16] Vedasi *infra* per la definizione di Internet delle Cose.

«*chaotic state of the art*»[17], è riconducibile a quattro gruppi distinti secondo gli elementi su cui si concentra la descrizione del fenomeno.

i. Un primo insieme di autori ha definito il fenomeno dei *Big Data* facendo riferimento alle sue caratteristiche fondamentali. Gli attributi dei *Big Data* sono le famose "V": volume (dei dati raccolti), velocità (di tecniche di produzione, raccolta e analisi), varietà (delle tipologie dei dati acquisiti[18]), veracità (o veridicità, cioè la capacità di un *dataset* di essere attendibile e privo di elementi superflui, c.d. *noise*) e valore (*id est* la capacità dei *datasets* di essere trasformati in informazioni da cui le imprese e la società in generale ricavano valore). A questi attributi se ne sono poi aggiunti altri, quali la complessità (cioè la maggiore difficoltà di ricavare informazioni di valore da *datasets* di maggiori dimensioni[19]).

ii. Un secondo gruppo di definizioni fa riferimento in via privilegiata ai ricavati tecnologici necessari alla raccolta e all'analisi di grandi quantità di dati. Secondo un *report* della *Microsoft*, l'espressione *Big Data* fa riferimento a procedimenti in cui si impiegano grandi capacità di calcolo per condurre attività su «*seriously massive and often highly complex sets of information*»[20].

iii. Un terzo gruppo di nozioni si basa sull'idea del superamento di soglie di grandezza. Per esempio, secondo Dumbill si può parlare di

---

[17] A. DE MAURO ET AL., *A formal definition of Big Data based on its essential features*, in 65(3) *Library Review*, 2016, 128. La distinzione e l'analisi dei gruppi di definizioni individuati *infra* sono basati su quest'ultimo lavoro. Nello stesso senso, Pagallo asserisce che «*Big Data remains a fuzzy concept*» (U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in 1 *European Data Protection Law Review*, 2017, 36). Come suggerisce FLORIDI, *op. cit.*, 13, vi è la tentazione, in casi del genere, di far riferimento alla descrizione della pornografia di *Justice* Potter Stewart della Corte Suprema degli Stati Uniti: «*difficult to define, but "I know when I see it"*»…

[18] Pur non menzionando esplicitamente i *Big Data*, Doug Laney ha introdotto il modello delle "3 V" (volume, velocità e varietà). Vedasi D. LANEY, *3-D data management: controlling data volume, velocity and variety*, META Group Research Note, 2001.

[19] S. SUTHAHARAN, *Big Data classification: problems and challenges in network intrusion prediction with machine learning*, in 41(4) *Performance Evaluation Review*, 2014, 70 ss.

[20] *The big bang: how the Big Data explosion is changing the world*, in *Microsoft*, 11 febbraio 2013 (http://news.microsoft.com/2013/02/11/the-big-bang-how-the-big-data-explosion-is-changing-the-world, ultimo accesso 12 settembre 2017).

Big Data se si oltrepassa la capacità di immagazzinamento e organizzazione delle tradizionali banche dati[21].

iv. Il quarto raggruppamento è di particolare interesse ai fini del presente lavoro. Si tratta delle nozioni che si basano sull'impatto della tecnologia dei *Big Data* sulla realtà sociale. Fra le altre, lo sforzo definitorio di Mayer-Schönberger e Cukier appare particolarmente rilevante. I due autori fanno notare che «*i Big Data trasformano il nostro modo di capire e di esplorare il mondo*», giacché «*la nostra comprensione sarà guidata più dall'abbondanza dei dati che dalle ipotesi*»[22]. Inoltre, «*i benefici per la società saranno innumerevoli, perché i Big Data entreranno a far parte della soluzione a problemi globali impellenti*», segnando «*una tappa importante nel processo di avvicinamento del genere umano alla quantificazione e alla comprensione del mondo*»[23].

Dalla sintesi dei vari gruppi di nozioni, De Mauro e i suoi collaboratori ricavano una nozione operativa di *Big Data*: «*Big Data is the Information asset characterised by such a High Volume, Velocity and Variety to require specific Technology and Analytical Methods for its transformation into Value*»[24].

Esaurite le questioni definitorie, occorre soffermarsi ora su ulteriori tecnologie strettamente connesse ai *Big Data*. Si tratta del *Cloud Computing* e dell'Internet delle Cose (*Internet of Things*).

Il *Cloud Computing* è un modello di fornitura di risorse informatiche basato sull'accesso «*ubiquitous, convenient, on-demand*» dei dati attraverso un *network*

---

[21] E. DUMBILL, *Making sense of Big Data*, in 1(1) *Big Data*, 2013, 1 ss.
[22] V. MAYER-SCHÖNBERGER – K. CUKIER, *op. cit.*, 99. Secondo gli autori, coi *Big Data* l'umanità può comprendere il mondo mediante l'analisi per correlazione; questo tuttavia non implica, come paventato da alcuni (C. ANDERSON, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, in *Wired*, 23 giugno 2008 (http://www.uvm.edu/~cmplxsys/wordpress/wp-content/uploads/reading-group/pdfs/2008/anderson2008.pdf, ultimo accesso 19 settembre 2017)), la fine del metodo scientifico.
[23] V. MAYER-SCHÖNBERGER – K. CUKIER, *op. cit.*, 30-31. Vedasi anche D. BOYD – K. CRAWFORD, *Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon*, in 15(5) *Information, Communication & Society*, 2012, 662 ss.
[24] A. DE MAURO ET AL., *op. cit.*, 131.

(solitamente, attraverso *Internet*[25]). La principale funzione del *Cloud Computing* è la gestione accentrata di enormi quantità di risorse digitali a potenze di calcolo elevatissime. In particolare, esso ha un impatto notevole sull'architettura delle tecnologie di immagazzinamento, poiché offre soluzioni operative efficaci per l'archiviazione "distribuita" e l'organizzazione di *datasets* di grandi dimensioni[26].

L'Internet delle Cose (o Internet degli Oggetti, *Internet of Things*, IoT) è un'evoluzione della Rete[27]. Esso si basa sull'idea di collegare oggetti del mondo reale (quali, per esempio, veicoli, *wearables*, elettrodomestici, reti elettriche, edifici…) per scambiare i dati raccolti da questi e perseguire un obiettivo comune[28]. I dispositivi dell'Internet delle Cose, muniti (*embedded*) di *software*, sensori e attuatori[29], sono in grado di produrre e comunicare quantità di dati incalcolabili alla mente umana in tempo reale[30]. A ben vedere, l'IoT si accosta alla nozione di *ubiquitous computing* di Weiser[31].

Fra il 2013 e il 2014, l'IoT si è sviluppato rapidamente grazie al crollo dei prezzi dei sensori e degli attuatori collegati alle apparecchiature, il cui costo, in quel periodo, è sceso del 40%[32]. Tuttavia, si è ancora agli inizi di un'enorme diffusione degli oggetti intelligenti: per taluni studiosi, allo stato attuale delle cose non esiste

---

[25] Vedasi, più nello specifico, P. MELL – T. GRANCE, *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology Special Publication 800-145, 2011 (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, ultimo accesso 13 settembre 2017).

[26] M. CHEN ET AL., *Big Data: Related Technologies, Challenges and Future Prospects*, Springer, 2014, 12 («*The distributed storage technology based on cloud computing allows effective management of Big Data; the parallel computing capacity by virtue of cloud computing can improve the efficiency of acquiring and analyzing Big Data*»).

[27] M. PAEZ – M. LA MARCA, *The Internet Of Things: Emerging Legal Issues For Businesses*, in 43 *Northern Kentucky Law Review*, 2016, 31 («*In sum, the IoT marks a paradigmatic departure from the Internet technology of previous decades: instead of simply facilitating human interaction through machine-to-machine communications, the IoT allows devices to measure and interact with the physical environment, gather information from that environment, and transmit that information to other devices, people, or environments*»).

[28] M. CHEN ET AL., *op. cit.*, 13.

[29] Un attuatore è la componente di un oggetto che è responsabile del movimento e del controllo di un meccanismo o di un sistema.

[30] Si rimanda all'analisi approfondita di ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 2014. Per una prospettiva sociologica, vedasi P. HOWARD, *Pax Technica. How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press, 2015.

[31] M. WEISER, *Hot Topics - Ubiquitous Computing*, in 10 *Computer*, 1993, 71 ss.

[32] J. RIFKIN, *Società a costo marginale zero*, Mondadori, 2014, 198-99.

ancora un insieme di *standard* riconducibile all'Internet delle Cose come tale[33]. Secondo alcune stime, entro il 2020, fra i venti e i trenta miliardi di dispositivi saranno connessi all' Internet delle Cose[34]; inoltre, stando a un rapporto dell'istituto statunitense McKinsey, l'IoT ha un impatto economico potenziale dai 4,9 agli 11,1 miliardi di dollari americani annui nel 2025, l'equivalente dell'11% dell'economia globale dello stesso anno[35].

Gli oggetti dell'Internet delle Cose sono impiegati in una pluralità di scenari economici, cui corrispondono le diverse tipologie di dati acquisiti dai sensori quali, fra gli altri, i dati ambientali, termici, aerei, astronomici, corporei ecc. L'Internet delle Cose è stato introdotto nella quasi totalità dei settori dell'industria e del commercio, e contribuisce ad acquisire e condividere ingenti quantità di dati in un ampio spettro di ambiti, «*dai mutamenti di prezzo dell'energia elettrica in rete al traffico logistico nelle catene di fornitura, dai flussi di produzione nelle linee di montaggio allo stato dei servizi nei front office e nei back office, fino al monitoraggio in tempo reale dei movimenti dei consumatori*»[36].

Grazie all'utilizzo dei plessi tecnologici presentati pocanzi (*Big Data*, *cloud computing* e Internet delle Cose), diversi soggetti, a vario titolo, possono aumentare l'efficienza delle proprie attività (*data-driven innovation*, DDI). Come opportunamente illustrato in un rapporto dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE), la DDI contribuisce principalmente alla crescita della produttività dei soggetti economici, al benessere dei cittadini e al progresso economico e sociale dei Paesi in via di sviluppo. Occorre soffermarsi brevemente su ciascuno di questi tre elementi.

---

[33] U. PAGALLO ET AL., *What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT*, in R. LEENES ET AL. (CUR.), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017, 61.

[34] A. NORDRUM, *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, in *IEEE Spectrum*, 18 agosto 2016 (http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, ultimo accesso 15 settembre 2017).

[35] MCKINSEY GLOBAL INSTITUTE, *The Internet of Things: Mapping the value beyond the hype*, 2015, 2 (http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx, ultimo accesso 16 settembre 2017).

[36] J. RIFKIN, *Società a costo marginale zero*, *op. cit.*, 196.

In primo luogo, l'innovazione guidata dai dati rappresenta una nuova fonte di crescita che si estende in maniera dirompente a una pluralità di settori. La DDI non riguarda solo il settore dei fornitori di servizi in rete che, come si vedrà nel prossimo capitolo, riescono a creare, indirizzare e comprendere le preferenze dei consumatori grazie all'analisi dei dati personali di costoro e a migliorare l'offerta di beni e servizi, ma anche i settori più tradizionali, quali l'agricoltura, la distribuzione e il manifatturiero. *In primis*, la DDI apporta benefici notevoli alle attività agricole, migliorandone la produttività e riducendone l'impatto ambientale. Mediante l'utilizzo di sensori collegati ai macchinari, gli imprenditori agricoli possono ridurne i tempi di inattività e ottimizzare e predire la produzione agricola[37]. *In secundis*, il settore della distribuzione beneficia delle informazioni ricavate dall'analisi dei dati raccolti mediante le c.d. "carte di fedeltà" dei propri clienti; inoltre, grazie ai dati prodotti dai sistemi di refrigerazione, i gruppi di distribuzione possono risparmiare fino a 25 milioni di dollari statunitensi all'anno di costi energetici[38]. In ultima istanza, riguardo al manifatturiero, le tendenze all'automazione delle tecnologie di produzione e allo scambio di dati sulla produzione generati dai dispositivi (c.d. Industria 4.0) sono oggetto di crescente interesse da parte delle autorità pubbliche. In questo settore, i dati prodotti dai sensori servono al monitoraggio dell'efficienza dei prodotti, all'ottimizzazione delle operazioni di assemblaggio e alla fornitura di servizi dopo la vendita (*after-sale services*), quale, per esempio, l'assistenza per la manutenzione[39].

In secondo luogo, la DDI ha un impatto notevole sul benessere dei cittadini. Infatti, se si prendono in considerazione le politiche di apertura dei dati cui le autorità pubbliche hanno accesso (i cc.dd. *open data* nel dibattito americano, o *public sector information* nel discorso giuridico europeo), emerge che la DDI incide sul benessere dei cittadini sotto due aspetti: da una parte, le politiche fondate sugli *open data* favoriscono la trasparenza e il buon andamento delle attività delle istituzioni pubbliche; dall'altra, i dati aperti favoriscono l'erogazione di molteplici servizi

---

[37] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being, op. cit.*, 28.
[38] M. VAN RIJMENAM, *Tesco and Big Data Analytics, a Recipe for Success?*, in *Datafloq*, 22 dicembre 2016 (http://datafloq.com/read/tesco-big-data-analytics-recipe-success/665, ultimo accesso 18 settembre 2017).
[39] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being, op. loc. cit.*

commerciali e sociali[40]. Inoltre, i settori della ricerca scientifica, dell'istruzione e della sanità beneficiano ampiamente della DDI, dal momento che «*they employ the largest share of people who perform work related to the collection, processing and analysis of information and data*»[41].

Infine, la DDI fornisce nuove opportunità per la crescita dei Paesi in via di sviluppo. Dall'analisi in tempo reale di *datasets* di ingenti dimensioni le istituzioni e le organizzazioni internazionali possono prevenire crisi e disastri naturali. Per esempio, l'Organizzazione delle Nazioni Unite (Onu) dall'analisi dell'uso di *Twitter* in Indonesia ha scoperto che le conversazioni degli utenti riflettono i movimenti dei prezzi del cibo, e sono utili per la gestione delle situazioni critiche di aumento vertiginoso dei prezzi[42]. Inoltre, della DDI beneficiano gli attori privati e i consumatori di quei Paesi, spesso privi delle infrastrutture pubbliche essenziali. Ad esempio, la piattaforma digitale nigeriana *Tsaboin* raccoglie i dati del traffico prodotti da chi è in viaggio per informare in tempo reale gli utenti sulle condizioni delle vie di comunicazione[43].

Terminate queste considerazioni generali, è necessario passare all'analisi approfondita dei mercati dei *Big Data* (capitolo secondo), e, successivamente, dedicarsi all'esame dei limiti all'accesso ai dati personali (capitolo terzo) e non personali (capitolo quarto).

---

[40] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being, op. cit.*, 29. Per la trattazione sul ruolo delle autorità del settore pubblico e sugli *open data*, si rimanda al § 6.1 del capitolo secondo.

[41] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being, op. loc. cit.*

[42] UN GLOBAL PULSE, *Mining Indonesian Tweets to Understand Food Price Crises*, 2014 (http://www.unglobalpulse.org/sites/default/files/Global-Pulse-Mining-Indonesian-Tweets-Food-Price-Crises%20copy.pdf, ultimo accesso 18 settembre 2017).

[43] Per maggiori informazioni, si rimanda al sito ufficiale della piattaforma: www.tsaboin.com (ultimo accesso 18 settembre 2017).

CAPITOLO SECONDO.
IL "CICLO" DEI *BIG DATA*. L'ACCESSO AI DATI NEI SOTTOMERCATI DEI *BIG DATA*

Abstract

I Big Data *sono l'*asset *fondamentale dell'economia dell'informazione. Imprese, consumatori e autorità del settore pubblico sono gli agenti economici che costituiscono il c.d. ciclo dei* Big Data *(o catena del valore), all'interno del quale sono individuate le attività che conferiscono valore ai dati: la raccolta, l'archiviazione, l'analisi e l'utilizzo dei dati. A ogni attività tipica delle fasi della catena del valore corrisponde un sottomercato dei* Big Data*, caratterizzato da qualità economiche e attori differenti. In ogni anello della catena del valore, inoltre, sono presenti limiti all'accesso ai* Big Data *più o meno insormontabili, che determinano l'insorgere di vantaggi competitivi in capo alle imprese operanti in ciascun passaggio della catena del valore. In questo capitolo saranno presi in esame i distinti* Big Data sub-markets*; in particolare, se ne analizzeranno le caratteristiche economiche e si individueranno i limiti all'accesso propri di ogni fase della catena del valore. Infine, nell'ultimo paragrafo ci si concentrerà sui soggetti coinvolti nei passaggi del* Big Data cycle.

1. Considerazioni generali

Taluni studi che hanno ad oggetto i rapporti fra *Big Data* e mercato condividono un elemento semplificatorio comune: quello di considerare il mercato dei *Big Data* un *unicum*, prescindendo da un'accurata analisi dei diversi stadi di trattamento dei dati in cui i diversi attori economici operano[44]. È certamente utile individuare la struttura del c.d. *Big Data market* nella sua interezza allo scopo di comprendere i settori economici maggiormente toccati dall'innovazione *data-driven*. Tuttavia, questa visione, da sola, può risultare riduttiva e, per certi versi, mistificatoria, in quanto non soltanto conduce a una considerazione limitata di una questione più ampia, ma è anche dannosa per i ragionamenti portati avanti sulla base di tale impostazione.

La realtà è di gran lunga più complessa. Pertanto, occorre «dare ordine al caos»[45]. Un buon punto di partenza è la ripartizione del mercato dei *Big Data* in distinti sottomercati sulla base delle operazioni che conferiscono un valore aggiunto ai dati[46]. Occorre fare alcune considerazioni generali in via preliminare, così articolate: in primo luogo, si prenderà in esame la nozione di catena del valore e lo si applicherà ai *Big Data*; in secondo luogo, si analizzeranno le funzioni che assumono i *Big Data* nei diversi stadi della catena in cui operano le imprese; infine, si individueranno le caratteristiche economiche generali dei sottomercati che sono oggetto di analisi.

Anzitutto, il concetto di catena del valore è stato teorizzato dall'economista Michael E. Porter in un fortunato saggio del 1985[47]. Com'è noto, con questa espressione gli studiosi dell'economia fanno riferimento alla sequenza delle attività strategicamente rilevanti mediante le quali l'impresa genera, nelle fasi di produzione

---

[44] In questo senso, D.L. RUBINFELD – M.S. GAL, *Access Barriers to Big Data*, in 59 *Arizona Law Review*, 2017, 344. Secondo questi insigni autori, tale semplificazione si riscontra, in particolare, nei report prodotti dalle autorità nazionali della concorrenza e da alcune autorità europee (si vedano, *inter alios*, gli studi dell'autorità *antitrust* britannica e del supervisore europeo della protezione dei dati: COMPETITION AND MARKETS AUTHORITY, *The Commercial Use of Consumer Data*, 2015, 5 ss.; EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, 2014).

[45] M. OREFICE, *I Big Data. Regole e concorrenza*, in 4 *Politica del diritto*, 2016, 702 ss.

[46] I sottomercati sono oggetto di trattazione dei paragrafi successivi.

[47] M.E. PORTER, *Competitive Advantage: creating and sustaining superior Performance*, Free Press, 1985.

del bene o erogazione del servizio gli *output* (cioè dai beni e dai servizi) che l'azienda mette a disposizione dei consumatori e delle imprese operanti sul mercato. Maggiore è il valore aggiunto conseguito in ogni "anello", maggiore è il vantaggio competitivo che l'attore economico ottiene sul mercato. La catena, in altre parole, consente di esaminare le strategie utilizzate dall'impresa per la produzione dei beni o dei servizi introdotti sul mercato, a partire da determinati fattori (*input*).

La nozione di catena del valore, pur facendo riferimento alle entità fisiche nell'elaborazione di Porter, è stata applicata anche all'ambiente virtuale delle informazioni[48]. Infatti, il loro apporto strategico muta a seconda delle differenti attività conferenti valore aggiunto alle informazioni stesse condotte da parte dell'impresa. Tali operazioni (quali, ad esempio, la raccolta, l'organizzazione, la selezione, l'analisi e l'utilizzo delle informazioni) sono collocate in una sequenza che è stata definita "catena del valore virtuale[49]".

Più recentemente, la nozione è stata ripresa dagli studiosi dell'economia per spiegare il fenomeno dei *Big Data*[50]. La letteratura parla, infatti, di "catena del valore dei dati" (*data value chain*[51]) o di "ciclo dei dati[52]". All'interno di tale catena è individuata una successione di attività che generano valore aggiunto ("anelli" o fasi): la raccolta, l'archiviazione, l'analisi e l'utilizzo dei dati[53].

---

[48] La nozione di "informazione" (semantica) indica ogni dato dotato di un significato.

[49] J. F. RAYPORT – J. J. SVIOKLA, *Exploiting the virtual value chain*, in *Harvard Business Review*, 1995, 73 ss. Un'analisi completa sul tema dell'economia dell'informazione si trova in T. WU, *An Introduction to the Law & Economics of Information*, Columbia Public Law Research Paper n. 14-399, 2016, 1 ss.

[50] Si veda E. CURRY, *The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches*, in *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, a cura di J.M. CAVANILLAS – E. CURRY – W. WAHLSTER, Springer, 2016, 31 (l'autore parla di «*value chain metaphor*»).

[51] Si vedano, *inter alios*, D.L. RUBINFELD – M.S. GAL, *op. cit.*, 339 ss.; H. GILBERT MILLER – P. MORK, *From Data to Decisions: A Value Chain for Big Data*, in 15(1) IT Professional, 2013, 57-59; E. CURRY, *op. cit.*, 29 ss.; EUROPEAN COMMISSION DIRECTORATE GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT & TECHNOLOGY (DG CONNECT), *European strategy on the data value chain*, 2013; M. OREFICE, *op. cit.*, 717-21.

[52] FTC, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, 2016, 3-5; V. BAGNOLI, *The Big Data relevant market*, in *Concorrenza e Mercato*, 23, 2016, 90-93; H. ZECH, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, in 11 *Journal of Intellectual Property Law & Practice*, 2016, 461-62.

[53] I termini utilizzati dagli studiosi per descrivere gli anelli della catena del valore sono molteplici. Il presente lavoro segue la classificazione scelta da Rubinfeld e Gal.

La raccolta consiste nell'acquisizione dei dati da parte di un soggetto. In seguito, i *datasets*, che sono ancora in uno stato grezzo (c.d. *raw data*), sono archiviati e organizzati; quindi, i *Big Data* sono analizzati mediante l'uso di algoritmi e sono combinati fra loro (c.d. *matching and pooling*); infine, il risultato di tali processi consiste in informazioni[54] che possono essere riusate dalla stessa impresa, ovvero cedute a terzi come un prodotto mediante strumenti contrattuali. L'accesso ai dati è il presupposto comune per svolgere ciascuna delle attività tipiche della catena del valore.

Il concetto di catena del valore nella versione di base prende in considerazione l'operato di una sola impresa. In realtà, le complesse relazioni degli agenti economici del *Big Data ecosystem* rendono l'esame di un solo soggetto troppo limitato. A ben vedere, per ogni anello della catena del valore è identificabile un sottomercato in cui diversi attori economici operano. Pertanto, ai fini della presente analisi, le fasi della catena sono prese in considerazione singolarmente[55]. A complicare il quadro sta il fatto che i soggetti di questi sottomercati possono operare non solo in uno di questi, ma anche in diversi stadi della catena del valore dei *Big Data*[56]: molti fra gli *stakeholders* digitali più noti – si considerino le piattaforme digitali, come *Google* e *Facebook*, soprannominati "signori dei dati[57]" – sono dediti a tutte le attività caratterizzanti il ciclo dei dati. Queste imprese raccolgono i dati (soprattutto quelli di natura personale), li analizzano mediante l'uso di avanzati algoritmi e li riutilizzano, elaborando strategie e modelli predittivi per capire i comportamenti dei consumatori, ovvero vendendo le informazioni a soggetti terzi[58].

Si può passare ora all'analisi delle funzioni che i *Big Data* ricoprono nei diversi anelli della catena. I dati attengono a una vasta pluralità di contenuti e sono utilizzabili come *input* da imprese operanti in diversi mercati del prodotto[59]. In altre

---

[54] Vedasi § 1 del capitolo primo.
[55] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 348-49; V. BAGNOLI, *op. cit.*, 90-93.
[56] V. BAGNOLI, *op. cit*., 93.
[57] A. MANTELERO, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in 1 *Diritto dell'informazione e dell'informatica*, 2012, 135; C. BUZZACCHI, *La politica europea per i* Big Data *e la logica del single market: prospettive di maggiore concorrenza?*, in 23 *Concorrenza e mercato*, 2016, 166.
[58] M. OREFICE, *op. cit.*, 718-19.
[59] «*Il mercato del prodotto rilevante comprende tutti i prodotti e/o servizi che sono considerati intercambiabili o sostituibili dal consumatore, in ragione delle caratteristiche dei prodotti, dei loro*

parole, nessun'impresa si dedica alla raccolta generica e indiscriminata di *Big Data*, poiché «*different markets often need different types of Big Data as inputs*»[60]. Ne consegue che soggetti operanti in differenti settori abbiano bisogno di diverse tipologie di dati, e che i soggetti che se ne servono come *input* non siano in concorrenza fra loro. I *Big Data*, dunque, sono un *input*, ossia un fattore produttivo necessario all'impresa per il compimento delle proprie attività economiche e utile alla produzione di beni e servizi. Tuttavia, il loro ruolo all'interno del processo economico non si esaurisce qui. Per gli attori economici operanti nel *data cycle*, infatti, i *Big Data* svolgono funzioni differenti in relazione allo stadio della catena cui sono trattati. In particolare, i dati, oltre a essere una risorsa, sono anche una tecnologia e un prodotto[61]. Queste ultime due qualità emergono soprattutto nell'ambito dell'analisi e dell'uso dei *Big Data*: le tecnologie di analisi dei dati mediante gli algoritmi, infatti, determinano l'agire del soggetto economico che li utilizza e sono funzionali alla produzione di informazioni di grande valore economico, che possono essere vendute nel mercato come un prodotto. Si pensi, per esempio, alle piattaforme digitali, che migliorano i beni e i servizi che offrono sul mercato sulla base dell'analisi dei *Big Data* acquisiti.

Il fatto che l'accesso ai *Big Data* sia un *asset* strategico per i soggetti operanti nei sottomercati individuati nelle diverse fasi catena del valore emerge ancora più chiaramente se si fa riferimento a qualche dato. Secondo un sondaggio condotto da *New Vantage Partners* fra imprese operanti in vari settori (fra cui quello finanziario e quello sanitario), il 48% dei dirigenti di azienda intervistati ha dichiarato che le imprese hanno conseguito notevoli benefici come risultato dei cambiamenti

---

prezzi e dell'uso al quale sono destinati» (Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza, G.U. n. C. 372 del 09/12/1997, par. 7).

[60] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 346.

[61] C. TANG, *The Data Industry. The Business and Economics of Information and Big Data*, Wiley & Sons, 2016, 46.

dovuti all'introduzione di tecnologie di *Big Data analytics*, mentre il 21% ha dichiarato che queste ultime hanno avuto addirittura effetti dirompenti e trasformativi[62] (*disruptive and transformational*[63]).

È necessario ancora esaminare le caratteristiche dei mercati che sono oggetto di analisi e, contestualmente, sulle implicazioni dei limiti all'accesso ai *Big Data*. Secondo il paradigma di mercato della scuola neoclassica, gli individui che compongono il processo economico si trovano in uno stato di informazione simmetrica. Tale condizione implica che i beni e i servizi siano venduti al prezzo di equilibrio, la cui entità corrisponde al punto di incontro della domanda con l'offerta. Tuttavia, queste presupposizioni non trovano adeguato riscontro nei mercati dominati dalla presenza delle tecnologie della comunicazione e dell'informazione (*ICTs*), per cui «*the rise of* Big Data […] *means that control of information is skewed towards a few players with both the concentrated data processing power and supply of* […] *data to dominate a particular sector*»[64]. Infatti, i soggetti economici che fruiscono maggiormente dei *Big Data* e delle tecnologie relative ai dati acquisiscono un notevole vantaggio competitivo nei confronti degli altri attori del medesimo mercato di riferimento, ponendo limiti all'accesso al patrimonio informativo da loro detenuto. In particolare, i soggetti operanti nei diversi anelli della catena del valore incorrono in molteplici limiti all'accesso ai *Big Data* che provocano la concentrazione del potere informativo digitale in capo a un numero limitato di soggetti[65] – si tratta, ancora una volta, delle piattaforme digitali (*Google*, *Facebook*) e delle società *leader* nel settore delle *ICTs* (*Apple*, *Microsoft*). Questa situazione si riscontra, in modo più o meno evidente, in ciascun sottomercato corri-

---

[62] NEW VANTAGE PARTNERS, *Big Data Business Impact: Achieving Business Results through Innovation and Disruption*, 2017 (www.newvantage.com/wp-content/uploads/2017/01/Big-Data-Executive-Survey-2017-Executive-Summary.pdf, ultimo accesso 14 giugno 2017).

[63] Non a caso, i *Big Data* sono annoverati fra le c.d. *disruptive technologies*.

[64] N. NEWMAN, *Search, Antitrust and the Economics of the Control of User Data*, in 30(3) *Yale Journal on Regulation*, 2014, 3-4.

[65] A. MANTELERO, *op. cit.*, 135-37. Sul tema della limitata accessibilità ai *Big Data*, vedasi *infra*. Per una prospettiva sociologica, vedasi D. BOYD – K. CRAWFORD, *Critical Questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon*, in 15(5) *Information, Communication & Society*, 2012, 662 ss.

spondente ai singoli anelli della catena del valore, e incide sul principio dell'allocazione Pareto-efficiente delle risorse, per il quale ogni attore economico può migliorare la propria posizione fino a non compromettere quella di un altro agente.

Pertanto, ogni sottomercato dei *Big Data* è esposto a disfunzioni (i c.d. "fallimenti di mercato", *market failures*) che pregiudicano la massimizzazione del benessere degli attori facenti parte del ciclo. Come si vedrà nei prossimi paragrafi, tali malfunzionamenti sono causati dalla presenza di fenomeni (invero ben noti agli studiosi della microeconomia) che determinano, a loro volta, i limiti all'accesso ai dati nei diversi passaggi della catena del valore dei *Big Data*: esternalità, asimmetrie informative e potere di mercato detenuto da un esiguo numero di imprese[66]. Oltre a questi elementi, le difficoltà delle istituzioni nazionali e internazionali di fronte a scenari economici radicalmente nuovi e la mancanza di regole adeguate a favorire l'ottimizzazione della posizione dei diversi agenti dei *Big Data submarkets* rendono il quadro più complicato e confusionario[67].

Premesse queste considerazioni generali, occorre procedere alla valutazione degli anelli della catena del valore, indicandone per ciascuno gli aspetti essenziali e soffermandosi sulle barriere all'ingresso presenti nei rispettivi sottomercati e, appunto, sui limiti all'accesso ai *Big Data*.

2. La raccolta dei dati

La raccolta dei dati (*data capture* o *data collection*[68]) costituisce la prima fase della catena del valore dei *Big Data*. Più precisamente, tale passaggio presup-

---

[66] Y. BENKLER, *Degrees of Freedom, Dimensions of Power*, in 145 *Daedalus*, 2016, 19 («*Big Data may ultimately allow a small number of companies – those large enough to control, access, and analyze sufficient data – to predicts, shape, and "nudge" the behaviors of hundreds of millions of people*»).

[67] Sulla tematica della regolamentazione dell'accesso ai *Big Data*, si vedano i capitoli successivi. Tale problematica concerne soprattutto le autorità *antitrust*, che da qualche tempo denunciano la carenza di norme e di parametri idonei a una valutazione adeguata del potere informativo in capo alle imprese. In questo senso, si vedano le soluzioni prospettate dall'autorità *antitrust* della Catalogna in un *report* del 2016 (AUTORITAT CATALANA DE LA COMPETÈNCIA, *The Data-Driven Economy. Challenges for Competition*, 2016, 32 ss.).

[68] Come già accennato, alcuni autori denominano la fase della raccolta utilizzando altra terminologia, come "acquisizione" dei dati (V. BAGNOLI, *op. cit.*, 91, 19 ss.; M. CHEN ET AL., *Big Data: Related Technologies, Challenges and Future Prospects*, Springer, 2014, 19 ss.; H. ZECH, *A Legal*

pone un altro momento: la produzione del dato, ossia la circostanza in cui quest'ultimo è generato (o prodotto) e messo a disposizione da una determinata fonte (*data source*) ad altri soggetti. Contestualmente, questi ultimi procedono all'acquisizione dei *Big Data*, che può avvenire mediante il diretto o l'indiretto intervento del soggetto produttore (*data provider*); quindi, il soggetto procede all'archiviazione (*storage*) dei dati acquisiti nei suoi sistemi di memoria.

2.1. La produzione dei dati e le principali "fonti" dei *Big Data*

Oggi, com'è noto, ingenti quantità di dati sono prodotte in diversi contesti. Questo fenomeno è stato opportunamente definito "datizzazione" (*datafication*): "datizzare" un fatto «*significa convertirlo in forma quantitativa, in modo da poterlo tabulare e analizzare*»[69]. Il costante sviluppo delle *ICTs* ha determinato, infatti, un notevole aumento del volume dei dati generati e la facilità dell'accesso a questi: secondo uno studio del 2013, il 90% dei dati allora esistenti nel mondo era stato prodotto nei due anni precedenti[70].

I *Big Data* provengono da una molteplicità di fonti (*data sources*), cioè da entità che pongono in essere il dato e lo immettono nel mercato al pari delle altre risorse. È evidente che conferire ordine al caos delle fonti è un'operazione poco agevole, poiché la produzione di dati, come già accennato, avviene su larga scala e in diversi contesti, e tocca realtà imprenditoriali di ogni settore, salvo nei casi in cui la documentazione dell'impresa sia tenuta in via manuale o in formati analogici.

Framework for a Data Economy in the European Digital Single Market: Rights to Use Data, *op. cit.*, 461).

[69] V. MAYER-SCHÖNBERGER – K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013, 109. Si veda anche H. HOSNI – A. VULPIANI, *Forecasting in Light of Big Data*, in *Philosophy & Technology*, 2017, 1 ss. e M. LYCETT, *"Datafication": making sense of (big) data in a complex world*, in 22(4) *European Journal of Information Systems*, 381–386. Per un'accezione negativa del termine, vedasi J. VAN DIJCK, *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in 12 *Surveillance and Society*, 2014, 197 ss.

[70] SINTEF, *Big Data, for better or worse: 90% of world's data generated over last two years*, in *ScienceDaily*, 22 maggio 2013 (www.sciencedaily.com/releases/2013/05/130522085217.htm, ultimo accesso 14 giugno 2017). «*It is estimated that humanity accumulated 180 EB of data between the invention of writing and 2006. Between 2006 and 2011, the total grew ten times and reached 1,600 EB. This figure is now expected to grow fourfold approximately every 3 years*» (L. FLORIDI, *Big Data and Their Epistemological Challenge*, in 25 *Philosophy and Technology*, 2012, 435).

In particolare, le *data sources* possono distinguersi sulla base della presenza o meno di un soggetto che fornisce l'accesso ai *Big Data* (*data provider*[71]). Ai fini della presente analisi, pertanto, si è scelto di esaminare la produzione dei *Big Data* facendo riferimento a una classificazione di carattere soggettivo, basata sulle peculiarità del *data provider*: le fonti si distinguono a seconda che quest'ultimo (sia esso una persona fisica o una persona giuridica) abbia personalità di diritto privato o pubblico[72]. Nel primo caso, le principali fonti dei *Big Data* cui attingono i soggetti economici comprendono i dati (in stato grezzo) direttamente o indirettamente forniti dagli utenti-consumatori in Rete, i dati interni delle imprese[73], e quelli forniti dalle imprese che vendono i dati sul mercato (c.d. *data brokers*); nel secondo caso, si tratta dei c.d. *public data*, fra i quali sono compresi gli *open data*, o *open government data* (OGD), cioè i dati raccolti e messi a disposizione dagli enti del settore pubblico per il riutilizzo anche a fini commerciali[74].

La maggior parte degli studiosi si è soffermata sui dati prodotti dalle interazioni e dalle attività degli utenti-consumatori sulle piattaforme digitali: si pensi, per esempio, alle ricerche effettuate su un motore di ricerca, al flusso di *click* (*clickstream*) a determinati contenuti digitali, alle transazioni commerciali effettuate in un dato periodo.

Consistenti quantità di dati, inoltre, sono prodotte nell'Internet delle Cose (*Internet of Things*, *IoT*[75]), il *network* che consente la trasmissione di dati mediante

---

[71] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, 2015, 71 ss.

[72] B. LUNDQVIST, *Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. The Issue of Accessing Data*, Faculty of Law, University of Stockholm Research Paper n. 1, 2016, 2; OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, op. *loc. cit.* Si veda anche, con riguardo al contesto statunitense, il report della *Federal Trade Commission* (FTC) sui *data brokers* (FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, 2014, 11 ss.).

[73] In un'accurata analisi condotta dall'IBM nel 2013, si spiega che i dati interni delle imprese (*internal data*) costituiscono la maggiore fonte di *Big Data.* «[*Internal data*] *has been collected, integrated, structured and standardized through years of enterprise resource planning, master data management, business intelligence and other related work*» (IBM INSTITUTE FOR BUSINESS VALUE, *Analytics: The real-world use of Big Data. How innovative enterprises in the midmarket extract value from uncertain data*, 2013, 8). Si veda anche M. CHEN AT AL., *op. cit.*, 19-20.

[74] Gli *open data* sono disciplinati dalla Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico (d'ora in poi: Direttiva PSI), G.U. n. L. 345 del 31/12/2003, modificata dalla Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013, G.U. n. L. 175 del 27/06/2013.

[75] «*The internet of things is only going to make Big Data gargantuan. Much of what we have is often called "dark data." Such data is unstructured, unprocessed, and not easily turned into information*»

il collegamento di oggetti dotati di sensori e attuatori[76] (quali, ad esempio, *smartphones* e veicoli). In questo caso, il soggetto acquisitore può non dipendere da un *data provider*, giacché i dati acquisiti sono prodotti e raccolti mediante le misurazioni e le rilevazioni dei dispositivi degli oggetti interconnessi: si considerino, ad esempio, i dati prodotti dai sensori delle *smart cars*, i dati di localizzazione forniti dagli *smartphones* o alle rilevazioni effettuate dalle reti elettriche "intelligenti" (*smart grids*).

2.2. L'acquisizione dei dati

Come si è visto, i *Big Data* sono prodotti in una molteplicità di contesti. Una volta che i dati sono prodotti, un soggetto che ha accesso alle fonti può procedere alla loro acquisizione. Tale processo, che avviene secondo diversi metodi, è contraddistinto da alcune delle qualità proprie dei *Big Data* (le c.d. "*Vs*"): il volume, la velocità e la varietà. L'estrazione, infatti, avviene su larga scala, *real time*, mediante algoritmi che svolgono un lavoro preliminare di "selezione" e organizzazione dei dati rilevanti per il soggetto acquisitore. La maggior parte delle imprese procede alla fase di classificazione in seguito all'archiviazione dei *datasets*[77].

Due tematiche presentano un rilievo fondamentale riguardo all'acquisizione dei dati. Da una parte, è necessario approfondire le modalità tecnologiche mediante cui il dato è raccolto; dall'altra, è opportuno soffermarsi sui soggetti interessati dalla fase di acquisizione.

Le modalità tecnologiche con cui il dato è acquisito assumono un ruolo centrale nella fase di raccolta dei dati. I metodi di estrazione dei dati, infatti, variano a seconda che la produzione del dato avvenga in Rete, in un ambiente *IoT*, ovvero *offline*.

(P. HOWARD, *Pax Technica. How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press, 2015, 140).

[76] Vedasi § 1 del capitolo primo.

[77] K. LYKO ET AL., *Big Data Acquisition*, in *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, a cura di J.M. CAVANILLAS – E. CURRY – W. WAHLSTER, Springer, 2016, 40.

Anzitutto, molti dati sono raccolti in *Internet*, nei limiti previsti dalla normativa della protezione dei dati personali[78]. L'accesso a questi dati non presenta barriere rilevanti: si tratta, infatti, di dati ricavabili dalle imprese e accessibili al pubblico. Com'è noto, i consumatori-utenti delle piattaforme digitali generano ingenti quantità di dati in Rete secondo varie modalità: si pensi, per esempio, all'utente che si iscrive a un *social network* o acquista un prodotto su un sito di *e-commerce*. A partire dal secondo decennio del Duemila, l'accesso degli utenti a *Internet* si è consolidato notevolmente grazie alla diffusione capillare degli *smarphones*[79]. Presi singolarmente, tali dati possiedono un valore limitato, ma, a seguito della raccolta, dell'accumulo in quantità consistenti e della combinazione con altri dati (c.d. *matching and pooling*), assumono un maggior valore. La raccolta è svolta principalmente mediante i *log files*, che registrano le attività degli utenti e sono prodotti automaticamente dalla fonte di produzione, oppure mediante i c.d. *web crawlers*, programmi che consentono la registrazione e l'indicizzazione di pagine *web*. Finanche l'accesso alle banche dati delle pubbliche amministrazioni avviene *online*, attraverso i portali presenti sui siti *web* delle stesse[80].

In secondo luogo, ingenti quantità di dati sono acquisite mediante l'utilizzo di oggetti interconnessi a una rete (c.d. *Internet of Things*, *IoT*). Tali dati, che sono di diverso genere (si tratta di dati geografici, ambientali, o generati dagli elettrodomestici *smart*, o ancora mediante tecnologie *wearable*[81]) sono raccolte in tempo reale e si riferiscono a coordinate spazio-temporali precise[82]. Come già accennato,

---

[78] Si considerino le prescrizioni imposte dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora in poi: Regolamento (UE) 2016/679), G.U. n. L. 119/1 del 4/5/2016. I limiti giuridici all'acquisizione dei *Big Data* sono oggetto di trattazione dei capitoli terzo e quarto.

[79] Y. BENKLER, *op. cit.*, 21 («*By the middle of 2014, Internet access by smartphone had surpassed Internet access from desktops and laptops*»).

[80] A. MANTELERO, op. cit., 136.

[81] A. MEOLA, *Wearable technology and IoT wearable devices*, in *Business Insider*, 19 dicembre 2016 (www.businessinsider.com/wearable-technology-iot-devices-2016-8?IR=T, ultimo accesso 8 giugno 2017).

[82] M. CHEN ET AL., *op. cit.*, 21. I dati riferiti allo spazio e al tempo di acquisizione del dato stesso sono detti "metadati".

i dati prodotti nell'Internet delle Cose sono raccolti mediante sensori, che trasformano le rilevazioni effettuate in entità digitali[83]. Si pensi, per esempio, ai dati prodotti da una *smart car*, alla localizzazione effettuata da uno *smartphone*, alle temperature acquisite dal termostato di sistema di riscaldamento centralizzato.

Infine, alcuni dati sono raccolti *offline* in vari modi: si pensi ai sondaggi e ai "programmi fedeltà" (*loyalty programs*) dei supermercati[84].

Dall'analisi condotta fino a questo punto, si deduce che consumatori e imprese possano essere parte integrante della catena del valore dei dati, giacché essi da un lato possono essere coloro cui il dato si riferisce, dall'altro i soggetti che producono il dato[85]. Pertanto, si è scelto di distinguere le tipologie di raccolta dei dati secondo la presenza e il grado di intervento del *data provider* (individuale o collettivo) nell'acquisizione del dato stesso[86]. Un soggetto può essere coinvolto direttamente nella raccolta, ovvero essere presente indirettamente, o del tutto assente. Occorre analizzare ciascuna delle tre ipotesi.

In primo luogo, alcuni dati sono posti in essere e messi a disposizione direttamente da una persona fisica, che li fornisce per accedere a determinati prodotti o servizi: si tratta dei c.d. *volunteered data*. Si pensi, per esempio, ai commenti a un *post* su un *social network*, alle foto o i video caricati su una piattaforma digitale, alle preferenze e ai gusti indicati su una *chat* di incontri.

In secundis, altri dati sono raccolti indirettamente, cioè senza la volontaria immissione dell'utente cui si riferiscono. Tali dati derivano dall'osservazione e dalla registrazione delle sue azioni in Rete (*observed data*) mediante i *log files*, e, com'è noto, rivestono un ruolo fondamentale nella comprensione dei comportamenti dei consumatori: le imprese li utilizzano per fornire a questi ultimi messaggi

---

[83] M. CHEN ET AL., *op. cit*., 23-25.
[84] FEDERAL TRADE COMMISSION, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, 2016, 4.
[85] H. ZECH, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, *op. cit.*, 461-62. Per la trattazione sui soggetti coinvolti negli anelli della catena, vedasi § 2.6.
[86] V. BAGNOLI, *op. cit.*, 91; G. COLANGELO, *Big Data, piattaforme digitali e antitrust*, in *Mercato concorrenza regole*, 3*,* 2016, 427. La letteratura si è soffermata principalmente sui dati prodotti dai soggetti individuali in Rete, al cui accesso il legislatore europeo si è preoccupato di ergere barriere di natura giuridica, soprattutto per conferire tutela adeguata al diritto alla *privacy*. Si rimanda al capitolo terzo per la trattazione di questo genere di limiti.

pubblicitari di prodotti di loro interesse e di migliorare la qualità dei servizi. Si considerino, per esempio, i dati di accesso a determinate pagine *web* e il numero di acquisti di album di genere musicale affine su uno negozio di musica *online*. I *volunteered data* e gli *observed data* che si riferiscono a una persona fisica sono denominati "dati personali" e sono sottoposti alla disciplina europea della protezione dei dati[87]. Il soggetto interessato, pur non perdendone la disponibilità, ne perde il controllo nel momento in cui li immette sul web[88].

In terzo luogo, altri dati sono acquisiti senza la presenza di un soggetto che li produce: si tratta dei dati ricavati dai sensori degli oggetti interconnessi negli ambienti *IoT* (*machine-generated data*). Tale tipologia di dati può riferirsi a una persona fisica: si pensi, per esempio, ai dati di localizzazione di uno *smartphone* o alle informazioni raccolte dal sensore di un termostato collegato alla Rete di un'abitazione privata. In queste ipotesi, i dati sono riconducibili a un determinato soggetto individuale, e godono della tutela accordata dal Regolamento (UE) 2016/679[89]. Tuttavia, i dati raccolti nell'*IoT* possono non riguardare alcun soggetto individuale. Si considerino le rilevazioni digitali effettuate da un termometro digitale (collegato a un *network*) collocato in una via pubblica. In questo caso, le informazioni non sono riferibili ad alcuna persona e non ricadono nel campo di applicazione delle norme del Regolamento (UE) 2016/679[90].

2.2.1. L'accessibilità dei dati e i suoi limiti

Alcuni autori affermano che il mercato dell'acquisizione dei *Big Data* sia caratterizzato dalla scarsità di barriere all'ingresso derivanti da limiti all'accesso di carattere tecnologico[91]. Questa considerazione si basa su tre ragioni. Anzitutto, i

---

[87] Secondo la terminologia del diritto derivato dell'Ue, il soggetto in questione è denominato "interessato". Si veda l'art. 4 par. I del Regolamento (UE) 2016/679.

[88] Secondo M. OREFICE, *op. cit.*, 718, il soggetto «*ne perde immediatamente la disponibilità, nel momento stesso in cui li produce, immettendoli sul web*». In realtà l'utente non perde la disponibilità dei suoi dati, in quanto può comunque accedere alle sue informazioni.

[89] Si rimanda al capitolo terzo.

[90] Si rimanda al capitolo quarto.

[91] In questo senso, *inter alios*, D. S. TUCKER – H. B. WELLFORD, *op. cit.*, 1 ss.; D. SOKOL – R. COMERFORD, *Does Antitrust Have A Role to Play in Regulating Big Data?*, in *Cambridge Handbook of Antitrust, Intellectual Property and High Tech*, a cura di R.D. BLAIR – D. SOKOL, Cambridge University Press, in corso di pubblicazione; A. LERNER, *The Role of "Big Data" in Online Platform*

dati sono *assets* tendenzialmente non rivali[92], nel senso che l'acquisizione di un *dataset* da parte di un'impresa non ne pregiudica la successiva raccolta da parte di un altro agente economico. Il carattere di non-rivalità dei dati è ulteriormente valorizzato dalla diffusione pervasiva delle informazioni dei consumatori, che disseminano le loro "tracce" su *Internet* allo scopo di accedere ai servizi digitali offerti da diversi *providers* (*multihoming*)[93].

In seconda istanza, la notevole espansione del numero delle fonti dei *Big Data* implica un aumento proporzionale dei dati prodotti. Dunque, si ritiene comunemente che i dati possano essere ricavati dappertutto (c.d. "ubiquità" dei dati[94]). Inoltre, l'aumento del numero delle *sources* comporta che una consistente quantità di questi possa ricavarsi da fonti alternative che forniscono le medesime informazioni. Ne consegue che la maggior parte dei dati è annoverabile nella categoria dei beni succedanei. Si pensi, per esempio, ai dati meteorologici provenienti da due *data providers* diversi: a fronte del rifiuto da parte di un soggetto, un'impresa può avere accesso alle rilevazioni analoghe effettuate da un altro *provider*. Pertanto, quando il costo dell'acquisizione di dati provenienti da fonti alternative è pari o vicino allo zero, non vi è alcuna barriera all'ingresso nel mercato.

Infine, le tecnologie di acquisizione dei dati non richiedono costi elevati per le imprese di maggiori dimensioni, che «*raccolgono i dati come un sottoprodotto di altre attività produttive*»[95].

Queste considerazioni sono poco rilevanti rispetto al tema dell'accessibilità dei dati se sono prese in esame singolarmente, e possono far presumere un accesso

---

Competition, in *Online Platform Competition*, SSRN library, 2014, 20 ss. (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780, ultimo accesso 3 giugno 2017). *Contra*, fra gli altri, D.L. RUBINFELD – M.S. GAL, *op. cit.*, 1 ss., M.E. STUCKE – A.P. GRUNES, *Big Data and Competition Policy*, Oxford University Press, 2016.

[92] La non rivalità e la non escludibilità sono le caratteristiche fondamentali dei c.d. beni pubblici (*public goods*). I dati sono perlopiù beni non rivali, ma escludibili, poiché un soggetto può esserne escluso dalla fruizione ponendo limiti al loro accesso (vd. *supra*, § 1.1, e *infra*; N.P. SCHEPP – A. WAMBACH, *On Big Data and Its Relevance for Market Power Assessment*, in 7(2) *Journal of European Competition & Practice*, 2016, 121; W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, Macie Discussion Paper n. 3, 2016, 10-11).

[93] G. COLANGELO, *op. cit.*, 429; AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *Competition Law and Data*, 2015, 36-37 (*report* congiunto delle autorità *antitrust* francese e tedesca).

[94] In questo senso, D.S. TUCKER – H.B. WELLFORD, *Big Mistakes Regarding Big Data*, in *The Antitrust Source*, 2014, 2.

[95] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 346 e 377; D. S. TUCKER – H. B. WELLFORD, *op. cit.*, 3.

indiscriminato ai *Big Data* da parte di ogni agente economico. L'accesso da parte di numerosi attori, tuttavia, non trova adeguato riscontro nella realtà empirica. Infatti, «*se i* data *non avessero un valore strategico e fossero accessibili facilmente e a buon prezzo, mal si comprenderebbe la corsa delle imprese ad accumularne il più possibile attraverso un numero crescente sia di acquisizioni* Big Data related *sia di servizi offerti agli utenti a prezzi nulli*»[96]. In altre parole, è pur vero che i dati sono beni tendenzialmente non rivali, ma questo non impedisce che siano caratterizzati anche dalla non escludibilità, alla stregua dei c.d. beni pubblici puri, poiché un soggetto può esserne escluso dal godimento mediante una serie di limiti all'accesso. I *newcomers*, infatti, fronteggiano difficoltà notevoli allorché tentano l'ingresso nel sottomercato rilevante, in quanto devono intraprendere significativi investimenti per raccogliere una quantità di dati tale da poter competere con gli ingombranti *incumbents* (le grandi piattaforme digitali e i motori di ricerca), che detengono un notevole potere di mercato[97]. Chiaramente, questi ultimi non hanno un sufficiente incentivo a condividere i dati in loro possesso (*data sharing*), giacché questo significherebbe perdere parte del vantaggio competitivo acquisito mediante la raccolta diretta dei *Big Data* su larga scala.

Le limitazioni all'accesso e il potere di mercato sono parzialmente affievoliti dalle attività economiche di soggetti intermediari, come i *data brokers*, che si procurano e rivendono i dati sul mercato. L'accesso indiretto ai dati forniti dai *brokers* è meno costoso, poiché i costi di raccolta sono distribuiti fra un numero più elevato di imprese[98]. Pertanto, il modello di organizzazione preferito dagli agenti economici che solitamente non detengono un elevato vantaggio competitivo, *id est* le piccole e medie imprese (PMI), è il mercato (opzione *buy*), e non la gerarchia (opzione *make*[99]). Tuttavia, il contributo dei *data brokers* risulta insufficiente ri-

---

[96] G. COLANGELO, *op. cit.*, 432.
[97] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. cit.*, 38.
[98] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. cit.*, 39 («*a company may buy from the data broker only the data that it needs in terms of volumes and variety without incurring a large fixed cost*»).
[99] COMMISSIONE EUROPEA*, Final Commission Working Staff Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 12-13 («*The number of organizations and companies seeking to sell their data or purchase new data sets from others to provide new business models and additional revenue streams is expected to increase exponentially. The growing*

spetto alle attività di raccolta diretta, condotte su larga scala, da parte degli *incumbents*, giacché le informazioni acquisite da questi ultimi difficilmente possono surrogarsi con altre raccolte in via diretta[100]. Inoltre, per la maggior parte degli agenti economici, il *data sharing* presenta più costi che benefici, poiché i costi degli investimenti sopportati dai *data brokers* per la raccolta di dati di elevata qualità sono in seguito trasferiti sui loro clienti, che devono pagare un prezzo comunque elevato per accedere ai dati[101].

I limiti all'accesso dei dati presenti nel mercato della raccolta sono essenzialmente di due tipologie: limiti tecnologici – quali l'unicità dei dati, le esternalità di rete, le economie di scala, di gamma e di velocità e i mercati multiversante – e limiti giuridici – di cui ci si occuperà nei capitoli terzo e quarto del presente lavoro.

2.2.2. L'"unicità" dei dati (*data uniqueness*)

Come spiegato *supra*, i dati sono beni tendenzialmente non rivali e, in presenza di numerose fonti, succedanei, poiché possono essere facilmente sostituiti da dati analoghi provenienti da fonti alternative.

Nondimeno, alcuni dati sono considerati "unici" (*unique*), giacché possono essere raccolti solo in determinati punti di accesso o in precise circostanze temporali, per cui la loro replicabilità risulta difficile o impossibile. Si pensi, per esempio, alla rilevazione analitica del comportamento dei consumatori condotta da un *social network* sulla base dei *posts* ivi pubblicati, o alla raccolta dei dati geografici prima dell'accadimento di un disastro ambientale.

---

number of data marketplaces […] *will give organizations, in particular smaller ones who have data sets to sell, additional routes to market as well as easier billing and subscription mechanisms*»). Vedasi pure O.E. WILLIAMSON, *Markets and Hierarchies: Analysis and Antitrust Implications*, Free Press, 1975; G. WALKER – D. WEBER, *A Transaction Cost Approach to Make-or-Buy Decisions*, in 29(3) *Administrative Science Quarterly*, 1984, 373 ss.; R.M. GRANT, *Toward a knowledge-based theory of the firm*, in 17 *Strategic Management Journal*, 109 ss.

[100] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. cit.*, 39-40.

[101] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 198 («*The provision of high-quality data can require significant up-front investments. These costs can sometimes exceed the private benefits expected from data sharing, and thus present a barrier to data sharing*»).

Lo sviluppo economico di determinate zone geografiche, inoltre, incide sulla tipologia di dati raccolti in tali scenari[102]. In alcuni Paesi dell'Africa equatoriale e dell'Asia meridionale, infatti, le principali fonti di dati sono costituite dai telefoni cellulari; i computer, invece, sono poco utilizzati dalle popolazioni locali, e l'acquisizione di informazioni mediante l'utilizzo di elaboratori è più contenuta. Non a caso la maggior parte delle imprese di questi Paesi tiene i documenti e le scritture in forma analogica. In una siffatta situazione, i dati in questione sono difficilmente sostituibili da dati provenienti da altre fonti, anche per la scarsità di quelle alternative[103].

2.2.3. Esternalità di rete

Le esternalità di rete caratterizzano la domanda di alcune tipologie particolari di beni e servizi. Queste occorrono quando la quantità del bene (o del servizio) acquistato da un consumatore dipende dal numero di altri compratori che hanno comprato lo stesso bene o servizio. Se la domanda del bene o del servizio aumenta al crescere del numero di consumatori che l'hanno comprato, l'esternalità è positiva; viceversa, se la domanda aumenta quando meno consumatori hanno comprato il bene, l'esternalità è negativa. I servizi offerti da un operatore di telefonia mobile sono un chiaro esempio di domanda condizionata dalla presenza del primo tipo[104].

Le esternalità di rete positive sono la cifra distintiva della domanda della maggior parte dei servizi condotti *online*, e, più specificamente, delle attività svolte dalle piattaforme digitali (*Facebook*, *LinkedIn*, *WhatsApp*[105]): al crescere del nu-

---

[102] Si rimanda al § 2 del capitolo primo.
[103] La letteratura non ha ancora affrontato in maniera sistematica il tema dell'"unicità" di alcune tipologie di dati. Il contributo più significativo in questo senso è di D.L. RUBINFELD – M.S. GAL, *op. cit.*, 350-51.
[104] Per una trattazione analitica sulle esternalità di rete, si veda D. BESANKO – R.R. BRAEUTIGAM, *Microeconomics*, Wiley & Sons, 2014, 186 ss.
[105] M.E. STUCKE – A.P. GRUNES, *op. cit.*, 164 («*So if your family and friends use WhatsApp to text, you will more likely use WhatsApp as well. Likewise, as more people join the social network Facebook, it becomes easier to connect and communicate with friends and acquaintances (and befriend others). Thus, Facebook and WhatsApp both enjoy traditional network effects, whereby one's utility from the product increases as others use the product*»).

mero degli utenti connessi e della popolarità di tali siti, la domanda dei servizi offerti conosce un aumento notevole (c.d. effetto "carrozzone", *bandwagon effect*[106]). Esse, inoltre, rappresentano un'elevata barriera all'entrata (dal lato della domanda) per i *newcomers* nel mercato di riferimento, poiché il benessere del consumatore non è legato esclusivamente a scelte idiosincratiche, bensì al comportamento congiunto degli altri utenti. I costi per superare tale barriera all'entrata potrebbero essere insormontabili soprattutto per gli agenti economici di minori dimensioni e popolarità.

Le esternalità di rete di cui si è detto finora dipendono dal comportamento degli utenti, ma non presentano nulla di nuovo rispetto alle ipotesi "tradizionali" (si pensi, per esempio, all'operatore telefonico sopra citato) e sono scarsamente influenzate dall'accesso ai *Big Data* da parte di un agente economico[107].

Nei mercati digitali si riscontrano finanche particolari esternalità di rete *data-driven*. Queste si verificano quando la qualità e la quantità dei dati e l'efficienza degli algoritmi incidono sulla qualità del prodotto (c.d. *positive feedback loop*[108]). In altri termini, s'inserisce un elemento nuovo nella definizione-base di esternalità di rete: le preferenze del consumatore non dipendono direttamente dal numero di utenti che utilizzano il medesimo servizio, bensì dalla qualità di quest'ultimo, a sua volta influenzata dalla quantità di dati acquisiti dall'impresa e dall'utilizzo di algoritmi efficaci ("*learning by doing*" e *trial and error*[109]). Per comprendere meglio la portata di queste ipotesi, si pensi alle attività dei motori di ricerca. Il

---

[106] D. BESANKO – R.R. BRAEUTIGAM, *op. cit.*, 187-88; W.W. FU ET AL., *The bandwagon effect on participation in and use of a social networking site*, in 17(5) *First Monday*, 2012 (http://firstmonday.org/ojs/index.php/fm/article/view/3971/3207#author, ultimo accesso 1° giugno 2017).

[107] In questo caso, i *Big Data* assumono un ruolo fondamentale nella comprensione del successo del bene o del servizio presso determinate categorie di consumatori mediante l'uso di correlazioni. Per esempio, i dati personali raccolti da un *social network* potrebbero essere fondamentali per capire la crescita del numero di profili di consumatori di un determinato orientamento sessuale.

[108] G. COLANGELO, *op. cit.*, 435-36 («*Maggiori sono le informazioni sulle caratteristiche della domanda e dell'offerta, più efficiente risulterà il servizio offerto dal* matchmaker *e, dunque, più numerosi saranno gli utenti attratti dalla piattaforma e, a sua volta, maggiore sarà il volume complessivo di informazioni che questi ultimi rilasceranno alla piattaforma e, di conseguenza, maggiore sarà la qualità dei servizi offerti dai providers*»); nello stesso senso, M.E. STUCKE – A.P. GRUNES, *op. cit.*, 170 ss., N.P. SCHEPP – A. WAMBACH, *op. cit.*, 121.

[109] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. cit.*, 38 («*In such context data collection and exploitation could possibly also reinforce network effects, when an increase in a firm's user share enables it to collect more data than its competitors, leading to higher quality*

successo di un *search engine* è strettamente connesso alla capacità di suggerire agli utenti i risultati più cliccati, generati mediante la raccolta dei dati delle ricerche più effettuate e l'utilizzo di algoritmi che classificano i risultati in base alle maggiori probabilità di ricerca da parte degli utenti. Si consideri, per esempio, un gruppo musicale di nome "La Teiera di Russell". Qualora tale formazione avesse successo, le ricerche degli utenti che si riferiscono a quest'ultima aumenterebbero in modo esponenziale; di conseguenza, nelle ricerche future, il *search engine* anteporrebbe i risultati inerenti alla *band* a quelli riguardanti la metafora filosofica omonima[110]. Tuttavia, se un numero esiguo di utenti utilizza un motore di ricerca, la raccolta di dati aggiornati e la classificazione dei risultati più probabili mediante gli algoritmi risultano precluse a quest'ultimo. All'agente economico in questione, quindi, risulterebbe molto difficile competere con le altre imprese presenti nel mercato di riferimento, dovendo fronteggiare notevoli costi per contrastare tali esternalità *data-driven*.

Altre esternalità di rete *data-driven* occorrono in presenza di molteplici servizi offerti dalla medesima piattaforma e di una pluralità di punti di interazione fra l'utente e il soggetto raccoglitore dei dati. Si pensi, per esempio, al caso di *Google*: i dati non provengono solo dai risultati della ricerca, ma anche dagli account di posta elettronica degli utenti (*Gmail*) e dalle visualizzazioni dei video pubblicati su *YouTube*[111].

Ci s'interroga sui fattori che consentono il superamento di tale barriera all'ingresso. È chiaro che, per competere sul mercato, l'impresa minore si accolla il costo di acquisizione dei dati mediante altre fonti; inoltre, l'"altezza" delle barriere dipende dalle caratteristiche dei mercati di riferimento, che possono cambiare notevolmente l'uno dall'altro[112].

---

products or services and to further increases in market shares»). Per la trattazione sugli algoritmi, si veda *infra*, § 2.4.2.

[110] Nello stesso senso, AUTORITAT CATALANA DE LA COMPETÈNCIA, *op. cit.*, 11-12.

[111] AUTORITAT CATALANA DE LA COMPETÈNCIA, *op. loc. cit.*

[112] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 356.

2.2.4. Economie di scala, di gamma e di velocità

Le economie di scala, di gamma e di velocità, a differenza delle esternalità di rete, si pongono sul lato dell'offerta (*supply side*), ma, al pari delle esternalità, si riscontrano tipicamente nei mercati monopolistici e oligopolistici. Se molto estese, infatti, esse costituiscono una notevole barriera all'ingresso nel mercato di riferimento[113].

In particolare, un'impresa raggiunge economie di scala quando il costo medio di produzione diminuisce al crescere della quantità offerta (*output*[114]); in altri termini, il costo marginale (cioè il costo necessario alla produzione di un'altra unità del bene) è pari o prossimo allo zero. Le economie di gamma, invece, caratterizzano le imprese che producono diverse tipologie di beni, e, in particolare, occorrono quando il costo necessario per produrre una data quantità di due beni nella medesima impresa è minore del costo necessario alla produzione della stessa quantità in due imprese specializzate nella produzione di uno solo dei beni[115]. Col concetto di economie di velocità (*economies of speed*), teorizzato dallo storico dell'economia Alfred Chandler[116], si fa riferimento all'aumento della produzione del bene o del servizio che si verifica al crescere del volume e della velocità del *throughput*, cioè del flusso di risorse in una infrastruttura[117].

Le economie di scala riguardano l'acquisizione dei *Big Data* "in orizzontale", dal momento che ineriscono alla quantità dei dati raccolti; le economie di gamma, invece, concernono l'estrazione di dati "in verticale", giacché ciò che conta è l'entità dei dati acquisiti per ciascuna persona. Come si deduce facilmente, le economie di scala, di gamma e di velocità si riferiscono rispettivamente a tre delle caratteristiche tipiche dei *Big Data* (c.d. *Vs*) che contribuiscono a determinarne il valore: il volume, la varietà e la velocità. Infatti, maggiore è il volume (o la varietà,

---

[113] N.P. SCHEPP – A. WAMBACH, *op. cit.*, 121. In particolare, «*a monopolist that owes its existence to economies of scale is sometimes called a natural monopoly*» (R. COOTER – T. ULEN, *Law & Economics*, Addison-Wesley, 2012, 29).
[114] D. BESANKO – R.R. BRAEUTIGAM, *op. cit.*, 300 ss.
[115] D. BESANKO – R.R. BRAEUTIGAM, *op. cit.*, 314 ss.
[116] In particolare, si rimanda a A.D. CHANDLER, JR., *The Visible Hand. The Managerial Revolution in American Business*, Harvard University Press, 1977, e A.D. CHANDLER, JR., *Scale and Scope. The Dynamics of Industrial Capitalism*, Harvard University Press, 1990.
[117] A.D. CHANDLER, *The Visible Hand*, *op. cit.*, 281.

o la velocità) raggiunto, maggiore è l'estensione dell'economia di scala (o di gamma, o di velocità) determinata, e, quindi, maggiore è il vantaggio competitivo raggiunto rispetto agli altri agenti economici[118].

Benché non sia stata accertata con esattezza la portata delle economie di scala e di gamma nel mercato della raccolta dei *Big Data*, numerosi fattori ne rendono probabile la presenza. L'estensione di tali caratteristiche economiche dipende in larga misura dalla tipologia del servizio offerto, e richiede, pertanto, una valutazione *in concreto*[119]. Generalmente le imprese sopportano solo i costi fissi necessari al mantenimento dell'infrastruttura di acquisizione dei dati, che aumentano a seconda della pluralità di fonti a disposizione dell'impresa. Tali costi, quindi, aumentano quando l'attore economico usufruisce di dati generati dagli oggetti dell'Internet delle Cose[120]. L'attività di raccolta dei *Big Data* in sé comporta costi marginali assai bassi[121].

Alle economie di scala e di gamma corrispondono rendimenti di scala e di gamma crescenti (*increasing returns to scale and scope*)[122]. Da un lato, infatti, la raccolta di una maggiore quantità di dati consente notevoli miglioramenti dei servizi offerti dall'impresa, e, di conseguenza, comporta la creazione di un circolo virtuoso, nel quale ai miglioramenti dei servizi *data-driven* dell'impresa corrisponde una maggiore diffusione di questi ultimi fra gli utenti, e, quindi, l'acquisizione di un volume maggiore di dati[123]; dall'altro, la raccolta di dati di diverso genere, provenienti da svariate fonti, permette all'impresa un notevole vantaggio competitivo rispetto alle altre. Mediante le attività di *matching and pooling* e l'offerta di servizi di diverso genere, infatti, l'agente economico costruisce «*even more detailed profiles about its users that were not possible with each single service*»[124].

---

[118] N.P. SCHEPP – A. WAMBACH, *op. loc. cit.* («*Generally speaking, the more data a company can combine, the better its chances to gain knowledge that can be used to strengthen its market position*»).
[119] N.P. SCHEPP – A. WAMBACH, *op. cit.*, 121.
[120] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 352.
[121] AUTORITÉ DE LA CONCURRENCE - BUNDESKARTELLAMT, *op. cit.*, 49.
[122] «*The concept of returns to scale tells us the percentage increase in output when a firm increases all of its input quantities by a given percentage amount*» (D. BESANKO – R.R. BRAEUTIGAM, *op. cit.*, 234)
[123] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being: Interim Synthesis Report*, 2014, 29.
[124] OCSE, *op. loc. cit.*

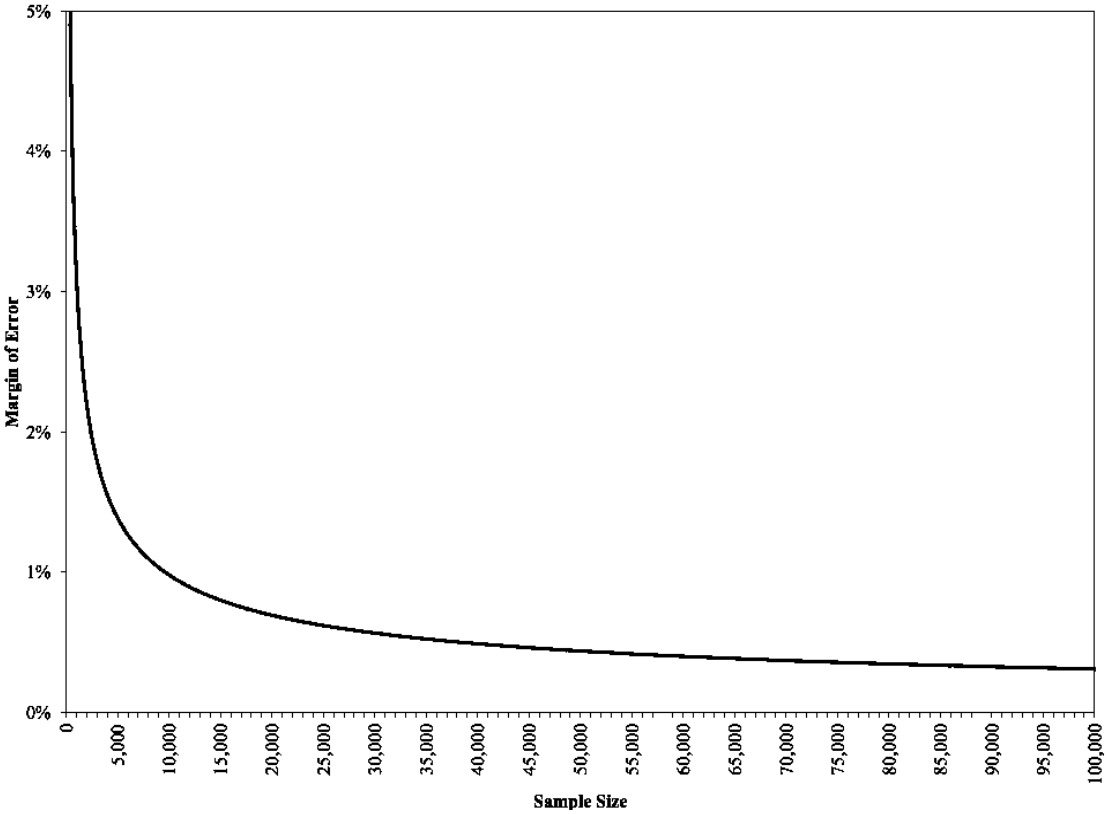

Figura 3. Errore di campionamento e rendimenti di scala decrescenti. Fonte: A. LERNER, *op. cit.*, 36.

Il vantaggio competitivo determinato dalle economie di scala e di gamma incontra tuttavia taluni limiti. Anzitutto, i benefici derivanti dalle economie di scala sono attenuati dall'insorgere di rendimenti di scala decrescenti. In seguito alla raccolta di una quantità notevole di dati, il valore marginale dei dati ulteriormente acquisiti diminuisce notevolmente, soprattutto qualora le informazioni siano utilizzate per generare *insights*[125]. La progressiva diminuzione del valore marginale è simile a quella tipica dell'errore di campionamento in statistica (Figura 1), per il quale il tasso di diminuzione cala al crescere dei soggetti intervistati in un sondaggio[126].

Un altro fattore che riduce la consistenza delle barriere all'entrata determinate dalle economie di scala e di gamma è la perdita del valore dei dati nel tempo (c.d. obsolescenza[127]). È chiaro che, sebbene un'impresa abbia acquisito una consistente quantità di dati, i *datasets* non aggiornati e riferiti a un determinato momento

[125] Per gli algoritmi e i modelli di analisi, si veda *infra.*
[126] A. LERNER, *op. cit.*, 35 ss.; AUTORITÉ DE LA CONCURRENCE - BUNDESKARTELLAMT, *op. cit.*, 48.
[127] AUTORITÉ DE LA CONCURRENCE - BUNDESKARTELLAMT, *op. cit.*, 49.

della realtà storica perdono il loro valore dopo un certo intervallo temporale. Tale considerazione vale soprattutto per talune tipologie di *Big Data*: si pensi, per esempio, ai dati relativi alle domande (*queries*) più frequentemente immesse nei motori di ricerca, il cui accumulo risulta vantaggioso a un'impresa se svolto più velocemente rispetto ad altri agenti economici (si è in presenza, quindi, di *economies of speed*). Al contrario, sono soggetti a obsolescenza in misura minore i c.d. *historical data* e alcuni dati personali (per esempio, informazioni sul nome, sul genere, sull'orientamento sessuale di una persona[128]).

Come si è visto, un soggetto economico può raggiungere economie di scala e di gamma sulla base del volume e della varietà dei *Big Data* cui accede. Può accadere, tuttavia, che l'accesso a dati in quantità elevate e di diverso genere non consenta all'impresa di pervenire ai vantaggi sperati, bensì che questa incorra in talune conseguenze indesiderate, secondo previsioni e risultati derivanti da dati che risultano essere devianti: l'acquisizione di dati insignificanti rispetto all'obiettivo di ricerca può portare a gravi distorsioni dei risultati dell'analisi. Ne consegue che l'impresa abbia interesse ad accedere a dati il più possibile privi di elementi fuorvianti o irrilevanti. L'entità della barriera all'ingresso determinata dalle economie di scala e di gamma, dunque, è limitata da un'altra caratteristica dei *Big Data*: la veridicità (o veracità, *veracity*), cioè l'attitudine di un *dataset* a essere attendibile e privo di informazioni superflue (c.d. *noise*). Più i dati sono accurati, maggiore è il valore che l'impresa è in grado di estrarre: «*the ability to collect and process highly topical data might be of higher importance than the sole size of a dataset that might also include outdated data*»[129]. Questa perizia svolge un ruolo fondamentale soprattutto per agenti economici che necessitano di dati costantemente aggiornati: si pensi, per esempio, al *targeted advertising*.

In conclusione, le economie di scala, di gamma e di velocità possono porre ostacoli notevoli all'entrata di potenziali *newcomers*. L'accumulo di grandi quantità di dati, tuttavia, non causa necessariamente un *first-mover advantage*. Questa con-

---

[128] Una persona fisica può decidere di rettificare il proprio sesso, di modificare il proprio orientamento sessuale o di cambiare il nome. Tali situazioni, tuttavia, si verificano meno spesso.
[129] N.P, SCHEPP – A. WAMBACH, *op. cit.*, 122.

siderazione trova conferma nella realtà empirica. Celebri, in questo senso, la superiorità di *Google* e *Yahoo!* rispetto al motore di ricerca *AltaVista* (acquisito nel 2003 dal secondo e chiuso definitivamente dieci anni dopo[130]), il rimpiazzamento di *MySpace* con *Facebook* come principale piattaforma digitale[131], o la progressiva perdita di terreno di *Snapchat*, *social* di condivisione di fotografie e video, a vantaggio di *Instagram*, in seguito all'introduzione di opzioni di condivisione di fotografie e video simili a quelle del primo[132]. Tale argomento è spesso utilizzato dagli autori per dimostrare la sostanziale assenza di barriere all'entrata nel mercato della raccolta dei dati, che sarebbe caratterizzato, al contrario, da una "concorrenza dinamica[133]". A parere di chi scrive, tuttavia, sussistono più elementi che fanno propendere per la tesi contraria. Anzitutto, la presenza di economie di scala e di gamma rappresenta solo uno degli elementi che determinano le barriere all'ingresso nel relativo mercato: i *newcomers*, infatti, devono fronteggiare spese di diversa natura per competere con le imprese maggiori, quali «*research and development expenses, tangible assets to operate it, marketing expenses to make the service known by its potential users etc.*»[134]. In secondo luogo, le caratteristiche del mercato sono notevolmente mutate rispetto ai primi anni del Duemila, quando non esisteva ancora una molteplicità di servizi *online* personalizzati e basati sulle preferenze e sui gusti del singolo consumatore. Per questo motivo, «*it remains to be assessed to which extent the importance of data in developing new services is higher today than a few years ago*»[135]. Il fallimento dell'esperienza del *social network Google+* è una conferma empirica di questo fattore. In terzo luogo, sussiste la marcata tendenza delle

---

[130] J. ROSSITER, *Keeping our Focus on What's Next*, in *Yahoo! Tumblr.com*, 28 giugno 2013 (http://yahoo.tumblr.com/post/54125001066/keeping-our-focus-on-whats-next, ultimo accesso 19 giugno 2017).
[131] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 354.
[132] *Le Storie di Instagram crescono e Snapchat accusa il colpo*, Wired.it, 31 gennaio 2017 (https://www.wired.it/internet/social-network/2017/01/31/storie-snapchat-instagram, ultimo accesso 3 giugno 2017).
[133] D.S. TUCKER – H.B. WELLFORD, *op. cit.* parlano addirittura di «*tremendous amount of entry and rapid gains often enjoyed by innovative new challengers*». Analogamente, la Commissione, nell'analisi della concentrazione *Facebook-WhatsApp*, ha ritenuto che «*consumer communications apps are a fast-moving sector, where customers' switching costs and barriers to entry/expansion are low*» (COMMISSIONE EUROPEA, 3 ottobre 2014, caso n. COMP/M.7217 – *Facebook/Whatsapp*, par. 132).
[134] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. cit.*, 30.
[135] AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *op. loc. cit.*

imprese di maggiori dimensioni ad acquisire i promettenti *newcomers* che operano in settori specifici, al fine di prevenire un'eventuale perdita del vantaggio competitivo acquisito in precedenza e diversificare i servizi offerti: si pensi, per esempio, alla fusione *Facebook/WhatsApp*, avvenuta nel 2014, e all'acquisizione della società britannica di intelligenza artificiale *Deep Mind* da parte di *Google* dello stesso anno[136].

2.2.5. Mercati multiversante (*multi-sided markets*) ed esternalità di rete indirette

L'acquisizione dei dati incontra ulteriori limiti a causa della complessità della struttura di taluni mercati, per i quali sono fondamentali i concetti di *multi-sided platforms* e *multi-sided markets*[137].

Alcune imprese operano come piattaforme multi-versante (*multi-sided platforms*), cioè generano valore promuovendo e agevolando i rapporti commerciali fra due (o più) gruppi di agenti economici. In altri termini, tali soggetti agiscono come intermediari (o *matchmakers*[138]), costituendo un luogo di incontro comune (*marketplace*) che consente un abbattimento notevole dei costi transattivi[139]. I mercati in cui operano queste piattaforme sono denominati mercati multi-versante, o *multi-sided markets*. Nei mercati della *old economy*, le piattaforme multi-versante erano diffuse soprattutto nei settori basati su *media* finanziati mediante pubblicità (si pensi, per esempio, ai giornali, alla televisione e alla radio, in cui interagiscono i

---

[136] S. GIBBS, *Google buys UK artificial intelligence startup Deepmind for £400m*, in *The Guardian*, 27 gennaio 2014 (www.theguardian.com/technology/2014/jan/27/google-acquires-uk-artificial-intelligence-startup-deepmind, ultimo accesso 19 giugno 2017). Si rimanda alle considerazioni svolte nel § 7.1 del capitolo quarto.
[137] Lo studio cui si deve il maggior contributo in materia è J.C. ROCHET – J. TIROLE, *Platform Competition in Two-Sided Markets*, in 1 *Journal of European Economic Association*, 2003, 990 ss. Si vedano anche, *inter alios*, M. RYSMAN, *The Economics of Two-sided Markets*, in 23(3) *Journal Of Economic Perspectives*, 2009, 125 ss. e M. ARMSTRONG, *Competition in Two-Sided Markets*, in 37(3) *Rand Journal Of Economics*, 2006, 668 ss.
[138] G. COLANGELO, *op. cit.*, 434.
[139] R.H. COASE, *The Nature of the Firm,* in 4(16) *Economica, New Series*, 1937, 386 ss.

consumatori e gli inserzionisti[140]). In seguito, i mercati multiversante hanno conosciuto una rapida diffusione in contesti digitali a causa del successo di *social network* e siti di *e-commerce* (*Facebook*, *Amazon* ecc.).

Occorre distinguere due tipologie di *multi-sided markets*. Anzitutto, alcune imprese realizzano luoghi d'incontro virtuale in forza del modello di *business* adottato, dando luogo a mercati multiversante molto simili a quelli tipici dell'economia tradizionale. *Amazon* e *eBay* sono un ottimo esempio di questo tipo di *marketplace*. Queste imprese, infatti, consentono le interazioni e favoriscono le transazioni di due categorie di agenti economici: venditori e compratori. Anche *Apple* opera come intermediario fra una pluralità di soggetti, costituendo diversi luoghi di incontro: si consideri l'*iTunes Store*, in cui artisti e imprese di distribuzione possono offrire i propri lavori discografici (album, brani musicali, *videoclip* ecc.) ai consumatori, e l'*App Store*, dove gli sviluppatori vendono le applicazioni agli utenti.

In secondo luogo, altri soggetti costituiscono piattaforme multiversante mediante la cessione dei dati di un gruppo di agenti economici all'altro. In questa categoria di piattaforme *multi-sided* rientrano *Facebook*, *Google*, *LinkedIn* e *Spotify*, che forniscono «*online services to consumers while (re-)using consumer data to provide marketing services to third parties*»[141]. I dati degli utenti sono particolarmente vantaggiosi per gli inserzionisti, che li utilizzano per intercettare le preferenze e i comportamenti dei primi e, sulla base di questi, migliorare le strategie di *marketing* individuando contenuti pubblicitari mirati per ciascun consumatore (c.d. pubblicità comportamentale, o *behavioural targeting*).

La piattaforma, inoltre, stabilisce prezzi differenti alle categorie che ne fanno parte[142]. Agli utenti, infatti, sono offerti servizi in via gratuita; agli inserzionisti, viceversa, «*viene applicata una tariffa per gli spazi pubblicitari messi a disposizione per il* behavioural targeting»[143].

---

[140] AUTORITAT CATALANA DE LA COMPETÈNCIA, *op. cit.*, 10; D.S. EVANS – R. SCHMALENSEE, *Markets with Two-Sided Platforms*, in 1 *Issues In Competition Law And Policy*, 2008, 667.
[141] OCSE, *Data-driven Innovation for Growth and Well-being: Interim Synthesis Report*, *op. cit.*, 27.
[142] Si tratta, quindi, di prezzi asimmetrici.
[143] G. COLANGELO, *op. cit.*, 435.

Le caratteristiche di questa tipologia di piattaforme hanno una serie di implicazioni in tema di accesso ai *Big Data*. Anzitutto, emerge con evidenza la tendenziale assenza di rivalità dei dati: da un lato, le informazioni dei consumatori sono utili alla piattaforma per personalizzare e migliorare i servizi offerti, dall'altro costituiscono un *input* essenziale per le attività degli inserzionisti. In secondo luogo, i mercati multiversante sono caratterizzati dalla presenza massiva di esternalità di rete positive indirette (*indirect network externalities*[144]), cioè di *spill-overs* che coinvolgono i soggetti di ciascun versante della piattaforma. I benefici riguardanti i soggetti di un versante, inoltre, dipendono non solo dal numero degli utenti dell'altro versante, ma anche dalla quantità e dalla varietà dei dati raccolti – si tratta, quindi, di esternalità *data driven*[145].

Secondo certi autori, i *multi-sided markets* della raccolta dei dati dei consumatori sono contraddistinti dalla presenza di elevate barriere all'ingresso, che favoriscono la concentrazione del potere di mercato in capo a un numero ristretto di agenti economici (c.d. *tipping*)[146]. Gli utenti-consumatori, pertanto, contribuiscono indirettamente a erigerle, preferendo certi servizi ad altri secondo parametri di scelta personali[147].

Tuttavia, secondo un'altra parte della letteratura, le interazioni fra diversi gruppi delle piattaforme multiversante non hanno come conseguenza necessaria la presenza di esternalità di rete indirette e l'innalzamento di barriere all'ingresso al mercato della raccolta dei *Big Data*. Questa considerazione è giustificata da una serie di ragioni, alcune riguardanti la categoria degli inserzionisti, altre concernenti gli utenti. Anzitutto, il prezzo imposto agli inserzionisti pubblicitari varia a seconda del numero di *click* sull'inserzione. Perciò, nelle piattaforme più grandi, il gruppo

---

[144] Per la trattazione sulle esternalità di rete, vedasi § 2.2.2.3.
[145] Vedasi *supra*, § 2.2.2.4. Per una trattazione completa sul tema delle esternalità di rete indirette nelle piattaforme digitali, vedasi M. MAGGIOLINO, *Concorrenza e piattaforme: tra tradizione e novità*, in *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, a cura di G. COLANGELO – V. FALCE, Il Mulino, 2017, 53 ss.
[146] COMPETITION AND MARKETS AUTHORITY, *op. cit.*, 80; G. COLANGELO, *op. cit.*, 436.
[147] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 358 («*Their choice of which products and services to use is affected by a combination of parameters, including users' (mis)information regarding the quality and price of competing goods or services from which the data are collected, switching costs, and (mis)information or (in)difference about the indirect price they pay in terms of lost privacy, in objectification, in the right to be forgotten, or in the erection of entry barriers*»).

degli inserzionisti ottiene non solo maggiori benefici, ma anche costi proporzionalmente più alti, derivanti, appunto, dal maggior numero di *click* degli utenti[148]. I costi delle inserzioni, inoltre, aumentano a causa della scarsità degli spazi dedicati a contenuti pubblicitari sui siti. In secondo luogo, la presenza di un elevato numero di concorrenti potrebbe determinare la propensione di taluni inserzionisti a evitare le piattaforme più grandi, rendendo più appetibile l'attività in siti minori e limitando, quindi, la portata delle esternalità di rete indirette (c.d. effetto *congestion*[149]). Per comprendere meglio il funzionamento dell'effetto *congestion*, si pensi al caso di un bar per *single* (c.d. *single bar*) eterosessuali. Qualora un numero elevato di uomini *single* frequentasse il bar, molti clienti maschi potrebbero essere poco inclini a recarsi al locale, giacché la concorrenza nel "fare colpo" sulle donne presenti sarebbe maggiore. Allo stesso modo, «*having a greater number of rivals advertising on a given web site may make that site a less desirable place to advertise*»[150], dal momento che gli inserzionisti competono per conquistare l'attenzione dei visitatori del sito. Per le ragioni appena esposte, gli inserzionisti sono incentivati al c.d. *multihoming*, cioè a promuovere campagne pubblicitarie in contemporanea su diverse piattaforme digitali; questa pratica, peraltro, è ulteriormente rafforzata dai bassi costi di trasferimento dei dati da un sito all'altro.

Anche il gruppo degli utenti sembra essere influenzato dalle esternalità di rete indirette in maniera poco rilevante. La maggior parte dei consumatori preferisce piattaforme dotate di un numero ristretto di spazi pubblicitari. Pertanto, il *newcomer* che offre il medesimo servizio in una piattaforma priva di un numero eccessivo di annunci pubblicitari è tendenzialmente preferito all'*incumbent* che, viceversa, è tempestato di *ads*. Anzi, la pervasiva diffusione di *software opensource* ed estensioni dei *browser* che bloccano il caricamento di contenuti pubblicitari sui siti visitati dall'utente (c.d. *adblockers*; si pensi, per esempio, ad *Adblock Plus*[151] o *Ghostery*) comporta l'assenza totale di *spill-overs* fra i gruppi di agenti delle piattaforme. I consumatori, infatti, ritengono le inserzioni inopportune o fastidiose se

---

[148] M. ARMSTRONG, *op. cit.*, 669; A. LERNER, *op. cit.*, 58.
[149] A. LERNER, *op. cit.*, 59. La presenza di numerosi concorrenti provoca, quindi, un'esternalità negativa che riguarda solo il gruppo degli inserzionisti (*single-sided externality*).
[150] A. LERNER, *op. loc. cit.*
[151] www.adblockplus.org (ultimo accesso 5 giugno 2017).

non consentono una navigazione efficiente o non sono di loro interesse. Queste cautele sono state recepite dalle piattaforme, che hanno elaborato linee guida e *policies* allo scopo di limitare le turbative e le molestie a danno degli utenti. Per esempio, *Google*, aderendo all'iniziativa promossa da talune imprese *online Coalition for Better Ads*[152], ha annunciato lo sviluppo di un *software*, operativo dal 2018, che opera come un "filtro" delle inserzioni più importune agli utenti[153] (si pensi alle pubblicità che provocano l'apertura di *pop-up* e finestre del *browser*). La diffusione di iniziative di tal genere riduce notevolmente la presenza delle esternalità di rete indirette nelle piattaforme più utilizzate.

In conclusione, dall'analisi condotta emerge che le esternalità di rete indirette costituiscono una barriera all'ingresso la cui entità è controversa.

3. L'archiviazione dei dati

Nella catena del valore dei *Big Data*, alla fase dell'acquisizione segue quella dell'archiviazione (*storage*), che consiste nell'immagazzinamento e nell'organizzazione (*sorting*) dei *datasets*.

L'ordinamento dei dati non è solo l'attività più importante svolta dagli elaboratori, ma anche una delle ragioni per cui i *computer* sono nati[154]. Com'è intuibile, l'organizzazione, effettuata su larga scala mediante l'utilizzo di algoritmi, serve a rendere intellegibili i dati raccolti: «*sorting is* […] *key to the human experience of information*»[155]. In altre parole, in assenza di un ordinamento efficiente sarebbe impossibile utilizzare le informazioni acquisite.

---

[152] «*Leading international trade associations and companies involved in online media formed the Coalition for Better Ads to improve consumers' experience with online advertising. The Coalition for Better Ads will leverage consumer insights and cross-industry expertise to develop and implement new global standards for online advertising that address consumer expectations*» (www.betterads.org, ultimo accesso 6 giugno 2017).

[153] G. SLOANE, *New Google Ad Filter Frightens Some Publishers and Ad Tech Players*, in *AdvertisingAge*, 5 giugno 2017 (www.adage.com/article/digital/google-ad-blocker-frightens-publishers/309252, ultimo accesso 6 giugno 2017).

[154] B. CHRISTIAN – T. GRIFFITHS, *Algorithms to live by*, William Collins (ebook), 2016 («*Sorting is at the very heart of what computers do. In fact, in many ways it was sorting that brought the computer into being*»). Per una trattazione completa e divertente del tema dell'archiviazione, vedasi il cap. III del lavoro appena citato.

[155] B. CHRISTIAN – T. GRIFFITHS, *op. cit.*

L'immagazzinamento comporta costi notevoli. Al contrario di quanto visto per la raccolta, infatti, grandi quantità di dati sono foriere di elevati costi di archiviazione. Nel gergo degli economisti, si parla di diseconomie di scala[156]. Fino a qualche decennio fa, tali costi, uniti al modesto sviluppo tecnologico di sistemi efficienti di archiviazione, precludevano le attività di immagazzinamento alla maggior parte dei soggetti economici, compresi quelli di maggiori dimensioni. Solo le istituzioni pubbliche erano dedite all'attività di accumulo di informazioni relative ai cittadini: si pensi, per esempio, ai *databases* delle amministrazioni pubbliche.

L'avvento dei *Big Data* ha segnato un notevole cambiamento di rotta sotto almeno tre aspetti: i primi due concernono l'archiviazione dei *datasets*, il terzo riguarda l'attività di organizzazione. In primo luogo, con la riduzione notevole dei costi di immagazzinamento delle informazioni[157] e la riduzione delle dimensioni dei sistemi di memoria è caduto il monopolio dei soggetti pubblici in tale attività a vantaggio delle imprese, che hanno rapidamente intuito le potenzialità economiche inerenti allo sfruttamento dei dati.

In secondo luogo, i *Big Data* hanno richiesto un notevole superamento delle tradizionali tecnologie di archiviazione, fondate su sistemi di gestione dei dati relazionali (RDBMS)[158]. Se fino a qualche tempo fa i costi di immagazzinamento impedivano l'entrata nel sottomercato dell'archiviazione a numerosi soggetti, oggi la maggior parte dei limiti tecnologici è venuta meno, da un lato per l'abbattimento dei costi, dall'altro per gli avanzamenti tecnologici in termini di efficienza di immagazzinamento[159]. I sistemi di archiviazione dei *Big Data* (*storage infrastractures*) attengono a una delle caratteristiche dei *Big Data* ("*Vs*") in particolare: il volume. Da tale assunto si deducono i quattro elementi essenziali di una struttura di archiviazione funzionale, ognuno dei quali comporta la sopportazione di costi determinati: elevata capacità, efficiente meccanismo di accesso ai dati raccolti, buon

---

[156] B. CHRISTIAN – T. GRIFFITHS, *op. cit.*
[157] L. FLORIDI, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.
[158] M. STROBACH ET AL., *Big Data Storage*, in *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, a cura di J.M. CAVANILLAS – E. CURRY – W. WAHLSTER, Springer, 2016, 123. Sui modelli relazionali di *database*, vedasi E.F. CODD, *A Relational Model of Data for Large Shared Data Banks*, Addison Wesley, 1970.
[159] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 363-64.

livello di sicurezza e basso consumo energetico[160]. Lo spazio di memoria e l'efficienza organizzativa dei *datasets* non costituiscono barriere tecnologiche all'archiviazione dei dati troppo elevate. Più problematici, invece, sono i profili riguardanti la sicurezza, i costi energetici dell'immagazzinamento dei *Big Data* e i costi di transizione dovuti al passaggio da una tecnologia a un'altra (c.d. *switching costs*). Tali fattori saranno oggetto di trattazione separata nei successivi sotto-paragrafi.

In terzo luogo, gli algoritmi svolgono un ruolo-chiave nell'organizzazione dei *datasets* secondo le esigenze dell'agente economico[161]. I procedimenti di calcolo più efficienti consentono all'operatore di evitare di organizzare i *datasets* per intero, bensì di limitare l'ordinamento dei dati a quelli che servono, cioè gli elementi che saranno oggetto di ricerca (*searching*). In informatica, infatti, si parla del *search-sort tradeoff*, che si basa sulla seguente considerazione: «*sorting something that you will never search is a complete waste; searching something you never sorted is merely inefficient*»[162]. In altri termini, l'organizzazione dei *Big Data* secondo le esigenze dell'agente economico è funzionale ai suoi interessi, cioè alle ricerche che svolgerà in seguito. Un ordinamento "indiscriminato" dei dati comporterebbe costi notevoli al soggetto che archivia i dati, dal momento che svolgerebbe un'attività inutile. Su questa logica si basa il funzionamento dell'organizzazione dei dati svolta dai motori di ricerca, per i quali «*sorting is done by machines ahead of time, before the results are needed, and searching is done by users for whom time is of the essence*»[163].

3.1. Lo spazio di archiviazione e i meccanismi di accesso ai *Big Data*

Per essere idonei all'immagazzinamento di grandi quantità di dati, i sistemi di memoria devono rispondere a due caratteristiche essenziali: da un lato, devono

---

[160] M. CHEN ET AL., *op. cit.*, 33 ss.; V. BAGNOLI, *op. cit.*, 92; D.L. RUBINFELD – M.S. GAL, *op. cit.*, 26-27.
[161] Dagli anni '80 del Novecento, gli informatici hanno sviluppato procedure computazionali sempre più efficienti per l'organizzazione dei *datasets* (si pensi, per esempio, al celebre algoritmo *Mergesoft*). Vedasi B. CHRISTIAN – T. GRIFFITHS, *op. cit.*
[162] B. CHRISTIAN – T. GRIFFITHS, *op. cit.*
[163] B. CHRISTIAN – T. GRIFFITHS, *op. cit.*

essere muniti di uno spazio notevole di archiviazione e, dall'altro, di meccanismi di organizzazione adeguati a consentire un accesso rapido ai dati stessi.

Anzitutto, i sistemi di archiviazione postulano una capacità sufficiente ad accogliere ingenti quantità di dati. Dato che la registrazione avviene a velocità elevate, l'*hardware* deve essere dotato di buona elasticità e dinamicità per la riconfigurazione[164]. I principali tipi di tecnologie di immagazzinamento *Big Data* sono due: i sistemi diretti di archiviazione (*Direct Attached Storage*, *DAS*), basati sul collegamento diretto degli *hardwares* ai *servers*, e i sistemi network (*Network Storage*), mediante i quali gli utenti possono fare accesso ai dati in modo uniforme e condividere le informazioni[165]. Inoltre, le imprese di maggiori dimensioni non custodiscono i *Big Data* in un unico *hard drive*, bensì in serie distribuita di *servers* di memoria, che ne consentono la conservazione strategica per le successive operazioni di analisi e sintesi[166]. Con lo sviluppo del *Cloud Computing*, inoltre, i costi dell'archiviazione dei dati si sono ulteriormente abbattuti[167]. Il *cloud*, infatti, consente alle imprese e agli utenti finali dei servizi l'efficace immagazzinamento e l'accesso ai dati forniti mediante un diretto collegamento alla Rete[168]. Per le prime, infatti, è essenziale il caricamento dei dati e l'accesso da una pluralità di luoghi a basso costo; per gli utenti, invece, la nuvola costituisce un'efficiente modalità di *backup* dei dati dei propri *computer* e dispositivi.

In secondo luogo, l'immagazzinamento richiede un'organizzazione precisa, incardinata su meccanismi di accesso ai dati funzionali alle operazioni di selezione analitica. I dispositivi di accesso si organizzano su due livelli di organizzazione: il *file system*, che rappresenta l'organizzazione dei dati all'interno della memoria, e la banca dati (*database*), cioè il gruppo di dati raccolti e organizzati[169]. I costi necessari alla creazione di questi meccanismi di accesso sono notevolmente diminuiti,

---

[164] M. CHEN ET AL., *op. cit.*, 33.
[165] M. CHEN ET AL., *op. cit.*, 34.
[166] Si pensi alla *Blockchain*, sistema di database distribuiti in cui sono registrate le transazioni effettuate con la criptovaluta *Bitcoin* (vedasi *infra*, § 3.3).
[167] Vedasi § 1 del capitolo primo.
[168] H. ZECH, *Information as Property*, in 6 *JIPITEC*, 2015, 193.
[169] In passato, i *databases* si fondavano su un modello relazionale, nel quale l'organizzazione delle informazioni è gerarchica e costituita, appunto, dai rapporti fra i dati stessi. I dati contenuti nelle banche dati relazionali sono detti "strutturati" (*structured data*). I *Big Data* difficilmente possono

soprattutto grazie alla diffusione di *software open-source*[170] (fra gli altri, si ricordino *Cassandra* e *HBase*).

3.2. La sicurezza dei sistemi di immagazzinamento dei dati

I sistemi di archiviazione dei *Big Data*, e soprattutto quelli basati sul *cloud*, pongono serie problematiche giuridiche, legate alla *privacy* informazionale e alla protezione dei dati dei consumatori[171] e, soprattutto, alla sicurezza della conservazione dei dati. Secondo una dichiarazione dell'attuale vicepresidente di *Amazon*, infatti, entro il 2018 tutti i dati caricati sulla nuvola saranno protetti mediante crittaggio di *default*[172].

Si ritiene comunemente che la questione più spinosa in tema di sicurezza sia la minaccia di intrusione nei sistemi di memoria da parte di soggetti terzi, quali *hackers* e governi stranieri. Accanto a queste eventualità, tuttavia, occorre prendere in considerazione anche la possibilità di malfunzionamenti e guasti ai sistemi di memoria (c.d. *hardware failures*) e i disastri naturali, che provocano la parziale o totale distruzione delle informazioni in maniera analoga alle violazioni dei *database* di malintenzionati. Per far fronte a tali problematiche, le imprese di solito procedono al *backup* dei dati su una pluralità di *servers*, affinché la rottura di uno di questi non provochi la perdita dei dati e, di conseguenza, l'impossibilità di accesso alle informazioni.

I *Big Data*, inoltre, hanno segnato un cambiamento di prospettiva nelle modalità di sicurezza dei dati. L'approccio tradizionale prevede la creazione di un sistema "statico" che minimizza il pericolo di perdita e la minaccia alla disponibilità, l'integrità e la confidenzialità delle informazioni (la c.d. triade "*AIC*", *availability-integrity-confidentiality*)[173]. Tale apparato si fonda su meccanismi di salvaguardia

---

essere ordinati già nella fase di archiviazione, a causa dell'elevato volume e della velocità di raccolta. Pertanto, i *datasets* formati da grandi quantità di informazioni sono non relazionali e dotati di elevata scalabilità, cioè di capacità di crescita efficiente all'aumento dei dati raccolti (M. STROBACH ET AL., *op. cit.*, 124).

[170] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 364; M. STROBACH ET AL., *op. cit.*, 122.

[171] Al tema della *privacy* informazionale e della protezione dei dati personali è dedicato il capitolo terzo del presente lavoro.

[172] M. STROBACH ET AL., *op. cit.*, 127.

[173] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 209.

come il crittaggio, la cifratura, i *firewalls* e programmi *anti-virus*, che chiudono l'accesso ai dati e risultano di gran lunga inadeguati allo sfruttamento economico di grandi *datasets*, che, al contrario, si fonda sulla flessibilità e sull'interconnessione delle informazioni. Inoltre, il volume e la varietà dei dati richiedono sistemi di sicurezza di maggiore complessità, idonei a comprendere l'utilizzo non previsto e flussi di informazione: tale versatilità, nondimeno, ha un costo in termini di stabilità dell'archiviazione stessa.

I limiti dell'approccio tradizionale al tema della sicurezza e le nuove esigenze dettate dall'avvento dei *Big Data* hanno determinato nuovi problemi e sviluppi in tema di *cybersecurity*, fondata su un modello di valutazione dei rischi (*risk assessment*) già noto ad altri settori[174]. La soluzione *risk-based*, a differenza di quella tradizionale, è integrata nella catena del valore dei *Big Data*: i rischi legati alla sicurezza sono, infatti, le conseguenze negative, dovute a eventi incerti e imprevisti, dei benefici sperati nello sfruttamento economico del ciclo dei *Big Data*. Tali benefici sono dovuti proprio a tecnologie interconnesse e versatili. Ne consegue che un certo livello di incertezza è inevitabile nell'immagazzinamento dei dati, quantunque siano adottati sistemi di sicurezza (c.d. rischio residuale[175]). Se questi ultimi comportassero una chiusura totale dell'accesso ai *Big Data*, viceversa si annullerebbero i benefici *data-driven*.

L'adeguamento dei sistemi di archiviazione a livelli di sicurezza idonei alle caratteristiche dei *Big Data* e un'appropriata valutazione dei rischi possono costituire una barriera all'entrata per i potenziali *newcomers* nel sottomercato dell'archiviazione. Per alcuni soggetti, infatti, l'immagazzinamento in numerosi *servers* implica, com'è facile intuire, che i costi si moltiplichino esponenzialmente in base alla quantità dei dati archiviati.

L'Unione Europea ha innovato notevolmente il quadro legislativo in tema di protezione dei dati personali, imponendo obblighi e limiti all'archiviazione dei dati personali e, in particolare, prevedendo lo svolgimento della valutazione dei rischi (o di impatto).

---

[174] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 211 ss.
[175] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. loc. cit.*

Nel capo IV del Regolamento (UE) 2016/679 sono previsti taluni obblighi in capo al titolare del trattamento in materia di sicurezza dei dati personali[176]. Da un lato, questi deve mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, che comprendono, appunto, la valutazione dei rischi (o di impatto); dall'altro, deve notificare all'autorità di controllo indipendente[177] e comunicare all'interessato ogni violazione dei dati personali, a meno che quest'ultima non presenti (o sia improbabile che presenti) un rischio per i diritti e le libertà delle persone fisiche[178].

Il Regolamento (UE) 2016/679 prevede poi che i detentori dei dati personali procedano alla valutazione dei rischi[179] (o di impatto) e adottino sistemi di immagazzinamento che raggiungano un adeguato livello di sicurezza, «*tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere*»[180]. Tali rischi possono derivare da «*trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale*»[181], cioè, in particolare, «*dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*»[182].

La valutazione di impatto è postulata in modo particolare nelle situazioni di "rischio elevato", secondo la formulazione del Regolamento (UE) 2016/679[183]. Pur non essendo definite unitariamente nel testo, tali ipotesi condividono due caratteristiche comuni: da un lato, si tratta di trattamenti che avvengono su larga scala, giac-

---

[176] Artt. 32-34 Regolamento (UE) 2016/679.
[177] L'istituzione di tale autorità è prevista all'art. 51 Regolamento (UE) 2016/679.
[178] Artt. 33-34 Regolamento (UE) 2016/679.
[179] Art. 35 Regolamento (UE) 2016/679.
[180] Cons. 83 Regolamento (UE) 2016/679. Nel Regolamento, inoltre, la sicurezza dei sistemi di archiviazione è definita come «*la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi*» (cons. 49).
[181] Cons. 75 Regolamento (UE) 2016/679.
[182] Art. 32 par. II Regolamento (UE) 2016/679.
[183] Per ulteriori approfondimenti, vedasi lo studio CENTRE FOR INFORMATION POLICY LEADERSHIP, *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL GDPR Interpretation and Implementation Project*, 2016 (http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf, ultimo accesso 19 giugno 2017).

ché coinvolgono «*una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati*»[184]; dall'altro, il rischio elevato riguarda i diritti e le libertà delle persone fisiche[185]. Da queste prescrizioni si desume che le situazioni di rischio elevato sono riconducibili a quelle in cui il titolare del trattamento opera nei mercati della raccolta e dell'archiviazione dei *Big Data*.

L'art. 35 par. III Regolamento (UE) 2016/679 menziona tre esempi di situazioni altamente rischiose, per le quali è assolutamente necessaria la valutazione di impatto. Anzitutto, tali circostanze si verificano nei casi in cui il titolare del trattamento proceda a «*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche*»[186]. Si consideri, per esempio, l'ipotesi in cui il titolare del trattamento utilizzi algoritmi nel trattamento delle informazioni personali degli utenti. In secondo luogo, situazioni di alto rischio occorrono quando il titolare si occupa del trattamento su larga scala di categorie particolari di dati personali[187] (i c.d. "dati sensibili[188]" e quelli relativi a condanne penali e a certi tipologie di reati). Infine, rischi notevoli derivano dall'attività di «*sorveglianza sistematica su larga scala di una zona accessibile al pubblico*»[189].

Com'è intuibile, le imprese che conducono attività ritenute altamente rischiose, in particolare quelle rientranti nelle ipotesi esposte *supra*, si accollano un costo notevolmente maggiore e incontrano un limite giuridico più elevato rispetto a quelle il cui operato risulta meno pericoloso. Lo svolgimento della valutazione dei rischi, infatti, richiede esperti del settore che siano in grado di costituire un sistema informatico in grado di fronteggiare situazioni di tal genere.

---

[184] Cons. 91 Regolamento (UE) 2016/679.
[185] Art. 35 par. I Regolamento (UE) 2016/679.
[186] Art. 35 par. III lett. a) Regolamento (UE) 2016/679.
[187] Art. 35 par. III lett. b) Regolamento (UE) 2016/679.
[188] I dati sensibili sono quei «*dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale,* […] *dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*» (art. 9 Regolamento (UE) 2016/679).
[189] Art. 35 par. III lett. c) Regolamento (UE) 2016/679.

3.3. Il consumo energetico dei centri di archiviazione

La distribuzione dei *Big Data* in centri di immagazzinamento comporta notevoli costi energetici: nel 2005, i *data centres* rappresentavano lo 0,5% circa del consumo mondiale di elettricità[190]; nel 2016, il tasso è salito al 3%, e si stima che l'impiego di energia triplicherà nel prossimo decennio[191].

Le voci maggiori dei costi sono quelle relative al mantenimento in attività e al raffreddamento dei *disc drives*. Solo le imprese maggiori sono in grado di sopportare tali costi; le piccole e medie imprese, invece, condividono i dati in grandi strutture comuni, allo scopo di abbattere i costi d'installazione e manutenzione.

L'aumento vertiginoso dei consumi energetici, che pone serie problematiche ambientali[192], è dovuto principalmente a due fattori. Anzitutto, tale crescita smisurata è provocata dallo sviluppo delle tecnologie inerenti al *cloud computing*[193].

In secondo luogo, notevoli consumi energetici sono dovuti alla *Blockchain*, cioè dai *databases* distribuiti che consentono le transazioni degli operatori che utilizzano la criptovaluta digitale *Bitcoin*, inventata nel 2009 dal programmatore (o dal gruppo di programmatori) conosciuto sotto lo pseudonimo di Satoshi Nakamoto. La *Blockchain* opera come un enorme libro-mastro digitale, in cui sono registrati i dati degli utilizzatori della valuta e delle transazioni secondo un elevatissimo *standard* di sicurezza. Le dimensioni della *Blockchain* sono proporzionali al numero degli utilizzatori, che cresce in maniera considerevole ogni anno[194]: nel 2017,

---

[190] J.K. KOOMEY, *Worldwide electricity used in data centers*, in 3(3) *Environmental Research Letters*, 2008, 1.

[191] T. BAWDEN, *Global warming: Data centres to consume three times as much energy in next decade, experts warn*, The Independent, 23 gennaio 2016 (http://www.independent.co.uk/environment/global-warming-data-centres-to-consume-three-times-as-much-energy-in-next-decade-experts-warn-a6830086.html, ultimo accesso 27 aprile 2017).

[192] Si veda, per esempio, I. BURRINGTON, *The Environmental Toll of a Netflix Binge*, in *The Atlantic*, 16 dicembre 2015 (www.theatlantic.com/technology/archive/2015/12/there-are-no-clean-clouds/420744, ultimo accesso 21 giugno 2017).

[193] D. KLIAZOVICH ET AL., *GreenCloud: a packet-level simulator of energy-aware cloud computing data centers*, in 3 *Journal of Supercomputing*, 2010, 1263 ss. («*The operation of large geographically distributed data centers requires considerable amount of energy that accounts for a large slice of the total operational costs for cloud data centers*»).

[194] M. DEMARY – V. DEMARY, *Blockchain: cheap, fast and accurate (but consumes a huge amount of energy),* in *LSE Business Review Blog*, 19 gennaio 2017 (http://blogs.lse.ac.uk/businessreview/2017/01/19/blockchain-cheap-fast-and-accurate-but-

la media delle transazioni *Bitcoin* giornaliere è di 250mila operazioni[195]. Questo rapporto ha un'ulteriore implicazione, cioè che i consumi energetici dei *databases* crescano altrettanto notevolmente. In particolare, si stima che, nel 2030, i consumi annuali dei c.d. *miners*, computer dotati di potenze di calcolo elevatissime che gestiscono i flussi di denaro, potrebbero superare l'attuale approvvigionamento energetico del 14%[196].

3.4. I costi di transizione e l'effetto *lock-in*

Un soggetto sopporta costi di transizione (*switching costs*) al momento del cambiamento delle tecnologie dei sistemi di informazione. Si pensi, per esempio, al passaggio dall'uso di un programma per *computer* di fotoritocco a un altro analogo: l'utilizzatore si accolla non solo il costo del nuovo prodotto, ma anche quello inerente all'apprendimento delle modalità di utilizzo di quest'ultimo. In maniera del tutto simile, su un agente economico che opera nel mercato dell'archiviazione gravano i costi derivanti dal passaggio ad altre tecnologie, quali *software* di accesso, meccanismi di organizzazione dei *database* differenti e sistemi di sicurezza di maggior complessità. Secondo alcuni, i costi di transizione costituiscono una notevole barriera all'entrata nel sottomercato dell'archiviazione dei *Big Data*, e, se molto elevati, comportano effetti di *lock-in*[197]: al soggetto, in questo caso, è impedito il passaggio a nuove tecnologie di archiviazione.

Come si vedrà meglio *infra*[198], il Regolamento (UE) 2016/679 prevede gli utenti abbiano il diritto di trasmettere i propri dati personali a un altro titolare del trattamento (c.d. diritto alla portabilità dei dati[199]).

---

consumes-a-huge-amount-of-energy, ultimo accesso 19 giugno 2017) («*Depending on participation in the system, projections for 2030 estimate the size of Bitcoin's blockchain to lie between 0.1 terabyte and 1.9 billion terabyte*»).

[195] http://blockchain.info (ultimo accesso 19 giugno 2017).

[196] M. DEMARY – V. DEMARY, *op. cit.* («*Projections for 2030 show that an increase in participation would result in a yearly energy consumption by the miners that could exceed today's worldwide energy supply by 14 per cent*»).

[197] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 364.

[198] Vedasi § 4.3.3 del capitolo terzo.

[199] Art. 20 Regolamento (UE) 2016/679.

4. L'analisi dei dati

4.1. Il ruolo della *Big Data analytics*

Un famoso economista ha affermato scherzosamente: «*so what's getting ubiquitous and cheap? Data. And what is complementary to data? Analysis*»[200]. Invero, la fase dell'analisi costituisce un passaggio fondamentale del ciclo di vita dei *Big Data*. I dati, raccolti e accumulati in grandi quantità nei *data centres*, sono sottoposti a processi che consentono all'impresa di ottenere informazioni, cioè dati dotati di significato (*inferred data*[201]). In altre parole, la *Big Data analytics* consiste nel conferimento di una struttura uniforme ai dati e nell'utilizzo delle informazioni ottenute a fini strategici (*decision making*[202]).

È necessario approfondire taluni aspetti per comprendere l'importanza di tale fase. In prima istanza, si farà riferimento alla diffusione attuale delle tecniche di analisi nelle realtà aziendali; poi, si prenderanno in esame le diverse tipologie di *analytics* e, quindi, i metodi più utilizzati; in seguito, s'indagheranno le finalità e gli scopi conseguiti mediante l'analisi; infine, si cercherà di capire se sono presenti o meno barriere all'ingresso a tale sottomercato.

In tempi recenti, lo sviluppo di tecniche di analisi innovative ha conosciuto un processo di "democratizzazione", dal momento che numerosi sviluppatori, anche indipendenti rispetto alle grandi aziende che utilizzano tali tecnologie, si dedicano all'elaborazione di algoritmi nuovi e sempre più complessi. Alla crescita del numero degli sviluppatori, tuttavia, non si accosta un altrettanto elevato numero di aziende che ricorrono a tecniche di *analytics*. Tale preclusione vale soprattutto per le piccole e medie imprese (PMI): la mancata diffusione di tecniche di analisi dei *Big Data* in questi contesti è connessa alla necessità di raccogliere grandi quantità di dati da analizzare[203] e di investire un capitale notevole, che consenta la creazione

---

[200] H. VARIAN, Hal *Varian Answers Your Questions*, 28 febbraio 2008 (http://freakonomics.com/2008/02/25/hal-varian-answers-your-questions, ultimo accesso 29 aprile 2017).

[201] V. BAGNOLI, *op. cit.*, 92; G. COLANGELO, *op. cit.*, 427.

[202] FEDERAL TRADE COMMISSION, *Big Data op. cit.*, 2016, 4-5.

[203] Peter Norvig, direttore della ricerca di Google, ha affermato: «*We don't have better algorithms. We just have more data*». «*Big Data threatens to create a deep divide between the have-datas and the have-no-datas, with big corporations gaining advantage by crunching the numbers and small firms left to stumble in the dark*» (C. DONNELLY – G. SIMMONS, *Small Businesses Need Big Data,*

di un'infrastruttura di analisi dei *Big Data*, coinvolgendo in tale progetto esperti, informatici e sviluppatori. Nelle imprese di maggiori dimensioni, le attività di *data analytics* sono svolte all'interno della realtà aziendale (*insourcing*); le piccole e medie imprese, invece, preferiscono esternalizzare tali operazioni a soggetti esterni specializzati per non sopportare gli elevati costi necessari a costituire una struttura di analisi permanente[204].

Occorre ora passare in rassegna le diverse tipologie di *analytics*.

In primo luogo, l'analisi è caratterizzata dalla sintesi, che consiste nell'organizzazione e nella combinazione dei dati secondo le esigenze del soggetto che li ha archiviati. Tuttavia, l'organizzazione dei *datasets* secondo i bisogni propri dell'impresa costituisce un limite all'interoperabilità e alla compatibilità dell'utilizzo dei dati da parte di altri soggetti[205].

In secondo luogo, esistono tre tipologie di analisi dei *Big Data*, ognuna delle quali è contraddistinta da un differente grado di presenza di un operatore umano. Anzitutto, vi è una forma di *data analytics* descrittiva, basata su tecniche di *data mining*, mediante cui si estraggono combinazioni (*patterns*) e caratteristiche comuni dai *datasets*. Esiste poi una forma di analisi più complessa, di natura predittiva, che implica l'applicazione ai risultati prodotti di modelli statistici al fine di orientare meglio l'agire dell'impresa sul mercato[206]. Infine, più complessi ancora sono gli strumenti della *analytics* automatizzata, avente natura prescrittiva, i quali, sulla base dei risultati ottenuti, forniscono all'utilizzatore dei dati le strategie operative migliori, senza l'intervento di una mente umana (c.d. *machine learning*).

I procedimenti di ispezione dei *Big Data* e trasformazione in informazioni richiedono particolari cautele, che innovano notevolmente le tecniche conosciute

---

Too, in *Harvard Business Review*, 5 dicembre 2013 - www.hbr.org/2013/12/small-businesses-need-big-data-too, ultimo accesso 15 giugno 2017).

[204] Vedasi § 2.2.1.

[205] D. RUBINFELD – M. GAL, *op. cit.*, 365. Secondo altri, si tratta già di un'operazione di analisi, detta *cluster analysis* (M. CHEN ET AL., *op. cit.*, 51). Riguardo al tema dell'interoperabilità, «*substantial impediments prevent data from being easily reused. One set of challenges is purely technical: because data is often recorded and published in a wide variety of formats,* [businesses] *have difficulty aggregating data from multiple sources*» (M. MATTIOLI, *Disclosing Big Data*, in 99 *Minnesota Law Review*, 2014, 545).

[206] FEDERAL TRADE COMMISSION, *Big Data op. cit.*, 2016, 4-5.

fino a pochi decenni fa[207]: si pensi, per esempio, al ruolo cardinale che gli algoritmi svolgono in tale ambito[208]. È necessario soffermarsi ulteriormente sui tre metodi più utilizzati: l'analisi mediante correlazione, le tecniche di analisi statistica e il *data mining*.

Anzitutto, i *Big Data* hanno segnato l'esplosione dell'analisi delle informazioni mediante correlazione, concetto che in statistica indica una relazione non-causale fra fenomeni per la quale al verificarsi dell'uno si verifica l'altro con una certa regolarità. La correlazione, quindi, è essenziale nell'analisi dei *Big Data*: essa consente di «*scoprire il cosa*», ma non di «*analizzare il perché*»[209], la cui rivelazione è affidata alle indagini causali. Nella *data analytics* a scopi commerciali, tuttavia, la ricerca di rapporti di causa-effetto risulta talvolta superflua, bensì è sufficiente l'osservazione dei *trends* e delle correlazioni fra fenomeni al fine di capire i comportamenti dei consumatori.

In secondo luogo, è facilmente intuibile che l'apporto della statistica all'analisi dei dati sia fondamentale. Nel settore commerciale e in quello medico, la teoria della probabilità svolge un ruolo fondamentale nella descrizione di ampi *datasets*[210], al fine dell'elaborazione di modelli predittivi.

Infine, il *data mining* è una delle tecniche di analisi più note ed efficaci. Come dice il nome, tale metodo, imprescindibile per analisi di successo, consiste nell'estrazione di informazioni utili da un ammasso di dati incompleti e non tutti rilevanti (c.d. *noise*). Tale operazione, opportunamente paragonata alla ricerca di un ago in un pagliaio[211], non avviene mediante l'intervento di operatori umani, ma si basa prevalentemente sull'utilizzo di algoritmi e metodi di *machine learning*.

---

[207] *Contra* M. CHEN ET AL., *op. cit.*, 51, per il quale la *Big Data analytics* non è altro che l'analisi di un "tipo speciale" di dati con metodi già noti agli esperti da tempo.
[208] Vedasi § successivo.
[209] V. MAYER-SCHÖNBERGER – K. CUKIER, *op. cit.*, 96. Sulle implicazioni epistemologiche dei *Big Data* e sui loro rischi, si veda H. HOSNI – A. VULPIANI, *Forecasting in Light of Big Data*, in *Philosophy & Technology*, 2017, 1 ss.
[210] M. CHEN ET AL., *op. cit*., 52.
[211] M. MATTIOLI, *op. cit.*, 557.

I metodi di analisi dei *Big Data*, inoltre, avvengono in tempi diversi. Una tipologia di *analytics* avviene *offline*: i *Big Data* "storici" (*historical data*, cioè riferibili a un determinato momento di raccolta e archiviazione)[212] sono analizzati attraverso metodi statistici e sono estratti i dati mediante gli algoritmi e il *machine learning*; in seguito, le informazioni ottenute sono archiviate. Si tratta, quindi, di risultati il cui valore aggiunto ai dati conseguito è notevole. Un genere più costoso di *analytics* avviene in tempo reale. Tali metodi, che consentono il costante rinnovamento dei risultati dell'analisi in tempi brevi, sono diffusi soprattutto in settori, come quello finanziario, in cui i flussi di informazioni da esaminare sono soggetti a aggiornamenti continui e rapidi.

L'analisi dei *Big Data* è utile a perseguire una varietà di scopi commerciali. Le tipologie della *data analytics* più comuni in contesti di *business* (*business intelligence and analytics*, *BI&A*) sono quella predittiva e quella descrittiva. Due, infatti, sono i principali obiettivi cui mira un'impresa con le attività di *analytics*: capire le preferenze dei consumatori e prevedere i *trends* del mercato. Oggetto di analisi sono, in primo luogo, le attività dei consumatori in Rete che rivelano direttamente le loro preferenze e i loro gusti e consentono, quindi, il miglioramento dei prodotti dell'impresa. Si pensi, per esempio, ai dati del numero di click su determinati contenuti (*search and user logs*) e alla serie di acquisti di un dato bene. Lo sviluppo del *web 2.0*[213], basato sulle crescenti interazioni degli utenti sulle piattaforme digitali (*Facebook*, *Twitter*, *Instagram*), ha provocato l'esplosione di una quantità enorme di contenuti creati dagli utenti stessi (*user-generated*) in questi ambiti, quali immagini e video, da cui emergono indirettamente le predilezioni dei consumatori: così, dunque, le imprese sono in grado di ottenere ulteriori *feedback* da diverse categorie di clienti[214].

---

[212] J. DOMINGUE ET AL., *Big Data Analysis*, in *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, a cura di J.M. CAVANILLAS – E. CURRY – W. WAHLSTER, Springer, 2016, 75.

[213] T. O'REILLY, *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, in *OReilly*, 30 settembre 2005 (www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, ultimo accesso 29 aprile 2017).

[214] H. CHEN – R.H.L. CHIANG – V.C. STOREY*, Business Intelligence And Analytics: From Big Data To Big Impact*, in 36(4) *MIS Quaterly*, 2012, 1167 («*Web 2.0 applications can efficiently gather a large volume of timely feedback and opinions from a diverse customer population for different types of businesses*»).

In conclusione, l'analisi dei *Big Data* costituisce in capo agli attori economici operanti in tale mercato un'innovazione prolifica. Il valore delle informazioni ottenute in esito alle procedure di analisi dipende, da un lato, dalla mole dei dati sottoposti a tali processi, e, dall'altro, da parametri di scalabilità, cioè dall'attitudine del sistema di analisi ad aumentare e diminuire di volume secondo la quantità di dati disponibili. Le informazioni che ne risultano sono idonee all'utilizzo: possono essere cedute a terzi, ovvero essere utilizzate dall'impresa stessa. In quest'ultima ipotesi, esse costituiscono un notevole vantaggio competitivo in capo a questa[215].

Le barriere tecnologiche all'ingresso al mercato dell'analisi rilevano sotto due profili: l'uno quantitativo e l'altro qualitativo. Da una parte, infatti, l'efficienza dell'analisi dipende dalla quantità (*volume* e *variety*) dei *Big Data* analizzati[216], dall'altra dai metodi e dalle tecnologie cui ricorre per trarre informazioni di valore dai *datasets*. Anche nel mercato dell'*analytics*, dunque, si riscontrano potenziali economie di scala e di gamma[217]. Un'impresa che non dispone di tecniche sufficientemente efficienti si vede preclusa l'entrata nel mercato in questione.

Occorre ora soffermarsi sull'elemento su cui si fonda l'attività di analisi dei *Big Data* e che, per l'importanza centrale che possiede, richiede un'apposita trattazione: gli algoritmi.

4.2. Il ruolo degli algoritmi

Gli algoritmi sono procedimenti di calcolo che, inseriti in un programma informatico, consentono la risoluzione di problemi[218]. La definizione-base di algoritmo è di carattere formale: si tratta, infatti, di una procedura matematica mediante la quale si raggiunge un determinato scopo secondo regole prestabilite[219]. Si tratta, quindi, di una categoria molto vasta, che comprende elementi molto diversi fra

---

[215] V. BAGNOLI, *op. cit.*, 92.
[216] N.P. SCHEPP – A. WAMBACH, *op. cit.*, 122.
[217] Si veda il § 2.2.2.4.
[218] B. CHRISTIAN – T. GRIFFITHS, *op. cit.* («[…] *an algorithm is just a finite sequence of steps used to solve a problem*»).
[219] Un'ottima analisi della definizione di "algoritmo" si trova in R.K. HILL, *What an Algorithm Is*, in 29(1) *Philosophy & Technology*, 2016, 47 («*An algorithm is a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions*»).

loro[220]: una ricetta culinaria, un'operazione di addizione algebrica e *Facebook PageRank* sono tre esempi di algoritmo.

La definizione appena riportata è integrata, nell'accezione più diffusa del termine, da due elementi ulteriori: l'implementazione della procedura matematica in un programma di calcolo e la configurazione di quest'ultimo per lo svolgimento di un compito preciso[221].

Gli algoritmi hanno semplificato notevolmente la vita delle persone, rimodellando «*the environment of people's interaction and their daily lives*»[222]. Attività come cercare un appartamento o un ristorante *online* e interagire con i programmi di riconoscimento vocale degli *smartphones* sono solo alcuni degli ambiti in cui l'operato degli algoritmi è divenuto fondamentale.

Ai fini della presente analisi, tuttavia, è presa in considerazione solo una tipologia di algoritmi, cioè quella il cui apporto risulta fondamentale a compiere le attività di analisi dei *Big Data*[223]. È necessario analizzare il ruolo di questo tipo sia dal lato dell'offerta (*id est* le imprese che li utilizzano), sia da quello della domanda (cioè i consumatori-utenti coinvolti dalle operazioni condotte mediante l'uso di algoritmi).

Primariamente, si considerino le imprese. Mediante l'utilizzo degli algoritmi, i soggetti economici possono individuare le correlazioni e i *patterns* dei dati raccolti e determinare «*which features are relevant to a given decision*»[224]. I *Big Data* costituiscono sia la materia grezza, sia il prodotto finale delle operazioni algoritmiche[225]: «*critical decisions are made not on the basis of the data per se, but*

---

[220] U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, in *Philosophy & Technology*, 2017 («*There is a panoply of algorithms "out there"*»).
[221] B.D. MITTELSTADT ET AL., *The ethics of algorithms: Mapping the debate*, in *Big Data & Society*, 2016, 2; U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*
[222] U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*
[223] B. CHRISTIAN – T. GRIFFITHS, *op. cit.* («*For many people, the word "algorithm" evokes the arcane and inscrutable machinations of Big Data, big government, and big business*»).
[224] B.D. MITTELSTADT ET AL., *op. cit.*, 3; L. FLORIDI, *Big Data and their epistemicological challenge*, *op. cit.*
[225] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data* in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione), 3.

on the basis of data analyzed algorithmically: that is, in calculations coded in computer software»[226]. Pertanto, il benessere delle imprese operanti nel mercato dell'analisi dei *Big Data* e dei consumatori è largamente influenzato dall'utilizzo di algoritmi: da una parte, questi consentono ai venditori di risparmiare costi del lavoro, riducendo il numero di lavoratori necessario per lo svolgimento di una determinata attività; dall'altra, «*they also create benefits for consumers if such lower costs* [*of labour*] *are translated into lower prices, and a better availability of preferred products*»[227].

L'utilizzo degli algoritmi nell'ambito della *Big Data analytics*, inoltre, ha causato la progressiva sostituzione degli operatori umani nella successiva fase di utilizzo dei dati e di *decision making*. Numerosi sistemi di calcolo, infatti, si fondano sul *machine learning* e su tecnologie di intelligenza artificiale che, adattandosi all'ambiente di analisi, migliorano le proprie qualità computazionali automatiche[228] e raggiungono, quindi, un certo livello di autonomia[229].

Due elementi determinano il funzionamento efficace di un algoritmo in una struttura di *Big Data analytics*. Anzitutto, secondo taluni autori, l'efficienza di un algoritmo non dipende tanto dalla complessità computazionale, bensì dalla sua *performance* di calcolo[230]. Ne consegue che un algoritmo migliore è in grado di analizzare una maggiore quantità di dati rispetto a uno meno efficiente nel medesimo intervallo di tempo. In secondo luogo, l'efficienza di un algoritmo dipende dall'esperienza e dalle conoscenze del programmatore, che sviluppa il procedimento matematico secondo le proprie abilità acquisite nel tempo[231].

---

[226] F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015, 21-22.
[227] M.S. GAL, *Competition and innovation in the digital environment*, in *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, a cura di G. COLANGELO – V. FALCE, Il Mulino, 2017, 23.
[228] M. VAN OTTERLO, *A Machine Learning View on Profiling*, in *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, a cura di M. HILDEBRANDT – K. DE VRIES, Routledge, 2013 («*machine learning is a branch of AI that seeks to develop computer systems that improve their performance automatically with experience*»); J.M. BALKIN, *op. loc. cit.* («*Collection and processing of data produces ever more data, which in turn, is used by algorithms to improve themselves*»).
[229] B.D. MITTELSTADT ET AL., *op. cit.*, 3.
[230] F. OHLHORST, *Big Data Analytics. Turning Big Data Into Big Money*, Wiley & Sons, 2013, 90.
[231] B.D. MITTELSTADT ET AL., *op. cit.*, 7 («*An algorithm's design and functionality reflects the values of its designer and intended uses, if only to the extent that a particular design is preferred as the*

A ben vedere, l'uso degli algoritmi nelle attività di *analytics* può determinare l'insorgere di economie di apprendimento (*economies of experience*) in capo all'impresa che ne fa uso. Tale concetto di microeconomia indica la diminuzione dei costi che consegue all'accumulo di conoscenze da parte dell'impresa stessa in un determinato intervallo temporale (c.d. *learning by doing*[232]), e differisce dalla nozione di economie di scala, che si verificano allorché la produzione degli *output* cresce e il costo medio di produzione diminuisce[233]. Le economie di apprendimento sono rappresentate dalla curva di apprendimento (*experience curve*), che indica il rapporto fra i costi medi del prodotto e la produzione di beni o servizi cumulati nel tempo.

L'impiego di algoritmi basati su tecnologie di *machine learning* e intelligenza artificiale, come già spiegato, consente il raggiungimento di attività innovative e maggiormente efficienti. L'impresa che ne fa uso, infatti, può raggiungere un vantaggio competitivo rispetto alle altre dopo un certo periodo di accumulo di conoscenze, dal momento che detiene algoritmi più efficienti. Si pensi, per esempio, al caso di una società assicurativa. Mediante l'uso di procedimenti computazionali automatizzati di *profiling* e di tracciamento degli utenti, il rischio che grava sull'impresa di contrattare con soggetti poco affidabili o più inclini ad attività rischiose si riduce notevolmente e, nel contempo, le possibilità di successo sono di gran lunga maggiori. Tale rischio, infatti, diminuisce in proporzione alle maggiori conoscenze accumulate dall'algoritmo sulla base dei dati raccolti. Si consideri ora un sito *web* di traduzione di testi in diverse lingue. La qualità di un servizio *online* di traduzione di testi da una lingua all'altra migliora non solo grazie alla raccolta dei dati delle ricerche più effettuate, ma anche sulla base delle informazioni derivanti dai *feedback* forniti dagli stessi utenti accumulati nel tempo. Tali elementi consentono all'algoritmo di selezionare i risultati migliori, presentandoli per primi nei risultati delle ricerche future.

---

best or most efficient option»). Nello stesso senso, K.N.J. MACNISH, *Unblinking Eyes: The Ethics of Automated Surveillance*, in 14(2) *Ethics and Information Technology*, 2012, 151 ss.

[232] D. BESANKO – R. BRAEUTIGAM, *op. cit.*, 317 ss.

[233] Vedasi *supra*, § 2.2.4.

Riguardo al lato della domanda, gli algoritmi comportano taluni costi per i consumatori. L'utilizzo "negligente[234]" di procedimenti automatizzati per l'analisi dei *Big Data*, infatti, provoca esternalità negative[235] nei confronti di soggetti terzi, nel senso che «*la loro curva di indifferenza (o di utilità) è affetta da comportamenti di altri individui, al di fuori dai consueti meccanismi dello scambio di mercato*»[236]. Tali *spill-overs*, che nel mondo giuridico sono riconducibili alla nozione civilistica delle immissioni (*nuisances*[237]), comprendono quattro fattori differenti[238]. Anzitutto, alcuni soggetti possono rimanere esclusi dai rapporti con il resto della società sulla base dei dati analizzati mediante l'uso di algoritmi. In altre parole, si pongono problematiche legate alla discriminazione dei consumatori interessati dalle operazioni algoritmiche. In secondo luogo, l'utilizzo di algoritmi può provocare danni alla reputazione di talune categorie di consumatori, tracciandone profili identitari distorti. In terzo luogo, l'accumulo dei dati degli utenti e la classificazione di questi ultimi in base alla valutazione dei rischi connessi alla persona può precludere l'accesso a determinati servizi[239]. Infine, le decisioni prese mediante l'uso di algoritmi sono poco trasparenti, e un'adeguata comprensione di queste richiede la collaborazione degli operatori e delle imprese che hanno elaborato le modalità di funzionamento dell'algoritmo[240].

In conclusione, i consociati coinvolti nel *decision making* automatizzato sopportano un costo sociale più o meno elevato a seconda del verificarsi di questi fattori[241]. Tuttavia, come si vedrà meglio nel capitolo terzo, «*harm caused by*

---

[234] Così J.M. BALKIN, *op. cit.*, 18.
[235] Sulle esternalità negative provocate dagli algoritmi, vedasi § 6.2 del capitolo terzo.
[236] U. MATTEI, *La proprietà*, in *Trattato di diritto privato*, diretto da R. SACCO, 2ª ed., UTET Giuridica, 2015, 328. In questo caso, il comportamento non è di altri individui, bensì è il risultato delle operazioni degli algoritmi.
[237] J.M. BALKIN, *op. loc. cit.*
[238] Vedasi J.M. BALKIN, *op. cit.*, 19-20; U. PAGALLO, *op. cit.* Nello stesso senso, vedasi il discorso di B.D. MITTELSTADT ET AL., *op. cit.* sugli «*ethical concerns raised by algorithms*».
[239] M. FERTIK – D. THOMPSON, *The Reputation Economy. How To Optimise Your Digital Footprint In a World Where Your Reputation Is Your Most Valuable Asset*, Crown Business, 2015.
[240] J.M. BALKIN, *op. cit.*, 21; F. PASQUALE, *op. cit.*, 189 ss. In questo senso, la giurisprudenza amministrativa italiana è pervenuta a importanti conclusioni nel 2017, estendendo la tutela del diritto di accesso (previsto dagli artt. 22 ss. della Legge n. 241 del 1990) ai codici sorgente del *software* dell'algoritmo per garantire la trasparenza degli atti amministrativi c.d. "informatici" in senso stretto (TAR Lazio, sede Roma, sez. III bis, sentenza 22 marzo 2017, n. 3769). Si rimanda al dibattito intorno al diritto alla spiegazione dell'algoritmo (§ 6.2.2 del capitolo terzo).
[241] R.H. COASE, *The problem of social cost*, in 3 *Journal of Law & Economics*, 1960, 1 ss. Balkin parla di *algorithmic externalities*.

algorithmic activity is hard to debug […and] *it is rarely straightforward to identify who should be held responsible for the harm caused*»[242].

5. L'utilizzo dei dati

L'uso dei *Big Data* costituisce l'ultimo anello della catena del valore. Tale fase inerisce a due attività fondamentali. Il detentore dei dati, infatti, può decidere di utilizzare le informazioni ai propri fini, allo scopo di operare scelte strategiche sul mercato, ovvero cedere le informazioni a terzi.

Nella prima eventualità, si fa riferimento a uno snodo determinante della vita di un'impresa: il *decision making*. L'analisi delle informazioni e il loro successivo utilizzo, infatti, conducono a una maggiore efficienza e a nuove opportunità per le imprese, in quanto il rischio di esiti negativi è notevolmente mitigato. Inoltre, non è necessario che chi prende le decisioni dell'impresa comprenda la ragione delle azioni condotte sulla base dell'analisi delle informazioni: anzi, il "perché", solitamente, viene dopo l'aver agito[243]. Talvolta, l'utilizzatore è addirittura escluso dalla fase di *decision making* (si pensi, per esempio, alla *Big Data analytics* automatizzata). Questi processi pongono un problema allorché i risultati dell'analisi e i modelli predittivi non si rivelino attendibili[244]: si consideri il celebre caso di *Knight Capital Group*, società americana operante come intermediario finanziario, che nel 2012 perse ben 440 milioni di dollari in soli 45 minuti a causa del malfunzionamento di un algoritmo deputato alla vendita di azioni (c.d. *flash trading* o *algorithmic trading*), che ne provocò il tracollo economico e la successiva acquisizione da parte di una concorrente[245].

In alternativa all'uso interno, l'impresa può cedere le informazioni a terzi. Com'è noto, la compravendita dei *Big Data* è molto diffusa nel settore dei *data*

---

[242] B.D. MITTELSTADT ET AL., *op. cit.*, 5.
[243] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 155 («*Decision makers do not necessarily need to understand the phenomenon before they act on it. In other words: first comes the analytical fact, then the action, and last, if at all, the understanding*»).
[244] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 156 ss.; J.M. BALKIN, *op. cit.*, 1 ss.
[245] N. POPPER, *Knight Capital Says Trading Glitch Cost It $440 Million*, in *The New York Times*, 2 agosto 2012 (http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/?_r=0, ultimo accesso 16 giugno 2017).

brokers, che ricavano i dati da una pluralità di fonti, li aggregano e li vendono ai propri clienti[246].

Le principali barriere all'entrata nel sottomercato dell'utilizzo dei dati hanno natura contrattuale. Fino a qualche anno fa, il soggetto acquisitore poteva imporre limiti di natura contrattuale alla portabilità dei dati personali dell'utente, cioè al trasferimento degli stessi a un altro soggetto titolare del trattamento[247], pur non essendo molto diffuso nella pratica. L'utente era costretto a sopportarne costi di transizione (*switching costs*) e, se questi ultimi erano troppo elevati, gli era precluso il passaggio a un altro titolare del trattamento (effetto *lock-in*[248]). Nelle recenti riforme della normativa europea in materia di protezione dei dati personali, il legislatore europeo ha introdotto una nuova situazione giuridica in capo all'interessato. Il Regolamento (UE) 2016/679, infatti, prevede che il diritto alla portabilità dei dati sia esercitato senza impedimenti da parte del primo titolare, qualora il trattamento si effettui con mezzi automatizzati[249].

In senso contrario, il soggetto che utilizza i dati può limitarne il proprio uso. Ciò avviene, nella prassi, per chi opera in un segmento di mercato in cui la *privacy* e la custodia dei dati dei consumatori sono assai rilevanti[250]. Tali limiti hanno natura contrattuale, giacché l'obbligo (di natura negativa) di astenersi dal concedere i dati dell'utente a terzi dei dati grava sull'utilizzatore in forza di un accordo stipulato con l'utente stesso.

Vi sono poi ulteriori limiti di carattere giuridico all'utilizzo dei *Big Data*. Da un lato, l'utilizzo dei dati personali da parte dei soggetti titolari del trattamento

---

[246] Per un inquadramento generale e le problematiche più rilevanti inerenti alle attività dei *data broker*, si veda il report FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, 2014.

[247] Sulla definizione di "titolare del trattamento" vedasi art. 4 n. 7 Regolamento (UE) 2016/679 («*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*»).

[248] D. RUBINFELD – M. GAL, *op. cit.*, 366.

[249] Art. 20 Regolamento (UE) 2016/679. Per una trattazione specifica sul diritto alla portabilità dei dati, si veda il § 4.3.3 del capitolo terzo.

[250] AUTORITÉ DE LA CONCURRENCE - BUNDESKARTELLAMT, *op. cit.*, 2015, 41 («[…] *The operator generally guarantees its users that their personal data will not be communicated to a third party without their consent. Without such a guarantee users may be reluctant to communicate their personal data*»); D. RUBINFELD – M. GAL, *op. cit.*

incontra limiti nella normativa europea della protezione dei dati[251]; dall'altro, nel 2017 la Commissione ha emanato una Comunicazione in materia di *data ownership* dei dati non personali. La previsione di tale situazione giuridica soggettiva costituisce un'ulteriore barriera[252].

6. I soggetti coinvolti negli anelli della catena del valore dei Big Data

Come spiegato nei paragrafi precedenti, le fasi della raccolta, dell'archiviazione, dell'analisi e dell'utilizzo costituiscono gli anelli della catena del valore dei *Big Data*. A questi corrispondono diversi sotto-mercati in cui una molteplicità di attori interagisce.

Una pluralità di imprese utilizza i *Big Data* come risorsa infrastrutturale per migliorare le proprie attività e per rendere più efficiente la produzione di beni e l'erogazione di servizi[253]. Numerosi settori dell'economia si sono radicalmente evoluti a causa dell'innovazione *data-driven*. È chiaro che l'apporto dei *Big Data* e delle tecnologie connesse al loro utilizzo muta a seconda delle caratteristiche tipiche dei diversi settori. Fra questi ultimi, occorre ricordare la sanità, il settore pubblico, la finanza, il settore assicurativo, le telecomunicazioni, il settore dello spettacolo, quello energetico e quello dei trasporti[254].

L'analisi di ogni singolo settore, tuttavia, non rientra nei fini del presente lavoro. In questa sede, invece, ci si vuole soffermare sugli attori economici del ciclo dei *Big Data* su cui la letteratura si è soffermata maggiormente: le autorità del settore pubblico, le piattaforme digitali, i *data brokers* e i consumatori.

Prima di prendere in esame tali soggetti, occorre tenere presenti preliminarmente alcune considerazioni.

---

[251] Si pensi al diritto alla cancellazione dei dati personali detenuti dal titolare del trattamento (o diritto all'oblio) previsto all'art. 17 del Regolamento (UE) 2016/679.
[252] Per la trattazione specifica sulle questioni di appartenenza dei dati non personali (*data ownership*), si rimanda al capitolo quarto. Si vedano la Comunicazione della Commissione *Building a European Data Economy*, 2017 e l'annesso *Working Staff Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017.
[253] Per i dati sull'utilizzo dei *Big Data* nelle realtà imprenditoriali, vedasi § 1.
[254] S. ZILLNER ET AL., *Big Data-Driven Innovation in Industrial Sectors*, in J.M. CAVANILLAS – E. CURRY – W. WAHLSTER, *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, Springer, 2016, 172 ss.

- I consumatori sono i soggetti che pongono in essere e diffondono i propri dati, fornendoli agli altri soggetti economici soprattutto mediante l'utilizzo di *Internet*.
- Gli agenti economici coinvolti nella fase di raccolta e in quella di archiviazione sono le autorità del *public sector*, i *data brokers*, le piattaforme digitali e le altre imprese che dispongono di un'infrastruttura di acquisizione dei *Big Data*.
- Il sottomercato dell'analisi dei *Big Data* comprende le imprese che svolgono attività di *data analytics*, cioè principalmente le piattaforme digitali, le istituzioni pubbliche e i *data brokers*[255].
- Infine, gli imprenditori operanti in svariati settori che utilizzano le informazioni derivanti dalla sintesi e dall'analisi dei *Big Data* e i *data brokers* (nella fase di vendita dei *datasets*) sono gli agenti economici che operano del mercato corrispondente all'ultimo anello della catena del valore[256].

6.1. I governi e le autorità del settore pubblico

Le autorità del settore pubblico sono attive principalmente in due mercati costituenti il *Big Data cycle*: l'acquisizione e l'archiviazione dei dati. Inoltre, i dati detenuti dal settore pubblico costituiscono una fonte di dati per altri soggetti[257].

Storicamente, le autorità del settore pubblico hanno condotto per prime attività di sfruttamento dei dati. Da diversi decenni, infatti, i governi e, in particolare, le amministrazioni pubbliche raccolgono informazioni riguardanti la collettività in basi di dati (c.d. *public data*). Questa attività si è particolarmente intensificata negli ultimi anni del secolo scorso, quando le istituzioni pubbliche hanno cominciato a intraprendere attività di raccolta e organizzazione di ampi *datasets* riguardanti contenuti eterogenei mediante l'utilizzo del denaro pubblico.

---

[255] Le attività di analisi dei *Big Data* sono svolte da una pluralità di soggetti diversi da quelli elencati, fra cui rientrano anche grandi imprese *brick and mortar* (B&M).
[256] L'elenco di questi soggetti è un adattamento dell'analisi svolta dall'OCSE nel report del 2015 (vd. OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 34).
[257] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, *op. cit.*, 84.

Fino a qualche decennio fa, fra i governi e le istituzioni pubbliche prevaleva la tendenza a limitare l'accesso dei cittadini a tali risorse. Successivamente, a partire dagli anni Novanta del secolo scorso, l'atteggiamento delle autorità del settore pubblico è mutato radicalmente sulla base di due ragioni fondamentali. Anzitutto, è prevalso l'orientamento ideologico e politico per il quale la fruizione comune e condivisa delle risorse digitali in questione è una funzione pubblica essenziale di uno Stato democratico: già Thomas Jefferson, infatti, affermava che «*information is the currency of democracy*»[258]. I dati del *public sector*, infatti, se accessibili ai cittadini, consentono una maggiore trasparenza dell'azione pubblica e un'ottimizzazione notevole della partecipazione dei cittadini: «[…] *free access to data contributes to an enhancement of democratic institutions from a citizen's point of view*»[259]. In secondo luogo, i notevoli avanzamenti nell'ambito delle *ICTs* hanno aperto la strada a riutilizzi innovativi dei dati, che operano alla stregua di *input* di nuovi beni e servizi.

Occorre soffermarsi sull'evoluzione del ruolo delle autorità del settore pubblico nel versante americano e in quello europeo, ripercorrendo brevemente l'evoluzione normativa in tema di accesso ai dati pubblici, e, quindi, analizzare più dettagliatamente il ruolo innovativo che tali risorse digitali hanno assunto in seguito all'avvento dei *Big Data*, indagando il valore che generano in capo alla molteplicità dei soggetti coinvolti (cittadini, imprese e autorità del settore pubblico).

Negli Stati Uniti, fino a pochi decenni fa l'accesso ai *public data* incontrava limiti notevoli. La versione originaria del *Freedom of Information Act* (FOIA), entrato in vigore nel 1966, pur prescrivendo l'accesso libero al materiale degli archivi di Stato, non affrontava il tema della disponibilità pubblica delle risorse informative in formato elettronico, all'epoca pressoché inutilizzate. Nella Circolare A-130 del 1985 dell'Ufficio per la gestione e il bilancio (*Office of Management and Budget*), organo di consulenza del Presidente degli Stati Uniti, si prevedevano ancora limiti notevoli alla diffusione dei dati pubblici da parte delle istituzioni[260]. A partire dagli

---

[258] Riportato in J. STIGLITZ ET AL., *The role of government in the digital age*, Report commissionato dalla *Computer & Communications Association*, 2000, 53.
[259] J.L. MOLINO – S. SEDKAOUI, *op. cit.*, 24.
[260] J. STIGLITZ ET AL., *op. cit.*, 53-54.

anni Novanta del secolo scorso, le crescenti istanze di maggiore trasparenza delle autorità pubbliche nei confronti degli amministrati hanno segnato la nascita di meccanismi di *disclosure* delle informazioni in formato digitale. Da quel momento, infatti, l'accesso ai dati, inteso come strumento indispensabile per garantire l'efficienza e la trasparenza delle amministrazioni pubbliche, è stato incoraggiato mediante l'emanazione di norme volte all'apertura dei *databases* al pubblico. Nel 1993, la Circolare A-130 è stata modificata per promuovere l'accesso pubblico alle informazioni delle autorità pubbliche. I principi alla base di questa modifica sono confluiti poi nel *Paperwork Reduction Act* del 1995[261]. Nel 1996, il Presidente Bill Clinton ha firmato gli *Electronic Freedom of Information Act Amendments* (c.d. E-FOIA), con cui si sanciva l'accesso libero alle informazioni detenute dalle autorità pubbliche e l'istituzione di *electronic reading rooms* che consentono l'«*electronic availability* […] *through on-line access*» ai dati[262].

La problematica dell'accesso si ripropone più recentemente a causa dello sviluppo notevole di *Internet.* Sfruttando tale tecnologia, le autorità possono migliorare notevolmente le interazioni coi cittadini e la qualità dei servizi offerti (c.d. amministrazione digitale, o *e-government*). A partire dai primi anni del Duemila, infatti, le amministrazioni hanno aperto siti e portali ufficiali allo scopo di registrare le proprie attività e mettere a disposizione del pubblico servizi più efficienti. Parallelamente a questa tendenza, si è diffusa l'idea che le amministrazioni centrali e locali debbano esercitare il potere con ancora maggiore trasparenza, servendosi sistematicamente delle tecnologie dell'informazione e della comunicazione nell'espletamento delle proprie funzioni (c.d. *open government*). Nel dicembre del 2007, trenta esperti di *Internet* e nuove tecnologie (fra i quali figuravano Lawrence Lessig e Tim O'Reilly) si sono incontrati a Sebastopol, in California, allo scopo di

---

[261] J. STIGLITZ ET AL., *op. loc. cit.*

[262] *Foia update: Congress enacts Foia amendments*, in *The United States Department of Justice*, 1° gennaio 1996 (www.justice.gov/oip/blog/foia-update-congress-enacts-foia-amendments, ultimo accesso 24 giugno 2017).

elaborare una definizione unitaria di *open government data*[263], delineandone i principi regolatori[264]. Tale nozione indica i dati prodotti dalle autorità pubbliche, accessibili a tutti e riutilizzabili liberamente, e mutua numerosi contenuti dal concetto economico-giuridico di bene comune (*commons*[265]), valorizzandone, in particolare, tre aspetti: apertura, partecipazione e collaborazione (*openness*, *participation and collaboration*). In seguito al convegno del 2007, il concetto di *open government data* si è diffuso ampiamente nel versante americano e in tutto il mondo, influenzando inevitabilmente le attività legislative di diversi Paesi. Meno di due anni dopo, nel gennaio del 2009, il Presidente degli Stati Uniti Barack Obama firma un *Memorandum on Transparency and Open Government*, con cui si accoglievano le tesi dei trenta esperti elaborate a Sebastopol[266] e si inauguravano politiche di *disclosure* delle informazioni detenute dalle autorità del settore pubblico negli Stati Uniti. Nel maggio del 2009, il governo americano ha aperto il portale di accesso ai dati detenuti dalle istituzioni pubbliche, *data.gov*[267]. Nel 2014, è entrato in vigore il *Digital Accountability and Transparency Act* (c.d. *DATA Act*), finalizzato alla uniformizzazione e alla pubblicazione *online* dei dati di spesa delle autorità federali. Mediante questo strumento legislativo, il governo statunitense ha rafforzato ulteriormente la trasparenza in materia di spese pubbliche, «*which the US Government regards as a means to achieve greater accountability to the taxpayers*»[268].

Come già accennato, talune tipologie di dati raccolti e organizzati in grandi quantità dalle istituzioni pubbliche costituivano un *input* essenziale per la produzione di beni e l'erogazione di servizi innovativi da parte di soggetti privati. È il

---

[263] Per essere precisi, con l'espressione *open data* si fa riferimento a dati prodotti sia da istituzioni pubbliche sia da soggetti collettivi privati, cui è consentito a tutti l'accesso e il riutilizzo. Negli *open data*, infatti, oltre agli *open government data*, rientrano anche i dati della ricerca scientifica e quelli dei soggetti privati il cui accesso è pubblico (vedasi J.L. MOLINO – S. SEDKAOUI, *Big Data, Open Data and Data Development*, ISTE Ltd. and Wiley & Sons, 2016, 23 ss.)

[264] S. CHIGNARD, *A brief history of open data*, in *Paris Innovation Review*, 29 marzo 2013 (www.parisinnovationreview.com/2013/03/29/brief-history-open-data, ultimo accesso 22 giugno 2017).

[265] Sui beni comuni vedasi, *inter alios*, E. OSTROM, *Governing the Commons. The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990.

[266] *Transparency And Open Government. Memorandum For The Heads Of Executive Departments And Agencies*, in *Obama White House*, 21 gennaio 2009 (http://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government, ultimo accesso 22 giugno 2017).

[267] A. BODE BODE, *Open Data: a History*, in *Data.gov*, 4 aprile 2013 (www.data.gov/blog/open-data-history, ultimo accesso 22 giugno 2017).

[268] OCSE, *Data-Driven Innovation. Big Data for growth and well-being*, *op. cit.*, 431.

caso, per esempio, dei dati geografici, aerei e postali. In particolare, i dati delle amministrazioni possono essere riutilizzati per attività imprevedibili al momento della raccolta, per ragioni diverse da quelle per cui l'autorità ha proceduto all'archiviazione. Nell'ordinamento statunitense, il riutilizzo dei *datasets* incontra numerosi incentivi, dal momento che le risorse digitali in questione non sono tutelate dal *copyright*[269] e fanno parte, pertanto, del pubblico dominio.

Dal canto suo, l'Unione europea ha affrontato congiuntamente le problematiche dell'accesso e del riutilizzo ai dati delle pubbliche amministrazioni nella Direttiva PSI del 2003, che ha conferito un *minimum* di armonizzazione alle diverse normative degli Stati membri riguardanti l'accesso alle informazioni del *public sector*. L'obiettivo della Direttiva PSI è quello di incentivare l'accesso e il riutilizzo dei documenti degli organismi di diritto pubblico (c.d. *public sector information*), a fini commerciali e non commerciali[270]. Il concetto di "documento del settore pubblico" è una categoria ampia, che comprende tutte le «*information (including data) generated by the public sector as part of its public task*»[271]. Fra queste sono annoverabili una molteplicità di tipologie di dati, come quelli meteorologici, statistici, geografici, ma anche i contenuti digitali delle biblioteche, dei musei e degli archivi pubblici ecc.

La disciplina europea, tuttavia, presenta due punti deboli rispetto alla legislazione americana. Anzitutto, la versione originaria della Direttiva PSI «*non prescrive […] l'obbligo di consentire l'accesso ai documenti o l'obbligo di consentire il riutilizzo di documenti. La decisione di autorizzare o meno il riutilizzo spetta agli Stati membri o all'ente pubblico interessato*»[272]. In secondo luogo, dal momento

---

[269] Il titolo 17 dello US Code prevede che le opere create dalle autorità pubbliche siano di pubblico dominio: «*copyright protection under this title is not available for any work of the United States Government, but the United States Government is not precluded from receiving and holding copyrights transferred to it by assignment, bequest, or otherwise*» (chapter 1, § 105).

[270] Vedasi art. 3 Direttiva PSI. La nozione di "documento" è notevolmente estensiva (art. 2.3 Direttiva PSI).

[271] OCSE, *Data-Driven Innovation. Big Data for growth and well-being*, *op. cit.*, 405. In questo caso il termine *information* non designa necessariamente il dato munito di significato, bensì ogni contenuto derivante dal settore pubblico. Nel *report* OCSE, *Recommendation for enhanced access and more effective use of Public Sector Information (PSI)*, 2008 le PSI sono definite le «*information, including information products and services, generated, created, collected, processed, preserved, maintained, disseminated, or funded by or for a government or public institution*».

[272] Cons. 7 Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013 che modifica la direttiva 2003/98/CE, G.U. n. L. 175 del 27/06/2013.

che non sono contemplate limitazioni ed eccezioni specifiche al diritto d'autore[273], le informazioni del settore pubblico ricadono nel campo di applicazione della tutela giuridica delle banche dati prevista dalla Direttiva 96/9/CE[274], per la quale, di conseguenza, si applica un regime di licenze regolamentato diversamente in ogni Stato membro[275].

All'inizio degli anni Dieci del Duemila, i dibattiti della dottrina americana e le soluzioni legislative adottate negli Stati Uniti in tema di *open data* hanno smosso le istituzioni europee. La nozione di *open data*, infatti, è comparsa nell'agenda politica dell'Unione europea con un certo ritardo rispetto al versante americano. Nel 2011, la Commissione ha emanato una Comunicazione in tema di *open data*, con cui si è inaugurata l'Agenda Digitale europea. Tale atto circoscrive la categoria dei dati pubblici ai fini delle istituzioni dell'Unione europea e degli Stati membri, identificandola come una *species* della più ampia nozione di *public sector information*, che comprende anche i documenti non digitali. I *public data*, infatti, sono «*tutte le informazioni che gli organismi pubblici nell'Unione europea producono, raccolgono o acquisiscono* […]»[276]. Inoltre, nello stesso provvedimento si è stimato che i guadagni derivanti dallo sfruttamento di tali risorse ammontino a 40 miliardi all'anno[277]: «*digitized PSI is* […] *a valuable commodity and recognized as a valuable source of income*»[278]. Sulla scorta di tale atto, il legislatore

---

[273] L'art. 5 della Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, G.U. n. L. 167 del 22/06/2001, prevede eccezioni e limitazioni del diritto d'autore a livello europeo.

[274] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, G.U. n. L. 077 del 27/03/1996.

[275] Ciò è previsto all'art. 8 della Direttiva PSI, non modificato in maniera significativa dalla Direttiva 2013/37/UE.

[276] Comunicazione della Commissione *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, 2011, 2.

[277] Comunicazione della Commissione *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, 2011, 2. La Commissione parla di «*potenzialità inutilizzate*».

[278] B. LUNDQVIST, *"Turning Government Data Into Gold": The Interface Between EU Competition Law and the Public Sector Information Directive – With Some Comments on the Compass Case*, in 44 *IIC International Review of Intellectual Property and Competition Law*, 2011, 79.

europeo, prendendo atto dei radicali cambiamenti tecnologici, è intervenuto riformando la Direttiva PSI, in quanto le norme del 2003 non sono parse più in grado di «*rispondere efficacemente ai mutamenti e alle esigenze*»[279].

Proprio su questi cambiamenti tecnologici è necessario soffermarsi. In particolare, occorre esaminare il rapporto fra i *public data* – che, come si è visto, sono *open government data* se l'accesso è aperto a tutti – e i *Big Data*.

Public data, *open government data* e *Big Data* sono tre categorie concettuali distinte che presentano taluni punti di intersezione. È chiaro che, «*by releasing Big Data as Open Data, governments around the world can boost their countries' economies and improve the lives of their citizens*»[280]. L'innovazione derivante dall'accumulo dei dati in grandi quantità risulta ancora più evidente dalla molteplicità dei settori coinvolti nelle politiche governative di incentivo all'utilizzo degli *open data*. Secondo un sondaggio sulla varietà degli *open government datasets* condotto dall'OCSE nel 2013, i contenuti maggiormente interessati dalle *policies* di apertura dei dati pubblici sono i seguenti: meteorologici, geografici, socio-culturali, economici, relativi ai trasporti e turistici[281].

I dati pubblici, soprattutto se raccolti e organizzati in grandi quantità, sono una risorsa strategica fondamentale, e generano un valore differente per una pluralità di attori: cittadini, imprese private e le stesse autorità del settore pubblico.

Nei primi due casi, le autorità del settore pubblico operano come fonte dei dati stessi, occupandosi della raccolta e dell'archiviazione. Anzitutto, il riutilizzo di tali informazioni consente ai cittadini di partecipare più attivamente alla vita politica e, in generale, di compiere scelte in maniera più libera e informata (c.d. *self-empowerment*). Per esempio, le iniziative in tema di *smart disclosure*, che consistono in «*timely release of data in standardized, machine readable formats in ways that enable consumers to make better decisions about finance, healthcare, energy or other contexts*»[282]. Inoltre, con l'avvento dei *Big Data*, i servizi offerti

---

[279] C. BUZZACCHI, *La politica europea per i Big Data e la logica del single market: prospettive di maggiore concorrenza?*, in 23 *Concorrenza e mercato*, 2016, 164.
[280] J. GURIN, *Big Data and Open Data: How Open Will the Future Be?*, in 10 *Journal of Law and Policy for the Information Society*, 2014/2015, 692.
[281] OCSE, *Data-Driven Innovation. Big Data for growth and well-being*, *op. cit.*, 406.
[282] A. HOWARD, *What is smart disclosure?*, in *Radar O'Reilly*, 1° aprile 2012 (http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html, ultimo accesso 23 giugno 2017).

alla collettività sono più efficienti a causa del mescolarsi di dati provenienti da diverse fonti. Si pensi, per esempio, al sito *web FixMyStreet*, creato da all'associazione benefica britannica *mySociety*, in cui l'utente può segnalare e richiedere alla pubblica amministrazione competente gli interventi di manutenzione delle strade.

In secondo luogo, gli *open data* organizzati in ampi *datasets* generano valore per una molteplicità di imprese. Tuttavia, a differenza di quanto visto per i *Big Data* acquisiti da soggetti privati, «*when government data are open* […]*, access to data per se does not provide a competitive advantage to firms with exclusive data-access agreements*»[283], poiché l'accesso a tali informazioni non è esclusivo, ma è aperto a tutti i soggetti economici. Le imprese riutilizzano i dati forniti dalle autorità del settore pubblico per una varietà di scopi commerciali, usandoli come "risorsa grezza" (*raw material*) strumentale allo sviluppo di nuovi prodotti e servizi con notevole valore aggiunto. In particolare, i soggetti economici privati operano come intermediari che agevolano le interazioni fra le autorità del settore pubblico e gli utenti finali del servizio[284]. Si consideri, per esempio, che gli *open data* provenienti dal servizio meteorologico nazionale degli Stati Uniti sostentano l'industria meteorologica privata per un valore stimato di un miliardo e mezzo di dollari all'anno[285].

Infine, i dati detenuti dal *public sector* generano valore per gli stessi governi e le autorità del settore pubblico. Mediante l'utilizzo di queste risorse digitali, tali soggetti da una parte migliorano sensibilmente l'efficienza dei servizi erogati alla collettività e delle attività del settore pubblico (*data-driven innovation*), dall'altra ottengono vantaggi finanziari dalla *disclosure* dei dati a titolo oneroso o la tassazione delle attività commerciali condotte mediante tali dati.

In primo luogo, l'efficientamento dei servizi pubblici è legato a due fattori che ne concernono l'erogazione. Anzitutto, la pubblicazione dei dati *online* implica una notevole riduzione dell'ammontare di lavoro dei pubblici impiegati. Per esempio, alle richieste che le amministrazioni ricevono quotidianamente possono essere

---

[283] B. UBALDI, *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, OCSE Working Papers on Public Governance, 2013, 12.
[284] G. VICKERY, *Review Of Recent Studies On Psi Re-Use And Related Market Developments*, *report* commissionato dalla Commissione europea, 2011.
[285] CAPGEMINI CONSULTING, *The Open Data Economy Unlocking Economic Value by Opening Government and Public Data*, 2013, 8.

date risposte più celeri, istituendo l'accesso alle informazioni mediante portali *online*. Inoltre, «*OGD can also help foster collaboration across and within public agencies and departments*»[286]. Un secondo elemento di innovazione concerne lo sviluppo di nuove modalità di accesso ai servizi pubblici. Si pensi, per esempio, alla creazione delle *app* ufficiali degli enti pubblici, quali le università e i Comuni, mediante le quali gli utenti possono accedere ai servizi.

In secondo luogo, l'accumulo dei dati in ampi *datasets* consente alle autorità di comprendere in maniera più accurata i bisogni dei cittadini mediante l'elaborazione di modelli predittivi sulla base di attività di *analytics*. Infatti, «*greater ability to combine different (public and private) data sets can help develop enhanced insights*»[287]. Le autorità del settore pubblico ottengono due principali benefici dall'innovazione *data-driven*. Anzitutto, i servizi forniti dalle amministrazioni sono personalizzati in base ai diversi profili degli utenti. *In secundis*, i risultati di analisi costituiscono importanti risorse statistiche che consentono la predisposizione di *policies* in tempo reale (c.d. *nowcasting*), che sono spesso integrati con dati raccolti da attori privati. Si pensi, per esempio, a *Google Insights*, che, sulla base dei dati delle parole-chiave più frequentemente immesse nel motore di ricerca, fornisce informazioni utili alla misurazione precisa e alla predizione di vari fenomeni, quali la disoccupazione o la diffusione di malattie in certe zone[288]. La presenza pervasiva del *nowcasting* si riscontra finanche nell'ambito delle previsioni economiche: taluni membri del Comitato federale del mercato aperto (*Federal Open Market Committee*, FOMC), organismo della *Federal Reserve*, hanno dichiarato che le *policies* condotte dall'autorità in questione sono "dipendenti dai dati[289]".

Gli *open data*, infine, possono apportare guadagni finanziari per i governi. I governi, infatti, perseguono tali rendite mediante la previsione dell'accesso ai dati a titolo oneroso e l'imposizione di tributi sulle attività commerciali svolte con l'utilizzo degli *open data*. Nell'Unione europea, i dati sono accessibili e riutilizzabili

---

[286] B. UBALDI, *op. cit.*, 14.
[287] OCSE, *Data-Driven Innovation. Big Data for growth and well-being*, *op. cit.*, 408.
[288] OCSE, *Data-Driven Innovation. Big Data for growth and well-being*, *op. cit.*, 408; V. MAYER-SCHÖNBERGER – K. CUKIER, *op. cit.*
[289] K.L. KLIESEN – M.W. MCCRACKEN, *Tracking the U.S. Economy with Nowcasts*, in *The Regional Economist*, 2016, 1.

mediante il pagamento del solo costo marginale di raccolta e di organizzazione sostenuto dalle istituzioni[290]: l'entità limitata dei prezzi di accesso è un incentivo notevole al riutilizzo delle risorse digitali delle autorità pubbliche. Secondo uno studio condotto dalla Commissione, infatti, nel 2013 si è verificato un aumento del numero dei ri-utilizzatori dei dati aperti del 10.000%[291].

6.2. Le piattaforme digitali

Le piattaforme digitali sono soggetti economici di natura privata la cui presenza nei *Big Data submarkets* è fondamentale. Come già accennato nei paragrafi precedenti, tali attori operano a ogni livello della catena del valore: acquisizione, archiviazione, analisi e uso dei dati[292]. Fra le piattaforme digitali si annoverano siti *web* dalle caratteristiche eterogenee, che, offrendo sul mercato servizi di diversa natura (*social networking*, *e-commerce* ecc.), hanno cambiato radicalmente il nostro modo di vivere. Si pensi, per esempio, a siti come *Google*, *Facebook*, *Amazon*, *eBay*, *LinkedIn*.

È sufficiente considerare qualche dato per comprendere il ruolo predominante di questi agenti economici nei vari mercati. Nella classifica delle società maggiori al mondo per capitalizzazione azionaria[293] relativa all'anno 2016, quattro operano come piattaforme digitali[294] (*Apple*[295], *Google Alphabet*, *Facebook*, *Amazon*) (Figura 4). Rispetto a dieci anni prima, tali società, e, in generale, quelle del settore tecnologico, si sono imposte sulle altre anche perché impiegano un basso numero di dipendenti: *Facebook*, per esempio, dà lavoro a circa 15mila persone, mentre

---

[290] Art. 6 Direttiva PSI.
[291] CAPGEMINI CONSULTING, *op. cit.*, 9.
[292] Vedasi *supra*, § 1.
[293] La capitalizzazione azionaria indica il valore di mercato delle azioni di una società in un determinato periodo di tempo.
[294] *Top 10 Companies By Market Capitalization in the World*, in *Trending Top Most*, 17 aprile 2017 (www.trendingtopmost.com/worlds-popular-list-top-10/2017-2018-2019-2020-2021/business/companies-market-capitalization-world-largest, ultimo accesso 27 giugno 2017).
[295] *Apple* opera come una piattaforma digitale nell'erogazione di vari beni e servizi: si pensi, per esempio, all'*App Store* e all'*iTunes Store*.

General Electric, che si trova al nono posto nella medesima classifica, ha 330mila persone alle sue dipendenze[296].

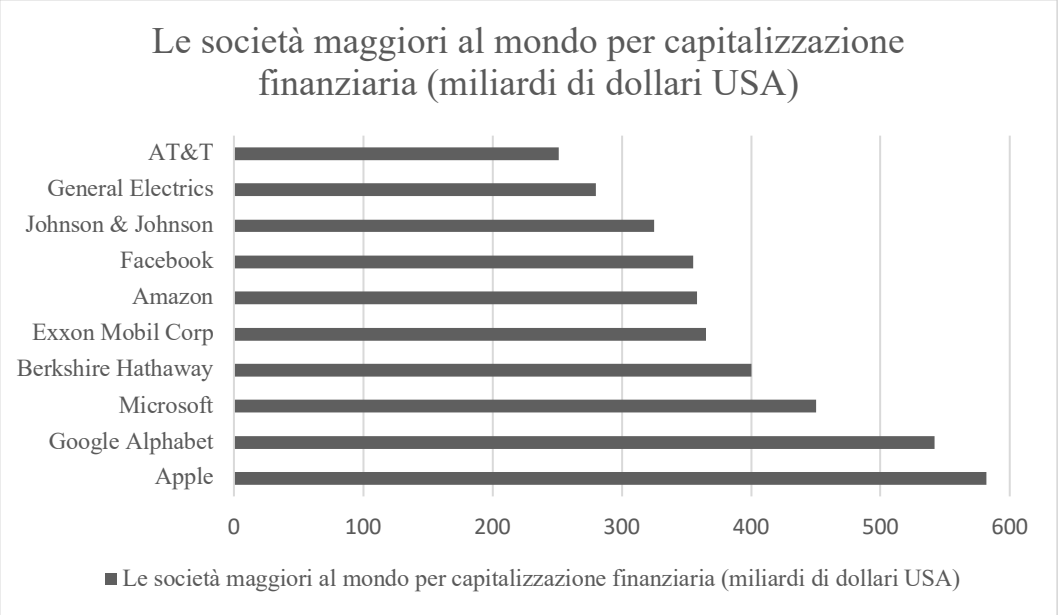

Figura 4. Le società maggiori al mondo per capitalizzazione azionaria. Fonte: *Trending Top Most* (www.trendingtopmost.com/worlds-popular-list-top-10/2017-2018-2019-2020-2021/business/companies-market-capitalization-world-largest).

Ora occorre analizzare più dettagliatamente le caratteristiche principali delle piattaforme digitali, soffermandosi su due fattori: la gratuità dei servizi offerti dalle piattaforme e la nozione di *attention markets*. È necessario riprendere preliminarmente due punti di analisi già toccati nei paragrafi precedenti[297].

In prima istanza, come già detto, il funzionamento delle piattaforme digitali e dei mercati in cui operano è stato efficacemente descritto in letteratura con le nozioni di piattaforme multiversante e mercati multiversante. Come già spiegato, le *multisided platforms* si pongono come intermediari fra due gruppi di attori economici (cioè i compratori e i venditori di due mercati separati, quali consumatori-utenti e inserzionisti), facilitandone le interazioni e le transazioni. Sulla base delle

[296] A. GRAY, *These are the world's 10 biggest corporate giants*, in *World Economic Forum*, 16 gennaio 2017 (www.weforum.org/agenda/2017/01/worlds-biggest-corporate-giants, ultimo accesso 27 giugno 2017). *Apple* e *Google Alphabet* occupano rispettivamente il primo e il secondo posto della classifica.
[297] Vedasi, in particolare, § 2.2.5 e § 1.

informazioni degli utenti acquisite dalle piattaforme, gli inserzionisti possono raggiungere i potenziali clienti in maniera oltremodo efficace mediante campagne pubblicitarie mirate e personalizzate, offrendo loro beni e servizi su misura (c.d. *behavioural targeting*).

In secondo luogo, occorre ricordare che le piattaforme digitali si dedicano alla raccolta massiccia dei dati personali degli utenti, utili allo svolgimento efficiente delle attività di intermediari. Tali *datasets* sono sia un *input* produttivo che consente il miglioramento dei servizi offerti ai consumatori-utenti sulla base delle loro preferenze personali, sia un *asset* strategico che determina l'insorgere di un vantaggio competitivo in capo all'impresa quando le stesse informazioni non sono egualmente disponibili ai soggetti concorrenti[298].

Si viene dunque alla prima caratteristica fondamentale delle piattaforme digitali: l'offerta di servizi gratuiti. Le piattaforme digitali solitamente non offrono prodotti ai consumatori-utenti in cambio di un corrispettivo. Nell'intermediazione fra gruppi di attori, le piattaforme fissano un prezzo per uno solo di questi, cioè quello degli inserzionisti, consentendo all'altra categoria di agenti di accedere ai servizi a prezzi nulli o quasi nulli[299] (c.d. *zero-price markets*). Si pensi ad attività quotidiane ben note al pubblico, come, per esempio, l'iscrizione a *Facebook*, la creazione di un *account Gmail*, l'utilizzo dei servizi di *cloud computing Google Drive*, l'installazione sullo *smartphone* dell'applicazione *Outlook*. L'offerta gratuita di prodotti ha determinato non pochi problemi per la comprensione adeguata del funzionamento dei relativi mercati e, in particolare, l'applicabilità delle regole

---

[298] H. SHELANSKI, *Information, innovation, and competition policy for the Internet*, in 161(6) *University of Pennsylvania Law Review*, 2013, 1680 ss.; A. GRUNES – M.E. STUCKE, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, in *The Antitrust Source*, 2015, 1 ss.

[299] Fino al gennaio del 2016, l'applicazione *Whatsapp* costava agli utenti 0,99 € all'anno. Oggi il servizio è gratuito per tutti gli utenti. Vedasi F. ZAFFARANO, *Whatsapp diventa gratuito, tolti i 99 cent all'anno*, in *La Stampa*, 18 gennaio 2016 (www.lastampa.it/2016/01/18/tecnologia/whatsapp-diventa-gratis-tolti-i-cent-allanno-LYzdZGYpdA22S3hGZxBE8M/pagina.html, ultimo accesso 7 luglio 2017).

del diritto *antitrust*, che si incardinano su uno dei principi fondamentali dell'economia neoclassica: la teoria dei prezzi[300]. Tuttavia, l'assenza di un "costo monetario[301]" non significa che i consumatori-utenti non debbano sopportarne altri. Fra questi, se ne possono individuare i due principali: il costo derivante dalla produzione dell'informazione da parte dell'utente e il costo derivante dall'attenzione dell'utente. La presenza di queste due variabili rende inadeguato il concetto di gratuità applicato alle piattaforme digitali.

La prima entità è già stata ampiamente affrontata nei precedenti paragrafi. Numerosi esperti e autori hanno affermato che le informazioni dei consumatori sono una nuova valuta (*new currency*) che consente le interazioni economiche e le transazioni fra diversi soggetti[302]. Infatti, «*to provide this information to the firm in exchange for a free product or service is to engage in trade, even if the trade occurs without a price*»[303].

In secundis, la gratuità dei servizi offerti dalle piattaforme incide sul grado di popolarità e diffusione delle stesse. In altre parole, mediante l'offerta di servizi *gratis*, l'attenzione dei visitatori, cioè il tempo impiegato sul sito *web*, aumenta notevolmente[304], dal momento che sono maggiormente stimolati a usufruire dei servizi e dei beni offerti e, soprattutto, di cliccare sulle inserzioni pubblicitarie, mediante le quali la piattaforma genera ricavi.

Ci si sofferma, dunque, su tale qualità essenziale delle piattaforme digitali, cioè la ricerca dell'attenzione degli utenti, che coinvolge alcuni profili oltremodo utili a capire il funzionamento delle piattaforme digitali. In talune analisi[305] si è

---

[300] G. COLANGELO, *op. cit.*, 427; J.M. NEWMAN, *Antitrust in zero-price markets: Foundations*, in 164(1) *University of Pennsylvania Law Review*, 2015, 149. Su questo tema, vedasi più nel dettaglio il § 7 del capitolo quarto.

[301] J.M. NEWMAN, *op. cit.*, parla di *exchanged monetary cost*.

[302] J.M. NEWMAN, *op. cit.*, 167 («*Customers frequently surrender information as payment in exchange for access to zero-price products like webmail, search, social networking, and creative-content services. This personal information serves as a form of currency, taking the place of money*»).

[303] C. HOOFNAGLE – J. WHITTINGTON, *Free Accounting for the Costs of the Internet's Most Popular Price*, in 61 *UCLA Law Review*, 2014, 625.

[304] D. EVANS, *Attention to Rivalry among Online Platforms and Its Implications for Antitrust Analysis*, Coase-Sandor Institute for Law & Economics Working Paper No. 627, 2013, 18.

[305] Si vedano, *inter alios*, T. WU, *Attention Markets and the Law*, in *SSRN Library*, 2017 (http://ssrn.com/abstract=2941094, ultimo accesso 27 giugno 2017); D. EVANS, *op. cit.*; J.M. NEWMAN, *op. cit.*; J. RATLIFF – D. RUBINFELD, *Is there a market for organic search engine results*

dimostrato che questi soggetti cercano di attirare l'attenzione degli utenti-consumatori in svariati modi, e, nel tentativo di guadagnarsela e "rivenderla" a soggetti interessati a essa, sono in concorrenza fra loro. Misurare l'entità dell'attenzione non è un'operazione affatto semplice se non si introduce un'ulteriore variabile: il tempo. Per calcolare il grado di attenzione degli utenti sui siti occorre far riferimento al tempo impiegato dagli stessi sulle pagine *web*[306]. Taluni dati parlano chiaro: nel 2012, i siti in cui gli utenti passano più tempo in assoluto sono *Facebook*, *YouTube*, *Yahoo* e *Google* (che occupano rispettivamente il primo, il secondo, il terzo e il quarto posto nella classifica). Inoltre, nello stesso anno, gli utenti iscritti a *Facebook* hanno passato ben 872 milioni di ore sulla piattaforma[307].

In primo luogo, è necessario esaminare il concetto di attenzione; *in secundis*, si indagheranno le ragioni per cui l'attenzione degli utenti è una risorsa scarsa; infine, si spiegherà il ruolo di *attention brokers* assunto dalle piattaforme.

Si inizia dalla nozione di attenzione. Le scienze psicologiche hanno dato ampi contributi di analisi al tema: diversi autori hanno tentato di elaborare una definizione unitaria e soddisfacente di attenzione. Pur essendo risalente, quella del filosofo William James resta oggi la più efficace. Nella sua opera più famosa, *I principi di psicologia*, il pensatore statunitense intuisce che «*everyone knows what attention is. It is the taking possession by the mind, in clear and vivid form, of one out of what seem several simultaneously possible objects or trains of thought*»[308]. Successivamente, le moderne scienze cognitive hanno poi confermato l'intuizione di James. Il nostro cervello, infatti, è in grado di processare solo un numero limitato di informazioni, e, di conseguenza, «*we ignore, or filter, almost everything, focusing attention on only a tiny subset of the information made available*»[309]. La mente umana ripone l'attenzione su determinate informazioni secondo due modalità[310].

---

and can their manipulation give rise to antitrust liability?, in 10(3) *Journal of Competition Law and Economics*, 2014, 517 ss.

[306] D. EVANS, *op. cit.*, 3.

[307] I dati sono ricavati da D. Evans, *op. cit.*, 7 ss.

[308] W. JAMES, *The Principles of Psychology*, Henry Holt and Company, 1890.

[309] T. WU, *op. cit.*, 4-5.

[310] E.E. SMITH – S.M. KOSSLYN, *Cognitive Psychology: Mind And Brain*, Pearson, 2007, cap. 3; T. Wu, *op. cit.*, 5-6.

Da una parte, infatti, una persona può stabilire consciamente quanta attenzione allocare (c.d. modello attenzionale *top-down* o *goal-driven*); dall'altra, l'attenzione è stimolata a prescindere dalla nostra volontà, agendo come risposta a stimoli esterni (movimenti rapidi, rumori ecc.) (c.d. modello attenzionale *down-top* o *stimulus-driven*). In una pagina *web*, è evidente che, per attirare l'attenzione dei propri clienti, le imprese sfruttino il funzionamento del secondo modello: si pensi, per esempio, a inserzioni colorate e animate, impossibili da ignorare perché poste in posizioni strategiche all'interno della pagina *web*.

Tornando alle piattaforme digitali, è chiaro che, in tali contesti, l'attenzione degli utenti è un'entità limitata da due fattori. Da un lato, come si è visto, il nostro cervello può acquisire solo un numero ristretto di informazioni; dall'altro, esiste un limite ulteriore, determinato dalla crescita del numero delle informazioni nel mondo. Secondo un'affermazione profetica dell'economista Herbert Simon, l'aumento delle informazioni disponibili nel mondo comporta «[…] *a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients*»[311]. Perciò, l'attenzione è una risorsa scarsa che i soggetti economici presenti nel mercato tentano di procacciarsi per conseguire un vantaggio competitivo (c.d. *attention markets*). Tale fenomeno economico è stato individuato in taluni studi sull'economia dei media e sull'industria dell'intrattenimento televisivo, in cui si è spiegato che i modelli di *business* adottati dalle imprese operanti in tale settore si basano sul conferire valore economico all'attenzione del pubblico e trarne profitto. In questo senso, i telespettatori divengono *audience commotidies*, che, al pari di altri beni, sono venduti agli agenti pubblicitari

[311] H.A. SIMON, *Designing Organizations for an Information-Rich World*, in *Computers, Communications, And The Public Interest*, a cura di M. GREENBERGER, John Hopkins Press, 1971. Nello stesso senso, T.H. DAVENPORT – J.C. BECK, *The Attention Economy: Understanding The New Currency Of Business*, Harvard Business School Press, 2001.

(c.d. *audience commodification*[312]). Con la crescita recente delle principali piattaforme digitali, e, soprattutto, quelle operanti nel settore del *social networking*, tali studi e le rivisitazioni a questi connesse sono notevolmente tornati *in auge*[313].

Occorre soffermarsi sul ruolo che svolgono le piattaforme digitali nell'allocazione dell'attenzione. Questi attori economici operano come intermediari fra diversi gruppi di soggetti e tentano di aggiudicarsi l'attenzione per rivenderla a terzi che ne beneficiano – cioè principalmente agli inserzionisti, ma anche ad altri soggetti, come politici o artisti che utilizzano la piattaforma per promuovere la loro immagine[314]. Tale meccanismo operativo è stato efficacemente descritto con l'espressione "*attention brokers*[315]". Le piattaforme digitali intercedono fra gli utenti-consumatori (*attention providers*) e coloro che traggono benefici economici dall'attenzione degli utenti (*attention seekers*). Il funzionamento di tale intermediazione è spiegato in Figura 5.

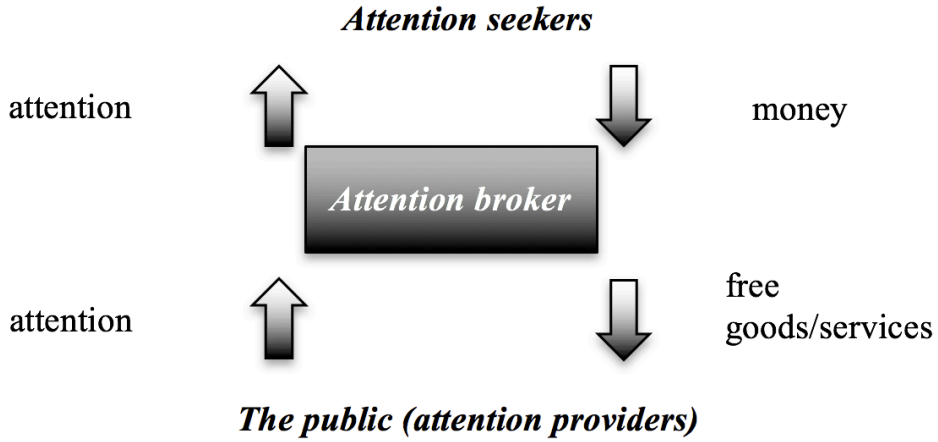

Figura 5. Il modello-base dell'*attention broker*. Fonte: T. Wu, *Attention Markets and the Law*, in *SSRN Library*, 2017, 16.

[312] Si vedano, *inter alios*, D.W. SMYTHE, *Communications: Blindspot of Western Marxism*, in 1(3) *CTheory*, 1 ss.; D.W. SMYTHE, *On the Audience Commodity and Its Work*, in *Media and Cultural Studies: Keyworks*, a cura di M.G. DURHAM – D.M. KELLNER, Wiley-Blackwell, 1981; A. ARVIDSSON – T. BONINI, *Valuing Audience Passions: From Smythe to Tarde*, in 18(2) *European Journal of Cultural Studies*, 2015, 158 ss.

[313] L. MCGUIGAN – V. MANZEROLLE (CUR.), *The Audience Commodity in a Digital Age: Revisiting a Critical Theory of Commercial Media*, Peter Lang, 2014.

[314] T. WU, *op. cit.*; D. EVANS, *op. cit.*, J.M. NEWMAN, *op. cit.*

[315] T. WU, *op. cit.*; D. EVANS, *op. cit.* Secondo Wu, gli *attention brokers* sono un caso particolare di piattaforma multiversante.

Le piattaforme riescono a procacciarsi l'attenzione degli utenti in due modalità. Da una parte, come già visto, offrono servizi gratuiti per raggiungere il più ampio pubblico possibile; dall'altra, inseriscono nelle pagine *web* contenuti di diversa natura, che attirano l'attenzione dell'utente e funzionano come una sorta di esca[316]. Si pensi, per esempio, alle notizie, alle informazioni meteorologiche, ai *posts* condivisi dagli amici o dalle pagine seguite, ai *videoclip* correlati a quello visualizzato dall'utente, e, nelle piattaforme digitali attive nella telefonia mobile, alle c.d. "storie", cioè le fotografie e i video pubblicati dagli utenti e visibili solo per un determinato periodo di tempo dai propri *followers*. I dati degli utenti acquisiti dalla piattaforma servono a fornire agli utenti contenuti personalizzati, sulla base delle preferenze, delle ricerche effettuate in precedenza e delle informazioni personali fornite[317] (c.d. *targeting*).

Le piattaforme digitali sono in concorrenza con le altre (come affermano alcuni studiosi, «*they compete for eyeballs*»[318]) nella vendita dell'attenzione, che è diversificata secondo le qualità personali di ogni utente e i bisogni degli inserzionisti. In altri termini, «*the Attention Broker resells not just attention in bulk, but specific, tailored tranches of attention designed to meet the needs of the buyer*»[319]. *Google+* e *Facebook*, grazie all'analisi delle parole chiave mediante gli algoritmi, sono specializzate nella comprensione degli stati di bisogno dei consumatori comunicati attraverso i *posts*. Si pensi, per esempio, all'utente che pubblica un *post* su *Facebook* in cui avverte la sua cerchia di amici di voler comprare un nuovo *smartphone*. Sulla bacheca di tale consumatore facilmente appariranno le inserzioni dei negozi *online* dei principali venditori di telefoni.

Infine, occorre prendere in considerazione i due elementi principali che determinano l'insorgere di vantaggi competitivi a favore di alcuni soggetti operanti negli *attention markets*. Anzitutto, è chiaro che l'*attention broker* si trova di fronte a un notevole *trade off* fra l'inserimento dei contenuti "attrattivi" e la collocazione

---

316 J. RATLIFF – D. RUBINFELD, *op. cit.*, paragonano questi contenuti al miele (*honey*), che «*attract consumers willing to devote attention to advertisers' message*».
317 J. RATLIFF – D. RUBINFELD, *op. cit.*,
318 T. WU, *op. cit.*, 2.
319 T. WU, *op. cit.*, 16.

delle inserzioni pubblicitarie nella piattaforma. In particolare, all'aumentare del numero dei primi, lo spazio dedicato alla pubblicità diviene minore, con il conseguente calo della principale fonte di guadagno della piattaforma; all'aumentare del numero delle inserzioni, invece, la presenza di contenuti e servizi dedicati agli utenti si riduce, e, di conseguenza, diminuisce il numero degli utenti, poiché la presenza massiccia di spazi pubblicitari infastidisce e allontana il pubblico dei consumatori[320]. Sulla comprensione adeguata dell'equilibrio fra queste due opzioni si basa l'entità del vantaggio competitivo che l'impresa può acquisire. Sfruttando tali conoscenze, infatti, i *newcomers* possono entrare nel mercato e fronteggiare gli *incumbents*, come dimostrano alcuni casi storici. Per esempio, *Facebook*, al momento dell'ingresso nel mercato, ha adottato una strategia competitiva magistrale, acquisendo un notevole privilegio competitivo nei confronti di *MySpace*[321]. Nei primi anni di attività *online*, *Facebook* era sostanzialmente privo di contenuti pubblicitari e offriva servizi più innovativi di quelli di altre piattaforme[322] (si pensi, per esempio, alla possibilità di pubblicare fotografie, "stati", *link* ad altre pagine ecc.). Tali elementi hanno segnato la fine del rivale *MySpace*, che, viceversa, proponeva agli utenti numerosi annunci. Dopo aver conseguito un notevole potere di mercato a detrimento dei suoi principali avversari, *Facebook* ha iniziato a introdurre contenuti pubblicitari per massimizzare il profitto derivante dalle inserzioni[323]. Come già visto in precedenza, il *boom* degli annunci ha provocato, a metà degli anni Dieci del Duemila, la diffusione di *software* ed estensioni che bloccano il caricamento delle inserzioni sui siti[324].

In seconda istanza, un ulteriore elemento che rafforza la posizione di potere è la conquista dei c.d. *attentional greenfields*, cioè quegli spazi di attenzione degli

---

[320] Vedasi § 2.2.5.
[321] Sulla perdita di terreno del *social network MySpace*, vedasi F. GILLETTE, *The Rise and Inglorious Fall of MySpace*, in *Bloomberg Businessweek*, 23 giugno 2011 (www.bloomberg.com/news/articles/2011-06-22/the-rise-and-inglorious-fall-of-myspace, ultimo accesso 28 giugno 2017).
[322] Per la storia delle origini di *Facebook* e le novità apportate al *social networking*, vedasi D. KIRKPATRICK, *The Facebook effect*, Simon & Schuster, 2010.
[323] P. TASSI, *Facebook's Advertising Is Starting To Spiral Out Of Control*, in *Forbes*, 1° luglio 2013 (www.forbes.com/sites/insertcoin/2013/07/01/facebooks-advertising-is-starting-to-spiral-out-of-control/#13ad1bcc699c, ultimo accesso 28 giugno 2017).
[324] Vedasi § 2.2.5.

utenti in precedenza non occupati da altre attività rilevanti a scopi commerciali (per esempio, tempo dedicato agli amici, alla famiglia ecc.). La diffusione di *smartphones* multi-funzione ha consentito la presenza pervasiva delle piattaforme digitali nella quasi totalità dei momenti quotidiani: «*in our times, computers, phones and other devices have managed to contest nearly every waking period of time and attention, including that spent at work, waiting for things, and just about every other period imaginable*»[325]. Questo spiega la ragione per cui *Google* ha deciso di sviluppare nuovi prodotti che consentono di incrementare il tempo dedicato dagli utenti alla fruizione dei servizi della piattaforma: si pensi, per esempio, alle *self-driving cars* (*Waymo*) e agli occhiali dotati di realtà aumentata (*Google Glasses*[326]).

6.3. I *data brokers*

La società dell'informazione è costituita da consumatori che utilizzano le tecnologie dell'informazione e della comunicazione (*ICTs*) per interagire fra loro e accedere a prodotti che rendono più semplice la vita quotidiana. In tali interazioni, gli utenti rilasciano ingenti quantità di dati personali, dal cui sfruttamento le imprese attive nei *Big Data submarkets* traggono enormi profitti. Si è visto, per esempio, che le piattaforme digitali utilizzano le informazioni dei consumatori iscritti per distinguere gli annunci degli inserzionisti in base alle preferenze personali.

Oltre a utilizzarle internamente, le imprese che raccolgono e archiviano i dati in prima battuta possono cederli a terzi dietro corrispettivo. In questo senso, come già visto nel paragrafo precedente, nell'era dei *Big Data* le informazioni personali divengono beni oggetto di transazioni economiche fra una pluralità di attori (c.d. commodificazione dell'informazione[327]), accrescendo notevolmente le possi-

---

[325] T. WU, *op. cit.*, 22.

[326] Il progetto *Google Glass*, tuttavia, è stato chiuso definitivamente (*Addio Google Glass, cancellati anche gli account sui social network*, in *Wired*, 26 gennaio 2016 - www.wired.it/internet/social-network/2016/01/26/google-glass-cancellati-account-social-network, ultimo accesso 29 giugno 2017).

[327] Vedasi M. CRAIN, *The limits of transparency: Data brokers and commodification*, City University of New York (CUNY) Academic Works, 2017.

bilità di accumulo di capitale da parte delle imprese. Alcuni agenti economici operano come intermediari fra gruppi di soggetti. Altri attori economici sono specializzati nella vendita dei dati dei consumatori acquisiti da altri: si tratta dei c.d. *data brokers*.

Si considerino alcuni dati che dimostrano l'espansione del fenomeno oggetto di analisi. Oggi, qualche migliaio di imprese opera nel settore in questione, che ha generato ricavi pari a 156 miliardi di dollari USA nell'anno 2012 (un importo che superava di gran lunga l'intero *budget* allora dedicato ai servizi di *intelligence* americani[328]). Due anni dopo, i ricavi annuali ammontavano a circa 200 miliardi di dollari[329]. Nel versante europeo, le dimensioni del mercato sono notevolmente più ristrette: «*the European revenues of large data brokers, such as* Acxiom*,* LexisNexis*, amount only to a fraction of their overall revenues*»[330].

Occorre soffermarsi sui profili problematici derivanti dalle attività commerciali in questione. In primo luogo, si analizzerà la nozione di *data broker*. Poi si passerà al funzionamento del relativo mercato e, quindi, ai prodotti offerti da tali soggetti. In seguito, si esamineranno i benefici e i rischi inerenti all'operato dei *data brokers*, approfondendone in particolare gli aspetti che coinvolgono i consumatori.

È difficile trovare una definizione unitaria di *data brokers* nella letteratura, anche perché l'espressione è di gran lunga più usata nel versante americano che in quello europeo[331]. Un'ottima definizione operativa, ai fini del presente lavoro, può essere la seguente: un *data broker* è «*a company or business unit that earns its primary revenue by supplying data or inferences about people gathered mainly*

---

[328] J.D. ROCKEFELLER IV, *What Information Do Data Brokers Have on Consumers, and How Do They Use It?*, in *US Senate Committee on Commerce, Science, & Transportation*, 18 dicembre 2013 (www.commerce.senate.gov/public/index.cfm/hearings?Id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=A47C081A-D653-4272-8D12-D6EDC1E04DC6, ultimo accesso 30 giugno 2017).

[329] N. MOTT, *The FTC condemns the data brokerage industry's collection practices*, in *Pando*, 27 maggio 2014 (http://pando.com/2014/05/27/the-ftc-condemns-the-data-brokerage-industrys-collection-practices, ultimo accesso 29 giugno 2017).

[330] R. AARON ET AL., *op. cit.*, 13.

[331] In Europa si parla più spesso di *information resellers* o *consumer data analytics* (R. AARON ET AL., *Data Brokers In An Open Society*, Open Society Foundations Report, 2016, 3-4).

from sources other than the data subjects themselves»[332]. Da quest'ultima, si desumono tre elementi fondamentali. Anzitutto, i *data brokers* offrono sul mercato una tipologia particolare di bene (i dati dei consumatori) o di servizio (*data analytics* sulla base di tali dati); in secondo luogo, conducono tale attività in via principale, traendone i maggiori guadagni; in terzo luogo, non acquisiscono gli *input* produttivi direttamente dai consumatori, ma li attingono da fonti diverse da questi ultimi (per esempio, imprese, siti, autorità del settore pubblico, *online stores*, piattaforme digitali ecc., vedasi Figura 6). Da quest'ultimo profilo emerge che soggetti come *Google*, *Apple*, *Facebook*, *eBay* non sono compresi nella categoria dei *data brokers*, giacché acquisiscono i dati degli utenti direttamente, in assenza di un soggetto interposto.

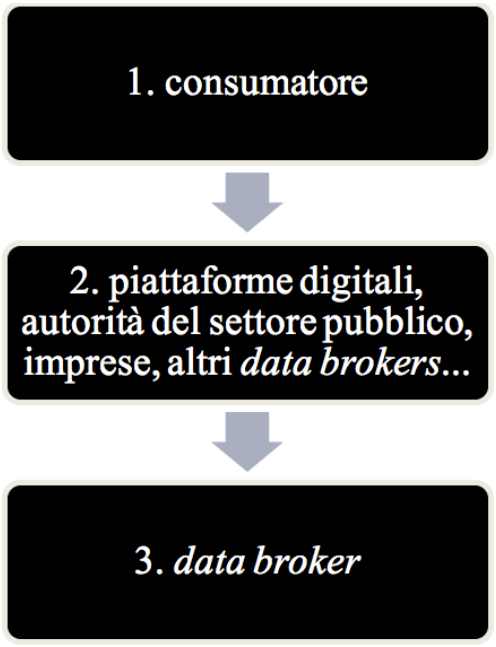

Figura 6. L'acquisizione dei *Big Data* e i *data brokers*.

I soggetti che forniscono i *Big Data* come *input* produttivo ai *data brokers* (Figura 6, punto 2) acquisiscono i dati dai consumatori sia *offline* (si pensi, per esempio, ai dati catastali raccolti dalle autorità del settore pubblico) sia *online*

[332] R. AARON ET AL., *op. cit.*, 4. Nello stesso senso, FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, *op. cit.*, 3 ss. (*report* redatto dalla Federal Trade Commission, agenzia indipendente del governo degli Stati Uniti).

(come i dati delle vendite negli *stores* digitali, le preferenze musicali, le informazioni personali inserite dagli utenti al momento dell'iscrizione a un sito ecc.). Chiaramente, un *data broker* può procurarsi i dati da un altro *data broker*.

I *data brokers*, in seguito, utilizzano i dati così raccolti come materia grezza di nuovi prodotti, utili a settori economici differenti. A prescindere dalla finalità perseguita dai clienti dei *brokers*, questi ultimi immettono sul mercato due principali tipologie di prodotti, "monetizzando" i dati acquisiti dalle loro fonti. Tali attori economici forniscono, da un lato, informazioni e dati dei consumatori ordinati e organizzati in liste (c.d. *actual data*), e, dall'altro, informazioni che sono il risultato di processi di *analytics* (che comprendono l'aggregazione e la combinazione dei dati, c.d. *matching and pooling*), mediante i quali si possono compiere inferenze ed elaborare modelli sulle persone cui i dati si riferiscono[333]. Della seconda categoria, si ricordino, fra gli altri, i c.d. *segments*, liste di consumatori distinti in base a caratteristiche comuni o comportamenti predetti (es. i soggetti che hanno comprato un'automobile, coloro che hanno divorziato ecc.), e i celebri *scores*, cioè le predizioni dei comportamenti futuri di una determinata persona sulla base dei dati personali, molto utilizzate nel settore creditizio.

Nel 2014, la *Federal Trade Commission*, un'agenzia indipendente del Governo americano, ha condotto uno studio sulle attività e sulle pratiche dei *data brokers*, intervistando nove grandi imprese statunitensi che operano nel settore[334]. In particolare, nel *report* emerge che i prodotti offerti da tali soggetti servono ai loro clienti per tre finalità commerciali, in ordine decrescente per mole di ricavi: *marketing*, mitigazione del rischio (*mitigation risk*) e ricerca di persone (*people search*).

Riguardo al primo scopo, le informazioni vendute dai *data brokers* ai propri clienti servono a creare promozioni e annunci personalizzati per ogni cliente. In secondo luogo, i dati forniti dai *brokers* servono a limitare il rischio di incorrere in consumatori poco affidabili o sui quali si dispone uno scarso numero di informazioni (c.d. *mitigation risk*): da una parte, infatti, i prodotti dei *brokers* servono a

---

[333] R. AARON ET AL., *op. cit.*, 11 ss.

[334] I *data brokers* intervistati sono: *Acxiom*, *Corelogic*, *Datalogix*, *eBureau*, *ID Analytics*, *Intelius*, *PeekYou*, *Rapleaf*, *Recorded Future* (FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, *op. cit.*, 7 ss.)

verificare l'identità di un utente[335]; dall'altra, sono utili a identificare e prevenire eventuali frodi perpetrate dai consumatori a danno delle imprese[336]. In terzo luogo, i dati sono utili alla ricerca generica di persone – per esempio, per ritrovare un vecchio amico di cui si sono persi i contatti, o per cercare un potenziale coinquilino[337].

I *data brokers* svolgono attività di cui beneficiano sia le imprese, sia i consumatori. Riguardo alle prime, si sono già analizzate le finalità commerciali dell'utilizzo dei dati organizzati e venduti dai *brokers*. Fra i vari agenti economici, le piccole e le medie imprese (PMI) godono di un beneficio economico notevole: tali soggetti, che, a differenza di quelle di maggiori dimensioni, non sono in grado di dotarsi di un'infrastruttura organizzativa di acquisizione e archiviazione, grazie alla compravendita dei dati riescono a fornire ai consumatori prodotti personalizzati secondo la pluralità e la varietà delle informazioni procurate[338].

Si considerino, ora, i consumatori[339]. Le attività commerciali dei *data brokers* danno origine a una molteplicità di profili problematici, riconducibili per la maggior parte alla nozione (già esaminata in precedenza[340]) di esternalità. Le transazioni che coinvolgono i *data brokers* e i loro clienti, infatti, provocano *spill-overs* positivi e negativi nei confronti di terzi, procurando loro benefici ed esponendoli a rischi. Da una parte, infatti, i consumatori traggono benefici dall'operato dei *data brokers*: secondo quanto affermato *supra*, mediante i dati forniti alle imprese si possono prevenire frodi, migliorare l'offerta dei servizi secondo le preferenze personali di ogni utente e mettere in contatto i consumatori coi propri conoscenti. Dall'altra, i consumatori sono esposti a una serie di rischi, di cui è necessaria un'analisi più dettagliata.

---

[335] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, *op. cit.*, 33 («*banks use such products to comply with "know your customer" identity verification requirements under the* [US legislation]»).
[336] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, *op. loc. cit.* («*for example, one data broker offers a product that indicates whether an email address has existed for a period of time or has a history of transactions related to it*»).
[337] In questo caso, i soggetti che più utilizzano i prodotti dei *data brokers* sono persone fisiche (FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency And Accountability*, *op. cit.*, 34).
[338] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency And Accountability*, *op. cit.*, 47-48.
[339] Si veda anche il paragrafo successivo.
[340] Vedasi § 4.2.

Le esternalità negative derivanti dalle attività dei venditori di informazioni hanno una causa principale e comune: la mancanza di trasparenza[341], che emerge sotto un duplice profilo. In primo luogo, i consumatori non hanno adeguata consapevolezza del fatto che i *data brokers* monetizzino i propri dati personali: secondo uno studio del 2013, il 64% delle persone intervistate non sa che un supermercato può rivendere ad altre imprese le informazioni sulle preferenze di acquisto dei consumatori[342]. Di conseguenza, questi ultimi subiscono una perdita asimmetrica del loro diritto alla *privacy* (*asymmetrical loss of privacy*[343]), dal momento che le società di *data brokerage* conducono attività di compravendita dei dati in assenza di consapevolezza del pubblico degli utenti, nel silenzio di un quadro legislativo americano ed europeo poco chiaro[344]. La maggior parte dei consumatori ignora addirittura l'esistenza dei *data brokers* stessi[345] e, quindi, la possibilità di cancellazione o correzione delle proprie informazioni prevista nei portali presenti nei siti *web* degli *information sellers*[346]. Alcuni *brokers* prevedono che gli interessati possano chiedere il c.d. *opting out*, *id est* l'esclusione dei dati a loro riferiti dalle operazioni di trattamento. Tuttavia, tale facoltà è ambigua, visto che, a seconda dei *data brokers*, assume significati e contenuti differenti. Per esempio, gli interessati hanno la facoltà di ottenere l'eliminazione permanente dei dati personali oggetto di trattamento

---

[341] M. CRAIN, *op. cit.*, 2 («*Transparency, while a laudable goal in many respects, runs up against insurmountable structural limitations within the political economy of the data broker industry*»); UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 2013, 32 ss.; A. KUEMPEL, *The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry*, in 36(1) Northwestern Journal of International Law & Business, 2016, 207 ss.

[342] D.J. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, in 126 Harvard Law Review, 2013, 1886.

[343] L'espressione è di M. ANDREJEVIC, *iSpy: Surveillance and Power in the Interactive Era*, University Press of Kansas, 2007, 7.

[344] Per la trattazione sulle legislazioni europea e americana in tema di *privacy* informazionale e protezione dei dati personali si rimanda al capitolo terzo.

[345] A. KUEMPEL, *op. cit.*, 222.

[346] Taluni soggetti, perseguendo politiche di trasparenza, hanno rivelato le informazioni dei consumatori. Per esempio, nel 2013 *Acxiom*, azienda *leader* nel settore del *data brokerage*, ha aperto un portale mediante cui i consumatori possono monitorare taluni dati posseduti dall'azienda (http://aboutthedata.com, ultimo accesso 30 giugno 2017). Secondo la *CNN*, tale iniziativa è lodevole e ha segnato la vittoria di chi postulava maggiore trasparenza (M. HICKEN, *Find out what Big Data knows about you (it may be very wrong)*, in *CNN Money*, 5 settembre 2013, http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/index.html, ultimo accesso 30 giugno 2017).

della *Acxiom*[347]. Altri venditori (come *Epsilon*), invece, conferiscono la mera possibilità ai soggetti interessati di chiedere che i dati siano esonerati dalla cessione a soggetti terzi, senza ricorrere alla cancellazione effettiva dei dati dai *databases*[348].

In secondo luogo, emerge un ulteriore profilo problematico: il c.d. *aggregation effect*[349]. I *data brokers* possono compiere attività di profilazione senza il consenso dei soggetti interessati mediante l'aggregazione dei numerosi dati acquisiti dalle diverse fonti: «*while each data broker source may provide only a few data elements about a consumer's activities, data brokers can put all of these data elements together to form a more detailed composite of the consumer's life*»[350]. I profili dei consumatori, in seguito, sono inseriti in categorie distinte a seconda delle caratteristiche comuni, sulla base delle quali i clienti dei *data brokers* possono condurre campagne pubblicitarie mirate, ovvero capire con quali individui sia più rischioso avere a che fare. Talune categorie pongono problemi notevoli, giacché si basano sui dati sensibili degli interessati (cioè quelli riguardanti l'etnia, quelli sulla salute degli interessati ecc.): si è a un passo dalla possibilità di discriminazione dei consumatori. Le discriminazioni più delicate concernono i soggetti delle fasce economicamente più deboli[351]. Per esempio, alcuni fra i *data brokers* oggetto di studio della *Federal Trade Commission* del 2014 usano i *segments Urban Scramble* e *Mobile Mixers* per indicare soggetti con un basso reddito, di origini africane o sudamericane[352]; ancora, il *segment Hard Times* della società *Experian* comprende «*older, down-scale and ethnically-diverse singles typically concentrated in inner-city apartments*», cioè «*the bottom of the socioeconomic ladder, the poorest lifestyle segment in the nation*»[353].

---

[347] UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *op. cit.*, 35.
[348] UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *op. loc. cit.*
[349] A. KUEMPEL, *op. cit.*, 219 ss.
[350] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency And Accountability*, *op. cit.*, 46.
[351] UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *op. cit.*, 24 ss.
[352] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency And Accountability*, *op. cit.*, 47.
[353] UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *op. cit.*, 25.

In conclusione, il settore dei *data brokers* deve parte della sua crescita dimensionale negli ultimi anni a una regolamentazione poco stringente negli Stati Uniti[354], sulla base della quale i soggetti economici conducono le proprie attività senza limiti sostanziali, idonei alla tutela efficace della *privacy* degli interessati. Le soluzioni di tutela prospettate dai *brokers* ai consumatori sono disponibili solo *ex post*, cioè «*after their data has been bought, aggregated, and sold*»[355]. Questo comporta che il livello di protezione delle informazioni degli interessati sia assai scarso, poiché, pur innestandosi una richiesta di *opting out*, i dati possono essere già stati trattati e ceduti a terzi[356]. Le questioni riguardanti le attività dei *data brokers* e il rapporto con il diritto alla *privacy* informazionale e la protezione dei dati personali dei consumatori restano aperte, e sono oggetto di analisi del capitolo successivo.

6.4. I consumatori

Com'è noto, i consumatori sono gli attori del sistema economico che utilizzano i beni e servizi offerti dalle imprese sul mercato e agiscono per scopi estranei a quelli commerciali e imprenditoriali[357]. La loro presenza nel ciclo dei *Big Data* è essenziale allo svolgimento delle attività di sfruttamento economico dei dati.

Dalle analisi condotte nei precedenti paragrafi, si evince il ruolo dei consumatori nella catena del valore: da una parte, sono gli utenti finali dei servizi e dei beni offerti dalle imprese, dall'altra, sono coloro che forniscono informazioni fondamentali per le attività commerciali. Come già visto in più occasioni, infatti, le imprese raccolgono e archiviano ingenti quantità di dati degli utenti, che li forniscono volontariamente (*volunteered data*) e li generano passivamente svolgendo attività *online* (*observed data*[358]).

---

[354] Nell'Unione europea, la disciplina in materia di protezione dei dati personali è assai più particolareggiata. Si rimanda la trattazione al capitolo successivo.
[355] A. KUEMPEL, *op. cit.*, 223.
[356] FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency And Accountability*, *op. cit.*, 49.
[357] Secondo il diritto europeo, il consumatore è «*qualsiasi persona fisica che, nei contratti oggetto della presente direttiva, agisca per fini che non rientrano nel quadro della sua attività commerciale, industriale, artigianale o professionale*» (art. 2 n. 1 Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori, G.U. n. L. 304 del 22/11/2011).
[358] Vedasi § 2.1.

A ben vedere, senza i dati dei consumatori non si potrebbe parlare di *data-driven innovation*, dal momento che i venditori (fra i quali spiccano le piattaforme digitali e i *data brokers*) adottano modelli di *business* il cui successo dipende in maniera sostanziale dall'accumulo dei dati personali di tali soggetti. L'uso di tali dati risulta decisivo pure per gli utenti stessi, giacché essi ne traggono importanti benefici, fra cui si annoverano l'offerta di prodotti migliori e personalizzati, la fruizione di servizi gratuiti, le pubblicità mirate secondo le preferenze di ogni utente ecc.[359]

Tuttavia, la raccolta, l'archiviazione e l'utilizzo delle informazioni personali da un lato generano preoccupazioni nei consumatori, dall'altro comportano rischi alla loro tutela. Occorre soffermarsi maggiormente su questi due aspetti non ancora toccati in altri punti del presente lavoro.

I consumatori condividono i propri dati personali non senza esitazioni. La comunità degli utenti ha espresso serie preoccupazioni riguardo alla raccolta e all'utilizzo dei dati personali, come emerge in alcune statistiche. Negli ultimi anni, infatti, si è assistito a una crisi profonda della fiducia dei consumatori nelle imprese che raccolgono e utilizzano i dati personali. In uno studio della *Royal Statistic Society* del 2014, il 78% degli intervistati ha ritenuto che le società usino le informazioni personali esclusivamente a proprio beneficio, e non a quello degli utenti interessati[360]. In un sondaggio condotto dal *think tank* britannico *Demos*[361], inoltre, si è visto che i consumatori adottano atteggiamenti differenti nella condivisione dei dati personali. A seconda della disposizione mentale adottata, gli utenti possono essere distinti in cinque categorie. Il 30% degli utenti è "*non-sharer*", poiché sceglie di minimizzare la diffusione dei propri dati e ha adeguata conoscenza delle problemi inerenti alla protezione dei dati; il 22% dei consumatori adotta un atteggiamento scettico, condividendo i dati solo quando il beneficio personale è evidente; il 20% è "pragmatico", nel senso che preferisce utilizzare i servizi offerti senza badare

---

[359] COMPETITION AND MARKETS AUTHORITY, *op. cit.*, 101.

[360] ROYAL STATISTIC SOCIETY, *Public attitudes to the use and sharing of their data*, 2014 (www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf, ultimo accesso 3 luglio 2017).

[361] DEMOS, *The Data Dialogue*, 2012 (www.demos.co.uk/files/The_Data_Dialogue.pdf?1347544233, ultimo accesso 3 luglio 2017).

troppo a questioni di protezione dei dati e *privacy*; il 19% è "*value hunter*", cioè comprende il valore dei dati personali e i benefici che derivano dalla loro condivisione, non badando troppo alla protezione delle proprie informazioni personali; infine, l'8% può essere definito "*enthusiastic sharer*", poiché «*they categorise a lot of their information as impersonal, and subsequently are comfortable with sharing it. They are amenable to sharing more information in future* […]»[362], spinti dal desiderio di accedere a servizi e beni gratuiti che semplificano la vita quotidiana. La preoccupazione che è ritenuta più grave dagli utenti è la perdita del controllo delle proprie informazioni, che comprende ipotesi come l'utilizzo dei dati personali senza permesso (80% degli intervistati) e la perdita degli stessi (76%[363]). Inoltre, i consumatori temono maggiormente l'operato delle imprese private rispetto a quello delle istituzioni pubbliche: secondo un sondaggio dell'*Information Commissioner's Office* (l'autorità indipendente britannica che si occupa di *data protection*) del 2014, il 64% degli intervistati ha affermato che i soggetti le cui attività di trattamento dei dati personali preoccupano maggiormente sono i motori di ricerca e le piattaforme digitali sociali (*social networks*), mentre solo il 27% ritiene che i soggetti maggiormente problematici siano le autorità pubbliche[364].

Tuttavia, la disposizione mentale dei consumatori differisce dal comportamento adottato. Benché tali dati dimostrino che la maggior parte dei consumatori sia preoccupata dell'operato delle imprese coi propri dati personali, numerosi utenti scelgono di condividere comunque i propri dati personali con le imprese. Si è di fronte, pertanto, a un vero e proprio "paradosso della *privacy*" (*privacy paradox*[365]), per il quale i consumatori accettano il rischio di perdere il controllo delle proprie informazioni, «*seeing the potential problems as being a "necessary evil"*»[366].

---

[362] DEMOS, *op. cit.*, 12-13.
[363] DEMOS, *op. cit.*, 15.
[364] INFORMATION COMMISSIONER'S OFFICE, *Annual Track 2014*, 2014 (https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf, ultimo accesso 3 luglio 2017).
[365] COMPETITION AND MARKETS AUTHORITY, *op. cit.*, 129 ss.
[366] INFORMATION COMMISSIONER'S OFFICE, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, 2015 (http://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf, ultimo accesso 3 luglio 2017). Nello stesso senso, COMMISSIONE EUROPEA, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, 2011, 27.

Ci si sofferma ora sui rischi derivanti dalle attività tipiche dei *Big Data sub-markets*. Nel perseguimento del profitto, le imprese svolgono attività di utilizzo dei dati personali che hanno un ovvio rovescio della medaglia per gli utenti. I rischi più rilevanti sono i. la perdita dei dati e i furti di identità (*identity fraud*); ii. la raccolta, la condivisione e l'utilizzo di dati in modalità non accordate o non previste; iii. gli usi impropri dei dati dei consumatori, che originano contatti indesiderati da terzi (c.d. *nuisance contacts*); iv. l'uso discriminatorio dei dati personali.

In primo luogo, la perdita dei dati interessa sia le imprese che archiviano i *Big Data*, sia i consumatori cui i dati si riferiscono. Da un lato, come si è esaminato in precedenza, la disciplina europea in materia di protezione dei dati personali impone alle imprese che immagazzinano ingenti quantità di dati *standards* di sicurezza molto elevati[367]; dall'altro, se i *databases* si danneggiano per attacchi di *hackers* o per calamità naturali, i consumatori fronteggiano situazioni notevolmente dannose, quali addirittura furti di identità. Per esempio, nel 2015 è stata irrogata una multa di 175mila sterline britanniche alla compagnia assicurativa britannica *Staysure* poiché, a causa di un malfunzionamento del sistema di sicurezza, *hackers* malintenzionati sono riusciti a utilizzare le carte di credito di cinquemila clienti della società[368]. Tuttavia, si contano ancora pochi casi di perdita delle informazioni e furto di identità nel territorio europeo: secondo il sondaggio annuale *Eurobarometro* della Commissione europea del 2011, solo il 2% degli intervistati ha dichiarato di essere stato vittima in prima persona di tali inconvenienti.

In secondo luogo, i consumatori possono non avere piena conoscenza di quali dati siano raccolti dall'impresa e delle modalità di utilizzo di tali informazioni. Spesso, infatti, le imprese non informano adeguatamente i consumatori del trattamento cui sono sottoposti i loro dati personali, violando le norme in materia di protezione dei dati[369]. La *Federal Trade Commission* (FTC), l'agenzia indipendente statunitense che si occupa della tutela dei consumatori, ha richiesto alla società che

---

[367] Vedasi § 3.2.
[368] *ICO fines insurance firm after hacked card details used for fraud*, in *Information Commissioner's Office*, 24 febbraio 2015 (http://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/02/ico-fines-insurance-firm-after-hacked-card-details-used-for-fraud, ultimo accesso 3 luglio 2017).
[369] Vedasi capitolo terzo.

ha creato l'applicazione per *smartphones Brightest Flashlight* di rimuovere i dati personali raccolti e di comunicare le modalità di acquisizione e utilizzo ai consumatori in modo chiaro, consentendo loro di esprimere il proprio consenso all'utilizzo dei dati di localizzazione[370]. Lo sviluppo dell'Internet delle Cose, inoltre, acutizza notevolmente il rischio in questione, dal momento che «[*it*] *can put device manufacturers and their commercial partners in a position to build or have access to very detailed user profiles.* […] *In fact, if uncontrolled, some developments of the IoT could go as far as develop a form of surveillance of individuals*»[371]. Si pensi, per esempio, ai c.d. *wearables*: con questi dispositivi è più probabile che le trasmissioni di dati ai venditori avvengano automaticamente, in assenza della consapevolezza e del consenso degli interessati.

In terzo luogo, se comunicate a terzi, le informazioni personali dei consumatori possono dare origine a una serie di contatti indesiderati (c.d. *nuisance contacts*), come *e-mail* e chiamate da terzi sconosciuti. In taluni casi, si tratta pure di tentativi di frode (c.d. *scams*), per cui i consumatori sono indotti a versare denaro o a fornire ulteriori informazioni personali. Recentemente, per tutelare maggiormente i consumatori, sono state sviluppate apposite applicazioni per *smartphones* e servizi di blocco delle telefonate in arrivo atti a contrastare le chiamate indesiderate[372].

Infine, come già visto in precedenza[373], un rischio notevole è rappresentato dalla possibilità di discriminazione derivante dall'utilizzo dei dati personali. Secondo il sondaggio *Eurobarometro* del 2015 in materia di protezione dei dati, solo il 5% degli intervistati reputa l'essere vittima di discriminazioni (per esempio, nell'assunzione per un determinato impiego, nell'accesso a servizi ecc.) un rischio derivante dalle attività di trattamento dei dati personali[374]. Tuttavia, le attività di profilazione svolte mediante l'accumulo di dati di diverso genere, che consente la

---

[370] *Android Flashlight App Developer Settles FTC Charges It Deceived Consumers*, in *Federal Trade Commission*, 5 dicembre 2013 (www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived, ultimo accesso 3 luglio 2017).
[371] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 2014, 4.
[372] M. WEAVER, *New BT service could end nuisance phone calls*, in *The Guardian*, 16 gennaio 2017 (www.theguardian.com/money/2017/jan/16/bt-says-new-service-could-block-up-to-30m-nuisance-calls-a-week, ultimo accesso 4 luglio 2017).
[373] Vedasi § 6.3.
[374] COMMISSIONE EUROPEA, *Special Eurobarometer 431: Data Protection Report*, 2015, 100-101.

predizione degli attributi personali anche se non resi pubblici dall'utente[375], hanno implicazioni discriminatorie in diversi contesti, potendo compromettere le fasce di popolazione più deboli. Infatti, «*if firms are able to identify consumers' characteristics, they might be able to discriminate against them on the basis of their willingness to pay, but also for their gender, race and sexual orientation*»[376].

In conclusione, quella dei consumatori è una categoria di soggetti che richiede forme di tutela giuridica efficaci ed elevate, dal momento che le attività di raccolta e trattamento dei dati incidono sul loro diritto alla *privacy* e alla protezione dei dati personali. Ma di questo ci si occuperà più specificamente nel capitolo successivo.

[375] Vedasi M. KOSINSKI ET AL., *Private traits and attributes are predictable from digital records of human behavior*, in 110(15) *PNAS*, 2013, 5802 ss.
[376] COMPETITION AND MARKETS AUTHORITY, *op. cit.*, 128.

CAPITOLO TERZO.
I LIMITI GIURIDICI ALL'ACCESSO AI DATI PERSONALI.
TRATTAMENTO E USO

Abstract

Le imprese e le autorità pubbliche che sottopongono a trattamento ingenti quantità di dati personali devono rispettare le norme in materia di privacy *informazionale (negli Stati Uniti) e di protezione dei dati personali (negli Stati membri dell'Unione europea). Lo scopo del presente capitolo è spiegare le caratteristiche fondamentali dei sistemi di tutela statunitense ed europeo alla luce delle nuove sfide poste dalle attività di sfruttamento dei* Big Data*. Dopo aver presentato a grandi linee i due modelli di protezione giuridica, ci si sofferma sui problemi determinati dal trattamento di grandi quantità di dati personali e, quindi, sulle risposte operative di ciascun ordinamento. Infine, si riservano trattazioni a parte per le questioni della c.d. proprietarizzazione dei dati personali, per i recenti sviluppi in materia di* group privacy *e per i limiti all'uso degli algoritmi.*

1. La privacy informazionale e la protezione dei dati personali: due modelli a confronto (cenni)

1.1. Premessa: nuove tecnologie e teorie giuridiche della *privacy*

La storia del diritto alla *privacy*, a ben vedere, è la storia del suo travagliato rapporto col progresso tecnologico. Questa considerazione si basa sul fatto che, a differenza di altri istituti giuridici, il diritto alla *privacy* vanta una varietà di concezioni differenti[377], che legislatori e commentatori di periodi storici diversi hanno avanzato al fine di conciliare le istanze di tutela della personalità degli individui con l'inesorabile innovazione tecnologica. In questo senso, la *privacy* ha dovuto fare i conti con diversi "riposizionamenti tecnologici" che ne hanno cambiato il significato e la portata. In questo senso, tre sono i fatti tecnologici che hanno segnato un mutamento di paradigma nel diritto alla *privacy*: la diffusione delle prime macchine fotografiche, l'impiego di *databases* per l'accumulo di dati personali, e il successo del *web 2.0*[378], cui si collega, in tempi più recenti, la raccolta di quantità smisurate di dati (*Big Data*) da parte di compagnie private che operano nel settore delle comunicazioni *online*. Si passa all'analisi più approfondita di ciascuno di questi mutamenti tecnologici.

Le prime macchine fotografiche portatili, destinate anche a fotografi non professionisti, compaiono sul mercato americano nella seconda metà del XIX secolo. Nel 1888, George Eastman fonda la Kodak, che per più di cent'anni ha prodotto macchine fotografiche che hanno raggiunto una grande popolarità. La diffusione delle fotografie, tuttavia, ha posto un problema giuridico assai rilevante, cioè la possibilità che il soggetto ritratto perdesse il controllo sulle fotografie in cui figurava, magari a sua insaputa. Le crescenti esigenze di tutela hanno avuto un'eco notevole fra i commentatori americani. Com'è ben noto, il celebre articolo *The*

---

[377] Ugo Pagallo individua cinque definizioni del concetto di *privacy*, avvertendo che «*pur mettendo in chiaro questo o quell'aspetto della tutela del diritto, finiscono nondimeno per essere fuorvianti, se assolutizzate*» (U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, 2014, 166 ss. (d'ora in poi: U. PAGALLO, *Il diritto nell'età dell'informazione*)). Nello stesso senso, vedasi H.T. TAVANI, *Philosophical theories of privacy: implications for an adequate online privacy policy*, in 38 *Metaphilosophy*, 2007, 1 ss.

[378] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 168 ss. Vedasi più dettagliatamente *infra*, § 1.2.

Right to Privacy degli avvocati bostoniani Samuel Warren e Louis Brandeis, pubblicato nel 1890 sull'*Harvard Law Review*[379], è considerato all'unanimità l'atto di fondazione teorica del moderno diritto alla *privacy*[380]. L'*incipit* del loro *magnum opus* svela il contesto culturale e politico liberale in cui ha origine tale nuova situazione giuridica soggettiva: «*that the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection*»[381]. Da tali parole, si comprende chiaramente che il diritto alla *privacy* risponde a crescenti esigenze di tutela negativa, consone ai desideri dominanti della borghesia conservatrice americana di quel periodo[382]. La «*full protection in person and in property*» di cui si parla, infatti, è il requisito giuridico necessario per parlare di diritti di libertà negativa, cioè di quelle situazioni giuridiche soggettive che garantiscono ai consociati una vita priva di intrusioni ingiustificate da parte dello Stato e di terzi, tali da poter mettere a repentaglio la sfera esistenziale individuale. In questa tradizione giuridica, che risale alle concessioni regali che Giovanni Senzaterra ha dovuto elargire ai sudditi nella Magna Carta del 1215, si è sviluppata la concezione moderna del diritto di proprietà, inteso, appunto, non solo come diritto di poter disporre dei propri beni, ma anche come diritto di esclusione degli altri dai propri spazi.

---

[379] S. WARREN – L. BRANDEIS, *The Right to Privacy*, in 4(5) *Harvard Law Review*, 1890, 193 ss.
[380] Come è stato acutamente osservato, poiché nei sistemi di *common law* si tutelavano già interessi simili a quello che poi è divenuto il moderno diritto alla *privacy*, «*Warren and Brandeis did not invent the right to privacy from a negligible body of precedent but instead charted a new path for American privacy law*» (D.J. SOLOVE – N.M. RICHARDS, *Privacy's Other Path: Recovering the Law of Confidentiality*, in 96 *Georgetown Law Journal*, 2007, 123). Per la trattazione sul diritto alla riservatezza prima del 1890, si rimanda a quest'ultimo articolo.
[381] S. WARREN – L. BRANDEIS, *op. cit.*, 193.
[382] L.M. FRIEDMAN, *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, Stanford University Press, 2007, 221 («*Warren and Brandeis thought of their shiny new tort as a dragon, guarding the privacy of elites. The mass media and the insatiable curiosity of the lower orders threatened the privacy of men and women who belonged to Warren and Brandeis's class*»).

In principio, dunque, il diritto alla *privacy* si configura come diritto a essere lasciati indisturbati (*right to be let alone*[383]), secondo il criterio del recinto proprietario[384]. Secondo i due eminenti avvocati americani l'estensione della logica dello *jus excludendi alios* risiede nei cambiamenti politici, economici e sociali, per i quali le minacce di intrusione non concernono solo la sfera proprietaria delle cose corporali, bensì coinvolgono anche altri beni (quale, appunto, la riservatezza del singolo) ritenuti egualmente meritevoli di tutela a fronte di novità tecnologiche che coinvolgevano più intensamente la vita dei consociati. La situazione presa in considerazione in tale sede è lo svelamento di fotografie o la pubblicazione di articoli, solitamente a sfondo scandalistico, raffiguranti momenti di intimità quotidiana di personalità celebri. Dal momento che non sussiste un accordo contrattuale fra i *reporters* e i soggetti ripresi, secondo gli autori di *The Right to Privacy* occorre concentrarsi non sugli obblighi derivanti dal contratto, ma sul danno che la condotta dei giornalisti e dei paparazzi *ante litteram*, il cui mercato è in crescente espansione in quel periodo, ha provocato alla sfera sentimentale e spirituale altrui[385]. Peraltro, il tentativo di Warren e Brandeis di concedere nuove forme di tutela in assenza di un quadro legislativo – operazione di estensione tipica del sistema giuridico americano, legato, da una parte, al giusrealismo, e, dall'altro, alle istanze della dottrina – risulta di successo. Dopo la pubblicazione dell'articolo, la giurisprudenza americana, pur con qualche esitazione, accoglie le tesi da loro proposte.

Il secondo passaggio tecnologico avviene nei primi decenni della Guerra Fredda. In questa fase storica, i governi occidentali costituiscono imponenti basi di dati al fine di raccogliere le informazioni rilevanti dei cittadini. A causa degli elevati costi economici, solo le autorità pubbliche possono permettersi la creazione di tali *databases*. Ma l'acquisizione dei dati dei cittadini, benché avvenga per interessi di

---

[383] L'espressione, pur richiamata e resa famosa dall'articolo di Warren e Brandeis, è del commentatore e giudice americano Thomas Cooley (T. COOLEY, *A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract*, Callaghan, 1888, 29).

[384] S. RODOTÀ, *Intervista su privacy e libertà*, Laterza, 2005, 8-9 («*Proprio il divieto di ingresso nello spazio altrui è lo snodo culturale legato alla vicenda originaria del concetto di privacy, di un ambito che appartiene solo a te e a coloro con i quali vuoi condividerlo. È il diritto a essere lasciato da solo. La vita privata veniva quindi tutelata con la logica del recinto*»).

[385] N.M. RICHARDS – D.J. SOLOVE, *op. cit.*, 1892.

pubblica sicurezza e di efficienza della pubblica amministrazione, si scontra necessariamente con l'esigenza opposta degli amministrati, che desiderano porre limiti sostanziali a tali pratiche. In tale contesto, dunque, lo spettro applicativo della *privacy* si estende notevolmente, fino a comprendere non solo situazioni di tutela da intrusioni della vita privata, ma anche la protezione delle persone dal punto di vista della raccolta dei dati e sul piano informazionale. Emerge una concezione informazionale (o informativa) della *privacy*, che ha sviluppi autonomi rispetto all'impostazione originaria, fondate sul concetto di non intrusione nella vita privata degli individui. Nella Comunità europea (poi Unione europea), tale concezione prende il nome di protezione dei dati (*data protection*[386]); negli Stati Uniti d'America, invece, non vi sono formule univoche, e si parla indifferentemente di *information privacy law*[387] o di *information rules*[388].

Il terzo prodotto tecnologico che pone nuove e notevoli problematiche è la rete del *world wide web* (www) nella versione 2.0[389], che segue allo statico *web 1.0* a metà del primo decennio del XX secolo. Nell'ambito del nuovo ricavato tecnologico, le persone svolgono una varietà di attività, che, in numerosi casi, diventano il surrogato di operazioni condotte nella realtà virtuale: comunicano, creano profili personali, conducono le loro professioni, comprano prodotti. Tali interazioni hanno un risultato comune, cioè il fatto che producono sterminate quantità di dati personali. Il processo di acquisizione e trattamento dei dati diviene «*invisibile, perché immanente alle azioni quotidiane e attuato in forma continuativa, discreta e disponibile, al limite, in tempo reale*»[390]. Così, il diritto alla *privacy* informazionale viene sottoposto a nuove sfide. Di questo ci si occuperà nei paragrafi successivi[391].

---

[386] Nella c.d. Carta di Nizza (Carta dei diritti fondamentali dell'Unione europea, G.U. C. 202 del 7.6.2016), infatti, il diritto alla protezione dei dati personali (art. 8) è considerato distintamente dal rispetto alla vita privata e familiare (art. 7). L'espressione "protezione dei dati" indica la scelta di una soluzione normativa onnicomprensiva, concernente il trattamento dei dati personali in ogni settore economico. Sulle differenze fra *privacy* informazionale e protezione dei dati personali, vedasi U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 225 ss.
[387] D. SOLOVE – P.M. SCHWARTZ, *Information Privacy Law*, Wolters Kluwer, 2015.
[388] N.M. RICHARDS – J. KING, *Big Data Ethics*, in 49(2) *Wake Forest Law Review*, 2014, 411 ss.
[389] T. O'REILLY, *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, in *OReilly*, 30 settembre 2005 (www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, ultimo accesso 29 aprile 2017).
[390] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 174.
[391] Vedasi § 2.

In via preliminare, occorre svolgere una rapida analisi per capire le caratteristiche e le principali differenze e affinità dei modelli di tutela dei due sistemi giuridici occidentali cui si farà riferimento nei paragrafi successivi, *id est* quello degli Stati Uniti d'America e quello dell'Unione europea.

1.2. Il modello statunitense

Il diritto alla *privacy* negli Stati Uniti ha conosciuto uno sviluppo assai complesso, che è il frutto delle interazioni dei formanti giurisprudenziale, dottrinale e legislativo[392]. Si possono individuare talune linee-guida di evoluzione della materia. Occorre distinguere, infatti, fra il diritto di origine giurisprudenziale (*case law*) e il diritto positivo degli *statutes*, cioè delle leggi che regolano il diritto alla *privacy* a livello federale e statale.

Il primo osservabile è il *judge-made law*. All'interno di esso, si trova, da una parte, l'operato dei giudici dei singoli Stati federati, che accordano una tutela basata sul *tort law*, e, dall'altra, quello della Corte Suprema federale.

Anzitutto, in seguito alla teorizzazione di Warren e Brandeis, la *privacy* si è sviluppata all'interno del *tort law*, che, *mutatis mutandis*, corrisponde approssimativamente alla categoria giuridica degli illeciti civili del *civil law*. Già i due avvocati di Boston inquadrano la tutela giuridica principalmente nella *law of torts*[393] e, in casi limitati, nei rimedi dell'*equity* (*injuctions*) e negli illeciti penali[394]. Dopo l'uscita dell'articolo, la giurisprudenza americana accoglie le tesi avanzate in dottrina e adotta la prima impostazione rimediale, estendendola a situazioni diverse da quelle originariamente concepite dai due giuristi americani[395]. Peraltro agli occhi dei giudici[396] il diritto alla *privacy* resta una categoria minoritaria e residuale del *tort law*[397] per quasi settant'anni. Il diritto alla *privacy* rimane oggetto di discussioni

---

[392] Sulla nozione di formante, si veda R. SACCO, *Introduzione al diritto comparato*, UTET Giuridica, 1992.
[393] Vedasi U. MATTEI, *Il modello di Common Law*, Giappichelli, 2014.
[394] S. WARREN – L. BRANDEIS, *op. cit.*, 219 ss.
[395] Fra i più importanti, si considerino *Roberson v. Rochester Folding Box Co.*, 64 N.E. 442 (1902); *Pavesich v. New England Life Insurance Co.*, 50 S.E. 68 (1905), *Brents v. Morgan*, 299 S.W. 967 (1927); *Melvin v. Reid*, 297 P. 91 (1931).
[396] N.M. RICHARDS – D.J. SOLOVE, *op. cit.*, 1895.
[397] G.E. WHITE, *Tort Law in America: An Intellectual History*, Oxford University Press, 2003, 174.

limitate[398] e di decisioni oscillanti fino al 1960, anno in cui William Prosser pubblica il famoso articolo *Privacy*[399]. In particolare, analizzando circa trecento casi giurisprudenziali riguardanti la *privacy*, l'autore prende atto che le corti americane hanno configurato il diritto alla *privacy* in una molteplicità di modi diversi, e tenta di conferire un ordine alle fattispecie differenti, distinguendo quattro tipologie differenti di *torts* che poco hanno in comune, «*except that they were injuries to the right to be let alone*»[400]. Prosser, che successivamente opera come *reporter* del *Second Restatement of Torts*[401], include la sua teoria quadripartita in quest'ultimo lavoro.

La *tort privacy* ha mostrato numerosi limiti rispetto alle nuove esigenze di tutela delle informazioni personali, dal momento che le quattro tipologie di *torts* si sono rivelate scarsamente applicabili al nuovo ambiente digitale di raccolta e trattamento dei dati[402].

In secondo luogo, la Corte Suprema ha dato un impulso decisivo allo sviluppo del diritto alla *privacy* nel versante nordamericano, riconducendone la tutela soprattutto al primo e al quarto emendamento della Costituzione americana, che tutelano, rispettivamente, la libertà di parola (*freedom of speech*[403]) e il diritto di non essere sottoposti a perquisizioni e sequestri irragionevoli. Nel celeberrimo caso *Katz v. United States*[404], la Corte Suprema estende la tutela del diritto alla *privacy*

---

[398] Fra i commentatori che hanno elaborato analisi in merito prima dell'opera di Prosser, si vedano, *inter alios*, D. O'BRIEN, *The Right of Privacy*, in 2 *Columbia Law Review*, 1902, 437 ss.; R. POUND, *Interests of Personality*, in 28 *Harvard Law Review*, 1915, 343 ss.

[399] W.L. PROSSER, *Privacy*, in 48 *California Law Review*, 1960, 383 ss. Già in precedenza, il giurista americano si era già dedicato all'elaborazione di nuove teorie sul diritto alla *privacy*. Si vedano le varie edizioni dell'altra celebre opera di Prosser, W.L. PROSSER, *Handbook on the Law of Torts*, West Pub. Co., 1941 (meglio noto come *Prosser on Torts*).

[400] N.M. RICHARDS – D.J. SOLOVE, *op. cit.*, 1899. Tali *torts* sono:

i. *intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;*
ii. *public disclosure of embarrassing private facts about the plaintiff;*
iii. *publicity which places the plaintiff in a false light in the public eye;*
iv. *appropriation, for the defendant's advantage, of the plaintiff's name or likeness.*

[401] I *Restatements of the Law* sono trattati su diverse materie giuridiche che raccolgono i principi adottati dai giudici nel tempo nei precedenti (*case law*) e servono a informare i giudici delle evoluzioni del diritto.

[402] In questo senso, N.M. RICHARDS – D.J. SOLOVE, *Prosser's Privacy Law: A Mixed Legacy*, in 98 *California Law Review*, 2010, 1887 ss.; N.M. RICHARDS, *The Limits of Tort Privacy*, in 9 *Journal of Telecommunications and High Technology Law*, 2011, 357 ss.

[403] Il primo emendamento non concerne solo la libertà di parola, ma anche, fra gli altri la libertà religiosa, il diritto di associazione e il diritto all'anonimato.

[404] *Katz v. United States*, 389 U.S. 347 (1967).

ai luoghi pubblici, sostenendo che la protezione del quarto emendamento riguarda il popolo, cioè i cittadini, e non i luoghi di proprietà degli stessi. Inoltre, tale precedente estende la tutela del diritto in questione a una serie eterogenea di ipotesi in cui la persona ha una "ragionevole aspettativa" di *privacy*. La protezione accordata dai supremi giudici, quindi, si è allargata progressivamente nel tempo, estendendosi alle nuove sfide tecnologiche dettate dalla raccolta e dal trattamento delle informazioni personali[405]: si pensi, per esempio, alla sorveglianza aerea (*Dow Chemical Co. v. United States*[406]), alle rilevazioni dei sensori termici (*Kyllo v. United States*[407]) e, da ultimo, come si vedrà, alla geo-localizzazione effettuata mediante i dispositivi di tracciamento GPS (*United States v. Jones*[408]).

Si passa, ora, all'altro punto dell'analisi: la tutela della *privacy* informazionale nel diritto degli *statutes* federali e degli Stati federati. Parallelamente agli sviluppi del *case law*, infatti, si è sviluppata una fitta rete di leggi federali che disciplinano la *privacy* informazionale. Questo *patchwork* è costituito da interventi settoriali che regolamentano «*only a specific context of information use*»[409] di specifici tipologie di enti. Tale approccio risulta pragmatico e reattivo, nel senso che, da una parte, offre soluzioni legislative concrete limitatamente a certi ambiti, e dall'altra, si configura come risposta specifica dell'ordinamento ai problemi che scaturiscono da ciascun ricavato tecnologico. Ne deriva il rischio, tuttavia, che il quadro legislativo non stia al passo coi tempi: «*when a new technology or practice emerges to challenge existing assumptions about privacy in the United States, months or years go by before it will be restricted in any way, since the new behavior falls within a gap in our sectoral statutory framework*»[410]. Fra i vari interventi normativi settoriali, si ricordino il Fair Credit Reporting Act (1970), il Privacy Act (1974) e il Video Privacy Protection Act (1988).

---

[405] Per una trattazione rigorosa e coerente sul tema, vedasi U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 193 ss.
[406] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).
[407] *Kyllo v. United States*, 533 U.S. 27 (2001).
[408] *United States v. Jones*, 565 U.S. 400 (2012).
[409] P. SCHWARTZ, *The Value of Privacy Federalism*, in B. ROESSLER – D. MOKROSINSKA, *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge University Press, 2015, 326.
[410] L. STRAHILEVITZ, *Toward a Positive Theory of Privacy Law*, in 126 *Harvard Law Review*, 2013, 2036.

Anche sul piano dello *statutory law* dei singoli Stati, la *privacy* informazionale trova adeguata tutela settoriale, ma le legislazioni di ogni Stato federato possono differire le une dalle altre. La Corte Suprema ha riconosciuto, nel sopracitato caso *Katz*, l'importanza dell'operato legislativo degli Stati in materia di *privacy*: secondo i giudici, «*the protection of a person's general right to privacy* […] *is* […] *left largely to the law of the individual States*»[411]. In particolare, le normative statali riguardano la notifica delle violazioni dei dati personali (*data breach notification statutes*) e l'eliminazione di tali informazioni (*data disposal law*[412]).

Infine, va aggiunta un'ultima considerazione riguardo al rango che il diritto ha assunto nella propria lunga evoluzione storica al di là dell'Oceano. In ambito europeo, come si vedrà *infra*, il legislatore ha configurato la *privacy* come diritto fondamentale; negli Stati Uniti, invece, la tutela di tale situazione giuridica si è configurata essenzialmente come una propaggine dei diritti del consumatore[413] e, quindi, come diritto disponibile, che può essere trasferito secondo la volontà e il consenso dell'interessato nei limiti degli accordi col titolare del trattamento. A conferma di questa considerazione, occorre notare che la *Federal Trade Commission* (FTC) è l'*authority* incaricata di controllare la corretta applicazione delle *privacy policies* da parte delle imprese private, benché il ruolo effettivo di questa agenzia sia molto limitato nella prassi[414].

1.3. Gli sviluppi nel versante europeo: la protezione dei dati personali come diritto fondamentale

Al di qua dell'Atlantico, la tutela dei dati personali ha conosciuto uno sviluppo differente da quello riscontrato negli Stati Uniti in materia di *privacy* informazionale.

---

411 *Katz v. United States*, 389 U.S. 347 (1967), 350-51.
412 P. SCHWARTZ, *The Value of Privacy Federalism*, *op. cit.*, 326-27; P.M. SCHWARTZ – E.J. JANGER, *Notification of data security breaches*, in 105 *Michigan Law Review*, 913 ss.
413 In questo senso, L. MIGLIETTI, *Profili storico-comparativi del diritto alla privacy*, in *Rivista di diritti comparati*, 2014 (www.dirritticomparati.it/profili-storico-comparativi-del-diritto-alla-privacy, ultimo accesso 14 luglio 2017).
414 U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 268. Sul ruolo della FTC in materia di *privacy*, vedasi D.C. VLADECK, *Charting the Course: The Federal Trade Commission's Second Hundred Years*, in 83 *George Washington Law Review*, 2015, 2101 ss.

Fra i molteplici punti di analisi che si potrebbero toccare riguardo alla tutela dei dati personali nell'Unione europea, occorre inquadrare, come si è fatto rispetto al diritto alla *privacy* nordamericano, quello che più si addice agli argomenti oggetto del presente lavoro: da un lato, soffermarsi sulla tutela concessa a un livello che può dirsi federale, e, dall'altro, sul diritto alla *privacy* intesa come diritto fondamentale.

Anzitutto, il modello di tutela cui ha aderito il Vecchio continente è essenzialmente di tipo federale. La tutela dei dati personali, infatti, è oggi disciplinata dal Regolamento (UE) 2016/679 (il c.d. Regolamento Generale sulla Protezione dei Dati, *General Data Protection Regulation*, o GDPR[415]), che sostituisce la precedente Direttiva 95/46/CE[416]. Al precedente sistema di protezione federale debole, in cui ogni Stato membro ha recepito la direttiva mediante atti normativi nazionali ed era vincolato nei principi espressi e nei risultati da raggiungere compresi nell'atto, è seguita una tutela federale forte, benché il Regolamento 2016/679 rappresenti un caso legislativo alquanto atipico in cui si mescolano norme direttamente applicabili ed elementi che necessitano di strumenti applicativi di diritto interno[417].

In secondo luogo, al di qua dell'Atlantico la protezione dei dati personali assume il rango di diritto della personalità. La Carta dei diritti fondamentali dell'Unione europea include, fra le libertà fondamentali, la tutela dei dati degli interessati, annoverandone alcuni contenuti: il principio di lealtà, il principio finalistico, quello consensualistico e, infine, il diritto di accesso e di rettifica dei dati da parte della persona interessata (art. 8 par. II). Il Trattato sul funzionamento dell'Ue richiama la protezione dei dati personali all'art. 16, par. I. La tradizione giuridica europea in materia di *privacy* si innesta sulla dignità della persona umana, secondo

---

[415] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora in poi: Regolamento (UE) 2016/679), G.U. n. L. 119/1 del 4/5/2016.

[416] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. n. L. 281 del 23/11/1995.

[417] Si pensi, per esempio, che gli Stati membri devono istituire un'autorità di controllo indipendente incaricata di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (art. 51 par. I Regolamento (UE) 2016/679).

quanto affermato nel 1983 dai giudici costituzionali tedeschi nella celebre sentenza *Volkszählungs-Urteil*, che ha sancito il diritto all'auto-determinazione informazionale degli individui (*informationelle Selbstbestimmung*[418]).

2. Big Data*: la privacy informazionale, la protezione dei dati personali e il loro letto di Procuste*

Come si è visto, il diritto alla *privacy* informazionale e la protezione dei dati personali hanno conosciuto sviluppi differenti rispettivamente nei sistemi giuridici degli Stati Uniti d'America e dell'Unione europea. Se oggi al significato originario della *privacy* come protezione dai fastidi delle intrusioni dei *media* nella vita privata se ne sono accostati altri[419], nuove tecnologie minacciano i fondamenti del diritto alla *privacy* informazionale, o quantomeno ne implicano il rinnovamento. C'è chi, addirittura, ne annuncia la morte: secondo una celebre dichiarazione di Mark Zuckerberg, la *privacy* come controllo delle informazioni è morta sotto il fuoco delle nuove tecnologie digitali dei *social network*[420]. Tuttavia, com'è stato acutamente osservato, la *privacy* non è un concetto obsoleto nella società dell'informazione, purché non se ne limiti il campo di applicazione a casi di diffusione di informazioni personali che i consociati desidererebbero non divulgare o tenere segrete: «*if we*

---

[418] «[…] *Un ordine sociale – e l'ordine giuridico che lo supporta – in cui i cittadini non siano più in grado di determinare chi conosce cosa su di essi, quando, con quali mezzi, sarebbe incompatibile con il diritto all'auto-determinazione informazionale. Chiunque abbia il dubbio che il proprio comportamento dissenziente possa essere registrato in qualsiasi momento e immagazzinato permanentemente sotto forma di informazione, tenterà di non attrarre l'attenzione tramite tale comportamento. Ciò osterebbe non solo alle possibilità di sviluppo personale degli individui, ma anche al bene pubblico, poiché l'auto-determinazione è un prerequisito per un ordine politico libero, basato sulla capacità di azione politica e collaborazione dei propri cittadini*» (Bundesverfassungsgericht, Urteil v. 15 Dezember 1983. Trad. it. di U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 231-32; vedasi anche A. GLORIOSO, *Un nuovo concetto di "auto-determinazione informazionale" come bussola concettuale per navigare il nuovo mondo digitale*, in M. DURANTE e U. PAGALLO, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet, 2012, 383 ss.).

[419] L.M. FRIEDMAN, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, in 30 *Hofstra Law Review*, 2002, 1125 («*In hindsight, it looks as if the Warren and Brandeis idea of privacy – protection from the despicable nosiness of the media – never got much past the starting post; and is now effectively dead*»).

[420] B. JOHNSON, *Privacy's dead: Facebook chief*, in *The Sydney Morning Herald*, 19 gennaio 2010 (http://www.smh.com.au/business/privacys-dead-facebook-chief-20100118-mgs8.html, ultimo accesso 11 luglio 2017).

think about privacy as the question of what rules should govern the use of personal information, then privacy has never been more alive»[421].

Dall'esame condotto nel precedente capitolo è emerso che la raccolta e il trattamento di ingenti quantità di dati personali siano divenute attività essenziale sia per i governi, sia per le grandi e piccole compagnie private del settore dei fornitori dei servizi in rete, che offrono prodotti *online* nei mercati di cui si è illustrato il funzionamento nel capitolo precedente. Per evitare che, con la diffusione dei nuovi ricavati tecnologici, la *privacy* informazionale sia stretta in un letto di Procuste, e, quindi, che le attività degli agenti economici ledano i diritti degli interessati, occorre bilanciarne i rispettivi interessi e diritti, tenendo in considerazione le esigenze degli attori che sfruttano i *Big Data* a fini commerciali e delle autorità pubbliche che li riutilizzano per diverse finalità (efficienza della pubblica amministrazione, pubblica sicurezza ecc.). Infatti, «*if it is true that Big Data (and technology in general) is changing the meaning of the word "privacy," then we all benefit by exploring what those changes are through a discussion of what is valuable about privacy. Understanding what is valuable about various aspects of privacy, even in light of recent rapid transformations, is helpful when deciding what action we should and should not take to honor individual privacy*»[422].

L'analisi dei prossimi paragrafi è bipartita. Da un lato, si passeranno in rassegna i problemi di maggiore rilievo inerenti all'attività di raccolta e trattamento dei dati personali, cioè all'accesso ai *Big Data*; dall'altro, si prenderanno in esame le soluzioni giuridiche vigenti e quelle prospettate negli ordinamenti nordamericano ed europeo. Entrambe le analisi prenderanno in considerazione gli anelli della catena del valore dei *Big Data*, oggetto di trattazione del precedente capitolo[423].

---

[421] N.M. RICHARDS – J. KING, *op. cit.*, 410.
[422] K. DAVIS – D. PATTERSON, *Ethics of Big Data*, O'Reilly, 2012, 17.
[423] Sulla catena del valore dei *Big Data*, si veda il capitolo secondo.

2.1. *Big Data*, grandi problemi

La rivoluzione dei *Big Data* ha comportato l'insorgere di problematiche concernenti le posizioni giuridiche delle persone fisiche interessate. Alcune tematiche riguardanti i consumatori sono già state affrontate in precedenza[424]. È necessario ora analizzare meglio i problemi che rilevano maggiormente ai fini del diritto alla *privacy* informazionale (nel versante americano) e della protezione dei dati personali (nell'Unione europea).

Interessanti spunti di riflessione provengono dagli Stati Uniti. A ben vedere, la *privacy* informazionale si configura come gestione e controllo dell'accesso ai dati in ciascuna delle diverse fasi della catena del valore dei *Big Data*[425].

Nella letteratura giuridica americana, svariati autori hanno osservato che i rapporti fra l'accesso alle informazioni personali e le relative norme di regolamentazione sono riconducibili a quattro problematiche essenziali (Figura 7):

i. invasione di spazi, relazioni e decisioni personali meritevoli di tutela;
ii. raccolta di informazioni personali;
iii. trattamento e uso di informazioni personali;
iv. diffusione di informazioni personali[426].

[424] Si rimanda al § 6.4 del capitolo secondo.
[425] Vedasi capitolo secondo.
[426] N.M. RICHARDS – J. KING, *op. loc. cit*. Nello stesso senso e più nello specifico, D.J. SOLOVE, *A Taxonomy of Privacy*, in 154(3) *University of Pennsylvania Law Review*, 2006, 477 ss.; D.J. SOLOVE, *Understanding Privacy*, Harvard University Press, 2008, 11.

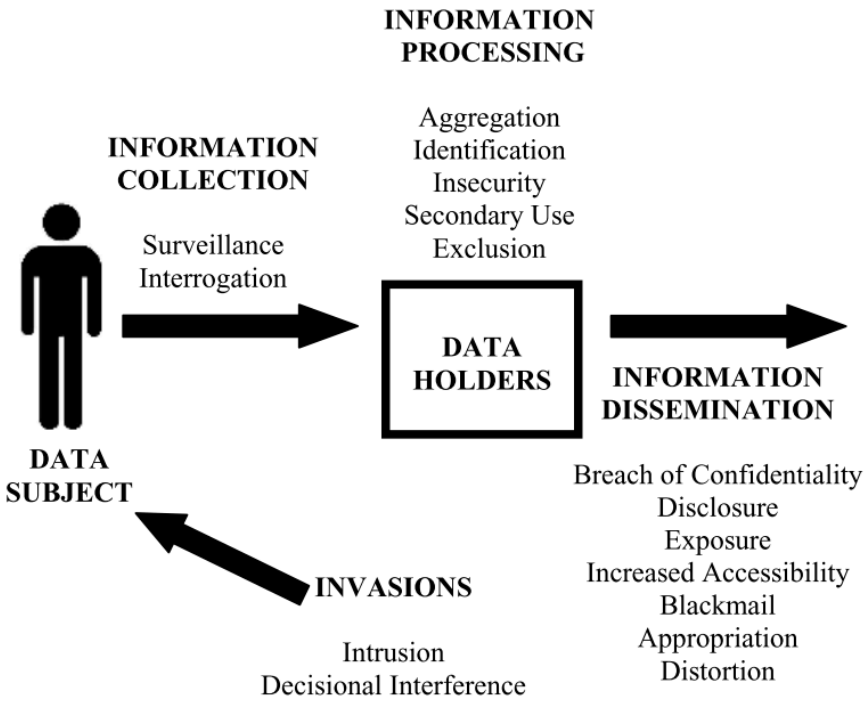

Figura 7. I problemi concernenti la *privacy* informazionale. Fonte: D.J. SOLOVE, *A Taxonomy of Privacy*, in 154(3) *University of Pennsylvania Law Review*, 2006, 490.

Questa tassonomia, che il legislatore statunitense ha idealmente seguito per tutelare i diversi beni giuridici, è uno strumento euristico utile a inquadrare distintamente i problemi posti dalla rivoluzione dei *Big Data* all'accesso ai dati personali.

In particolare,

i. l'acquisizione di dati personali pone problemi di sorveglianza di massa dei soggetti interessati (c.d. *dataveillance*);

ii. il trattamento dei dati personali, invece, concerne l'aggregazione dei dati, la sicurezza di archiviazione e l'identificazione degli interessati (Figura 1).

Si passa alla trattazione di tali questioni.

2.1.1. La raccolta di informazioni personali: *dataveillance*

Come si è visto, la raccolta di dati personali da parte di una pluralità di agenti, di natura privata e pubblica, determina un vantaggio informativo considerevole[427]. La straordinaria capacità di osservazione degli utenti, effettuata su larga scala, consente alle istituzioni pubbliche di tenere sotto controllo constante gli interessati come mai è stato fatto in precedenza, cioè di sottoporli a forme di sorveglianza di massa[428].

Prima di procedere con l'analisi di tali pratiche, ci si sofferma sugli aspetti definitori. È difficile trovare una definizione soddisfacente di "sorveglianza". Sul piano meramente formale, le attività di sorveglianza consistono in «*the watching, listening to, or recording of an individual's activities*»[429]. Ai fini del presente lavoro, più rilevante è la nozione "finalistica" di sorveglianza, maggiormente percepita dal significato popolare che le viene attribuito: la sorveglianza è «*the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction*»[430].

I governi e le istituzioni pubbliche si dedicano ad attività di sorveglianza dei cittadini da molto tempo. A differenza di quanto si potrebbe pensare, non solo i regimi autoritari intraprendono tali pratiche[431]. In seguito agli attentati terroristici dell'11 settembre 2001, la maggior parte degli Stati democratici occidentali ha investito ingenti quantità di denaro pubblico per la creazione di reti di sorveglianza ben ramificate, gestite da un'industria che opera dagli anni della Guerra fredda al servizio dei governi[432]. Secondo un sondaggio di *Privacy International* del 2007, il Regno Unito e gli Stati Uniti sono "*endemic surveillance societies*", al pari della

---

[427] Si rimanda al § 1 del capitolo secondo.
[428] Si parla, infatti, di "età della sorveglianza" (D. LYON, *Surveillance Studies: An Overview*, Polity Press, 2007; J. COHEN, *What Privacy is For*, in 126(4) *Harvard Law Review*, 2013, 1904 ss.; N.M. RICHARDS, *The Dangers of Surveillance*, in 126(7) *Harvard Law Review*, 2013, 1934 ss.; J. COHEN, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, in D. BARNEY ET AL., *The Participatory Condition in the digital age*, University of Minnesota Press, 2016).
[429] D.J. SOLOVE, *A Taxonomy of Privacy*, *op. cit.*, 490.
[430] D. LYON, *Surveillance Studies: An Overview*, op. *cit.*, 14.
[431] Per esempio, le autorità pubbliche della Repubblica Popolare Cinese utilizzano i dati ricavati da *Internet* per individuare e contrastare i dissidenti politici (N.M. RICHARDS, *The Dangers of Surveillance*, *op. cit.*, 1937).
[432] Vedasi PRIVACY INTERNATIONAL, *The global surveillance industry*, 2016.

Cina e della Russia[433]. Negli Stati Uniti, la National Security Agency (NSA) dispone di ampi poteri di sorveglianza, potendo svolgere attività di sorveglianza anche in assenza di precise autorizzazioni giudiziali (*judicial warrant*[434]).

Con l'avvento dei *Big Data*, poi, tali attività sono divenute molto più complesse e penetranti, e si è affermata una tipologia di sorveglianza di massa basata sui dati rilasciati dai cittadini *online* (*dataveillance*[435], o nuova sorveglianza[436]). Queste attività sono oltremodo penetranti, dal momento che, da un lato, sono effettuate sistematicamente, in assenza di scopi predeterminati, e, dall'altro, «*go well beyond the proposition of scrutinizing individuals as it penetrates every fiber of the social fabric*»[437].

Qualche anno fa, la sorveglianza *data-driven* ha richiamato l'attenzione degli studiosi e dell'opinione pubblica in seguito a due celebri casi che hanno assunto prontamente rilievo mediatico. Nel 2012, un'inchiesta condotta dall'edizione statunitense di *Wired* ha gettato luce sulla costruzione di un gigantesco *data centre* dell'NSA nel deserto dello Utah per l'immagazzinamento e l'analisi di dati degli utenti ricavati da *Internet*. L'anno successivo, l'informatico Edward Snowden ha svelato al quotidiano britannico *The Guardian* il funzionamento delle attività di sorveglianza di massa del governo americano, condotte dall'NSA mediante l'accesso diretto ai dati di *Google*, *Facebook*, *Skype*, *Yahoo*, *Microsoft* ed *Apple*[438]. In altri termini, al ruolo dei governi nel condurre operazioni di sorveglianza di massa si è accostato l'operato delle aziende private operanti nel settore dei fornitori dei servizi in rete. Dall'analisi dei *Big Data* raccolti *online*, infatti, si possono facilmente scovare abitudini, preferenze, caratteristiche personali e predire modelli di

---

[433] K. ZETTER, *World's Top Surveillance Societies – Updated with link*, in *Wired*, 31 dicembre 2007 (www.wired.com/2007/12/worlds-top-surv, ultimo accesso 12 luglio 2017).
[434] J. RISEN – E. LICHTBLAU, *Bush Lets U.S. Spy on Callers Without Courts*, in *New York Times*, 16 dicembre 2005 (www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html, ultimo accesso 13 luglio 2017).
[435] R. RALEY, *Dataveillance and Countervailance*, in L. GITELMAN, *"Raw Data" is an Oxymoron*, MIT Press, 2013; J. VAN DIJCK, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in 12 *Surveillance and Society*, 2014, 197 ss.
[436] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 179 ss.
[437] J. VAN DIJCK, *op. cit.*, 205.
[438] D. LYON, *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*, in *Big Data and Society*, 2014, 1 ss.

comportamento degli utenti[439]. I risultati dell'analisi sono dettagliati, precisi e accurati, dal momento che le imprese attingono a svariate fonti di produzione dei dati: oltre ai dati delle attività *online*, dispositivi come fotocamere digitali e *softwares* consentono di scandagliare le personalità degli interessati in modo pervasivo, e di tenerne sotto controllo le attività quotidiane. I dati ricavabili dall'*Internet of Things* consentono la creazione di profili oltremodo dettagliati: per esempio, i sensori dei c.d. *wearables* (orologi e braccialetti *smart*) possono rilevare dati inerenti alle caratteristiche psico-fisiche di un soggetto interessato, quale il ritmo delle pulsazioni cardiache[440].

Tali risorse informative giovano notevolmente alle autorità pubbliche, che non possono prescindere dalle operazioni di raccolta e archiviazione del settore privato. Le imprese, infatti, da una parte forniscono tecnologie innovative e informazioni dei loro clienti ai governi; dall'altra, conducono le operazioni di trattamento su larga scala con la partecipazione e il consenso formale degli interessati stessi (c.d. "sorveglianza liquida[441]").

Finora, «*l'automazione dei servizi ha* […] *offerto un equilibrio tra le aspettative di riservatezza da parte degli utenti, e le esigenze commerciali delle imprese, secondo un modello di auto-regolamentazione e concorrenza tra i diversi fornitori di servizi nelle società ICT-dipendenti*»[442]. Nondimeno, le attività di *dataveillance* hanno evidenti risvolti problematici in tema di diritto alla *privacy* informazionale, potendo compromettere una tutela effettiva se condotte senza limiti sostanziali. Vi sono principalmente due ordini di problemi strettamente interconnessi, oltre a quelli che saranno analizzati nei paragrafi successivi[443].

Anzitutto, la sorveglianza di massa influenza notevolmente il comportamento dei cittadini, che, percependo il rischio di tale controllo, sono reticenti o refrattari a compiere determinate azioni o a svolgerle in maniera continuativa (c.d.

---

[439] Vedasi § 6.4 del capitolo secondo.
[440] Sulle modalità di raccolta dei dati si rimanda al § 2 del capitolo secondo.
[441] L'espressione è di Z. BAUMAN – D. LYON, *Liquid Surveillance: A Conversation*, Polity Press, 2012.
[442] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 180.
[443] Si tratta delle esternalità negative di cui parla J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data* in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione), 1 ss. Per una trattazione più ampia si rimanda al § 6.2 del presente capitolo e al § 4.2 del capitolo secondo.

chilling effect[444]). Questo aspetto critico incide considerevolmente sul diritto all'auto-determinazione informazionale degli interessati, come sancito dal *Bundesverfassungsgericht* nel lontano 1983[445], minando la possibilità di sviluppo di un ordine politico libero, basato sulla capacità di azione politica e collaborazione dei propri cittadini.

In secondo luogo, com'è stato osservato nella letteratura americana, la *dataveillance* comporta una riduzione notevole della libertà di pensiero delle persone, influenzandone in maniera apprezzabile la facoltà di elaborare idee e convinzioni. In questo senso, è stato efficacemente proposto di ampliare lo spettro applicativo del diritto alla *privacy* informazionale, adottando una concezione che tuteli maggiormente gli interessati. Si tratta della dottrina della *intellectual privacy*, avanzata dal giurista americano Neil Richards[446]. Questa dimensione estesa si basa su una considerazione fondamentale, cioè che «*free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse*»[447].

---

[444] O. TENE – J. POLONETSKY, *Big Data for all: Privacy and user control in the age of analytics*, in 11(5) *Northwestern Journal of Technology and Intellectual Property*, 2013, 256.
[445] Vedasi *supra*, § 1.3.
[446] Si veda, in particolare, N.M. RICHARDS, *Intellectual Privacy*, in 87 *Texas Law Review*, 2008, 387 ss.
[447] N.M. RICHARDS, *The Dangers of Surveillance*, *op. cit.*, 1946.

2.1.2. Il trattamento delle informazioni personali: aggregazione e (re-)identificazione degli interessati

Il trattamento[448] dei dati personali effettuato su larga scala comporta, principalmente, due ordini di problematiche[449]: l'uno inerente alla discriminazione degli interessati[450], l'altro relativo alla *privacy*. Queste ultime, seguendo la mappa riportata in Figura 1, comprendono le questioni dell'(in-)sicurezza di archiviazione dei dati personali, quelle dell'aggregazione dei diversi dati acquisiti e dell're-identificazione dei soggetti interessati sulla base delle informazioni detenute.

Della sicurezza dei sistemi di immagazzinamento si è già detto ampiamente nel capitolo precedente[451]; dell'aggregazione e dell'identificazione dei dati si è parlato rispetto alle attività dei *data brokers*[452]. Occorre però aggiungere qualche considerazione riguardo a queste ultime due tematiche.

Col termine "aggregazione" (*aggregation*) s'intende «*the combination of various pieces of data about a person*»[453]. La raccolta di grandi quantità di informazioni personali e le avanzate tecniche di analisi, che si fondano sull'uso di algoritmi e sistemi di intelligenza artificiale[454], rendono l'aggregazione un meccanismo invasivo e rivelatore della personalità dei soggetti. Questo è evidente se si considerano due circostanze.

In primo luogo, dall'analisi di dati non sensibili, i soggetti che raccolgono e utilizzano i dati personali possono inferire informazioni sensibili[455], anche se l'utente non ha mai fornito siffatti dati. Per esempio, si è dimostrato che dall'analisi

---

[448] Il Regolamento adotta una definizione ampia di trattamento. Tale espressione indica «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».
[449] I. RUBINSTEIN, *Big Data: The End of Privacy or a New Beginning?*, in 3(2) *International Data Privacy Law*, 2013, 4.
[450] Vedasi § 4.2 del capitolo secondo.
[451] Vedasi § 3.2 del capitolo secondo.
[452] Vedasi § 6.2 del capitolo secondo.
[453] D.J. SOLOVE, *A Taxonomy of Privacy*, *op. cit.*, 490.
[454] Sul punto, vedasi capitolo secondo.
[455] Le informazioni sensibili comprendono i dati «[sul]*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché* […] *dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*» (art. 9 par. I Regolamento).

dei "mi piace" cliccati su *Facebook* da un utente, si possono dedurre etnia, età, orientamento sessuale, tipo di personalità, e opinioni politiche dell'utente[456].

In secondo luogo, le compagnie private utilizzano abitualmente meccanismi di de-identificazione dei dati, quali l'anonimizzazione, la pseudonimizzazione e la crittografia, per procedere all'analisi delle risorse informative nel rispetto del quadro legislativo vigente, che impone l'utilizzo di procedimenti per evitare il riconoscimento delle persone interessate coinvolte[457]. È stato dimostrato tuttavia che, mediante l'aggregazione dei dati di diverso genere, pur de-identificati (tra cui i metadati dei messaggi crittografati), si può facilmente re-identificare la persona in questione[458]. Per esempio, nel 2013, in uno studio condotto dall'MIT e dell'Università Cattolica di Lovanio (Belgio), dall'analisi dei dati sull'utilizzo del cellulare di un milione e mezzo di persone residenti in un piccolo borgo europeo, acquisiti nell'arco di tempo di 15 mesi, si è scoperto che erano sufficienti per l'identificazione precisa del 95% di loro[459].

I processi di anonimizzazione, nell'era dei *Big Data*, si rivelano di scarsa utilità ai fini della de-identificazione degli interessati, dal momento che dall'analisi delle quantità incalcolabili di dati emerge comunque il profilo delle persone interessate[460]. Di conseguenza, «*the Big Data tsunami should prompt companies to review their de-identification protocols, ensure that these protocols are being implemented properly, and reconsider if certain data should simply not be collected*

---

[456] *Facebook, il tasto Like è una spia*, in *BU ICT San Raffaele* (www.buict.sanraffaele.it/it/2012-09-28-15-27-47/21-notizie/newsflash/239-facebook-il-tasto-like-e-una-spia.html, ultimo accesso 17 luglio 2017).
[457] Vedasi *infra*.
[458] D.J. SOLOVE, *A Taxonomy of Privacy*, *op. loc. cit.*
[459] L. HARDESTY, *How hard is it to 'de-anonymize' cellphone data?*, in *MIT News*, 27 marzo 2013 (http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data, ultimo accesso 17 luglio 2017). Lo studio è Y. DE MONTJOYE ET AL., *Unique in the Crowd: The privacy bounds of human mobility*, in 3 *Scientific Reports*, 2013, 1 ss.
[460] P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in 57 *UCLA Law Review*, 2010, 1701 ss.; O. ANGIULI ET AL., *How to De-Identify Your Data. Balancing statistical accuracy and subject privacy in large social-science data sets*, in 13(8) *ACM Queue*, 2015, 1 ss.; S. STALLA-BOURDILLON – A. KNIGHT, *Anonymous data v. Personal data–A false debate: An EU perspective on anonymisation, pseudonymisation and personal data*, in *Wisconsin International Law Review*, 2017 (in corso di pubblicazione).

from individuals»[461]. Oggi alle tecniche di anonimizzazione sono preferite quelle di pseudonimizzazione, che meritano ulteriori approfondimenti[462].

3. L'accesso ai dati personali nel diritto statunitense

Come già evidenziato in precedenza, il quadro giuridico inerente alla protezione delle informazioni personali negli Stati Uniti è molto variegato, ed è il risultato delle interazioni fra diversi formanti: quello legislativo e quello giurisprudenziale. A questi ultimi, inoltre, occorre aggiungere il ruolo predominante affidato a sistemi di *governance* della *privacy*. In particolare, nell'ordinamento statunitense si registrano due tendenze.

i. I maggiori sforzi del legislatore (*supra* § 3.1) e della giurisprudenza (§ 3.2) riguardano le problematiche determinate dalla raccolta sistematica delle informazioni personali degli interessati da parte delle autorità pubbliche (*dataveillance*).

ii. In assenza di un quadro legislativo onnicomprensivo, le modalità di raccolta e trattamento dei dati personali sono disciplinate principalmente da strumenti privatistici di autoregolazione, quali codici di auto-condotta e termini di servizio redatti dalle stesse imprese, che sono la base di un sistema di *governance* della *privacy* informazionale. Le autorità governative (quali la FTC) hanno raccolto i principi regolatori e ispiratori di queste norme, che costituiscono i *Fair Information Practices Principles* (FIPPs) (§ 3.3).

3.1. La legislazione federale

Com'è noto, negli Stati Uniti non esiste uno strumento legislativo onnicomprensivo riguardante la *privacy* informazionale.

---

[461] J. PAVOLOTSKY, *Privacy in the age of Big Data*, in 69 *The Business Lawyer*, 2013, 221.
[462] L'analisi continua in riferimento alla disciplina dei dati personali prevista dal Regolamento (UE) 2016/679. Vedasi § 4.

Fra le leggi federali che assumono rilevanza in materia, merita menzione il *Fair Credit Reporting Act* (FCRA), che riguarda le informazioni finanziarie degli interessati. Ai sensi di questa fonte normativa, i consumatori possono accedere alle banche dati, rettificando le eventuali informazioni errate[463], e alle informazioni sul processo decisionale automatizzato che determina l'esclusione dall'accesso al credito (*credit score*[464]).

Recentemente, il Congresso americano ha dimostrato un certo interesse riguardo alle problematiche in questione e, in particolare, alla geo-localizzazione degli utenti. Nel 2012, il rappresentante Markey ha proposto il *Mobile Device Reporting Act*, che impone ai costruttori di *smartphones* e agli erogatori di servizi *online*, fra le varie prescrizioni, di consentire ai consumatori l'accesso alle informazioni riguardanti l'installazione e gli scopi dei *softwares* di geo-posizionamento, prevedendo che la FTC promulghi norme che prescrivano «*the express consent of a consumer before monitoring software begins collecting and transmitting information and giving the consumer the opportunity to prohibit such collection and transmission at any time*»[465]. Inoltre, la proposta di legge postula agli stessi soggetti di fornire informazioni dettagliate sull'acquisizione delle informazioni, sul responsabile della sicurezza e un procedimento per l'identificazione di vulnerabilità prevedibili in ogni sistema che contiene tali informazioni[466].

Nell'anno successivo, in concomitanza con le rivelazioni di Edward Snowden, il senatore Leahy ha proposto di modificare l'*Electronic Communications Privacy Act*, proibendo ai *providers* di servizi tecnologici e di telecomunicazione di divulgare a ogni autorità governativa i contenuti di ogni conversazione archiviata o comunque detenuta dal *provider*[467]. Nondimeno, la proposta non si è poi trasformata in un provvedimento legislativo.

---

[463] N. RICHARDS – J. KING, *op. cit.*, 426.
[464] B.D. MITTELSTADT ET AL., *The ethics of algorithms: Mapping the debate*, in 3(2) *Big Data & Society*, 2016, 14. Si veda *infra*, § 6.1.
[465] *H.R.6377 - Mobile Device Privacy Act*, *112th Congress (2011-2012)*, in *Congress.gov* (www.congress.gov/bill/112th-congress/house-bill/6377, ultimo accesso 17 luglio 2017).
[466] J. PAVOLOTSKY, *op. cit.*, 223.
[467] *S.607 - Electronic Communications Privacy Act Amendments Act of 2013, 113th Congress (2013-2014)*, in *Congress.gov* (www.congress.gov/bill/113th-congress/senate-bill/607, ultimo accesso 17 luglio 2017).

3.2. Il *case law*: il caso *Jones* e gli sviluppi giurisprudenziali

Com'è noto, il formante giurisprudenziale costituisce un importante elemento del sistema giuridico americano. In particolare, le sentenze della Corte Suprema hanno segnato una notevole evoluzione del diritto alla *privacy* informazionale sotto due aspetti importanti: da un lato, un gruppo di casi riguarda il tema della raccolta e dell'utilizzo dei dati di geo-posizionamento da parte delle autorità pubbliche; dall'altro, una serie di sentenze concerne la raccolta e l'utilizzo dei metadati delle compagnie telefoniche private da parte delle agenzie governative (NSA).

In primo luogo, al pari del legislatore federale, la Corte Suprema si è occupata della raccolta di ingenti quantità di dati di localizzazione degli utenti nel celebre caso *United States v. Jones* del 2012. Nel caso di specie, la persona sottoposta alle indagini, sospettata di traffico illecito di stupefacenti, è stata pedinata mediante un localizzatore GPS collocato nell'automobile della moglie. Il giudice ha concesso l'autorizzazione per soli dieci giorni, ma, allo scadere di tale termine, gli agenti dell'FBI hanno continuato le attività di sorveglianza. Pur prevalendo l'opinione di *Justice* Scalia, che ha qualificato il caso come intrusione illecita (*trespass*), cinque giudici, nelle loro opinioni concorrenti, hanno riconosciuto che il monitoraggio continuativo della posizione geografica di una persona è una violazione del criterio di "ragionevole aspettativa" della *privacy* sancito dalla sentenza *Katz* (c.d. test di Harlan[468]), e, quindi, in assenza di autorizzazione giudiziale, o, come nell'ipotesi presa in esame, alla scadenza del termine finale per effettuare le rilevazioni, l'attività di localizzazione della polizia è incostituzionale.

In secondo luogo, le corti americane si sono occupate della raccolta e dell'uso dei metadati, cioè quei dati che descrivono un altro gruppo di dati. Le tutele riguardanti la raccolta e l'archiviazione delle informazioni previste dalla legislazione federale non si estendono a tale tipologia di risorse informative, la cui aggregazione può rivelare molto facilmente le qualità personali di una persona interessata[469]. Basandosi sul precedente *Jones*, la Corte distrettuale di Columbia, nel caso

---

[468] Vedasi *supra*, 2.1.2.

[469] Per esempio, l'*Electronic Communications Privacy Act* (ECPA) «*prevents Internet service providers from selling the content of its customers' e-mails and text messages without written*

Klayman v. Obama[470], ha scelto un rimedio di *equity* (*preliminary injuction*) per inibire l'acquisizione dei metadati delle chiamate telefoniche da parte del governo, sulla base della tutela accordata dal quarto emendamento e, in particolare, dal test di Harlan. Tuttavia, poche settimane dopo questa sentenza, la Corte distrettuale del *Southern District* di New York, nel caso *ACLU v. Clapper*, ha negato che la raccolta di ingenti quantità di dati da parte del governo costituisca una violazione del quarto emendamento[471]. Questa decisione, che, come *Klayman*, è contemporanea alle celebri rivelazioni di Edward Snowden, ha creato una certa confusione nell'opinione pubblica, che ha manifestato notevoli preoccupazioni nei confronti delle attività condotte dalle autorità pubbliche, e, in particolare, dall'NSA[472]. Due anni dopo, la Corte d'appello del secondo circuito ha ribaltato la decisione di primo grado: nella sua opinione, *Judge* Lynch ha affermato che l'interpretazione governativa del *Patriot Act*, per la quale l'NSA può procedere alla raccolta di ingenti quantità di metadati delle compagnie telefoniche, è incostituzionale, dal momento che «[…] *if the government is correct, it could use § 215* [Patriot Act] *to collect and store in bulk any other existing metadata available anywhere in the private sector, including metadata associated with financial records, medical records, and electronic communications (including e-mail and social media information) relating to all Americans. Such expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans*»[473]. Nel 2015, la *Foreign Intelligence Surveillance Court* ha deciso che la raccolta di metadati può continuare, contrapponendosi alla decisione della Corte d'appello[474].

---

consent but provides more limited protection for noncontent metadata» (N. RICHARDS – J. KING, *op. cit.*, 417).

[470] *Klayman v. Obama*, 957 F. Supp. 2d 1 (2013).

[471] *ACLU v. Clapper*, 959 F. Supp. 2d 724 (2013).

[472] G. SCHMITT, *A tale of two judges*, in *Weekly Standard*, 13 gennaio 2014 (www.weeklystandard.com/tale-two-judges/article/773264, ultimo accesso 18 luglio 2017).

[473] *ACLU v. Clapper*, 14-42 2d Cir. (2015), 74.

[474] B. VAN DER SLOOT – S. VAN SCHENDEL, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, in 7 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2016, 122.

3.3. I *Fair Information Practices Principles* (FIPPs) e la *governance* della *privacy*. Il problema del sistema dell'"informativa e consenso"

Negli Stati Uniti, fuori dal campo di applicazione delle norme inserite nelle leggi federali e statali settoriali, la disciplina della raccolta e del trattamento delle informazioni da parte degli enti spetta a strumenti di auto-regolamentazione, quali codici di condotta e termini di servizi, sul cui rispetto vigilano le autorità federali. In particolare, come detto in precedenza, la FTC ha un ruolo centrale nel controllo dell'operato delle imprese[475]. Nell'ordinamento nordamericano, pertanto, prevale un sistema di *governance* della *privacy*[476], che si differenzia dall'*hard government* affidato all'operato legislativo delle istituzioni pubbliche. Questa tendenza è indice di «*an intense worry about the risks of state coercion and bumbling, combined with relative insensitivity to the ramifications of private power*»[477].

I mezzi di auto-regolamentazione si basano sui *Fair Information Practices Principles* (FIPPs, o semplicemente *Fair Information Practices*, FIPs), cioè cataloghi di pratiche commerciali e linee-guida di "informazione leale[478]" che regolano il controllo e la gestione delle informazioni personali agli interessati[479]. Occorre soffermarsi in primo luogo sull'evoluzione storica dei FIPPs, e, *in secundis*, sulle esigenze di rinnovo che scaturiscono dagli scenari di sfruttamento dei *Big Data*.

L'insieme di questi principi e regole, pur elaborati dapprima nell'ambito americano, ha avuto una notevole influenza sul piano internazionale. Originariamente, un *report* del 1973 del Dipartimento americano della Sanità, dell'Istruzione e del *Welfare*, al fine di regolamentare le crescenti esigenze di tutela delle informazioni personali degli interessati, ha raccolto tali prassi in una proposta di codice

---

[475] Vedasi *supra*, § 1.1.
[476] J. COHEN, *What Privacy is For*, *op. cit.*, 1904 ss. Sul concetto di *governance* e sul ruolo degli attori privati nella regolamentazione, vedasi J. FREEMAN, *The Private Role in Public Governance*, in 75 *New York Law Review*, 2000, 543 ss. e O. LOBEL, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, in 89 *Minnesota Law Review*, 2004, 342 ss.
[477] J. COHEN, *What Privacy is For*, *op. cit.*, 1930. Per una trattazione coerente sul passaggio dal *government* alla *governance*, vedasi J.L. SHORT, *The Paranoid Style in Regulatory Reform*, in 63 *Hastings Law Journal*, 2012, 633 ss.
[478] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 271.
[479] Vedasi R. GELLMAN, *Fair Information Practices: A Basic History*, in *SSRN Library*, 2017 (http://ssrn.com/abstract=2415020, ultimo accesso 18 luglio 2017).

delle pratiche di informazione leale (*Code of Fair Information Practices*). I principi di "informazione leale" affermati nel *report* del 1973 hanno ispirato da un lato le leggi statali e federali sul diritto alla *privacy* informazionale (*statutes*[480]), dall'altro le linee-guida in materia di *privacy* e flusso transfrontaliero dei dati personali elaborate dall'OCSE nel 1980[481], strumento di *soft law* che, a sua volta, ha influito sulle elaborazioni legislative successivamente adottate dagli Stati e dalle organizzazioni transazionali in materia di protezione dei dati personali (si pensi alla Direttiva 95/46/CE e al Regolamento (UE) 2016/679).

Più recentemente, i FIPPs sono stati oggetto di proposte normative e di accordi internazionali. Nel luglio del 2000, gli Stati Uniti e l'Unione europea hanno sottoscritto un accordo bilaterale, che ha istituito un programma di auto-certificazione volontaria per le imprese che seguono le pratiche di informazione leale. «*Queste norme prevedono uno standard di raccolta e trattamento dei dati simile più al modello europeo, che a quello americano*»[482], anche perché, com'è noto, negli Stati Uniti non esiste una tutela delle informazioni personali garantita da uno strumento legislativo onnicomprensivo in materia di *privacy* informazionale. Nel 2012, la FTC ha raccomandato alle imprese di rinnovare il quadro auto-regolativo precedente e ha evidenziato la necessità di tutele più elevate nei confronti dei consumatori[483]. Le norme proposte dalla FTC, pur estendosi a tutte le «*commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device*»[484], mantengono sostanzialmente intatta l'impostazione giuridica già accordata in precedenza, incardinata sull'"informativa e consenso". Nello stesso anno, il Dipartimento del commercio del governo statunitense ha proposto la Dichiarazione dei diritti alla *privacy* del consumatore (*Consumer Privacy Bill of Rights*[485]), che include una nuova versione dei FIPPs che ne estende

---

[480] Il *Privacy Act* (1974), il *Right to Financial Privacy Act* (1978) e il *Video Privacy Protection Act* (1988) seguono il modello introdotto nel *report* del 1973.
[481] OCSE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Le linee-guida sono state aggiornate nel 2013 (OCSE, *The OECD Privacy Framework*, 2013).
[482] U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 271.
[483] FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change*, 2012.
[484] FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change*, *op. cit.*, VII.
[485] WHITE HOUSE, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, 2012.

la portata a tutti i settori. I principi contenuti nel documento sono i seguenti: controllo individuale[486], trasparenza[487], rispetto del contesto[488], sicurezza[489], accesso ed esattezza[490], acquisizione limitata[491] e responsabilità[492]. Le modifiche del 2016 della Circolare A-130 dell'Ufficio per la gestione e il bilancio (*Office of Management and Budget*), organo di consulenza del Presidente degli Stati Uniti, includono l'enumerazione di alcuni FIPPs. Pur applicandosi alle attività di gestione delle informazioni condotta da ogni autorità pubblica americana (*agency*), tale circolare pone limiti notevoli alle attività di sorveglianza di massa effettuate dall'NSA. Fra i principi di "informazione leale" annoverati nel nuovo testo, si trovano il diritto di accesso e di rettificazione, i principi di responsabilità, di autorità, di minimizzazione dei dati personali, di qualità, di integrità, di partecipazione individuale, di specificazione delle finalità, di limitazione dell'uso, di sicurezza e di trasparenza.

La rivoluzione dei *Big Data* ha segnato l'insorgere di esigenze di radicali cambiamenti nel sistema di autoregolazione basato sull'informativa e consenso. Occorre prendere in esame i contenuti dei principi di informazione leale alla luce dei recenti sviluppi tecnologici. I FIPPs si basano sul principio dell'"informativa e consenso", per il quale il trattamento dei dati personali è legittimo se la persona interessata, informata delle ragioni e delle condizioni del trattamento, concede il proprio consenso al titolare del trattamento[493]. Pertanto, gli interessati sono muniti di un certo grado di controllo sui propri dati, «*and through this control people for themselves can decide how to weigh the costs and benefits of the collection, use, or*

---

[486] «*Consumers have a right to exercise control over what personal data companies collect from them and how they use it*» (WHITE HOUSE, *op. cit.*, 47).
[487] «*Consumers have a right to easily understandable and accessible information about privacy and security practices*» (WHITE HOUSE, *op. loc. cit.*).
[488] «*Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data*» (WHITE HOUSE, *op. cit.*, 48).
[489] «*Consumers have a right to secure and responsible handling of personal data*» (WHITE HOUSE, *op. loc. cit.*).
[490] «*Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate*» (WHITE HOUSE, *op. loc. cit.*).
[491] «*Consumers have a right to reasonable limits on the personal data that companies collect and retain*» (WHITE HOUSE, *op. loc. cit.*).
[492] «*Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights*» (WHITE HOUSE, *op. loc. cit.*).
[493] Si veda F.H. CATE – V. MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in 3(2) *International Data Privacy Law*, 2013, 67 ss.

disclosure of their information»[494]. I titolari del trattamento sono tenuti a fornire i termini del trattamento dei dati (*privacy policies*[495]) e, solitamente, meccanismi di *opting out*, cioè di esclusione dal trattamento di talune tipologie di dati personali. Tuttavia, il principio dell'"informativa e consenso mostra tutti i suoi limiti nella società dei *Big Data* per due ordini di motivi, gli uni di natura conoscitiva, gli altri di carattere strutturale[496].

Anzitutto, di solito gli interessati non forniscono il consenso sulla base di scelte informate. Spesso gli utenti non leggono le lunghe *privacy policies*, oppure, se provano a leggerle, non ne hanno una comprensione adeguata. Se consapevoli dei meccanismi di *opting out*, in pochi casi optano per tale possibilità. Come già visto in precedenza[497], se comprendono il significato dei termini del trattamento e non li condividono, prestano comunque il consenso per accedere ai servizi, conferendo uno scarso valore alla protezione dei dati[498] oppure credendo di poter controllare l'operato dei titolari del trattamento (c.d. *feeling of control*[499]).

In secondo luogo, problemi di natura strutturale minacciano un'opportuna formazione del consenso. Gli interessati, infatti, hanno a che fare con una miriade di entità che raccolgono, archiviano e riutilizzano una quantità sterminata di informazioni personali. «*Thus, even if all companies provided notice and adequate choices, this data management problem would persist; the average person just does not have enough time or resources to manage all the entities that hold her data*»[500]. Inoltre, gli interessati, fornendo varie tipologie di dati che, aggregati, formano profili molto dettagliati, difficilmente riescono a gestire le informazioni che si ricavano

---

[494] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, *op. cit.*, 1880.
[495] A. ESTEVE, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in 7(1) *International Data Privacy Law*, 2017, 36 ss.
[496] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, *op. cit.*, 1883.
[497] Vedasi § 6.4 del capitolo secondo.
[498] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, *op. cit.*, 1883 ss. Si veda anche il § 6.4 del capitolo secondo.
[499] L. BRANDIMARTE ET AL., *Misplaced Confidences: Privacy and the Control Paradox*, in 4(3) *Social Psychological and Personality Science*, 2012, 340 ss.
[500] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, *op. cit.*, 1889. Secondo A.M. MCDONALD – L.F. CRANOR, *The Cost of Reading Privacy Policies*, in *I/S: A Journal of Law and Policy for the Information Society*, 2008, 543 ss., se ognuno leggesse la *privacy policy* di ogni sito visitato nell'arco di un anno, sarebbe esposto a una perdita in produttività che ammonta a 781 miliardi di dollari americani!

da processi di *analytics*: è potenzialmente impossibile valutare adeguatamente i costi e i benefici inerenti alla rivelazione di certi dati, poiché bisognerebbe essere consapevoli di tutti gli eventuali pregiudizi e vantaggi e operare una scelta sulla base di un'analisi costi-benefici[501].

Come già accennato all'inizio di questo paragrafo, i FIPPs hanno ispirato la legislazione europea in materia di protezione dei dati, cioè, prima, la Direttiva 95/46/CE e, poi, il Regolamento (UE) 2016/679. Occorre passare ora all'analisi della disciplina del versante europeo.

4. L'accesso ai dati personali nel Regolamento (UE) 2016/679

A differenza degli Stati Uniti, l'Unione europea si è dotata di un sistema di tutela *omnibus* in materia di *privacy* informazionale. La protezione giuridica dei dati personali si estende a ogni ambito di sfruttamento, sia commerciale sia non commerciale, e si articola in ogni fase del ciclo di vita dei dati, dalla produzione, alla raccolta e al trattamento degli stessi. Interventi normativi settoriali non mancano nell'Unione europea, ma operano come «*backup used to increase the specificity of regulatory norms stemming from the initial statutory framework*»[502]. La minuziosa disciplina europea rappresenta un *unicum* a livello mondiale cui si sono ispirati alcuni legislatori di altre parti del mondo.

Il Regolamento (UE) 2016/679 (o Regolamento Generale sulla Protezione dei Dati, d'ora in poi "Regolamento"), le cui norme si applicano dal 25 maggio 2018[503], sostituisce la precedente Direttiva 95/46/CE (d'ora in poi "Direttiva"), apparsa obsoleta e superata dalle nuove esigenze della società dell'informazione a più di vent'anni dall'entrata in vigore. Gli Stati membri hanno recepito la Direttiva in testi normativi nazionali dal contenuto diverso, e «*began to differ quite significantly*

---

[501] D. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, *op. cit.*, 1890.
[502] P. SCHWARTZ, *The EU-U.S. privacy collision: A turn to institutions and procedures*, in 126 *Harvard Law Review*, 2013, 1974. Si pensi, per esempio, alla Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, G.U. n. L. 119 del 4/05/2016.
[503] Art. 99 par. II Regolamento (UE) 2016/679.

in how they implemented and enforced these national laws»[504]. Di fronte alle diversità legislative, la Corte di giustizia dell'Unione europea (CGUE) ha fornito linee-guida ermeneutiche per districare la matassa di norme diverse alla luce dei principi della Direttiva stessa[505].

Il Regolamento è chiaramente influenzato dalle diversità di vedute dei diversi Stati membri. Il testo finale, infatti, è una versione meno innovativa e più morbida della proposta originaria[506]. Esso riprende in larga parte i principi della precedente Direttiva, a sua volta ispirata ai FIPPs inclusi nelle linee-guida in materia di *privacy* e flusso transfrontaliero dei dati personali elaborate dall'OCSE[507].

Al bivio fra continuità e innovazione, talune norme del Regolamento presentano difficoltà applicative nella società dei *Big Data*, potendo limitarne la portata innovativa negli ambiti commerciali e non commerciali del versante europeo. Di ciò si sono preoccupate le grandi imprese del settore dei fornitori dei servizi in rete, che devono adeguare i termini del servizio ai principi e alle norme enunciati nel dettato legislativo regolamentare. Infatti, «*granting rights to the company in the privacy policy which would adversely affect the user's privacy rights granted in the EU Directive should be avoided, since such clauses will be found void, may invalidate the entire privacy policy, and could even be the subject of a complaint or class action*»[508].

Occorre prendere in considerazione le norme del Regolamento che impongono limiti al trattamento e alla raccolta dei dati di natura personale[509]. Il diritto alla

---

[504] V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, in 17 *Columbia Science & Technology Law Review*, 2016, 323.
[505] Per una visione di insieme sull'evoluzione giurisprudenziale della CGUE sul tema, vedasi V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, *op. cit.*, 324.
[506] Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, 2012.
[507] OCSE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *op. cit*. Vedasi U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in 1 *European Data Protection Law Review*, 2017, 40 (d'ora in poi: U. PAGALLO, *The Legal Challenges of Big Data*, *op. cit.*).
[508] A. ESTEVE, *op. cit.*, 38.
[509] Il trattamento comprende tutte le fasi della catena del valore dei dati (vedasi capitolo secondo). La raccolta è una di queste (si rimanda, più nel dettaglio, al § 2 del capitolo secondo).

portabilità e il diritto alla cancellazione dei dati meritano una trattazione specifica a parte.

4.1. I limiti al trattamento dei dati personali

Gli artt. 5 e 6 del Regolamento riflettono integralmente i principi del trattamento dei dati personali previsti dal combinato disposto degli artt. 6 e 7 della Direttiva, aggiungendo quello dell'integrità e della riservatezza[510] ed estendendo le condizioni di liceità del trattamento. Fra questi principi, quello della minimizzazione, che prevede che i dati personali siano «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»[511], il principio della limitazione della finalità, per il quale «*i dati personali sono* […] *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*»[512], e quello di liceità del trattamento, stabilito dall'art. 6 par. I del Regolamento[513], pongono limiti alle attività di trattamento dei dati personali. Riguardo al principio del consenso, e, in particolare, ai problemi inerenti al meccanismo dell'"informativa e consenso" si è già parlato in precedenza. Occorre soffermarsi sugli altri due.

In primo luogo, il principio di minimizzazione comporta un duplice adempimento del titolare del trattamento. Egli deve circoscrivere la raccolta e il tratta-

---

[510] «*I dati personali sono* […] *trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*» (art. 5 par. I lett. f Regolamento).

[511] Art. 6 par. I lett. c Regolamento.

[512] Art. 6 par. I lett. b Regolamento.

[513] Il trattamento è lecito se «*a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*» (art. 6 par. I Regolamento). Si rimanda al § 3.3.

mento dei dati allo stretto necessario rispetto alla finalità del trattamento, e cancellarli dai sistemi di memoria una volta che si sono raggiunte tali finalità. Il titolare del trattamento, inoltre, non può svolgere il trattamento dei dati secondo finalità diverse da quelle per le quali l'interessato ha prestato il proprio consenso. È chiaro che un siffatto principio pone seri problemi di legittimità della raccolta e del trattamento dei *Big Data*, giacché risulta radicalmente incompatibile col modello di *business* delle imprese che si dedicano all'aggregazione di diverse tipologie di dati[514].

In secondo luogo, analogamente al principio di minimizzazione, la limitazione della finalità si rivela sostanzialmente inconciliabile, nella sua enunciazione rigorosa, con le attività di sfruttamento dei *Big Data*. Le compagnie private, infatti, forniscono agli interessati informative tanto lunghe quanto vaghe nella definizione delle finalità, che consentono ai titolari del trattamento «*to hold on to personal data – even after the initial purpose has been fulfilled – and to repurpose personal data as long as they can show that there is another purpose covered by the consent that they are in the process of using the data for*»[515].

Per limitare fenomeni di elusione della disciplina, il legislatore ha disciplinato le condizioni del consenso in maniera più particolareggiata (art. 7 del Regolamento). Tre profili risultano particolarmente appropriati alla tutela dell'interessato. Anzitutto, l'onere della prova del consenso dell'interessato grava sul titolare del trattamento[516]. Secondariamente, la richiesta di consenso, se inserita nell'ambito di una dichiarazione scritta, dev'essere «*presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*»[517]. In terzo luogo, la persona interessata deve essere informata che ha la facoltà di revocare il consenso in qualsiasi momento, senza che l'esercizio della revoca comprometta retroattivamente la liceità delle attività di trattamento svolte in precedenza[518].

---

[514] O. TENE – J. POLONETSKY, *op. cit.*, 259.
[515] V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, *op. cit.*, 322.
[516] Art. 7 par. I Regolamento.
[517] Art. 7 par. II Regolamento.
[518] Art. 7 par. III Regolamento.

Fino a questo punto, le maglie del Regolamento paiono particolarmente strette per gli agenti economici che sottopongono a trattamento ingenti quantità di dati personali. Nondimeno, i titolari del trattamento possono ricorrere a tre strategie per rispettare il dettato normativo senza incorrere nella rigorosità dei principi del Regolamento visti poc'anzi.

In primo luogo, i soggetti in questione sono incentivati a sottoporre i dati a procedimenti di pseudonimizzazione, per cui il titolare del trattamento utilizza i dati personali «*in modo tale che* […] *non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*»[519]. Queste tecniche differiscono dai processi di semplice anonimizzazione, che rendono le informazioni non riferibili a un soggetto interessato e comportano l'uscita dal campo di applicazione del Regolamento[520], ma non garantiscono la piena de-identificazione dei *datasets*[521]. Il legislatore ha previsto che «*i dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni,* […] [sono] *considerati informazioni su una persona fisica identificabile*»[522], ma per il loro valore potenziale «*under somewhat looser conditions should and can be reused*»[523].

In secondo luogo, nel Regolamento sono previste deroghe al principio di limitazione della finalità. Di regola, il titolare può riutilizzare i dati personali per scopi compatibili con le finalità iniziali. Se però il trattamento è effettuato ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici,

---

[519] Art. 4 n. 5 Regolamento.
[520] Art. 4 n. 1 Regolamento definisce il dato personale come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».
[521] Vedasi § 2.1.2.
[522] Cons. 26 Regolamento.
[523] V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, *op. cit.*, 329.

la compatibilità è *in re ipsa*. L'ulteriore trattamento per fini statistici è particolarmente rilevante per il trattamento dei dati personali effettuato da compagnie private, ed è un appiglio molto conveniente ai titolari del trattamento. Da un lato, le finalità statistiche sono definite in maniera imprecisa e tautologica, e, quindi, possono essere interpretate in senso ampio[524]; dall'altro, si prevede comunque un meccanismo di salvaguardia degli interessati, poiché, in ogni caso, «*il risultato del trattamento per finalità statistiche non* [sono] *dati personali, ma dati aggregati, e* […] *tale risultato o i dati personali non* [devono essere] *utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche*»[525]. Inoltre, spetta al diritto europeo o a quello nazionale il compito di tracciare, nei limiti del Regolamento, il contenuto dei meccanismi di salvaguardia, cioè «*i contenuti statistici, il controllo dell'accesso, le specifiche per il trattamento dei dati personali per finalità statistiche e le misure adeguate per tutelare i diritti e le libertà dell'interessato e per garantire il segreto statistico*»[526]. Questa facoltà presenta un rischio significativo: gli Stati membri possono istituire diversi limiti normativi ai contenuti statistici, compromettendo l'efficacia dei tentativi di armonizzazione del Regolamento e dando origine a un quadro legislativo frammentato[527], che comporterebbe un costo di adeguamento alle diverse discipline di diritto interno più elevato alle imprese operanti in più Stati membri[528].

In terzo luogo, fuori dalle ipotesi di finalità statistiche, il Regolamento consente ai titolari di sottoporre i dati personali a trattamenti che prescindono dalle finalità iniziali, dal consenso dell'interessato e dalle norme previste in atti legislativi dell'Unione o degli Stati membri che limitano gli obblighi e i diritti degli interessati conformemente alle ragioni elencate all'art. 23 par. I del Regolamento. La compatibilità non è *in re ipsa*, ma dev'essere verificata dallo stesso titolare del trattamento. In tale controllo, si deve tenere conto di una pluralità di elementi, fra cui:

---

[524] «*Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici*» (cons. 162 Regolamento).
[525] Cons. 162 Regolamento.
[526] Cons. 162 Regolamento. Vedasi, nello stesso senso, l'art. 89 Regolamento.
[527] U. PAGALLO, *The Legal Challenges of Big Data*, *op. cit.*, 42.
[528] V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, *op. cit.*, 327-28.

i. il nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

ii. il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

iii. la natura dei dati personali;

iv. le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

v. l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione[529].

La differente disciplina delle diverse finalità di trattamento è sintetizzata nello schema (Figura 8).

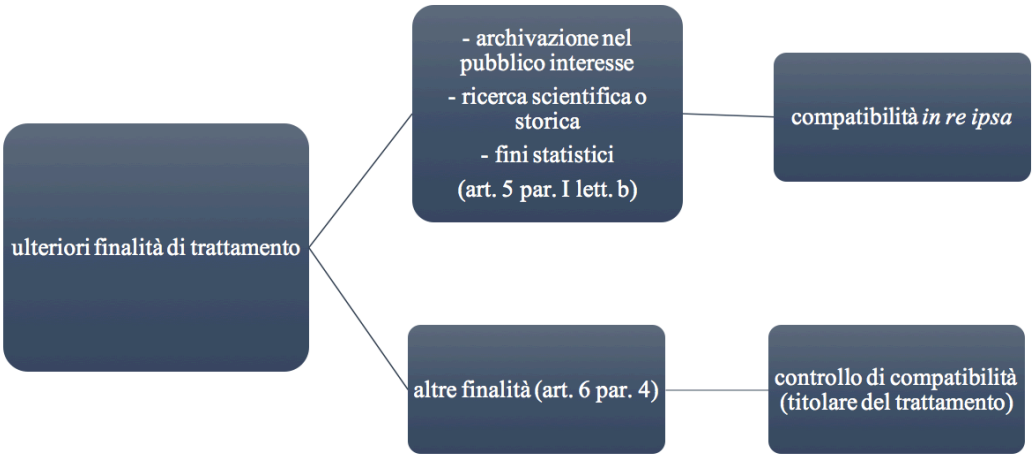

Figura 8. Le ulteriori finalità del trattamento dei dati personali nel Regolamento.

[529] Art. 6 par. IV Regolamento.

4.2. I limiti alla raccolta dei dati personali

Il Regolamento mantiene i limiti riguardanti acquisizione dei dati personali già previsti dalla Direttiva. Alle attività di raccolta, infatti, si applicano rigorosamente i principi di minimizzazione, di limitazione della finalità e di liceità del trattamento, senza che le imprese possano avvalersi delle deroghe per finalità statistici viste *supra*, che concernono le attività di riuso dei dati personali[530]. L'art. 6 del Regolamento estende sia le condizioni di liceità (par. I) sia le eccezioni di trattamento ulteriore (par. IV) alla raccolta.

Questo potrebbe limitare l'acquisizione di massa di dati personali anche da parte di autorità pubbliche. Tuttavia, il legislatore si è preoccupato di specificare che «*il regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale*»[531]. Pertanto, la raccolta di dati personali da parte delle autorità pubbliche a fini di pubblica sicurezza, che, come visto in precedenza, è essenziale per attività di sorveglianza di massa (*dataveillance*[532]), rientra nelle competenze esclusive degli Stati membri[533].

4.3. I diritti dell'interessato

Il Regolamento prevede una serie di situazioni giuridiche soggettive individuali in capo al soggetto interessato. Talune rientravano già nel dettato normativo della vecchia Direttiva e sono state rafforzate nella nuova disciplina regolamentare (quali il diritto di accesso e il diritto di opposizione), altre sono state introdotte *ex novo* (il diritto alla portabilità, il diritto alla cancellazione e il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato[534]).

---

[530] Art. 5 par. I lett. b Regolamento. Così V. MAYER-SCHÖNBERGER – Y. PADOVA, *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, *op. cit.*, 329.
[531] Cons. 16 Regolamento. Si veda anche l'art. 2 par. II lett. d Regolamento.
[532] Vedasi §.2.1.1.
[533] «[…] *La sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*» (art. 4 par. II Trattato sull'Unione europea (versione consolidata), G.U. n. C. 202 del 7/06/2016).
[534] Sul diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato si rimanda *infra* ai § 6.1 e 6.2.2.

4.3.1. Trasparenza, accesso e rettifica

I diritti dell'interessato, pur avendo contenuti e *rationes* diversi, rispondono a una comune esigenza di trasparenza del trattamento dei dati personali, che, per le sue caratteristiche, avviene "a porte chiuse", senza la partecipazione operativa e il controllo diretto degli interessati[535]. Il legislatore europeo ha ampliato la tutela soggettiva in maniera considerevole per fronteggiare le difficoltà inerenti agli sviluppi delle tecnologie dell'informazione e della comunicazione, e, in particolare, del trattamento di ingenti quantità di dati personali. Il principio di trasparenza, previsto all'art. 5 del Regolamento, risponde a queste esigenze di tutela, giacché «*impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*»[536].

Il diritto di accesso (art. 15 del Regolamento) e gli obblighi informativi dei titolari del trattamento (artt. 13 e 14 del Regolamento) sono corollari del principio di trasparenza.

Il diritto di accesso è previsto al par. I dell'art. 15 del Regolamento. In base a tale norma, «*l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali*» e a una pluralità di informazioni di diverso genere, quali le finalità del trattamento, le categorie di dati personali in questione e i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e l'esistenza di un processo decisionale automatizzato. Il par. II stabilisce un diritto dell'interessato a essere informato del trasferimento dei dati personali presso un Paese terzo o a un'organizzazione internazionale. Il par. III impone poi al titolare del trattamento di fornire una copia dei dati perso-

---

[535] P. DE HERT – V. PAPAKOSTANTINOU, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, in 28 *Computer Law & Security Review*, 2012, 136 («*Individuals are handicapped in the data processing process, in that processing does not take place in the open but rather behind closed doors. They are thus mostly unaware when and how their data are being processed*»).
[536] Cons. 39 Regolamento.

nali oggetto di trattamento, se gli viene richiesto. Inoltre, se l'istanza avviene mediante mezzi elettronici (cioè nella totalità dei casi), il titolare rilascia le informazioni «*in un formato elettronico di uso comune*»[537].

Già nella Direttiva, il diritto di accesso trovava la sua formulazione all'art. 12. La Corte di giustizia dell'Unione europea ne ha spiegato la funzione principale: esso è funzionale all'esercizio di altri diritti, quale quello di rettifica[538]. Mediante l'accesso ai propri dati personali, l'interessato può verificare che non siano presenti errori di registrazione, e, qualora questi sussistano, ha il diritto di chiedere che siano corretti[539]: secondo l'art. 16 del Regolamento, l'interessato ha il diritto, da un lato, di ottenere dal titolare del trattamento la correzione dei dati personali inesatti che lo riguardano senza ingiustificato ritardo, e, dall'altro, di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

La disciplina del Regolamento mira a risolvere i due problemi che il diritto di accesso presentava nella configurazione del precedente dettato legislativo. In primo luogo, questo era poco utilizzato, e pochi erano gli interessati consapevoli della sua esistenza[540]. Gli artt. 13 e 14 del Regolamento tentano di contrastare tale tendenza, prevedendo che il titolare del trattamento debba informare l'interessato circa il diritto all'accesso, alla rettifica, alla cancellazione e alla portabilità dei propri dati personali[541]. In secondo luogo, di solito le compagnie private fornivano le copie dei dati personali dopo molti mesi dalla richiesta dell'interessato, «*fail*[*ing*] *to provide details about sources, uses, and recipients of the information they collect*[*ed*]»[542], e provvedevano alla rettificazione delle informazioni in ritardo, in seguito a ripetute richieste dell'interessato. L'art. 16 del Regolamento stabilisce ora

---

[537] Art. 15 par. III Regolamento.
[538] Vedasi CGUE 7 maggio 2009 (Terza Sezione), causa C-553/07, College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer. L'accesso ai dati personali consente all'interessato di esercitare anche il diritto di limitazione del trattamento e di chiedere la cancellazione delle informazioni. Si veda il § 4.3.2.
[539] Secondo il principio di esattezza, i dati personali devono essere «*esatti e, se necessario, aggiornati;* [inoltre,] *devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*» (art. 5 par. I lett. d Regolamento).
[540] O. TENE – J. POLONETSKY, *op. cit.*, 263.
[541] Art. 13 par. II lett. b e art. 14 par. II lett. c Regolamento.
[542] O. TENE – J. POLONETSKY, *op. loc. cit.*

che il titolare del trattamento debba correggere i dati personali senza ingiustificato ritardo.

Resta da capire se il diritto di accesso come configurato dall'art. 15 Regolamento tuteli l'interessato anche rispetto alle informazioni inferite dal titolare del trattamento mediante processi di analisi dei dati, ma non ottenute né dall'interessato stesso, né da altre fonti. Secondo un'interpretazione sistematica del dettato legislativo, l'interessato deve poter accedere anche a tali dati, e, se il loro trattamento eccede il consenso fornito inizialmente, può altresì chiederne la cancellazione (art. 17 del Regolamento) o la limitazione del trattamento, cioè che non siano più oggetto di trattamento in futuro (art. 18 del Regolamento). Occorre rivolgere l'attenzione, quindi, a tali ulteriori posizioni giuridiche.

4.3.2. Limitazione e cancellazione

Oltre al diritto di rettifica e di integrazione, l'interessato può richiedere al titolare del trattamento operazioni che conferiscono all'interessato un controllo ancora più intenso dei dati personali. L'interessato, infatti, non ha un mero diritto di accesso ai dati, ma può pure disporre di questi, obbligando il titolare a interrompere il trattamento (diritto alla limitazione) o a cancellare i dati personali (diritto alla cancellazione). In modo simmetricamente opposto, il titolare del trattamento incontra in tali posizioni giuridiche una barriera all'uso dei dati personali[543].

Ci si sofferma su questi due istituti, che, pur già richiamati nella Direttiva, trovano nel Regolamento una disciplina organica e coerente.

L'interessato ha diritto di chiedere la limitazione del trattamento dei dati personali (art. 18 del Regolamento), cioè il «*contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*»[544]. Il titolare, dal momento della richiesta dell'interessato, deve interrompere le attività di analisi e riuso sui dati personali in questione, ma può mantenere i dati in questione nei propri si-

---

[543] D.L. RUBINFELD – M.S. GAL, *Access Barriers to Big Data*, in 59 *Arizona Law Review*, 2017, 367. Si veda, più nel dettaglio, il § 5 del capitolo secondo.

[544] Art. 4 par. III Regolamento. Nella Direttiva, tale operazione era chiamata, secondo una brutta traduzione, "congelamento" dei dati.

stemi di memoria. La limitazione non comporta l'eliminazione permanente di questi, ma consiste in un meccanismo di *opting out* che ha l'effetto di rendere inaccessibili i dati dell'interessato solo *pro futuro* e di escluderli dal trattamento. L'interessato può chiederla solo in determinate ipotesi tassative e alternative[545] (per esempio, quando il trattamento «*è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo*»[546]).

Il diritto alla cancellazione, meglio conosciuto come "diritto all'oblio" o *right to be forgotten*, è previsto all'art. 17 del Regolamento. Prima dell'entrata in vigore di quest'ultimo, le corti europee e nazionali avevano già configurato il contenuto e l'ambito applicativo di tale situazione giuridica sulla base della mera menzione che ne è fatta nel testo della Direttiva[547].

Nella letteratura giuridica, il tema del diritto all'oblio è stato oggetto di ampi e stimolanti dibattiti di carattere interdisciplinare[548]. La rivoluzione dell'informazione ha segnato l'inversione dei rapporti fra memoria e oblio. Prima della comparsa dei *databases* negli anni '50-'60 del Novecento[549], le modalità di registrazione delle informazioni postulavano che la memoria delle azioni umane passate

---

[545] Le condizioni sono previste allo stesso art. 18 par. I.
[546] Art. 18 par. I lett. b Regolamento.
[547] Si vedano, per esempio, CGUE 9 marzo 2012, causa C-131/12, Google Spain c. Agencia Espanola de Protección de Datos, e, per quanto concerne la giurisprudenza italiana, *inter alia*, Cass., Sez. III, sentenza 5 aprile 2012, n. 5525; Cass., Sez. I, sentenza 24 aprile 2016, n. 13161; Tribunale, Milano, sentenza 28 settembre 2016, n. 10374. La Direttiva configura la cancellazione come corollario del diritto di accesso (art. 12 lett. b Direttiva).
[548] Si veda, sulle questioni epistemologiche e ontologiche relative alla memoria e all'oblio, il fondamentale P. RICŒUR, *La marque du passé*, in 1 *Revue de Métaphysique et de Morale*, 1998, 7 ss. Si veda, sull'oblio in ambito digitale, V. MAYER-SCHÖNBERGER, *Delete: The virtue of forgetting in the digital age*, Princeton University Press, 2009. Si vedano, *inter alios*, sul diritto alla cancellazione in generale e nella legislazione europea, B.J. KOOPS, *Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten" in Big Data practice*, in 8(3) *SCRIPTed*, 2011, 229 ss.; R.H. WEBER, *The Right to Be Forgotten: More than a Pandora's Box?*, in 2 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2011, 120 ss.; J. ROSEN, *The right to be forgotten*, in 64 *Stanford Law Review Online*, 2012, 88 ss.; U. PAGALLO – M. DURANTE, *Legal Memories and the Right to Be Forgotten*, L. FLORIDI (CUR.), *Protection of Information and the Right to Privacy – A New Equilibrium?*, Springer, 2014, 17 ss.; G. SARTOR, *The Right to Be Forgotten: Dynamics of Privacy and Publicity*, in L. FLORIDI (CUR.), *Protection of Information and the Right to Privacy – A New Equilibrium?*, Springer, 2014, 1 ss.; G. SARTOR, *The right to be forgotten in the Draft Data Protection Regulation*, in 5 *International Data Privacy Law*, 2015, 64 ss.; G. SARTOR, *The right to be forgotten: balancing interests in the flux of time*, in 24 *International Journal of Law and Information Technology*, 2016, 72 ss.
[549] Vedasi § 1.1.

fosse soggetta a sforzi considerevoli. In altri termini, tentando di semplificare, dimenticare era la regola e ricordare l'eccezione. A partire dal secondo dopoguerra, i rapporti fra memoria e oblio si sono invertiti: oggi, com'è noto, diversi soggetti, a vario titolo, archiviano quantità incalcolabili di dati[550].

Nell'esigenza individuale di limitare la diffusione dei dati personali stanno le radici del diritto alla cancellazione: l'oblio digitale consente agli interessati di tutelare l'auto-determinazione informazionale, della quale i dati personali, alla stregua di "tracce del passato", sono un'importante componente[551]. Secondo un'acuta osservazione, il diritto alla cancellazione riguarda «*the way in which the passage of time affects the legitimacy of data processing*»[552], liceità che è soggetta al bilanciamento degli interessi dell'interessato (l'esclusione di altri dall'accesso ai propri dati) e del titolare del trattamento (libertà di espressione e libertà di iniziativa economica).

Secondo l'art. 17 del Regolamento, l'interessato può esercitare il proprio diritto alla cancellazione se si verifica una delle condizioni tipiche previste al par. I, *id est*:

i. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
ii. l'interessato revoca il consenso su cui si basa il trattamento conformemente, e non sussiste altro fondamento giuridico per il trattamento;
iii. l'interessato si oppone al trattamento ai sensi dell'articolo 21 del Regolamento;
iv. i dati personali sono stati trattati illecitamente;
v. i dati personali devono essere cancellati per adempiere a un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

---

[550] V. MAYER-SCHÖNBERGER, *op. cit.*
[551] U. PAGALLO – M. DURANTE, *Legal Memories and the Right to Be Forgotten*, *op. cit.*, 19.
[552] G. SARTOR, *The Right to Be Forgotten: Dynamics of Privacy and Publicity*, *op. cit.*, 2.

vi. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8 del Regolamento, che disciplina le condizioni del consenso fornito dai minori.

Se il trattamento dei dati personali continua nonostante l'esercizio di tale diritto, l'attività del titolare del trattamento diviene illecita: non a caso, le dette ipotesi in cui l'interessato può esercitare il diritto all'oblio riflettono tutte le situazioni di illiceità del trattamento previste dal Regolamento[553].

Il par. II dell'art. 17 prescrive un obbligo al titolare del trattamento particolarmente gravoso, che rende la cancellazione un diritto assoluto[554], cioè che può essere fatto valere nei confronti di tutti gli altri soggetti (*erga omnes*). Se l'interessato richiede la cancellazione dei dati personali, il titolare che li ha resi pubblici è tenuto a informare i titolari del trattamento che stanno trattando i dati personali in questione della richiesta dell'interessato di cancellare «*qualsiasi link, copia o riproduzione dei suoi dati personali*»[555], tenendo conto della tecnologia disponibile e dei costi di attuazione.

Il par. III elenca alcune eccezioni al diritto all'oblio. Anzitutto, se il trattamento è necessario all'esercizio del diritto alla libertà di espressione e di informazione, nel bilanciamento degli interessi il titolare prevale sull'interessato, che non può richiedere la cancellazione dei suoi dati personali. Secondariamente, prevale l'esigenza del titolare di mantenere i dati se il trattamento è necessario all'adempimento di un obbligo legale, allo svolgimento di un compito svolto nel pubblico interesse, e, se il titolare è un pubblico ufficiale, all'esercizio dei pubblici poteri[556]. In terzo luogo, sono fatti salvi i motivi di interesse pubblico nel settore della sanità pubblica[557] e di archiviazione nel pubblico interesse, di ricerca scientifica e a fini statistici, qualora il diritto alla cancellazione «*rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento*»[558]. Il titolare del trattamento facilmente invoca questa ipotesi, dal momento che, come si

---

[553] G. SARTOR, *The right to be forgotten in the Draft Data Protection Regulation*, *op. cit.*, 2016.
[554] Vedasi *infra*, § 5.2.
[555] Art. 17 par. II Regolamento.
[556] Art. 17 par. III lett. b Regolamento.
[557] Art. 17 par. III lett. c Regolamento.
[558] Art. 17 par. III lett. d Regolamento.

è visto, i dati sono spesso utilizzati per finalità statistiche dalle imprese private che sfruttano economicamente i *Big Data*. Infine, il diritto all'oblio non può esercitarsi allorché il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria[559].

4.3.3. Portabilità

Nei paragrafi precedenti, si è presa in considerazione la posizione giuridica dell'interessato. Questi, da una parte, può accedere ai propri dati personali e chiederne la rettifica, se errati; dall'altra, ha il diritto di disporre dei propri dati, cioè limitarne il trattamento e richiederne la cancellazione dai sistemi di memoria del titolare. Il legislatore, innovando il precedente quadro legislativo, ha previsto un ulteriore limite alle attività di (ri)uso dei dati personali[560]: l'interessato ha il diritto di trasferire e ottenere i propri dati in formato digitale.

Tale situazione giuridica è stata denominata diritto alla portabilità dei dati personali, ed è prevista all'art. 20 del Regolamento. Un recente lavoro delle Autorità europee garanti della protezione dei dati (*Article 29 Data Protection Working Party*, c.d. WP29) enuclea le caratteristiche e la portata applicativa della nuova posizione giuridica[561].

La *ratio* della norma sta nel rafforzamento del controllo dell'interessato sui propri dati personali. A tale finalità corrispondono i due contenuti essenziali del diritto, inseriti nelle disposizioni dei par. I e II del detto articolo del Regolamento. In primo luogo, l'interessato, se lo richiede, deve «*ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento*»[562], purché il trattamento si basi sul consenso o su un contratto[563] o sia effettuato mediante procedimenti automatizzati. In questo senso, la portabilità è un corollario dell'accesso ai dati personali, come

---

[559] Art. 17 par. III lett. e Regolamento.
[560] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 367. Si veda, più nel dettaglio, il § 5 del capitolo secondo.
[561] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, 2017.
[562] Art. 20 par. I Regolamento.
[563] Si vedano l'art. 6 par. I lett. a e b e l'art. 9 par. II lett. a Regolamento.

previsto dall'art. 15 del Regolamento. L'interessato può gestire e riusare le informazioni per fini personali, quali, per esempio, formulare inviti cartacei sulla base di un elenco dei contatti del proprio servizio di *email*[564].

In secondo luogo, alle stesse condizioni previste dal par. I, l'interessato ha diritto «*di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti*»[565], e, se risulta fattibile tecnicamente, «*ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro*»[566]. In questo senso, il Regolamento incentiva lo sviluppo di formati interoperabili di *file* contenenti i dati[567], ma non prevede specifici obblighi in capo ai titolari del trattamento. Una volta che i dati sono trasmessi, i titolari del trattamento *ad quem* sono soggetti agli stessi obblighi di trasparenza che discendono dai principi dall'art. 5 del Regolamento. Perciò, «*the "new" receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data*»[568].

Si considerino, ora, alcuni aspetti essenziali della disciplina del diritto alla portabilità prevista dal Regolamento: le condizioni di esercizio, i dati personali oggetto del diritto e le eccezioni e le limitazioni allo stesso.

Come già accennato, il diritto alla portabilità può esercitarsi solo se il trattamento si basa sul consenso dell'interessato, su un contratto o su un trattamento automatizzato. Le altre condizioni incluse nell'art. 6 par. I del Regolamento sono fuori dal campo di applicazione della norma.

Nello stesso par. I, il legislatore europeo si preoccupa di specificare che l'interessato ha il diritto di richiedere il trasferimento o la ricezione dei dati personali «*che lo riguardano forniti a un titolare del trattamento*»[569]. Tale espressione, pur concisa, ha un duplice risvolto ermeneutico. *In primis*, sono esclusi dal campo di

---

[564] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, *op. cit.*, 5.
[565] Art. 20 par. I Regolamento.
[566] Art. 20 par. II Regolamento.
[567] Cons. 68 Regolamento.
[568] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, *op. cit.*, 7.
[569] Art. 20 par. I Regolamento.

applicazione della norma i dati anonimizzati, ma non quelli pseudonimizzati riferibili alla persona interessata mediante le informazioni aggiuntive detenute dal titolare[570]. Secondariamente, ci si interroga sull'ampiezza dell'insieme dei dati "forniti dall'interessato a un titolare". Una interpretazione restrittiva suggerirebbe l'inclusione dei soli *volunteered data*; in realtà, più opportunamente, occorre conferire all'espressione un senso più ampio, comprendendo anche i c.d. *observed data*[571] (per esempio, *clickstreams*, dati di localizzazione). In ogni caso, due importanti ipotesi restano escluse. Non sono soggette a portabilità le informazioni personali inferite e ricavate mediante meccanismi di analisi e i dati personali di qualsiasi tipologia acquisiti dal titolare di un trattamento da terzi (si pensi, per esempio, ad agenti economici quali i *data brokers* o altri titolari del trattamento).

Analogamente al diritto alla cancellazione, il diritto alla portabilità è soggetto a talune eccezioni e limitazioni. L'interessato non può esercitarlo quando il trattamento dei dati personali è necessario all'esecuzione di un compito di pubblico interesse o connesso all'esercizio dei pubblici poteri del titolare[572].

Inoltre, l'esercizio del diritto in questione non può ledere i diritti e le libertà altrui[573]. Si possono individuare due ipotesi distinte. In primo luogo, i *datasets* che l'interessato intende ricevere o trasferire possono contenere dati personali relativi ad altri interessati. Si pensi, per esempio, alla corrispondenza mediante posta elettronica fra due persone o alle transazioni bancarie fra due soggetti. In tali casi, l'interessato che ha richiesto la portabilità dei dati può usarli esclusivamente per fini personali[574], ma non per scopi commerciali. Analogamente, il titolare cui il *datasets* è trasferito direttamente può svolgere operazioni di trattamento solo «*to the extent*

---

[570] Vedasi § 4.1.
[571] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, *op. cit.*, 10. Sulle nozioni di *volunteered data* e *observed data* si rimanda al § 2.2 del capitolo secondo.
[572] Art. 20 par. III Regolamento.
[573] Art. 20 par. IV Regolamento.
[574] Tale ipotesi è fatta salva dall'art. 6 par. I lett. f Regolamento: il trattamento è lecito se «*è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*».

that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs»[575]. In secondo luogo, può accadere che i dati richiesti dall'interessato contengano informazioni commerciali riservate, protette dal segreto industriale (*trade secret*). La presenza di tali forme di tutela non può limitare il diritto alla portabilità dei dati personali, nemmeno nelle ipotesi in cui esista il rischio potenziale di diffusione delle informazioni riservate. È compito del titolare trasmettere i *datasets* privi di queste ultime. La Direttiva (UE) 2016/943 conferma questa lettura della norma[576].

Il legislatore, inoltre, ha specificato che il diritto alla portabilità non pregiudica il diritto alla cancellazione[577]. Questa considerazione è di duplice valenza. Da un lato, il fatto che l'interessato richieda il trasferimento dei dati personali a lui stesso o direttamente a un altro titolare non implica che ne stia chiedendo, al contempo, l'eliminazione; dall'altro, il mero trasferimento non deve costituire un pretesto per il titolare del trattamento per evitare o ritardare la cancellazione per cui l'interessato ha fatto istanza.

Resta da considerare il trasferimento dei *datasets* di notevole entità. In tale ipotesi, l'interessato potrebbe riscontrare problemi nella fruizione dei dati, poiché questi ultimi potrebbero essere non facilmente processabili mediante elaboratori dalla modesta potenza di calcolo. Si prospettano tuttavia due soluzioni: da un lato, il titolare dovrebbe fornire i dati in forma concisa; dall'altro, l'interessato dovrebbe ottenere l'accesso alle informazioni mediante interfacce (*Application Programming Interfaces*, APIs) disponibili sul sito *web* del titolare del trattamento che consentano

---

[575] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, *op. cit.*, 12.

[576] «*La presente direttiva non dovrebbe pertanto pregiudicare i diritti e gli obblighi stabiliti dalla direttiva 95/46/CE, in particolare i diritti della persona interessata di accedere ai suoi dati personali che sono oggetto di trattamento e di ottenere la rettifica, la cancellazione o il congelamento dei dati incompleti o inesatti e, se del caso, l'obbligo di trattare i dati sensibili conformemente all'articolo 8, paragrafo 5, della direttiva 95/46/CE*» (Direttiva (UE) 2016/943 del Parlamento Europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, G.U. n. L. 157 del 15/6/2016). Nel testo si fa ancora riferimento ai diritti dell'interessato previsti nella precedente Direttiva 95/46/CE, ma il rimando deve considerarsi aggiornato al nuovo Regolamento. Per una panoramica generale sul rapporto fra protezione dei dati personali e segreto industriale nell'Unione europea, si veda G. MALGIERI, *Trade Secrets v Personal Data: a possible solution for balancing rights*, in 6(2) *International Data Privacy Law*, 2016, 102 ss.

[577] Art. 20 par. III Regolamento.

la selezione delle porzioni di *datasets* di cui l'interessato desidera il trasferimento[578].

5. Nuovi orizzonti. La "proprietarizzazione" dei dati personali

Nei precedenti paragrafi si è analizzata la disciplina dell'accesso ai dati personali in due ordinamenti, cioè quello statunitense e quello europeo. Dall'esame di diversi aspetti sono emerse le caratteristiche di ciascuno di questi: il primo è imperniato soprattutto su una tutela che afferisce al diritto dei consumatori, in un ambito di interazione dei diversi formanti; il secondo si basa sulla tutela della protezione dei dati come diritto fondamentale, per il quale l'informazione personale trova tutela in ogni stadio del suo ciclo di vita.

Entrambi i sistemi di protezione condividono due elementi comuni, se analizzati alla luce della dottrina giuseconomica. In primo luogo, ambedue forniscono uno strumentario giuridico che consente all'interessato di interrompere il trattamento illecito dei dati e di ottenere il risarcimento del danno derivante dalla violazione della sua *privacy*[579]. Si tratta, a ben vedere, di una duplice tutela di carattere inibitorio e risarcitorio dell'*entitlement*[580], riconducibile, rispettivamente, alle *property rules* e alle *liability rules* teorizzate nel celebre articolo di Calabresi e Melamed[581]. Le prime si basano su un potere "assoluto" del titolare, nel senso che questi può impedire a terzi ogni interferenza nell'esercizio del suo diritto, sanzionata mediante provvedimenti inibitori e punitivi dell'autorità giudiziaria; le seconde, invece, stabiliscono una tutela debole in capo al titolare dell'*entitlement*: i terzi possono assicurarsi il diritto anche senza il consenso del *dominus*, cui però spetta il

---

[578] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, *op. cit.*, 18-19.
[579] J.M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, in 123(2) *Yale Law Journal*, 2013, 516.
[580] L'*entitlement* è «*the fact of having right to something*» (*Entitlement*, in *Oxford online dictionaries*, http://en.oxforddictionaries.com/definition/entitlement, ultimo accesso 27 luglio 2017)
[581] Vedasi G. CALABRESI – A.D. MELAMED, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, in 85(6) *Harvard Law Review*, 1972, 1089 ss.

diritto di essere ristorato[582]. Per esempio, nell'Unione europea, le autorità di controllo istituite ai sensi dell'art. 51 del Regolamento[583] hanno il potere di ingiungere al titolare del trattamento di interrompere il trattamento illecito e conformare i trattamenti alle disposizioni del Regolamento in una determinata maniera ed entro un dato termine; inoltre, secondo l'art. 82 del Regolamento, chiunque (non solo, quindi, l'interessato) subisca un danno materiale o immateriale causato dalla violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento.

In secondo luogo, in nessuno dei due ordinamenti si arriva a riconoscere un vero e proprio regime proprietario sulle informazioni personali. Tuttavia, come già visto in precedenza, nell'economia dell'informazione si riscontra la marcata tendenza, in ambiti commerciali, di considerare queste ultime alla stregua di beni alienabili dotati di valore economico[584]. Il diritto, però, nel tutelare gli interessati, costringe le imprese a operare in «*legal grey zones when it comes to handling personal information assets*»[585]. Queste "zone grigie", a ben vedere, corrispondono ai casi in cui l'interessato trova dei limiti giuridici all'esercizio del controllo e della gestione delle proprie informazioni personali. Si pensi, per esempio, al trattamento svolto per finalità statistiche come disciplinato dall'art. 5 del Regolamento. Se si paragonano i principi e le norme in materia di *privacy* informazionale vigenti sia al di là, sia al di qua dell'Atlantico (per esempio, i principi di minimizzazione dei dati, di limitazione della finalità, di trasparenza ecc.), le imprese hanno margini di manovra alquanto più limitati nell'Unione europea[586].

Numerosi giuristi si sono sforzati di elaborare paradigmi di tutela proprietaria delle informazioni personali a partire dalla fine del secolo scorso. La maggior

---

[582] A. NICITA ET AL., *Le opzioni nel mercato delle regole*, SIDE Working Paper, 2005, 6.
[583] «*Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione*» (art. 51 par. I Regolamento).
[584] Nel capitolo secondo si è già parlato delle attività delle piattaforme digitali e dei *data brokers* e del fenomeno della commodificazione delle informazioni personali. Si rimanda la trattazione sul punto ai § 6.3 e § 6.4 del capitolo secondo e al capitolo quarto.
[585] S. SPIEKERMANN ET AL., *The challenges of personal data markets and privacy*, in 25 *Electronic Markets*, 2015, 162.
[586] Vedasi A. ESTEVE, *op. cit.*

parte dei contributi in tal senso proviene dal versante nordamericano[587]. Tali proposte non sono state esenti da critiche da parte di altri commentatori, che hanno ritenuto che lo schema di tutela proprietaria applicato alla *privacy* informazionale e lo sdoganamento degli scambi commerciali dei dati compromettano i diritti delle persone interessate[588].

Alla luce dell'analisi condotta nei precedenti paragrafi, ai fini del presente lavoro occorre capire se negli ordinamenti statunitense ed europeo, in cui non è previsto un regime proprietario dei dati personali, sono presenti almeno i germi di diritti dominicali in capo ai diversi attori.

5.1. Il dibattito negli Stati Uniti

Nel sistema statunitense, si registrano due tendenze: l'una del formante giurisprudenziale, l'altra di quello dottrinale.

In primis, in alcune sentenze i giudici americani hanno riconosciuto un diritto di proprietà dei dati personali alle imprese che li hanno acquisiti e organizzati in liste, ma mai in capo all'interessato[589]. Nel caso *US News & World Report, Inc. v. Avrahami*[590], la corte ha negato al convenuto Avrahami, il cui nome era stato scritto in modo errato su un elenco della società, un diritto di proprietà sul nome, ma ha statuito che la *US News* detiene un interesse proprietario (*proprietary interest*) alla raccolta di tali dati personali. Nella sentenza *Northwest Airlines Privacy*

---

[587] Per quanto concerne il dibattito americano sulla proprietà dei dati personali, si vedano, *inter alios*, R.S. MURPHY, *Property Rights in Personal Information: An Economic Defence of Privacy*, in 83 *Georgetown Law Journal*, 1995, 2381 ss.; L. LESSIG, *Code and Other Laws of the Cyberspace*, Basic Books, 1999; L. LESSIG, *The Architecture of Privacy*, in 1 *Vanderbilt Entertainment Law and Practice*, 1999, 56 ss.; J. LITMAN, *Information Privacy/Information Property*, in 52(5) *Stanford Law Review*, 2000, 1283 ss.; L. LESSIG, *Privacy as Property*, in 69(1) *Social Research*, 2002, 247 ss.; V. BERGELSON, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, in 37 *University of California Davis Law Review*, 2003, 379 ss.; P.M. SCHWARTZ, *Property, Privacy, and Personal Data*, in 117(7) *Harvard Law Review*, 2004, 2055 ss. In ambito europeo, si veda N.N. PURTOVA, *Property rights in personal data: A European perspective*, BOXPress BV, 2011.

[588] J. COHEN, *Examined Lives: Informational Privacy and the Subject as Object*, in 52(5) *Stanford Law Review*, 2000, 1373 ss.; P. SAMUELSON, *Privacy as Intellectual Property*, in 52(5) *Stanford Law Review*, 2000, 1125 ss.; M. LEMLEY, *Private Property*, in 52(5) *Stanford Law Review*, 2000, 1545 ss.; L. SCHOLZ, *Privacy as Quasi-Property*, in 101 *Iowa Law Review*, 2016, 1113 ss.

[589] J. VICTOR, *op. cit.*, 517.

[590] *U.S. News & World Report, Inc. v. Avrahami*, 95-1318 Va. Cir. Ct. (1996).

Litigation[591], i giudici hanno riconosciuto in capo a una compagnia aerea il diritto di proprietà dei *passenger name records*, cioè degli elenchi dei dati personali forniti dai passeggeri. Tali soluzioni giurisprudenziali hanno accordato alle imprese una protezione giuridica più forte di quella prevista dalla Direttiva 96/9/CE in ambito europeo, che, avendo ad oggetto la tutela delle banche dati «*che per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore*»[592], non si estende «*al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto*»[593].

In secondo luogo, come già detto, numerosi autori nordamericani hanno teorizzato un diritto di proprietà dei dati personali[594]. La maggior parte dei commentatori sopracitati sostiene che un meccanismo di tutela proprietaria faciliterebbe gli scambi sul mercato, in cui si raggiungerebbe «*optimal privacy by balancing the value of personal information to a company against the value of the information to the individual and the larger social value of data protection*»[595]. In particolare, di tre ordini sono gli elementi posti a sostegno della "proprietarizzazione" (*propertisation*) delle informazioni personali. Anzitutto, secondo alcuni autori, nei mercati dei dati personali una regola di *privacy* (*privacy rule*) si oppone alla regola di diffusione (*disclosure rule*). Per la prima, i beni informazionali personali sono allocati in prima battuta all'interessato; viceversa, secondo l'altra regola, essi spettano dapprima al titolare del trattamento. Gli scambi di tali risorse si informano poi al criterio di efficienza allocativa: alla luce del teorema di Coase[596], in un'ipotetica insignificanza dei costi transattivi, i dati personali vanno a chi conferisce maggior valore alle risorse in questione (*highest valuer*). Il ruolo del diritto è relegato a governare le situazioni reali, in cui, com'è noto, i costi transattivi sono presenti. Per valutare il benessere (o l'utilità) dei soggetti, occorre far riferimento non solo a criteri finanziari, ma anche a fattori psicologici e sociali, per i quali alla *privacy* è dato un

---

[591] *Northwest Airlines Privacy Litigation*, WL 1278459 (2004).
[592] Art. 3 par. I Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, G.U. n. L. 077 del 27/03/1996.
[593] Art. 3 par. II Direttiva 96/9/CE. Sulla tutela giuridica dei *databases*, si rimanda al § 5.2 del capitolo quarto.
[594] V. BERGELSON, *op. cit.*, N.M. RICHARDS – D.J. SOLOVE, *op. cit.*
[595] N.N. PURTOVA, *Property rights in personal data: Learning from the American discourse*, in 25(6) *Computer Law and Security Review*, 2009, 515.
[596] R.H. COASE, *The problem of social cost*, in 3 *Journal of Law & Economics*, 1960, 1 ss.

maggior valore rispetto alla diffusione delle informazioni personali[597]. In tali casi, l'iniziale allocazione dei dati personali agli interessati è più efficiente.

Secondariamente, secondo altri commentatori, una disciplina della *privacy* informazionale ispirata al diritto di proprietà consente di superare le ristrettezze della *tort privacy* di cui si è parlato in precedenza[598]. In particolare, questa si fonda essenzialmente su *liability rules*, per cui il trattamento illecito fa salvo solo il diritto al risarcimento dell'interessato. «*Tort remedy is available only post factum and has no preventive function. The value of transmitted personal data is determined not by the holder of the entitlement, i.e. an individual, but by the court*»[599]. Di conseguenza, secondo il criterio dell'efficienza, il titolare del trattamento che è in grado di sopportare il solo costo del risarcimento dell'interessato non è incentivato a rispettare le condizioni di liceità del trattamento; inoltre, l'interessato deve sostenere spese notevoli per attivare la macchina della giustizia. Al contrario, come già detto, le regole di proprietà forniscono all'interessato un elevato controllo e una tutela più forte ed efficace sui propri dati personali[600]. Alcuni autori, mescolando elementi della *law of property* e del *tort law*, propongono un'originale terza via di tutela: la c.d. "quasi-proprietà" (*quasi-property*[601]). Secondo questa dottrina, gli interessati hanno un diritto di esclusione dei terzi dall'utilizzo dei propri dati personali, ma solo in ragione della loro relazione coi titolari del trattamento, del contesto delle interazioni delle parti e del carattere dannoso delle azioni del titolare del trattamento.

Infine, un'altra parte della dottrina sostiene che la "proprietarizzazione" dei dati personali sarebbe la base di un sistema generale e onnicomprensivo di protezione dei dati personali, che regolerebbe i rapporti fra il mercato, il diritto e le tecnologie nel versante americano. Nel cyberspazio, i codici informatici e le architet-

---

[597] È questa la teoria di R.S. MURPHY, *op. cit*.
[598] Vedasi § 1.2.
[599] N.N. PURTOVA, *Property rights in personal data: A European perspective*, *op. cit.*, 129.
[600] V. BERGELSON, *op. cit.*, 419.
[601] S. BALGANESH, *Quasi-property: like, but not quite property*, in 160 *University of Pennsylvania Law Review*, 2012, 1889 ss., L. SCHOLZ, *op. cit.*

ture digitali hanno un ruolo preponderante nel governo dei rapporti interpersonali[602]. Tali tecnologie consentono sia di condurre il trattamento dei dati personali in modo efficiente, sia di porre limitazioni a quest'ultimo (si pensi, per esempio, alla crittografia). Se gli interessati fossero dotati di prerogative proprietarie sulle informazioni personali, «*then a negotiation would occur over whether, and how much, data should be used. The market could negotiate these rights, if a market in these rights could be constructed*»[603]. Inoltre, gli interessati potrebbero negoziare con i titolari l'utilizzo di tecnologie di protezione adeguata delle informazioni personali analoghe a quelle adottate, per esempio, nell'ambito del diritto d'autore[604] (si pensi ai *digital rights management*, DRM). Di conseguenza, «*the individual privacy would be better secured, not only by law but by interaction of the latter, market mechanisms and technologies*»[605].

5.2. La "proprietarizzazione" dei dati personali nel Regolamento (UE) 2016/679

Nella tradizione europea, com'è noto, la protezione dei dati personali detiene il rango di diritto fondamentale: la sua formulazione trova spazio nella Carta dei diritti fondamentali dell'Unione europea (art. 8) accanto al rispetto della vita privata e familiare (art. 7) e nel Trattato sul funzionamento dell'Unione europea (art. 16). Sul versante europeo, veri e propri diritti di proprietà sui dati personali sono difficilmente configurabili, dal momento che «*it is* [not] *possible to avoid human rights issues when discussing data protection matters. This conclusion is especially relevant when the data protection rights come into conflict with other interests, such as freedom of contract or free alienability of personal data for economic gain*»[606].

---

[602] L. LESSIG, *Code and Other Laws of the Cyberspace*, *op. cit.*; L. LESSIG, *The Architecture of Privacy*, *op. cit.*; U. PAGALLO, *Il diritto nell'età dell'informazione*, *op. cit.*, 132-33.
[603] L. LESSIG, *The Architecture of Privacy*, *op. cit.*, 63.
[604] J. COHEN, *Examined Lives: Informational Privacy and the Subject as Object*, *op. cit.*
[605] N.N. PURTOVA, *Property rights in personal data: Learning from the American discourse*, *op. cit.*, 517.
[606] N.N. PURTOVA, *Property rights in personal data: A European perspective*, *op. cit.*, 215.

Ciononostante, in seno al recente dibattito sulle questioni di appartenenza dei dati (*data ownership*[607]), taluni autori hanno intravisto in alcune regole del Regolamento i germi di una tutela di matrice proprietaria, benché il legislatore europeo non abbia adottato la terminologia tipica del diritto di proprietà. In particolare, questa tendenza si riscontra in tre punti particolari della disciplina[608].

Anzitutto, il par. I dell'art. 6 del Regolamento prevede che il trattamento è lecito se l'interessato ha fornito il proprio consenso e in una serie di altre ipotesi. Questo significa che il titolare dell'*entitlement* è, di norma, la persona interessata. In particolare, l'interessato non può cedere il proprio diritto sui dati personali. In base a questo assunto, quindi, la disciplina europea prevede una rigida regola-base di inalienabilità (*inalienabilities*), per la quale l'*entitlement* non può essere trasferito nemmeno se sussiste il consenso dell'alienante (l'interessato) e dell'acquirente (titolare del trattamento[609]). A ben vedere, l'interessato assume la medesima posizione dell'autore di un'opera nei sistemi giuridici continentali, in cui il contenuto del diritto d'autore ha un duplice contenuto: oltre ai diritti economici, sono previsti i c.d. diritti morali (o personali[610]). Com'è noto, tali situazioni giuridiche soggettive, ispirate alla concezione giusfilosofica hegeliana della proprietà[611], sono irrinunciabili e intrasmissibili, e proteggono l'opera in quanto emanazione della personalità dell'autore[612].

---

[607] Per la trattazione sulle questioni di appartenenza dei dati non personali, si rimanda al capitolo quarto.

[608] B. LUNDQVIST, *Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. The Issue of Accessing Data*, Faculty of Law, University of Stockholm Research Paper n. 1, 2016, 11 ss.; J. VICTOR, *op. cit.*, 522 ss.; A. WIEBE, *Protection of industrial data – a new property right for the digital economy?*, in 12(1) *Journal of Intellectual Property Law & Practice*, 2017, 65-66; H. ZECH, *Data As a Tradeable Commodity*, in A. DE FRANCESCHI (CUR.), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Intersentia, 2016, 66 ss.;

[609] Si vedano G. CALABRESI – A.D. MELAMED, *op. cit.*, 1089 ss.; S. ROSE-ACKERMAN, *Inalienability and the Theory of Property Rights*, in 85 *Columbia Law Review*, 1985, 931 ss.; S. ROSE-ACKERMAN, *Efficiency, Equity and Inalienability*, in J.M. GRAF VON DER SCHULENBURG – G. SKOGH, *Law and economics and the economics of legal regulation*, Kluwer, 1986, 11 ss.

[610] In questo senso, P. SAMUELSON, *op. cit.*, 1146 ss.

[611] Si ricordi il celebre passaggio: «*la persona ha il diritto di mettere la propria volontà in ogni cosa. In virtù di ciò, la cosa è la Mia e riceve la mia volontà come suo fine sostanziale (essa, infatti, non ha entro se stessa un tale fine), come sua determinazione e anima. Questo è l'assoluto diritto di appropriazione dell'uomo su ogni cosa*» (G.W.F. HEGEL, *Lineamenti di filosofia del diritto*, Bompiani, 2006, 139).

[612] Sui diritti di proprietà come tutela della personalità del titolare, vedasi M.J. RADIN, *Property and Personhood*, in 34 *Stanford Law Review*, 1982, 957 ss.

La posizione forte della persona interessata è avvalorata dalla previsione del diritto di limitazione (art. 18 del Regolamento) e del diritto alla cancellazione, previsto all'art. 17 del Regolamento. Infatti, com'è noto, se il trattamento diviene illecito per il venir meno di una delle condizioni previste dal par. I dell'art. 6 del Regolamento, l'interessato ha diritto di chiedere che i dati non siano più oggetto del trattamento o che siano cancellati[613]. Questo sistema di tutela, a ben vedere, rassomiglia a un regime di licenze, per il quale «*a data user may essentially receive a "license" to use the subject's data, since the data subject has temporarily waived her right to exclude it from using her information*»[614]. Al contempo, però, l'interessato mantiene la titolarità del diritto sui propri dati personali.

Tuttavia, l'interessato può cedere al titolare talune prerogative al titolare del trattamento. L'interessato può consentire che i dati personali siano raccolti e sottoposti al trattamento alle condizioni previste al par. I dell'art. 6 del Regolamento[615]. In particolare, le attività del titolare del trattamento sono legittime se l'interessato consente al trattamento[616] o in altre ipotesi. Fra queste, il legislatore europeo ha previsto che il trattamento è legittimo se è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento[617]. La formulazione di questa norma ricalca il principio espresso dal par. I dell'art. 17 della Carta dei diritti fondamentali dell'Unione europea (CDFUE) in materia di limiti del diritto di proprietà, per il quale «*nessuna persona può essere privata della proprietà se non per causa di pubblico interesse, nei casi e nei modi previsti dalla legge*».

In secondo luogo, come si è già visto[618], il diritto di protezione dei dati si configura come un diritto assoluto, nel senso che crea obblighi *erga omnes* in capo al titolare del trattamento e ai terzi. Si consideri di nuovo il diritto alla cancellazione. Secondo il par. II dell'art. 17 del Regolamento il titolare del trattamento che ha reso pubblici i dati personali ed è obbligato a cancellarli, tenendo conto della

---

[613] Vedasi *supra*, § 4.3.2.
[614] J. VICTOR, *op. cit.*, 524.
[615] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 68.
[616] Art. 6 par. I lett. a Regolamento.
[617] Art. 6 par. I lett. e Regolamento.
[618] Vedasi § 4.3.2.

tecnologia disponibile e dei costi di attuazione, deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Tale aspetto della disciplina risponde chiaramente a logiche proprietarie, giacché «*it creates a burden that "runs with" the data subject's information. Rather than conceiving of privacy protection as purely in personam, the* […] *Regulation instead grounds these rights in the data itself*»[619].

Infine, come già notato all'inizio del presente paragrafo, taluni rimedi previsti nel Regolamento sono chiaramente ispirati a *property rules*, per cui l'interessato ha una tutela forte nei confronti di tutti i consociati. Questa protezione giuridica consiste in provvedimenti di inibitoria delle attività di trattamento che violano il Regolamento e in sanzioni punitive dell'autorità. Secondo il dettato legislativo, le autorità nazionali di controllo previste dall'art. 51 hanno poteri "correttivi[620]", cioè possono: ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del Regolamento[621]; imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento[622]; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali[623]; infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83[624]. I par. IV e V dell'art. 83 stabiliscono sanzioni amministrative pecuniarie elevatissime per la violazione degli obblighi del titolare del trattamento, dei principi base del trattamento e dei diritti degli interessati. Fuori dalle ipotesi di queste norme, tocca agli Stati membri stabilire sanzioni «*effettive, proporzionate e dissuasive*»[625].

---

[619] J. VICTOR, *op. cit.*, 525.
[620] Art. 58 par. II Regolamento.
[621] Art. 58 par. II lett. d Regolamento.
[622] Art. 58 par. II lett. f Regolamento.
[623] Art. 58 par. II lett. g Regolamento.
[624] Art. 58 par. II lett. i Regolamento.
[625] Art. 84 par. I Regolamento.

6. I limiti all'analisi dei dati personali

Le attività di *data analytics* comportano due principali ordini di problematiche.

i. Mediante l'analisi delle incalcolabili quantità di dati rilasciati sul *web*, i titolari del trattamento suddividono gli interessati in gruppi sulla base delle caratteristiche e preferenze di questi ultimi[626]. Questi raggruppamenti *data-driven* comportano che la protezione dei dati assuma una dimensione "di gruppo".

ii. I grandi *datasets* sono analizzati mediante l'uso di algoritmi che provocano esternalità negative che concernono la posizione degli interessati[627].

Occorre procedere a un esame più approfondito di ciascuna di queste tematiche.

6.1. *Group privacy*: tentativi di tutela?

Per lungo tempo, il diritto alla *privacy* è stato concepito come posizione giuridica esclusivamente individuale[628]. In questo senso, il testo del Regolamento, in linea con la Direttiva, chiarisce che lo stesso «*stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati*»[629] e che «*protegge i diritti e le libertà fondamentali delle persone fisiche*»[630]. Ciò non significa, tuttavia, che l'esigenza di trasparenza del trattamento dei dati, al pari dell'esigenza di riservatezza, non possa coinvolgere anche soggetti collettivi, intesi sia come enti, sia come insiemi di persone fisiche accomunate da un'identità culturale o da convinzioni e interessi comuni, prive di un'indipendenza formale riconosciuta sul piano giuridico: com'è stato fatto opportunamente notare, nessun principio giuridico preclude

---

[626] Sul punto, vedasi § 6.4 del capitolo secondo.
[627] Sugli algoritmi si veda, più in generale, il § 4.2 del capitolo secondo.
[628] A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in 32 *Computer Law & Security Review*, 2016, 242.
[629] Art. 1 par. I Regolamento.
[630] Art. 1 par. II Regolamento.

all'estensione della nozione di "soggetto interessato[631]". Sulla base della necessità di rispondere a queste esigenze e di colmare un certo vuoto normativo, taluni commentatori e la giurisprudenza americana hanno tentato di elaborare due diverse nozioni di *group privacy*, che corrispondono a due situazioni giuridiche sovra-individuali distinte. Da un lato, la *privacy* è stata intesa come una componente del diritto delle entità collettive, quali, ad esempio, società, associazioni, enti pubblici; dall'altro, si è configurata alla stregua di un diritto collettivo in senso stretto, cioè di una posizione giuridica di cui si può fruire collettivamente in ragione di una medesima identità culturale o di interessi e convinzioni affini, e che opera come un prolungamento della *privacy* individuale[632]. Entrambe queste visioni giuridiche sono emerse rispettivamente in due sentenze della Corte Suprema americana: i casi *NAACP v. Alabama* e *Boy Scouts of America v. Dale*[633].

Dall'altro lato dell'Atlantico, l'attenzione verso la dimensione sovra-individuale è emersa in alcune norme di diritto processuale in materia di protezione dei dati personali. Nel 2013, la Commissione europea ha sottolineato il ruolo delle regole che favoriscono un accesso alla giustizia condiviso in una Comunicazione e in una Raccomandazione, invocando la necessità di un sistema più coerente e articolato soprattutto negli ambiti di tutela dei consumatori[634]. Il Regolamento va in questa direzione, innovando notevolmente il quadro legislativo precedente e dando la possibilità agli interessati di agire in giudizio collettivamente. Il par. I dell'art. 80, infatti, stabilisce che «*l'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle*

---

[631] U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, in L. TAYLOR ET AL. (CUR.), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017, 162.
[632] U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *op. loc. cit.*; E.J. BLOUSTEIN, *Group privacy: The right to huddle*, in 8(2) *Rutgers Camden Law Journal*, 1977, 219 ss.
[633] *NAACP v. Alabama*, 357 U.S. 449 (1958); *Boy Scouts of America v. Dale* 530 U.S. 640 (2000).
[634] Comunicazione della Commissione *Verso un quadro orizzontale europeo per i ricorsi collettivi*, 2013; Raccomandazione 2013/396/UE dell'11 giugno 2013 relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione, G.U. n. L. 201 del 26/7/2013.

libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 [diritto di proporre reclamo, diritto al ricorso giurisdizionale nei confronti dell'autorità di controllo e nei confronti del titolare del trattamento e del responsabile del trattamento] *nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82*». Il par. II aggiunge che gli Stati membri possono prevedere che l'organismo, organizzazione o associazione *non-profit* di cui al par. I, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare il diritto di proporre reclamo o ricorso giurisdizionale nei confronti dell'autorità di controllo, qualora ritenga che i diritti di cui un interessato gode a norma del Regolamento siano stati violati in seguito al trattamento. Insomma, il legislatore europeo ha adottato misure che rispondono a esigenze di tutela della rappresentanza delle persone interessate mediata dall'operato di tali organizzazioni, ma, a differenza della giurisprudenza statunitense, non ha stabilito norme a tutela della *privacy* informazionale di enti collettivi in quanto tali (*groups qua groups*[635]). Inoltre, a ben vedere, la formulazione dell'art. 80 del Regolamento è in linea con la visione individualistica cui si ispira l'intera disciplina della tutela della protezione dei dati personali: sia il par. I sia il par. II del presente articolo fanno riferimento alla posizione di un singolo interessato, la cui tutela in sede giudiziaria è affidata a un'organizzazione atta a far valere il suo diritto individuale. Pertanto, dalla lettura della norma emerge chiaramente che la dimensione collettiva resta una mera estensione della tutela individuale.

Tentando di sintetizzare, nel Regolamento si registra una duplice tendenza: da un lato, i soggetti del diritto alla protezione dei dati personali in senso stretto sono le persone fisiche; dall'altro, le persone fisiche possono essere rappresentate in giudizio da organizzazioni senza scopo di lucro, ai sensi dell'art. 80 del Regolamento. Questo impianto giuridico riflette una concezione marcatamente individualistica e atomistica, che mostra però tutti i suoi limiti nel contesto tecnologico

---

[635] U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *op. cit.*, 167.

odierno. In più occasioni, nei paragrafi precedenti, si è visto che le imprese e le autorità pubbliche sfruttano i *Big Data* e gli *open data* per comprendere le preferenze degli interessati e predirne i comportamenti. Mediante le attività di analisi su larga scala, i soggetti interessati sono raggruppati in base a caratteristiche personali comuni ricavate dalle "tracce" lasciate sul *web*. Si pensi, per esempio, ai c.d. *segments*, cioè le liste di interessati dalle stesse particolarità, e ai *credit scores*[636]. Perciò, «*most people are not targeted by ICTs as individuals but as members of specific groups, where the groups are the really interesting focus, as carriers of rights, values, and potential risks*»[637]. I componenti di tali gruppi non sono nemmeno consapevoli di esserne parte e di doverne affrontare le conseguenze derivanti dall'appartenenza[638], che è determinata dall'uso di algoritmi e tecniche di *machine learning*[639]. Dall'aggregazione e dalla combinazione dei dati personali di diverso genere (*clickstreams*, dati di geoposizionamento…) emergono profili dettagliati di gruppo, efficacemente definiti *demographically identifiable information* (DII[640]), di cui le informazioni personali di un singolo interessato (*personal identifiable information*) sono solo una parte.

Pertanto, le attività di raccolta e analisi dei dati su larga scala postulano un nuovo limite, «*represented by groups' need for the protection of their privacy and*

---

[636] Si rimanda la trattazione al § 6.2 e al § 6.3 del capitolo secondo.
[637] L. FLORIDI, *Open data, data protection, and group privacy*, in 27 *Philosophy and Technology*, 2014, 1.
[638] F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.
[639] L. KAMMOURIEH ET AL., *Group Privacy in the Age of Big Data*, in L. TAYLOR ET AL. (CUR.), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017, 41 («*As data and information retrieval processes become increasingly sophisticated, so does the process of group identification. Groups can now seem to automatically present themselves within data, even as the picture of the individual members remains fuzzy. Big Data thus changes what a group is and, in the same sweep, what an individual is*»).
[640] N.A. RAYMOND, *Beyond "Do No Harm" and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society's Use of Data*, in L. TAYLOR ET AL. (CUR.), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017, 75 («*Demographically Identifiable Information, or DII, is defined as either individual and/or aggregated data points that allow inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age, health condition, location, occupation, and/or other demographically defining factors*»).

their (aggregate) personal information»[641]. Il Regolamento, come la precedente Direttiva, è dotato di strumenti di tutela collettiva scarsamente adeguati a fronteggiare questo genere di problematiche[642]. Nondimeno, uno spiraglio di protezione in questo senso si intravede in due norme della disciplina europea sulla protezione dei dati. *In primis*, la disposizione del par. I dell'art. 22 del Regolamento prevede che l'interessato abbia il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Benché la norma intenda tutelare la sfera giuridica individuale dell'interessato, l'interruzione della profilazione potrebbe evitare che l'interessato in questione sia oggetto di raggruppamenti *data-driven*[643]. In secondo luogo, la portata dell'art. 33 del Regolamento si addice meglio alle problematiche in questione. Il par. I prevede che il titolare del trattamento debba effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali «*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*». Tale valutazione è una metanorma, o norma secondaria, che funziona «*as a means for the state to make corporations responsible for their own efforts to self-regulate*»[644]. Tale forma di verifica dell'impatto è richiesta, in particolare, per i casi previsti dal par. III del detto articolo, fra cui rientra «*la valutazione*

---

[641] A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in L. TAYLOR ET AL. (CUR.), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017, 145.

[642] L. FLORIDI, *Open data, data protection, and group privacy*, in 27 *Philosophy and Technology*, 2014, 3 («*There are very few Moby-Dicks. Most of us are sardines. The individual sardine may believe that the encircling net is trying to catch it. It is not. It is trying to catch the whole shoal. It is therefore the shoal that needs to be protected, if the sardine is to be saved. An ethics addressing each of us as if we were all special Moby-Dicks may be flattering and it is not mistaken, but needs to be upgraded urgently. Sometimes the only way to protect the individual is to protect the group to which the individual belongs*»). Si veda anche, più in generale, sulla necessità di un approccio etico meno individualistico e atomistico, L. FLORIDI, *The Ethics of Information*, Oxford University Press, 2013.

[643] Più in particolare vedasi § 6.1.

[644] R. BINNS, *Data protection impact assessments: a meta-regulatory approach*, in 7(1) *International Data Privacy Law*, 2017, 29. Nello stesso senso, U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, *op. cit.*, 10. Le norme primarie sono regole che riguardano direttamente la disciplina di un comportamento; le norme secondarie, invece, sono "regole sulle regole" (metanorme) che concernono le modalità di

sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche». Si noti che entrambe le norme si riferiscono non al singolo interessato, ma alle «*persone fisiche*», lasciando aperta la strada a un'estensione ermeneutica che comprenda le esigenze di tutela dei gruppi formati dalle attività di analisi dei *Big Data*.

Secondo una prospettiva *de iure condendo*, sembra difficile trovare un compromesso che accordi una tutela piena e adeguata ai gruppi e ai singoli interessati, senza pregiudicare gli interessi dei titolari del trattamento – cioè, soprattutto, degli *online service providers*, quali *Facebook*, *Google* ecc. Occorre bilanciare le esigenze di tre soggetti differenti: i gruppi costituiti mediante l'analisi dei dati personali, gli interessati e i titolari del trattamento. Il bilanciamento comporta due ordini di problemi, che corrispondono rispettivamente

i. al confronto degli interessi dei gruppi con quelli degli interessati, e
ii. al confronto degli interessi dei soggetti coinvolti con quelli dei titolari del trattamento.

Rispetto alla prima questione, il rischio maggiore è quello di conferire *de iure condendo* autonoma protezione a gruppi determinati dai procedimenti di *analytics*, in assenza di interessi comuni e convergenti delle persone che ne fanno parte[645]. Per esempio, la profilazione dei gruppi a scopi commerciali, agli occhi di diversi soggetti interessati, può essere accolta con favore se consente l'accesso ad alcuni *benefits*, ovvero ripudiata nel caso opposto (per esempio, si pensi al soggetto che non può accedere al credito bancario sulla base di un *credit score* basso).

La seconda questione appare maggiormente spinosa se si adottano soluzioni estreme, per le quali solo gli interessi di una parte sono presi in considerazione. La prevalenza delle esigenze dei titolari del trattamento (imprese o autorità pubbliche) farebbe venir meno il senso della tutela dei dati personali. Al contrario, se si fa

---

formazione, di applicazione e di cambiamento delle norme primarie. Vedasi G. GAVAZZI, *Norme primarie e norme secondarie*, Giappichelli, 1967.

[645] *De iure condito*, tale rischio non sussiste.

prevalere il solo interesse degli interessati, prevedendo la protezione non della posizione di questi ultimi, ma dei dati personali stessi anche in assenza di un danno[646], è chiaro che graverebbe sui titolari del trattamento un pregiudizio ingiustificato.

Si prospettano due soluzioni. Secondo alcuni, al fine di conciliare le opposte esigenze, occorre porre al centro del bilanciamento il precetto romanistico *alterum non laedere*[647]. In particolare, la protezione dei dati dei gruppi dovrebbe configurarsi «*as the right to limit the potential harms to the group itself that can derive from invasive and discriminatory data processing*»[648]. In questo senso, il rafforzamento dello strumento normativo della valutazione di impatto prevista dall'art. 33 del Regolamento può rappresentare una buona soluzione operativa. L'audit dovrebbe essere condotto da terzi (e non dagli stessi titolari del trattamento), sotto la supervisione delle autorità di controllo, che dovrebbero tratteggiare le qualifiche tecnico-professionali dei soggetti deputati alla valutazione[649].

Infine, un secondo approccio al problema si ravvisa nell'elaborazione di una nuova concezione della protezione dei dati personali basata sull'etica della virtù[650]. Questa dottrina filosofica, che trova una prima teorizzazione nell'*Etica Nicomachea* di Aristotele ed è tornata *in auge* nella seconda metà del Novecento[651], pone al centro dell'analisi il carattere virtuoso di un agente, cioè la sua disposizione a essere "buono moralmente". La distinzione della tutela di gruppi e di singoli interessati svanirebbe, dal momento che la *privacy* informazionale avrebbe come oggetto non solo gli interessi individuali, bensì il benessere dell'uomo, sia in quanto individuo, sia nei raggruppamenti di ogni tipo (*eudaimonía*, tradotto in inglese come *human flourishing*). In questo senso, «*virtue ethics could provide for claims by individuals who want to protect their personal interests, as well as claims by*

---

[646] Questa visione è emersa nella già citata sentenza *Google Spain* del 2014. Pagallo critica fortemente questa impostazione, denominata dall'autore "feticismo dei dati" (U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *op. loc.*, 168 ss.).
[647] U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, *op. loc.*, 171-72.
[648] A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, *op. cit.*, 148.
[649] A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, *op. cit.*, 153.
[650] B. VAN DER SLOOT, *Privacy as virtue: searching for a new privacy paradigm in the age of Big Data*, in E. BEVYERS ET AL., *Räume und Kulturen des Privaten*, Springer, 2017, 247 ss.
[651] Si considerino i lavori di Elizabeth Anscombe e Alasdair MacIntyre.

groups […] *who claim to defend a general, societal interest. It would allow for claims regarding direct and concrete personal harm, but also about abstract, hypothetical or a-priori damage*»[652]. Fra gli strumenti preferiti da questo approccio il *soft law* (codici di condotta ecc.) detiene una posizione privilegiata. Tuttavia, la previsione di un rischio "astratto" e aprioristico può finire per risolversi nella protezione dei dati *qua data*. Le conclusioni operative di tale approccio non differiscono dalle talune soluzioni avanzate nel versante americano per contrastare le esternalità negative inerenti all'uso di algoritmi e di tecniche di *machine learning*[653], per le quali il titolare del trattamento ha particolari doveri di diligenza e di buona fede (*duties of care*). Di questa tematica è dedicato il prossimo paragrafo.

6.2. Algo-ritmo serrato. La questione delle esternalità negative degli algoritmi nei sistemi giuridici statunitense ed europeo

Nel capitolo precedente si è affrontata la tematica dell'utilizzo degli algoritmi nelle attività di *business*, e si è concluso che questo comporta *spill-overs* che si ripercuotono sulla sfera giuridica dei consumatori. Occorre soffermarsi più specificamente su queste esternalità negative[654], che riguardano aspetti presi in considerazione in altri punti del presente capitolo.

Anzitutto, l'utilizzo degli algoritmi può compromettere la reputazione degli individui. Com'è ormai noto, mediante le attività di *data analytics*, il titolare del trattamento crea profili degli interessati, suddividendoli in gruppi sulla base di caratteristiche comuni. A tale meccanismo di classificazione del pubblico può seguire un'operazione di valutazione del rischio connesso alle caratteristiche dell'utente. Per esempio, il rischio può riguardare la propensione di una persona a commettere un reato[655], o la sua attitudine a dissipare ingenti quantità di denaro. L'attribuzione

---

[652] B. VAN DER SLOOT, *Privacy as virtue: searching for a new privacy paradigm in the age of Big Data*, *op. cit.*, 268.
[653] Ci si riferisce a J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, *op. cit.*, 1 ss.
[654] La tassonomia delle esternalità negative è di J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, *op. cit.*, 19-20. Vedasi § 4.2 del capitolo secondo.
[655] Michael Rich definisce tali algoritmi *Automated Suspicion Algorithms* (ASAs) (M.L. RICH, *Machine Learning, Automated Suspicion Algorithms, And The Fourth Amendment*, in 164 *University of Pennsylvania Law Review*, 2016, 871 ss.).

del rischio a un interessato, quindi, può comportarne la bollatura come soggetto socialmente pericoloso, col quale è sconsigliabile averci a che fare.

In secondo luogo, alla classificazione e alla valutazione del rischio può seguire la discriminazione. Sulla base delle informazioni analizzate, l'interessato o il gruppo di interessati possono vedersi negato l'accesso a determinati prodotti o servizi[656].

In terzo luogo, la consapevolezza degli interessati delle potenzialità discriminatorie derivanti dall'utilizzo degli algoritmi provoca mutamenti del loro comportamento al fine di evitare le ripercussioni negative, cioè essere reputati soggetti a rischio e discriminati (c.d. normalizzazione, *normalization*).

In quarto luogo, l'utilizzo di algoritmi incide più ampiamente sul comportamento degli interessati, spingendoli a compiere scelte più o meno prevedibili (c.d. manipolazione degli interessati) e minacciando la loro autonomia decisionale. Per esempio, l'algoritmo utilizzato da *Facebook* funziona come un filtro delle notizie che compaiono nella bacheca degli utenti, presentando loro solo i contenuti cui sono più interessati sulla base delle loro preferenze e conoscenze mostrate in passato[657].

Infine, gli algoritmi comportano un problema di mancanza di trasparenza, cioè di opacità (*opacity*)[658], su cui occorre soffermarsi ulteriormente. L'opacità degli algoritmi è riconducibile a tre ordini di problemi: l'inaccessibilità, l'incomprensibilità tecnico-formale e l'incomprensibilità sostanziale.

In primo luogo, gli algoritmi sono coperti da meccanismi di tutela proprietaria (quale, per esempio, il segreto industriale) che limitano l'accessibilità alle informazioni sul loro funzionamento. Il regime proprietario si spiega per diverse ragioni, quali il raggiungimento di vantaggi competitivi o fini di pubblica sicurezza[659]. Tale opacità "volontaria[660]" comporta un primo ostacolo alla conoscenza

---

[656] J.A. KROLL ET AL., *Accountable Algorithms*, in 165 *University of Pennsylvania Law Review*, 2017, 633 ss.
[657] J. DREXL, *Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics*, Max Planck Institute for Innovation and Competition Research Paper n. 16-16, 2016, 8.
[658] P. DOURISH, *Algorithms and their others: Algorithmic culture in context*, in 3(2) *Big Data & Society*, 2016, 6-7; J. BURRELL, *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in 3(1) *Big Data & Society*, 2016, 1 ss.
[659] B.D. MITTELSTADT ET AL., *op. cit.*, 6.
[660] J. BURRELL, *op. cit.*, 4.

del processo decisionale condotto mediante l'algoritmo, poiché, per esempio, secondo il Regolamento, il diritto di accesso previsto dall'art. 15 «*non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale*»[661].

In secondo luogo, se anche se tali informazioni fossero accessibili, solo un numero ristretto di individui, dotati di determinate qualifiche tecnico-professionali (per esempio, gli ingegneri informatici e i programmatori), sarebbe in grado di leggere e capire il linguaggio dei codici sorgente e gli schemi matematici che compongono gli algoritmi e ne determinano il funzionamento[662]. Si pone, quindi, un problema di comprensibilità del funzionamento degli algoritmi per la maggior parte delle persone.

In terzo luogo, sembra più difficile risolvere l'ultima questione. L'incomprensibilità sostanziale concerne il funzionamento degli algoritmi più complessi, che hanno la capacità di modificare e correggere i procedimenti di calcolo sulla base dei *datasets* forniti (*machine learning*)[663]. «*The internal decision logic of the algorithm is altered as it 'learns' on training data. Handling a huge number especially of heterogeneous properties of data* […] *adds complexity to the code*»[664]. Ne consegue che i risultati (*output*) dei procedimenti di analisi mediante algoritmi di questo genere sono imprevedibili e ignoti agli agenti umani. Perciò, anche se le informazioni sul funzionamento dell'algoritmo sono accessibili, rimane il problema di capirne le modalità decisionali.

Occorre soffermarsi sulle soluzioni prospettate nei due ordinamenti giuridici presi in considerazione.

---

[661] Cons. 63 Regolamento. Si veda il § 6.2.2 sul rapporto fra la trasparenza e il diritto di accesso ai sensi dell'art. 15 Regolamento.
[662] In questo senso, la giurisprudenza amministrativa italiana ha esteso la tutela del diritto di accesso (previsto dagli artt. 22 ss. della Legge n. 241 del 1990) ai codici sorgente del *software* dell'algoritmo per garantire la trasparenza degli atti amministrativi c.d. "informatici" in senso stretto (TAR Lazio, sede Roma, sez. III bis, sentenza 22 marzo 2017, n. 3769).
[663] Tali algoritmi apprendono dall'esperienza. Si è sviluppato questo punto nel § 4.2 del capitolo secondo.
[664] J. BURRELL, *op. cit.*, 5.

6.2.1. L'approccio statunitense

Negli Stati Uniti, per fronteggiare le esternalità negative degli algoritmi, si è proposta l'istituzione di nuovi obblighi in capo ai titolari del trattamento che utilizzano algoritmi nelle attività di *analytics*. In questo senso, secondo due celebri giuristi statunitensi, Paul Schwartz e Daniel Solove, occorre estendere a tali soggetti le obbligazioni previste dalla *law of negligence*, branca del *tort law* che riguarda le violazioni dei doveri di diligenza richiesti a certi soggetti in ragione della loro posizione giuridica. La trattazione dei due commentatori sul tema si conclude con il quesito: «*How should the law of tort define the duties owed to people regarding the use and disclosure of their personal data?*»[665].

Sull'interrogativo di Schwartz e Solove si innesta l'originale teoria di Jack Balkin sulla nozione di fiduciario informazionale (*information fiduciary*[666]). Secondo tale giurista statunitense, le attività di questa categoria di soggetti, che sono i titolari del trattamento di grandi quantità di dati personali (piattaforme digitali ecc.), sono tutelate dal primo emendamento della Costituzione americana (libertà di parola). Tuttavia, essendo dotati di un vantaggio informativo rispetto agli utenti, i fiduciari informazionali hanno anche speciali obblighi nei confronti dei loro clienti, destinatari dei prodotti immessi sul mercato. Gli utilizzatori degli algoritmi rientrano a pieno titolo nella categoria dei fiduciari informazionali. In particolare, due sono gli obblighi previsti. Il primo è il dovere di diligenza (*duty of care*), che impone all'utilizzatore di agire in maniera competente, senza trascurare gli interessi degli utenti; il secondo è il dovere di lealtà (*duty of loyalty*), per il quale «*fiduciaries must keep their clients' interests in mind and act in their clients' interests*»[667].

Muovendo da questo primo punto, l'analisi di Balkin tocca un ulteriore aspetto fondamentale. Secondo il commentatore statunitense, le operazioni condotte mediante l'utilizzo degli algoritmi, che pure consentono alle imprese di ri-

---

[665] P.M. SCHWARTZ – D. SOLOVE, *Reworking Information Privacy Law: A Memorandum Regarding Future ALI Projects About Information Privacy Law*, 2012.
[666] J.M. BALKIN, *Information Fiduciaries and the First Amendment*, in 49(4) *U.C. Davis Law Review*, 2016, 1183 ss.
[667] J.M. BALKIN, *Information Fiduciaries and the First Amendment*, *op. cit.*, 1208.

durre notevolmente i costi «*to perform tasks that would be prohibitively expensive*»[668], si estendono a persone che non hanno un rapporto fiduciario con i titolari del trattamento. Si pensi, per esempio, all'elaborazione di modelli predittivi del comportamento di certe categorie di individui sulla base dei *segments* e dei *credit scores*[669]. «*When we are not an end-user, client, or customer, there is no violation of a special relationship. Rather, the concern is about discrimination and manipulation that has effects on society in general*»[670].

Per ovviare a questo problema, occorre estendere la portata dei vincoli cui sono sottoposti gli utilizzatori degli algoritmi. *Nulla quaestio* nel caso in cui l'utilizzatore sia un'autorità pubblica, che intrattiene un rapporto di fiducia informazionale con gli amministrati. Resta da considerare la limitazione cui sono sottoposti i soggetti di natura privata, quali le piattaforme digitali. Oltre a dover rispettare obblighi di natura contrattuale inerenti al rapporto fiduciario con gli utenti, questi attori dovrebbero avere un più ampio dovere verso il pubblico di «*not to be algorithmic nuisances*»[671]. Tali "immissioni" consistono proprio nelle esternalità negative (*spill-overs*) di cui si è parlato all'inizio del precedente paragrafo.

L'analisi di Balkin merita ancora due puntualizzazioni. In primo luogo, dato che l'utilizzatore di algoritmi ha obblighi nei confronti della collettività (*public duties*), si passa dal piano della responsabilità contrattuale a quello della responsabilità extracontrattuale (*tortous liability*[672]). In secondo luogo, l'autore reputa le esternalità negative di cui si è detto in precedenza *public nuisances*, inquadrando il discorso riguardante i rimedi nell'ambito della *law of property*. Le immissioni di natura pubblica (in senso economico) si configurano come *public bads*, che sono il corrispondente simmetrico negativo del concetto di *public good* e ne condividono le caratteristiche (non-rivalità e non-escludibilità): il loro impatto riguarda un numero ampio e indefinito di soggetti[673]. L'utilizzo degli algoritmi modifica in peggio la sfera giuridica di un'ampia pluralità di consociati, la cui curva di utilità è affetta

---

[668] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione), 20.
[669] Vedasi § 6.4 del capitolo primo.
[670] J.M. BALKIN, *Information Fiduciaries and the First Amendment*, *op. cit.*, 1233.
[671] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, *op. cit.*, 17.
[672] U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, in *Philosophy & Technology*, 2017.
[673] L'inquinamento atmosferico è un buon esempio di questa nozione.

dal comportamento di terzi «*al di fuori dai consueti meccanismi dello scambio di mercato*»[674].

Secondo l'analisi economica del diritto, il rimedio risarcitorio è la soluzione più efficiente per far fronte alle immissioni di natura pubblica[675]. Vi sono due tipologie di risarcimento del danno provocato dalle immissioni. Il primo tipo può definirsi "temporaneo[676]", ed è essenzialmente rivolto al passato, poiché mira a reintegrare la sfera giuridica di un soggetto leso in precedenza dal comportamento di un altro consociato. È chiaro che, riconoscendo la risarcibilità del danno derivante dalle attività algoritmiche, l'utilizzatore può reiterarle in futuro, e, di conseguenza, «*the plaintiff must return to court in order to receive additional damages*»[677]. In altri termini, sul danneggiato grava il costo di intentare una nuova causa giudiziaria. L'utilizzatore, tuttavia, ha un incentivo a non perpetuare l'attività dannosa, dal momento che, qualora adotti misure per internalizzare l'esternalità negativa, il risarcimento riconosciuto nelle liti successive ha un'entità minore.

Un'alternativa a questa tipologia di risarcimento esclusivamente volto al passato è rappresentata dal c.d. *permanent damage* ("risarcimento permanente"), applicato nel famoso caso *Boomer v. Atlantic Cement Co.*[678]. Se il danneggiante è obbligato a tale rimedio, il danneggiato riceve una somma risarcitoria parametrata non solo rispetto all'attività nociva del passato, ma anche rispetto al «*present discounted value of all reasonably anticipated future harms*»[679]. Si tratta, quindi, di un risarcimento che volge sia al passato, sia alle attività future. Nondimeno, tale alternativa comporta costi notevoli per il danneggiato, giacché è difficile prevedere i cambiamenti tecnologici e procedere a un'accurata stima dei danni futuri. Inoltre, il danneggiante non è incentivato a ridurre la portata dell'esternalità, poiché tale modalità risarcitoria impedisce al danneggiato la possibilità di promuovere nuove

---

[674] U. MATTEI, *La proprietà*, in *Trattato di diritto privato*, diretto da R. SACCO, 2ª ed., UTET Giuridica, 2015, 328.
[675] R. COOTER – T. ULEN, *Law & Economics*, Addison-Wesley, 2012, 168.
[676] Cooter e Ulen distinguono fra *temporary damage* e *permanent damage.* Si veda R. COOTER – T. ULEN, *op. cit.*, 168 ss.
[677] R. COOTER – T. ULEN, *op. cit.*, 169.
[678] *Boomer v. Atlantic Cement Co.*, 26 N.Y.2d 219 (1970).
[679] R. COOTER – T. ULEN, *op. loc. cit*.

azioni giudiziarie in futuro rispetto allo stesso danno provocato dal danneggiante. La soluzione più efficiente, in definitiva, è la prima tipologia di risarcimento.

Tornando all'analisi di Balkin, la sua argomentazione termina con tre punti. Anzitutto, spetta allo Stato elaborare norme che regolano l'internalizzazione delle esternalità negative. In secondo luogo, occorre individuare le compagnie che usano gli algoritmi e che impongono costi sul resto della società. Infine, se gli agenti economici che utilizzano gli algoritmi sono anonimi, «*then the law will have to require disclosure of who is behind the algorithm in order to enforce a public duty*»[680].

In conclusione, l'approccio nordamericano rispetto alle esternalità negative determinate dagli algoritmi appare molto pragmatico ed è rivolto principalmente alla tutela *ex post* degli interessati, configurandosi come un superamento del sistema di tutela della *privacy* vigente basato su interventi settoriali e largamente delegato all'autoregolazione delle società delle telecomunicazioni.

6.2.2. L'approccio dell'Unione europea e il dibattito intorno al "diritto alla spiegazione"

Come visto in precedenza, il Regolamento (UE) 2016/679 prevede precisi obblighi in capo ai titolari del trattamento e, simmetricamente, una serie di diritti dell'interessato. Fra questi ultimi, taluni autori hanno riconosciuto la previsione di un "diritto alla spiegazione" (*right to explanation*) del funzionamento del processo decisionale automatizzato, col quale il legislatore europeo intende fronteggiare i costi imposti dalle attività degli utilizzatori degli algoritmi[681].

Preliminarmente, occorre distinguere fra due tipologie di spiegazione in base al momento in cui essa si colloca[682]. La spiegazione *ex ante*, ponendosi prima che la decisione automatizzata abbia luogo, concerne il funzionamento del sistema

---

[680] J.M BALKIN., *The Three Laws of Robotics in the Age of Big Data*, *op. cit.*, 21.
[681] Si vedano, *inter alios*, B. GOODMAN – S. FLAXMAN, *European Union regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine*, 2017, in corso di pubblicazione; U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*; S. WACHTER ET AL., *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in 7(2) *International Data Privacy Law*, 2017, 76 ss.
[682] U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*; S. WACHTER ET AL., *op. cit.*

del processo decisionale automatizzato, e si estende alla logica e alle conseguenze previste del sistema stesso. La spiegazione *ex post*, invece, comprende sia il funzionamento del sistema, sia la *ratio* di una specifica decisione, cioè «*reasons, and individual circumstances of a specific automated decision, e.g. the weighting of features, machine-defined case-specific decision rules, information about reference or profile groups*»[683].

Benché negli articoli del Regolamento non se ne faccia espressa menzione, da alcune norme del Regolamento si può evincere l'esistenza di un diritto alla spiegazione. Le possibili fonti di quest'ultimo si trovano nelle "misure di salvaguardia" previste al par. III dell'art. 22, negli obblighi di informazione stabiliti dagli artt. 13 e 14 e nel diritto di accesso ai sensi dell'art. 15. Occorre soffermarsi su ciascuna di queste basi giuridiche. La prima norma citata riguarda la spiegazione *ex post*, le altre due quella *ex ante*.

Anzitutto, si consideri la spiegazione *ex ante*. Com'è noto, gli artt. 13 e 14 del Regolamento impongono obblighi informativi in capo al titolare del trattamento. Fra gli altri, egli deve comunicare all'interessato «*l'esistenza di un processo decisionale automatizzato, compresa la profilazione* […]*, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*»[684]. Questa spiegazione si colloca prima del processo decisionale, nel momento in cui i dati sono raccolti per essere sottoposti al trattamento[685], e riguarda il funzionamento del sistema algoritmico. Si pongono problemi rispetto alla qualità delle informazioni cui l'interessato accede: la diffusione dei codici sorgente e le descrizioni tecniche dettagliate non soddisfano le esigenze di trasparenza dell'interessato, a meno che costui non sia un soggetto qualificato a livello professionale. Al contrario, «*a high-level, non-technical, description of the decision-making process is more likely to be meaningful*»[686].

---

[683] S. WACHTER ET AL., *op. cit.*, 78.
[684] La stessa espressione è utilizzata all'art. 13 par. II lett. f Regolamento e all'art. 14 par. II lett. g Regolamento.
[685] S. WACHTER ET AL., *op. cit.*, 82.
[686] C. KUNER ET AL., *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, in 7(1) *International Data Privacy Law*, 2017, 2.

In secondo luogo, un diritto alla spiegazione si può desumere dal diritto di accesso previsto all'art. 15 del Regolamento. Secondo questa norma, la cui formulazione riprende i due articoli precedenti, l'interessato ha diritto di ottenere l'accesso alle informazioni riguardanti «*l'esistenza di un processo decisionale automatizzato, compresa la profilazione* […]*, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*». L'esercizio del diritto di accesso, a differenza degli obblighi previsti dagli artt. 13 e 14, implica un'istanza dell'interessato al titolare del trattamento che non è soggetta a termini di decadenza. Stando a questa ricostruzione, all'interessato potrebbe essere garantito un diritto alla spiegazione *ex ante* ed *ex post*, a seconda del momento in cui è formulata la richiesta. Tuttavia, il riferimento alle "conseguenze previste" lascia intendere che il diritto di accesso abbia ad oggetto solo le spiegazioni *ex ante*.

In terzo luogo, il par. I dell'art. 22 del Regolamento stabilisce che la persona interessata abbia il diritto di non essere sottoposta a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che la riguardano o che incida in modo analogo significativamente sulla sua persona. La disposizione, tuttavia, è poco chiara: a ben vedere, "il diritto di non essere sottoposti a un processo decisionale automatizzato" può interpretarsi nel senso che l'interessato goda di un mero diritto di contestazione di tale decisione[687], ovvero che sul titolare gravi un vero e proprio divieto[688]. Inoltre, non si comprende la portata della decisione automatizzata che incide "significativamente" sull'interessato e che produce "effetti giuridici" che lo concernono[689]. A questa regola, che segue la *ratio* sottostante al principio della limitazione della finalità e, quindi, pare particolarmente adeguata per tutelare la posizione giuridica degli interessati, derogano le eccezioni previste al paragrafo seguente, che operano come "clausole di disinnesco" della norma in questione. Secondo il par. II dell'art. 22, la norma del par. I non si applica nel caso in cui la decisione: «*a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*

---

[687] Come si vedrà *infra*, il diritto alla contestazione della decisione è previsto all'art. 22 par. III.
[688] S. WACHTER ET AL., *op. cit.*, 94-95.
[689] U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato». Di solito, come si è visto, l'interessato fornisce il proprio consenso al trattamento senza badare troppo alle *privacy policies*, che possono comprendere anche decisioni automatizzate. Se l'art. 22 si limitasse a tali disposizioni, la norma difetterebbe di effettività. Per evitare che il par. I sia eluso nella prassi ricorrendo al consenso dell'interessato, il legislatore europeo ha stabilito che, nelle sole ipotesi *sub* a) e c), il titolare del trattamento debba attuare «*misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*»[690]. Come si può notare, il par. III dell'art. 22 non menziona espressamente un vero e proprio diritto alla spiegazione, ma configura misure di "salvaguardia" dell'interessato. Secondo alcuni commentatori, tale situazione giuridica può comunque desumersi adottando un'interpretazione estensiva e sistematica del dettato normativo regolamentare. Infatti, da un lato, pare poco sensato ammettere la possibilità di contestare la decisione automatizzata senza conoscere le modalità con cui è stata presa[691]; dall'altro, una spiegazione *ex post* del funzionamento dell'algoritmo e della decisione si desume dal par. I dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea[692], giacché «*without an explanation of how the algorithm works,* […] [*this right is*] *hard to enforce, because the decisions/evidence used will be impossible to contest in court*»[693]. Un'altra parte della dottrina nega l'esistenza di un diritto alla spiegazione *ex post* sulla base della letteralità del par. III dell'art. 22 del Regolamento, che, peraltro, contraddice il considerando 71, per il quale il titolare del trattamento do-

---

[690] Art. 22 par. III Regolamento.
[691] In questo senso, U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, *op. cit.*
[692] «*Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo*» (Art. 47 CDFUE).
[693] S. WACHTER ET AL., *op. cit.*, 91.

vrebbe fornire «*una spiegazione della decisione*» basato sul trattamento automatizzato. Poiché i considerando non hanno carattere giuridicamente vincolante[694], si deve concludere che il diritto alla spiegazione non è previsto dal Regolamento[695]. Chiaramente, la giurisprudenza avrebbe un ruolo fondamentale nell'ermeneutica della norma, ma, allo stato attuale delle cose, nessuna sentenza della Corte di giustizia europea riguarda direttamente la questione.

Le soluzioni prospettate dal dettato normativo regolamentare pongono taluni problemi applicativi. Anzitutto, l'esclusione dell'ipotesi prevista dalla lett. b) del par. II dell'art. 22 dal campo di applicazione del par. III pone problemi di frammentazione della disciplina: gli Stati membri potrebbero enumerare casi in cui l'applicazione del par. III sia esclusa[696], frustrando l'effettività della norma. In secondo luogo, la spiegazione *ex post* potrebbe rivelarsi poco appropriata per i sistemi algoritmici complessi, dotati di tecnologie di *machine learning*. Infatti, anche se il processo decisionale può essere teoricamente spiegato, «*what if it is impossible to do that in a way that is intelligible to a data subject?*»[697]. Perciò, la spiegazione della decisione potrebbe avere un'utilità limitata a prevenire l'eventuale pregiudizio subito dagli interessati. In altri termini, come notano alcuni autori, la trasparenza non sarebbe garanzia della correttezza del processo decisionale automatizzato[698].

In conclusione, la disciplina europea, pur non essendo priva di ambiguità, rappresenta comunque un primo tentativo per affrontare le problematiche che emergono dall'opacità degli algoritmi. Come già fatto notare, la spiegazione del processo decisionale, con cui si tenta di risolvere la questione della trasparenza, potrebbe comunque non essere sufficiente all'interessato per capire le logiche decisionali. Inoltre, la diffusione di talune informazioni sugli algoritmi potrebbero ledere i diritti di proprietà intellettuale dei titolari del trattamento (segreto industriale). Per ovviare ad entrambi i problemi, alcuni autori hanno proposto l'istituzione di meccanismi di verifica (*auditing*) da parte di autorità indipendenti (*trusted*

---

[694] T. KLIMAS – J. VAICIUKAITE, *The Law of Recitals in European Community Legislation*, in 15 *ILSA Journal of International & Comparative Law*, 2008, 32 ss.
[695] In questo senso, S. WACHTER ET AL., *op. cit.*, 80.
[696] S. WACHTER ET AL., *op. cit*., 94.
[697] C. KUNER ET AL., *op. cit.*, 1.
[698] J.A. KROLL, *op. cit.*; B. GOODMAN, *op. cit.*, 3-4.

auditors) che, pur mantenendo il segreto industriale nell'interesse degli utilizzatori, agiscono per il pubblico interesse, spiegando il funzionamento dell'algoritmo in termini comprensibili anche a soggetti non dotati di competenze tecnico-professionali[699].

[699] In questo senso, B. GOODMAN, *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*, 29th Conference on Neural Information Processing Systems Paper, 2016, 4-6; B.D. MITTELSTADT, *Auditing for Transparency in Content Personalization Systems*, in 10 *International Journal of Communication*, 2016, 12 ss.; F. PASQUALE, *op. cit.*, 141.

CAPITOLO QUARTO.
I LIMITI GIURIDICI ALL'ACCESSO AI DATI NON PERSONALI.
PROPRIETÀ E REGOLAMENTAZIONE

Abstract

I datasets *costituiti da quantità sterminate di dati non personali sono divenuti* assets *fondamentali per gli attori operanti nei mercati dei* Big Data *che li controllano. I commentatori e le autorità del versante europeo si sono chiesti se tali nuove utilità intangibili possano rientrare in taluni regimi di tutela attualmente esistenti, ovvero debbano essere oggetto di un nuovo diritto esclusivo, ovvero sia necessario rafforzarne l'accesso ricorrendo ad altri campi del diritto.*

1. La tutela giuridica dei dati non personali

Nel precedente capitolo, si è affrontata la questione dei dati personali, soffermandosi in particolare sulle sfide che la società dell'informazione pone ai principi tradizionali della tutela delle informazioni degli interessati e sulle tendenze delle forze del mercato a considerare i dati alla stregua di nuovi *assets* da cui i vari *stakeholders* traggono immensi benefici economici.

In questa parte del lavoro, ci si sofferma sulla tutela giuridica dei dati non personali. Anzitutto, è necessario distinguere preliminarmente due situazioni qualitativamente diverse cui l'espressione "dati non personali" si riferisce[700].

i. In primo luogo, vi sono i cc.dd. "beni digitali", quali *files* musicali, *ebook*, documenti di testo ecc. Tali risorse consistono nei formati digitali (quali *files mp3*, *doc* ecc.) che funzionano come i dispositivi analogici in cui è scritto il contenuto di un'opera dell'ingegno. Rispetto ai beni digitali, esiste una tutela giuridica di diritto d'autore, e, come si vedrà *infra*, il legislatore europeo ha preso in considerazione l'introduzione di nuove norme in materia di diritto dei contratti concernenti tali beni.

ii. In secondo luogo, nella nozione rientrano anche i grandi *datasets* raccolti, analizzati e (ri)utilizzati dai soggetti economici, che comprendono quantità incalcolabili di dati non personali prodotti da dispositivi (*machine-generated data*), «*created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real*»[701].

---

[700] W. KERBER, *Governance of Data: Exclusive Property vs. Access*, in 47 *IIC International Review of Intellectual Property and Competition Law*, 2016, 760.

[701] Comunicazione della Commissione *Building a European Data Economy*, 2017, 9. Un'efficace analisi di questa Comunicazione è quella di H. ZECH, *Building a European Data Economy*, in 48 *IIC International Review of Intellectual Property and Competition Law*, 2017, 501 ss. Si ricordi dal precedente capitolo che i dati dei grandi *datasets* si considerano personali se si riferiscono a una determinata persona fisica ("soggetto interessato") e non sono sottoposti a procedimenti di anonimizzazione. Si veda, in particolare, il § 4.1 del capitolo terzo.

Occorre poi tener presente che il livello di protezione dei dati è strettamente connesso alla distinzione di tre piani della nozione di informazione[702]:

i. il piano semantico, cioè quello del significato (si pensi, per esempio, alla successione di note e alla progressione armonica di un brano musicale);
ii. il piano sintattico, cioè quello dei *bits*, dei segni e dei codici, rappresentati nel sistema numerico binario (ad esempio, il *file mp3* dello stesso brano musicale);
iii. il piano fisico-strutturale, inerente all'infrastruttura, al supporto o al dispositivo che contiene i dati o, in senso più ampio, ai dati rappresentati dalla struttura di una cosa materiale (per esempio, il CD o la penna USB in cui è immagazzinata la traccia musicale).

I dati trovano diverse modalità di protezione giuridica per ciascuno di questi livelli. Per esempio, la protezione dei dati personali, il segreto commerciale e il brevetto sono esempi di tutela giuridica inerente al piano semantico[703]; il diritto di proprietà sul supporto contenente le informazioni, quale un CD di un album musicale, inerisce al piano fisico-strutturale.

Occorre ora soffermarsi sul dibattito intorno ai dati non personali nel versante europeo. In prima battuta si ripercorreranno brevemente gli interventi normativi delle autorità europee concernenti i beni digitali; in seconda istanza, ci si concentrerà sui *datasets* di grandi dimensioni.

---

[702] H. ZECH, *Data as a Tradeable Commodity*, in A. DE FRANCESCHI, *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Intersentia, 2016, 53-54. L'autore riprende la distinzione di Y. BENKLER, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, in 52 *Federal Communications Law Journal*, 2000, 562. A. WIEBE, A. WIEBE, *Protection of industrial data – a new property right for the digital economy?*, in 12(1) *Journal of Intellectual Property Law & Practice,* 2017, 62 ss. modifica leggermente tale impostazione.

[703] H. ZECH, *Information as Property*, in 6 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2015, 194.

2. Alle radici di un dibattito essenzialmente europeo. I beni digitali: dal diritto dei contratti alla proprietà

2.1. Dalla Direttiva 2011/83/UE alla proposta di Direttiva sui contratti di fornitura di contenuto digitale del 2015

Le autorità europee hanno dimostrato un notevole interesse verso una tutela giuridica più adeguata dei beni digitali in taluni interventi concernenti il diritto dei contratti dei consumatori all'inizio del secondo decennio del Duemila.

Con la Direttiva 2011/83/UE[704], il legislatore europeo ha conferito un *minimum* di armonizzazione alle normative interne degli Stati membri riguardanti i diritti dei consumatori, stabilendo «*norme standard per gli aspetti comuni dei contratti a distanza e dei contratti negoziati fuori dei locali commerciali*»[705]. Nel testo normativo, una disciplina speciale riguarda i contratti di fornitura di "contenuto digitale", che è definito in maniera alquanto tautologica come «*i dati prodotti e forniti in formato digitale*»[706]. Il dettato legislativo configura tali contratti come un *tertium genus* rispetto al contratto di vendita e al contratto di servizi[707], e prevede norme specifiche in materia di obblighi di informazione pre-contrattuale[708] e di diritto di recesso[709].

Nello stesso senso, la proposta di Regolamento relativo al diritto comune europeo della vendita del 2011[710], prevede che il contenuto digitale sia costituito dai «*dati prodotti e forniti in formato digitale, secondo o meno* [sic] *le indicazioni del consumatore, inclusi le registrazioni audio o video, le immagini o i contenuti*

---

[704] Direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011 sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, G.U. n. L. 304 del 22/11/2011 (d'ora in poi: "Direttiva 2011/83/UE"). Si veda, *inter alios*, N.W. MICKLITZ – N. REICH, *The Commission Proposal for a 'Regulation on a Common European Sales Law (CESL)' – Too Broad or Not Broad Enough?*, EUI Working Papers LAW n. 2012/04, 2012; M. LOOS, *The Regulation of Digital Content B2C Contracts in CESL*, Centre for the Study of European Contract Law Working Paper Series n. 2013-10, 2013.
[705] Cons. 2 Direttiva 2011/83/UE.
[706] Art. 2 n. 11 Direttiva 2011/83/UE.
[707] Cons. 19 Direttiva 2011/83/UE.
[708] Art. 5 par. I lett. g-h, art. 5 par. II, art. 6 par. I lett. r-s, art. 6 par. II Direttiva 2011/83/UE.
[709] Art. 9 lett. c, art. 14 par. IV lett. b, art. 16 lett. m Direttiva 2011/83/UE.
[710] Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita*, 2011.

digitali scritti, i giochi digitali, il software e il contenuto digitale che permette di personalizzare l'hardware o il software esistente […]»[711]. Inoltre, il testo della bozza normativa conferisce un rango autonomo ai beni in formato digitale[712], che divengono oggetto di contratti di compravendita, e non più di contratti di licenza di diritto d'autore[713]. Nonostante la portata innovativa di tale impostazione, la Commissione ha accantonato la proposta di Regolamento quattro anni più tardi[714].

Nel dicembre 2015, in concomitanza con la pubblicazione della strategia del Mercato unico digitale (MUD, *Digital Single Market*[715]), la Commissione ha apportato modifiche notevoli alla precedente bozza, mirando alla formulazione di norme armonizzate applicabili alla fornitura di contenuto digitale e alla vendita *online* di beni. A ciascuna di queste materie corrisponde una nuova proposta di Direttiva[716]. Secondo la nuova Proposta di Direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, la nozione di "contenuto digitale" comprende:

i) i dati prodotti e forniti in formato digitale, ad esempio registrazioni audio o video, applicazioni, giochi digitali e qualsiasi altro tipo di software;

---

[711] Art. 2 lett. j Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita*, 2011.

[712] «*Il diritto comune europeo della vendita può disciplinare: a) i contratti di vendita; b) i contratti di fornitura di contenuto digitale, su supporto materiale o meno, che l'utente possa memorizzare, trasformare o cui possa accedere e che possa riutilizzare, a prescindere che il contenuto digitale sia fornito contro il pagamento di un prezzo; c) i contratti di servizi connessi, indipendentemente dal fatto che per quei servizi sia stato pattuito un prezzo separato*» (art. 5 Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita*, 2011).

[713] N.W. MICKLITZ – N. REICH, *op. cit.*, 15 («*This seems to be a departure from the classical approach of licensing of intellectual property rights, which was regarded as a contract of its own in most Member States. It can be justified by the "commodification" (Verdinglichung) of digital content through modern technologies, in particular through downloading on the Internet which makes them a candidate for a standardised transaction similar to the traditional sales concept*»).

[714] *Legislative Train Schedule – Common European Sales Law (CESL)*, in *Europarl.europa.eu* (www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-common-european-sales-law, ultimo accesso 9 agosto 2017).

[715] Comunicazione della Commissione *Strategia per il mercato unico digitale in Europa*, 2015.

[716] Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale*, 2015; Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita online e di altri tipi di vendita a distanza di beni*, 2015.

ii) i servizi che consentono la creazione, il trattamento o la memorizzazione di dati in forma digitale, ove tali dati siano forniti dal consumatore, e

iii) i servizi che consentono la condivisione di dati in formato digitale forniti da altri utenti del servizio e qualsiasi altra interazione con tali dati[717].

Dal testo normativo emerge che il concetto di "contenuto digitale" è stato esteso notevolmente, e comprende anche talune tipologie di servizi, quali quelli di *cloud computing*. Inoltre, dalla formulazione scelta nel testo normativo, pare che l'oggetto del contratto riguardi il piano sintattico dell'informazione, cioè i dati nel loro formato digitale.

Come già visto nei capitoli precedenti, i dati personali dei consumatori sono divenute vere e proprie merci di scambio nella società dell'informazione[718]. Nella proposta di Direttiva, prendendo atto di tali mutamenti, si afferma che «*gli operatori del mercato tendono spesso e sempre più a considerare le informazioni sulle persone fisiche beni di valore comparabile al denaro. I contenuti digitali sono spesso forniti non a fronte di un corrispettivo in denaro ma di una controprestazione non pecuniaria, vale a dire consentendo l'accesso a dati personali o altri dati*»[719]. In questo senso, l'art. 3 della stessa bozza prevede che la Direttiva si applichi ai contratti in cui il fornitore somministra contenuto digitale, in cambio del quale il consumatore corrisponde un prezzo oppure fornisce una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato.

Questi sforzi normativi dimostrano un crescente interesse delle autorità europee verso l'incentivazione della commercializzazione dei beni digitali quali *ebooks*, *files mp3* ecc. Secondo le istituzioni europee, «*data are to be treated as commercial goods and subject in every way to sales law, irrispective of whether in*

---

[717] Art. 2 n. 1 Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale*, 2015.
[718] Vedasi § 6.4 del capitolo secondo.
[719] Cons. 13 Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale*, 2015.

the course of trade they are embodied on a tangible medium or intangibly, for example, in a digital network»[720]. I testi normativi appena esaminati, pur non riguardando apertamente le tendenze degli attori economici all'accumulo di grandi quantità di dati, costituiscono un primo importante passo verso la regolamentazione specifica delle obbligazioni aventi ad oggetto un *dare* a contenuto digitale.

2.2. Il caso *UsedSoft*

Nella sentenza *UsedSoft*[721], la Corte di giustizia dell'Unione europea ha affrontato la questione della proprietà dei beni digitali, e quindi, indirettamente, quella dei dati non personali.

In base alla Direttiva 2001/29/CE, il diritto esclusivo dell'autore di distribuire gli esemplari di un'opera incontra un limite nel c.d. principio dell'esaurimento (*exhaustion doctrine*, meglio conosciuta negli Stati Uniti come *first-sale doctrine*), per il quale il titolare del diritto non può impedire la rivendita delle copie dell'opera messe in commercio col suo consenso[722] dopo che ha proceduto alla prima vendita o al primo trasferimento della proprietà di tali esemplari all'interno del territorio europeo. In altri termini, l'acquirente della prima copia, divenuto proprietario di quest'ultima, non ha bisogno dell'autorizzazione dell'autore per alienarla in un secondo momento. Tale principio è il frutto della coordinazione della tutela del diritto d'autore col principio di libera circolazione delle merci, considerato prevalente in questo caso[723].

Fino all'intervento della giurisprudenza, si è ritenuto che la dottrina dell'esaurimento riguardasse solo le copie di un'opera registrate o iscritte su supporti "fisici", quali, ad esempio, i CD-ROM, i DVD ecc. Nel caso in questione, i

---

[720] A. DE FRANCESCHI – M. LEHMANN, *Data as Tradeable Commodity and New Measures for their Protection*, in 1(1) *Italian Law Journal*, 2015, 60.
[721] CGUE 3 luglio 2012, causa C-128/11, UsedSoft GmbH c. Oracle International Corp.
[722] Art. 4 par. II Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, G.U. n. L. 167 del 22/06/2001 («*Il diritto di distribuzione dell'originale o di copie dell'opera non si esaurisce nella Comunità, tranne nel caso in cui la prima vendita o il primo altro trasferimento di proprietà nella Comunità di detto oggetto sia effettuata dal titolare del diritto o con il suo consenso*»).
[723] Art. 26 e artt. 28-37 Trattato sul funzionamento dell'Unione europea (versione consolidata), G.U. n. C. 202 del 7/06/2016 (d'ora in poi: TFUE).

giudici europei, applicando il principio dell'equivalenza *offline-online*[724], hanno esteso la dottrina dell'esaurimento agli ambienti digitali, prevedendo che il principio possa applicarsi anche ai casi di scaricamento (*download*) delle copie digitali di un programma per elaboratore (*software*[725]) da *Internet*, se autorizzato dal titolare del diritto, anche a titolo gratuito. Alla luce della sentenza, quindi, «*where the copyright holder makes available to his customer a copy — tangible or intangible — and at the same time concludes, in return for payment of a fee, a licence agreement granting the customer the right to use that copy for an unlimited period, that right holder sells the copy to the customer and thus exhausts his exclusive distribution right. Such a transaction involves a transfer of the right of ownership of the copy*»[726].

Benché la sentenza si occupi specificamente di programmi per elaboratore, fra gli autori è prevalsa l'opinione che il principio dell'esaurimento "digitale[727]" possa ragionevolmente estendersi anche alle copie di altre tipologie di opere creative, quali brani musicali, *ebooks* ecc.[728] Più controversa è la configurabilità di tale precetto rispetto ai servizi di fornitura del contenuto dell'opera: secondo alcuni, attenendosi al testo della Direttiva 2001/29/CE, occorre escludere la fornitura di un servizio *online* dal campo di applicazione della dottrina dell'esaurimento[729]; tuttavia, così facendo, si perdono di vista le recenti evoluzioni tecnologiche, e si limita

---

[724] M. SAVIČ, *The Legality of Resale of Digital Content after UsedSoft in Subsequent German and CJEU Case Law*, in 37(7) *European Intellectual Property Review*, 2015, 415 («*This principle requires exhaustion to apply to intangible copies of software (and other digital goods) just as it does to tangible ones, because the situation online is in essence comparable to the situation offline*»).

[725] Il par. II dell'art. 4 della Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore, G.U. n. L. 111 del 5/05/2009, prevede che «*la prima vendita della copia di un programma nella Comunità da parte del titolare del diritto o con il suo consenso esaurisce il diritto di distribuzione della copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso*».

[726] P.L.C. TORREMANS, *Holyoak & Torremans Intellectual Property Law*, Oxford University Press, 2014, 342.

[727] Vedasi, più nel dettaglio, W. KERBER, *Exhaustion of Digital Goods: An Economic Perspective*, Macie Discussion Paper n. 23-2016, 2016, 1 ss.

[728] P.L.C. TORREMANS, *Holyoak & Torremans Intellectual Property Law*, *op. cit.*, 343.

[729] La Direttiva 2001/29/CE precisa che «*la questione dell'esaurimento del diritto non si pone nel caso di servizi, soprattutto di servizi "on-line"*» (cons. 29). Per un'analisi sulla distinzione fra beni e servizi nella recente giurisprudenza della CGUE, si rimanda a T. DREIER, *Online and Its Effect on the "Goods" Versus "Services" Distinction*, in 44 *International Review of Intellectual Property and Competition Law*, 2013, 137 ss.

notevolmente la portata del principio in questione a modelli di *business* che saranno presto surclassati[730].

La rivendita di una copia digitale dell'opera creativa comporta talune problematiche. A differenza di un prodotto su un supporto fisico, un *file* deve essere copiato per essere ulteriormente ceduto, ma ciò non comporta la contestuale eliminazione del prodotto dal dispositivo del primo acquirente. Perciò, la creazione di un'ulteriore copia può ledere il diritto esclusivo di riproduzione dell'autore dell'opera[731]. Tuttavia, negli ambienti digitali, venendo meno la differenza fra l'opera originale e quella riprodotta[732], la copia di un *file* è un elemento tecnologico accessorio e necessario perché il prodotto in questione possa circolare liberamente nel mercato[733]. Perciò, nel bilanciamento delle esigenze dell'autore e dei consumatori, il sacrificio delle prime è necessario a garantire il buon funzionamento del mercato.

In definitiva, la sentenza *UsedSoft* rappresenta un traguardo importante per l'evoluzione del diritto d'autore nell'età digitale, in cui la maggior parte delle opere protette è oggetto di scambi *online*. Il diritto di proprietà del licenziatario sulla copia digitale si estende ai dati non personali che la costituiscono. La Corte però non si è spinta a riconoscere un generale diritto di proprietà dei dati che possa estendersi a contesti diversi da quello delle opere creative in formato digitale, quali le questioni di appartenenza dei *Big Data*[734], su cui ora occorre dilungarsi.

---

[730] In questo senso, rispetto al versante americano, A. PERZANOWSKI – J. SCHULTZ, *Legislating Digital Exhaustion*, in 29 *Berkeley Technology Law Journal*, 2014, 1535 ss.
[731] Così ha concluso la Corte distrettuale del Distretto meridionale di New York nel caso *Capitol Records, LLC v. ReDigi Inc.*, 12-0095 U.S. Dist. (2013).
[732] «*Absent the baseline of visual intelligibility, there is no criterion for knowing which object legitimately embodies its eidos and which does not. The effects of this absence stand behind many of the battles surrounding digital reproduction*» (G. HULL, *Digital Copyright and the Possibility of Pure Law*, in 14 *Qui Parle*, 2003, 25).
[733] P.L.C. TORREMANS, *The Future Implications of the Usedsoft Decision*, CREATe Working Paper n. 2014/2, 2014, 9-10.
[734] J. DREXL, *op. cit.*, 28.

3. Lo stato degli scambi dei Big Data *nel mercato interno dell'Unione europea nell'esame della Commissione*

Nei precedenti paragrafi, materia di analisi sono state le opere in formato digitale quali *file mp3*, *ebooks* ecc., che corrispondono alla prima accezione di "dati non personali" descritta *supra* nel § 1. I dati non personali acquisiti in ampi *datasets* e da una pluralità di fonti fanno riferimento a scenari economici radicalmente diversi. Come si è visto in precedenza, i *Big Data* sono una risorsa fondamentale per la crescita economica delle imprese[735]. Molti dati sono generati senza il diretto intervento di un operatore umano (*machine-generated data*) mediante i sensori degli oggetti *smart* interconnessi dell'Internet delle Cose e, dopo essere sottoposti ad analisi, diventano informazioni di valore e sono riusati dalle imprese. Le imprese scambiano i *datasets* di grandi dimensioni come veri e propri beni commerciabili (*assets* o *commodities*) mediante strumenti contrattuali[736]. È chiaro che gli interventi delle istituzioni europee in materia di opere creative digitali esaminati nel precedente paragrafo riguardano solo la posizione giuridica degli autori e dei consumatori, lasciando disattese talune questioni giuridiche concernenti l'appartenenza dei *datasets* di grandi dimensioni da parte delle imprese che li sfruttano. Al contrario, «*raw machine-generated data are not protected by existing intellectual property rights since they are deemed not to be the result of an intellectual effort and/or have any degree of originality*»[737].

Rispetto alle prassi di sfruttamento e controllo dei *datasets*[738], i commentatori europei hanno tentato di capire se i regimi di tutela esistenti forniscano un qualche forma di protezione agli attori che controllano i *datasets*. Delineandosi, come si vedrà, una risposta negativa a tale interrogativo, si sono seguite due linee di pensiero opposte.

---

[735] Si rimanda al capitolo secondo.
[736] Come si è visto nel capitolo secondo, l'esistenza di barriere all'accesso ai *Big Data* comporta che il patrimonio digitale sia nelle mani di pochi soggetti (i c.d. "signori dei dati"). Di questa variabile si parlerà più approfonditamente *infra*.
[737] Comunicazione della Commissione *Building a European Data Economy*, 2017, 10.
[738] Si rimanda all'analisi condotta nel capitolo secondo e, in particolare, al § 1 di quel capitolo.

i. La Commissione[739] e alcuni autori[740] hanno proposto di costruire un nuovo diritto esclusivo, allocato in prima battuta ai soggetti che producono i dati[741];
ii. altra parte della dottrina, invece, ha respinto l'idea della designazione di un nuovo strumento di esclusiva, accogliendo la tesi per cui sia necessario far riferimento ad altre soluzioni e altri campi del diritto per regolamentare l'accesso ai dati[742].

Prima di passare all'analisi dei regimi di tutela e dei due orientamenti, cui sono dedicati i paragrafi seguenti, occorre ripercorrere brevemente gli interventi e le politiche della Commissione in materia di economia digitale e inquadrare il discorso dell'allocazione giuridica di nuovi beni immateriali, quali, appunto, i *datasets* di ingenti dimensioni.

Nel 2015, la Commissione ha individuato 16 iniziative per la creazione del Mercato unico digitale (MUD[743]), fra le quali talune sono destinate ad affrontare le questioni di appartenenza dei grandi *datasets* (*data ownership*) e di libera circolazione dei dati nell'Unione (*free flow of data*[744]). Secondo l'analisi della Commissione, nell'Unione europea la crescita dell'economia digitale è stata più contenuta rispetto allo sviluppo che hanno conosciuto gli Stati Uniti a causa della complessità e della frammentarietà del quadro giuridico e dei limiti all'accesso ai *datasets* di grandi dimensioni[745]. Due sono le ragioni principali di tale rallentamento.

i. In primo luogo, ancora poche imprese europee investono e operano nel settore dei dati[746], mentre numerosi agenti economici statunitensi

---

[739] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017. La Commissione inserisce la proposta di un nuovo diritto esclusivo in una pluralità di soluzioni legislative e non-legislative.
[740] Il principale sostenitore di tale soluzione è H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*
[741] Nel § 6.2 si cercherà di capire se un nuovo strumento di esclusiva trovi adeguate giustificazioni.
[742] In questo senso vedasi fra tutti J. DREXL, *op. cit.* Si rimanda al § 7.
[743] Comunicazione della Commissione *Strategia per il mercato unico digitale in Europa*, 2015; COMMISSIONE EUROPEA, *Roadmap for completing the Digital Single Market*, 2015 (http://ec.europa.eu/commission/sites/beta-political/files/roadmap_en.pdf, ultimo accesso 12 agosto 2017).
[744] Comunicazione della Commissione *Building a European Data Economy*, 2017; COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017.
[745] Comunicazione della Commissione *Verso una florida economia basata sui dati*, 2014, 3.
[746] Comunicazione della Commissione *Verso una florida economia basata sui dati*, 2014, 3.

del settore aprono le proprie filiali nel territorio europeo. Per esempio, Acxiom, Experian e Datalogix, società americane *leader* del settore del *data brokerage*, sono presenti in diversi Paesi membri dell'Unione europea[747].

ii. In secondo luogo, sussistendo scarsi incentivi al commercio dei *datasets* fra i diversi agenti economici, la produzione e l'analisi dei *Big Data* prodotti da un'impresa avviene principalmente all'interno della medesima realtà aziendale[748]. Secondo uno studio condotto da *Open Evidence* e *Deloitte* per la Commissione, il 78% delle imprese prese in considerazione conduce tali attività *in house* (17%), ovvero le esternalizza a un altro soggetto economico mediante strumenti contrattuali (61%). Viceversa, la divulgazione dei dati a terzi rimane una pratica poco frequente[749]: solo il 20% delle imprese condivide i *datasets* con altri attori, e, di questa percentuale, solo il 4% riguarda accordi fra operatori economici indipendenti. L'allocazione dei diritti di accesso e di riuso dei *datasets* avviene mediante strumenti contrattuali, ma le soluzioni normative esistenti del diritto dei contratti non appaiono sufficienti a garantire il buon funzionamento del mercato: «*where the negotiation power of the different market participants is unequal, market-based solutions alone might not be sufficient to ensure fair and innovation-friendly results, facilitate easy access for new market entrants and avoid lock-in situations*»[750]. Le imprese che cedono i *datasets* ad altri attori economici di solito inseriscono negli accordi clausole contrattuali che ostacolano o impediscono il riutilizzo dei dati per scopi diversi da quelli previsti nel contratto. Inoltre, alcuni *stakeholders* possono approfittare dei vuoti

---

[747] R. AARON ET AL., *Data Brokers In An Open Society*, Open Society Foundations Report, 2016, 14.

[748] Comunicazione della Commissione *Building a European Data Economy*, 2017, 7-8; COMMISSIONE EUROPEA*, Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, *op. cit.*, 14-16.

[749] COMMISSIONE EUROPEA*, Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, *op. cit.*, 15.

[750] Comunicazione della Commissione *Building a European Data Economy*, 2017, 8.

nel quadro normativo, imponendo condizioni contrattuali inique e, quindi, facendo crescere notevolmente i costi transattivi per gli attori economici più deboli[751].

Secondo la Commissione, occorre limitare gli approcci non coordinati dei singoli Stati membri e costituire un quadro normativo a livello europeo che persegua finalità univoche, in modo tale da migliorare l'accesso ai dati non personali, facilitare e incentivare gli scambi di tali dati (*data sharing*), tutelare gli investimenti e gli *assets*, evitare la diffusione di informazioni confidenziali, e, infine, minimizzare l'effetto *lock-in*[752] soprattutto per le piccole e medie imprese (PMI), le *startups* e le persone fisiche.

4. Big Data *e allocazione giuridica dei "nuovi" beni immateriali*

Come si è detto, nella società dell'informazione i *datasets* di grandi dimensioni sono considerati beni commerciabili. È necessario soffermarsi maggiormente sulla portata di tale affermazione, approfondendo, da un lato, la nozione di bene, e, dall'altro, le implicazioni in materia di diritti esclusivi.

Il concetto di "bene" ha significati variabili, e «*tale variabilità non deriva soltanto dagli usi, amplissimi, della parola bene nel linguaggio comune, ma anche dalle profonde diversità di concetti che tale termine evoca nel lessico delle diverse scienze sociali*»[753]. Ai fini del presente lavoro, occorre considerarne due nozioni: l'una economica e l'altra giuridica. In senso economico, un bene è un prodotto, una risorsa utile che consente il soddisfacimento di bisogni e desideri di un soggetto economico[754].

Il rafforzamento del legame fra il bene e il soggetto cui reca utilità si traduce, sul piano giuridico, nell'esigenza di tutelarne l'appartenenza. All'interno della tradizione giuridica di *civil law*, esistono diverse definizioni di "bene". Secondo il

---

[751] Comunicazione della Commissione *Building a European Data Economy*, 2017, 9.
[752] Sull'effetto *lock-in* nella fase di archiviazione dei *Big Data*, vedasi 3.4 del capitolo secondo.
[753] A. GAMBARO, *Dai beni immobili ai beni virtuali*, in *Enciclopedia Treccani* (http://www.treccani.it/enciclopedia/dai-beni-immobili-ai-beni-virtuali_%28XXI-Secolo%29/, ultimo accesso 30 agosto 2017).
[754] *«Bene»*, in *Enciclopedia Treccani Online* (http://www.treccani.it/enciclopedia/bene, ultimo accesso 14 agosto 2017).

diritto italiano, un bene è ogni cosa che può formare oggetto di diritti[755]; nell'ordinamento tedesco, col termine di "bene" (*Sache*) si indicano solo le cose materiali[756], che fanno parte dell'ampio *genus* dei *Rechtsobjekte*.

Secondo la distinzione tradizionale, i beni si dividono in beni materiali e beni immateriali.

i. I primi comprendono le risorse tangibili e corporee, che sono assoggettate in modo pacifico alle regole del diritto di proprietà "fisica" civilistica, lo strumento di tutela giuridica di carattere reale e assoluto per eccellenza.

ii. I secondi, invece, la cui teorizzazione più risalente si deve al giurista tedesco Josef Kohler, includono le creazioni intellettuali, quali le invenzioni, i segni distintivi e le opere dell'ingegno. La protezione giuridica di tali beni, che, a differenza degli altri, sono non rivali e non escludibili[757], consiste nell'istituzione di un monopolio nello sfruttamento del bene che risponde ugualmente alla retorica dominicale: si tratta della tecnica giuridica della c.d. privativa (o esclusiva), che, come il diritto di proprietà delle cose materiali, è un diritto reale e assoluto[758].

La tendenza alla creazione di nuove entità intangibili (fra cui rientrano i *datasets* di grandi dimensioni) che generano utilità e soddisfano interessi di natura patrimoniale dei soggetti che vi accedono e ne hanno il controllo non ha ancora trovato un'adeguata risposta in sede parlamentare e istituzionale. I "nuovi" beni

---

[755] Art. 810 cod. civ. italiano. Tale disposizione, pur formulata in modo ampio, in realtà rivela una notevole insufficienza definitoria, dal momento che non comprende direttamente le cose immateriali (in questo senso, U. MATTEI, *La proprietà*, in *Trattato di diritto privato*, diretto da Sacco R., 2ª ed., UTET Giuridica, 2015, 145). La c.d. "Commissione Rodotà", incaricata nel 2007 di revisionare il titolo I del libro III del cod. civ., ha proposto di modificare il testo dell'art. 810 cod. civ. al fine di includervi espressamente anche i beni immateriali (vedasi Ddl 2031 del Senato della Repubblica, XVI legislatura, 9).

[756] Art. 90 cod. civ. tedesco (BGB).

[757] Su tali nozioni vedasi *infra* § 5.5 e 6.

[758] Sui beni immateriali, si veda, più nello specifico, il classico P. GRECO, *I diritti sui beni immateriali,* Utet Giuridica, 1948.

immateriali (o beni immateriali atipici), infatti, sono (ancora) privi di una protezione giuridica espressamente riconosciuta dal legislatore, o «*comunque non* [sono] *riconducibili al catalogo tradizionale dei diritti di privativa*»[759].

Al pari di quello dei diritti reali sulle cose materiali, il sistema degli istituti di proprietà intellettuale è organizzato secondo il principio del *numerus clausus*, per il quale, da un lato, i diritti di esclusiva sono figure tipiche, cioè tassativamente predeterminate, e, dall'altro, «*gli interessi su entità diverse dalle cose e privi di un riconoscimento normativo (diretto o analogico) godono di una tutela limitata e caratterizzata dall'assenza di esclusività*»[760], non essendo applicabile l'interpretazione analogica o estensiva[761]. A ben vedere, tale impostazione appare irrinunziabile in un assetto politico liberaldemocratico, imperniato sul principio di separazione e bilanciamento dei poteri per il quale le scelte di natura allocativa spettano in via primaria e preferenziale al legislatore democraticamente eletto[762]. Tuttavia, a differenza del sistema che governa i diritti reali, il principio di tipicità ha una portata più limitata nell'ambito della proprietà intellettuale. In quest'ultimo campo, esso si riferisce esclusivamente ai diritti "primari" sulle entità intangibili, e non anche ai diritti "secondari" (o meglio, frazionari) di sfruttamento economico[763], che i consociati trasferiscono mediante lo strumento duttile della licenza a prescindere dall'esistenza di un istituto di privativa[764]. Il "numero chiuso" dovrebbe servire ad arginare il fenomeno della c.d. deriva protezionistica della proprietà intellettuale, benché le *lobbies* e i gruppi di pressione riescano facilmente ad avere la meglio nel tentativo di persuasione del legislatore[765].

---

[759] G. RESTA, *Nuovi beni immateriali e* numerus clausus *dei diritti esclusivi*, in G. RESTA (CUR.), *Diritti esclusivi e nuovi beni immateriali*, Utet Giuridica, 2011, 4.
[760] V. ZENO-ZENCOVICH, *Cosa*, in *Digesto civile*, IV, Utet, 1989, 438.
[761] In questo senso, N. ABRIANI ET AL., *Diritto industriale*, in *Trattato di Diritto Commerciale*, diretto da G. COTTINO, Cedam, 2001, 460.
[762] G. RESTA, *op. cit.*, 25.
[763] L.C. UBERTAZZI, *Introduzione al diritto europeo della proprietà intellettuale*, in *Contratto e impresa/Europa*, 2003, 1101.
[764] G. RESTA, *op. cit.*, 24-25.
[765] P. SPADA, *Conclusioni al Convegno su "IP e Costituzioni" organizzato presso l'Università di Pavia il 23 e 24 settembre 2005*, in *AIDA*, 2005, 217 ss. e 221.

La rigorosità formale del *numerus clausus* trova due correttivi nella prassi. In primo luogo, la giurisprudenza opera sulla base di un sistema delle fonti del diritto particolarmente frammentato e complesso, che non si esaurisce nel solo ambito nazionale. Oggi, le norme di diritto internazionale e di diritto sovranazionale (quali quelle di diritto europeo), le regole di *soft law* e la c.d. *lex mercatoria* tendono ad accostarsi al novero delle norme di diritto interno. Ne consegue che le probabilità di riconoscimento di diritti esclusivi su nuove entità immateriali aumentano, coinvolgendo dapprima l'operato della giurisprudenza, e, più raramente, l'azione del legislatore che recepisce il percorso ermeneutico consolidatosi. In secondo luogo, la legittimazione in sede legislativa avviene nella maggior parte dei casi in maniera "mascherata", *id est* «*mediante l'estensione in via interpretativa dell'ambito di operatività di istituti o categorie tradizionali* […] *o tramite l'affievolimento dei requisiti previsti per l'accesso alle privative classiche*»[766]: si pensi, per esempio, all'estensione della tutela autorale alle banche dati rispondenti a certe caratteristiche[767].

Le considerazioni sollevate in questo paragrafo sono necessarie a inquadrare le questioni di appartenenza dell'oggetto di trattazione, cioè i *datasets* costituiti da dati non personali. Come detto in precedenza, ora si cercherà di capire quale sia il grado di protezione accordata dai regimi di tutela esistenti agli agenti economici che controllano i *datasets*.

5. L'inadeguatezza dei regimi di tutela giuridica esistenti nell'Unione europea

Taluni regimi esistenti a livello europeo potrebbero accordare tutela sui *datasets* di grandi dimensioni. Essi sono:

i. il diritto d'autore, che potrebbe essere rilevante per la protezione dei singoli dati di *datasets*;

---

[766] G. RESTA, *op. cit.*, 31.
[767] Vedasi *infra*, § 5.2.

ii. la tutela giuridica delle banche dati prevista dalla Direttiva 96/9/CE[768];

iii. la tutela giuridica del segreto commerciale, stabilita dalla Direttiva (UE) 2016/943[769];

iv. la tutela brevettuale;

v. quello della proprietà privata fisico-civilistica.

Come si vedrà, tuttavia, nessuno di tali regimi conferisce al soggetto che controlla i *datasets* una protezione adeguata agli scenari di sfruttamento dei *Big Data* e del plesso tecnologico dell'Internet delle Cose.

5.1. Il diritto d'autore

La tutela autorale potrebbe riguardare i singoli dati costituenti un *dataset* se si opera un'estensione oggettiva della nozione di opera dell'ingegno. Nell'ordinamento interno degli Stati membri, la nozione di opera protetta, pur non univoca, è «*sufficientemente ampia ed elastica da potere tener conto dell'evoluzione della tecnica e delle forme espressive*»[770]. Il diritto d'autore conferirebbe una tutela sul piano semantico ai singoli dati[771].

Tuttavia, il requisito di originalità dell'opera limita l'applicazione della protezione autorale alle sole informazioni create da una mente umana. I dati non strutturati (*raw data*) raccolti mediante processi automatizzati e quelli generati mediante i sensori degli oggetti dell'Internet delle Cose non sono compresi nella tutela di diritto d'autore[772]. Per questa ragione, la protezione autorale non si può conciliare con gli scenari di sfruttamento economico dei *Big Data*.

---

[768] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, G.U. n. L. 077 del 27/03/1996.
[769] Direttiva (UE) 2016/943 del Parlamento Europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, G.U. n. L. 157 del 15/6/2016.
[770] P. AUTERI ET AL., *op. cit.*, 574.
[771] Vedasi § 1.
[772] A. WIEBE, *op. cit.*, 64; T.J. FARKAS, *Data Created by the Internet of Things: The New Gold without Ownership*, in 23 *Revista La Propiedad Inmaterial*, 2017, 8-9.

5.2. La tutela giuridica delle banche dati: la Direttiva 96/9/CE

La Direttiva 96/9/CE ha introdotto un regime armonizzato di protezione giuridica delle banche dati[773] che potrebbe accordare un grado di tutela ai soggetti controllori dei *datasets*. Occorre dapprima soffermarsi sulla disciplina prevista nel dettato normativo e, in seguito, configurarne l'applicabilità agli scenari dei *Big Data*.

Secondo la Direttiva 96/9/CE, una banca dati (*database*) è «*una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo*»[774]. Questa formulazione appare notevolmente ampia[775], accogliendo non solo le raccolte di elementi digitali, ma anche le banche dati non elettroniche[776]. La Corte di Giustizia dell'Unione europea (CGUE) ha confermato questa impostazione, asserendo che la definizione di banca di dati ai sensi dell'art. 1, n. 2, della Direttiva 96/9/CE concerne qualsiasi raccolta di opere, dati o altri elementi, separabili gli uni dagli altri «*senza che venga per questo intaccato il valore del loro contenuto, e che comporti un metodo o un sistema, di qualunque natura esso sia, che consenta di ritrovare ciascuno dei suoi elementi costitutivi*»[777]. I giudici degli Stati membri hanno varia-

---

[773] Vedasi, *inter alios*, M. SCHNEIDER, *The European Union Database Directive*, in 13(1) *Berkeley Technology Law Review*, 1998, 551 ss.; X. WU, *E.C. Database Directive*, in 17(1) *Berkeley Technology Law Journal*, 2002, 571 ss.; M. DAVISON, *The Legal Protection of Databases*, Cambridge University Press, 2003; E. DERCLAYE, *The Legal Protection of Databases: A Comparative Analysis*, Edward Elgar, 2008.

[774] Art. 1 par. II Direttiva 96/9/CE.

[775] Cons. 17 Direttiva 96/9/CE. Vedasi I. STAMATOUDI, *The EU Databases Directive: Reconceptualising Copyright and Tracing the Future of the Sui Generis Right*, in 50 *Revue hellénique de droit international*, 1997, 441-42. Addirittura, al momento della proposta di quella che poi sarebbe divenuta la Direttiva 96/9/CE qualcuno ha affermato che pure una pagina *web* potesse essere considerata un *database* «*as a collection of independent works - literary works (such as articles), graphic works (photos, diagrams, illustrations), video, sound and, in some cases, computer software*» (L. KAYE, *The proposed EU Directive for the legal protection of databases: a cornerstone of the information society?*, in 12 *European Intellectual Property Review*, 1996, 584).

[776] Cons. 14 Direttiva 96/9/CE.

[777] CGUE 9 novembre 2004 (Grande Sezione), causa C-444/02, Fixtures Marketing Ltd c. Organismos prognostikon agonon podosfairou AE (OPAP), par. 32. La nozione di banca dati ai sensi della Direttiva 96/9/CE è stata ampliata notevolmente in via ermeneutica dalla CGUE. Per esempio, «*i dati geografici che terzi estraggano da una carta topografica per la costituzione e la commercializzazione di un'altra carta conservano, successivamente alla loro estrazione, un valore informativo sufficiente per essere qualificati come «elementi indipendenti» di una «banca di dati» ai sensi di detta disposizione*» (CGUE 29 ottobre 2015 (Seconda Sezione), causa C-490/14, Freistaat Bayern c. Verlag Esterbauer GmbH, parte dispositiva).

mente interpretato l'oggetto della tutela giuridica prevista dalla Direttiva. Per esempio, in Italia, il Tribunale di Torino, seguendo la linea adottata dalla Corte Suprema degli Stati Uniti nel famoso caso *Feist*[778], ha negato la protezione accordata dal diritto d'autore agli elenchi telefonici[779].

Il dettato normativo prevede un duplice binario di tutela giuridica: l'una di diritto d'autore (cap. II della Direttiva 96/9/CE), l'altra di diritto *sui generis* (cap. III della Direttiva 96/9/CE).

Il primo riguarda le basi di dati che «*per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore*»[780]. Questo è l'unico criterio a stabilire l'assoggettabilità di una banca dati alla tutela autorale. Tali *databases* sono oggetto dell'esclusiva intellettuale «*in quanto tali*», essendo una *species* particolare di opera collettiva[781]. L'aggiunta dell'espressione "in quanto tali" è spiegata meglio nel par. II dello stesso art. 3 della Direttiva 96/9/CE, per il quale tale tutela concerne la struttura dei *databases*, ma «*non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto*». L'indipendenza della tutela giuridica della struttura dagli elementi che costituiscono la banca dati si riflette sulla valutazione del requisito di originalità della banca dati. Secondo la CGUE, la scelta e la disposizione del materiale devono costituire «*un'espressione originale della libertà creativa del suo autore*»[782], e tale valutazione non dipende dall'impegno intellettuale e dal *know-how* destinati alla creazione di detti dati, ma unicamente dagli sforzi creativi di assemblaggio del *database*. L'autore della base di dati è «*la persona fisica o il gruppo di persone fisiche che l'ha creata o, qualora la legislazione dello Stato membro interessato lo con-*

---

[778] *Feist Publications, Inc., v. Rural Telephone Service Co.*, 499 U.S. 340 (1991).
[779] «[…] [*L'*]*elenco telefonico ufficiale, per le modalità di creazione, per la sua stessa conformazione e per la sua funzione esclusivamente informativa, non può considerarsi opera protetta*» (Trib. Torino (ord.) 17 luglio 1997).
[780] Art. 3 par. I Direttiva 96/9/CE.
[781] Si confronti, nel diritto italiano, l'art. 3 della Legge 22 aprile 1941 n. 633 (Legge sul diritto d'autore e su altri diritti connessi al suo esercizio). In questo senso, P. AUTERI ET AL., *Diritto industriale: proprietà intellettuale e concorrenza*, Giappichelli, 2016, 591.
[782] CGUE 1° marzo 2012 (Terza Sezione), causa C-604/10, Football Dataco Ltd e altri c. Yahoo! UK Ltd e altri, parte dispositiva.

senta, la persona giuridica individuata da tale legislazione come titolare del diritto»[783]; inoltre, se il *database* è frutto della collaborazione fra più soggetti, i diritti esclusivi appartengono congiuntamente a ciascuno di questi[784]. Gli art. 5 e 6 della Direttiva 96/9/CE prevedono nello specifico, rispettivamente, il contenuto del diritto di cui all'art. 3 e le eccezioni e limitazioni all'esclusiva.

La seconda tipologia di tutela prevede che i costitutori delle banche dati per le quali «*il conseguimento, la verifica e la presentazione* […] [del contenuto] *attestino un investimento rilevante sotto il profilo qualitativo o quantitativo*» abbiano il diritto di «*vietare operazioni di estrazione e/o reimpiego della totalità o di una parte sostanziale del contenuto della stessa, valutata in termini qualitativi o quantitativi*»[785]. Questa protezione *sui generis*, a differenza del diritto d'autore, ha una durata più limitata, estinguendosi «*trascorsi quindici anni dal 1° gennaio dell'anno successivo alla data del completamento*»[786] della banca dati. L'investimento dev'essere rilevante, cioè deve consistere nell'impegno di mezzi finanziari, tempo, lavoro ed energie del costitutore[787]. La CGUE, nei casi *Fixtures Marketing* e *British Horseracing Board*[788], ha specificato ulteriormente la nozione di investimento introducendo tre criteri di valutazione. Secondo la Corte, l'investimento del costitutore necessario per l'attivazione della tutela giuridica *sui generis* concerne[789]:

i. i mezzi «*destinati alla ricerca di elementi esistenti e alla loro raccolta nella detta banca di dati*»[790] (fase di conseguimento-acquisizione degli elementi);
ii. quelli volti «*al controllo dell'esattezza degli elementi ricercati*»[791] (fase di verifica-selezione del materiale);

---

[783] Art. 4 par. I Direttiva 96/9/CE.
[784] Art. 4 par. III Direttiva 96/9/CE.
[785] Art. 7 par. I Direttiva 96/9/CE. Il par. II spiega le nozioni di "estrazione" e "reimpiego".
[786] Art. 10 par. I Direttiva 96/9/CE.
[787] Cons. 40 Direttiva 96/9/CE.
[788] CGUE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd.
[789] E. DERCLAYE, *op. cit.*, 92 ss.
[790] CGUE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd., parte dispositiva.
[791] CGUE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd., parte dispositiva.

iii. quelli che conferiscono al *database* una disposizione sistematica o metodica del materiale contenuto e un'organizzazione dell'accessibilità individuale degli elementi (fase di presentazione-organizzazione della base di dati)[792].

Il contenuto del diritto *sui generis* è più limitato rispetto a quello previsto in capo al titolare del diritto d'autore. Come già accennato, ai sensi del par. I dell'art. 7 della Direttiva 96/9/CE il costitutore della banca dati ha il diritto di impedire operazioni di estrazione e di reimpiego di tutto o parte del contenuto della banca dati, valutata in termini qualitativi o quantitativi[793]. Il par. II dello stesso articolo specifica che «*a) per «estrazione» si intende il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma; b) per «reimpiego» si intende qualsiasi forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione in linea o in altre forme*»[794]. Inoltre, al diritto di distribuzione compreso nel concetto di reimpiego si applica il principio dell'esaurimento. Sia l'estrazione sia il reimpiego rilevanti ai sensi del par. II devono riguardare "parti sostanziali" della banca dati. Analogamente ai *databases* protetti dal diritto d'autore, la Direttiva 96/9/CE non prevede alcuna protezione per i singoli dati che compongono il *database* oggetto di tutela *sui generis*[795], scelta giustificata dal fatto che «*the legislator wanted to keep the (semantic) information in the public domain*»[796]. Specularmente alle disposizioni del par. I dell'art. 7 della Direttiva 96/9/CE, l'art. 8 prevede che l'utente legittimo[797] possa estrarre e reimpiegare le parti non sostanziali della banca dati, valutate in termini qualitativi e quantitativi. Nondimeno, la

---

[792] CGUE 9 novembre 2004 (Grande Sezione), causa C-444/02, Fixtures Marketing Ltd c. Organismos prognostikon agonon podosfairou AE (OPAP), par. 43.
[793] Una parte sostanziale della banca dati in senso quantitativo è un'ingente porzione di materiale del *database* estratta o reimpiegata; una parte sostanziale in senso qualitativo è una porzione di materiale anche minima, ma per la quale è stato richiesto un investimento rilevante.
[794] Art. 7 par. II Direttiva 96/9/CE.
[795] A. DE FRANCESCHI – M. LEHMANN, *op. cit.*, 64 ; A. WIEBE, *op. cit.*, 64; H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 73.
[796] H. ZECH, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, in 11 *Journal of Intellectual Property Law & Practice*, 2016, 467.
[797] Tale espressione non trova una definizione univoca nel testo normativo e nella giurisprudenza europea.

lesione del diritto *sui generis* avviene anche nel caso in cui l'estrazione o il reimpiego riguardino parti non sostanziali del contenuto, purché siano ripetuti e sistematici e presuppongano operazioni contrarie alla normale gestione della banca dati o arrechino un pregiudizio ingiustificato ai legittimi interessi del costitutore della banca di dati[798].

La previsione di un diritto *sui generis* sulle banche dati a livello europeo ha sollevato aspre critiche, provenienti soprattutto dal versante americano. In particolare, taluni commentatori hanno ravvisato in tale tutela giuridica un potenziale anticoncorrenziale, dal momento che il costitutore-investitore della banca dati, pur per un periodo di tempo limitato, «*paradoxically obtains the strongest scope of protection available from any intellectual property regime except, perhaps, for the classical patent paradigm itself*»[799].

Le banche dati il cui creatore è l'unico soggetto ad avere accesso (le cc.dd. *sole-source databases* o *single-source databases*) pongono problematiche di distorsione della concorrenza ancora più serie. La tutela giuridica *sui generis* di tali *databases* si può tradurre in un forte monopolio. Per evitare conseguenze pregiudizievoli, i giudici europei hanno adottato un'interpretazione restrittiva della nozione di "investimento sostanziale". Il costitutore della banca dati non gode della tutela giuridica *sui generis* se gli investimenti per la costituzione di tali basi di dati sono relativi solo alla «*creazione dei dati costitutivi*»[800] della *databank* (cioè alla produzione di tali risorse), e non anche al conseguimento e all'acquisizione dei dati (da altre fonti[801]). Come affermato nella sentenza *Horseracing*, «*il fine della tutela, conferita dal diritto sui generis, introdotta dalla direttiva è infatti di incentivare la creazione di sistemi di memorizzazione e di gestione di informazioni esistenti, e non la creazione di elementi che possano essere successivamente raccolti in una banca*

---

[798] Art. 7 par. V Direttiva 96/9/CE.
[799] J.H. REICHMAN – P. SAMUELSON, *Intellectual Property Rights in Data?*, in 50 *Vanderbilt Law Review*, 1997, 94.
[800] CGUE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd., par. 38.
[801] M. BORGHI – S. KARAPAPA, *Contractual restrictions on lawful use of information: sole-source databases protected by the back door?*, in 37(8) *European Intellectual Property Review*, 2015, 505 ss. Si confronti quanto detto *supra* sulla valutazione del requisito di originalità delle banche dati. Per la distinzione fra produzione e acquisizione dei dati, vedasi § 2.1 e 2.2 del capitolo secondo.

di dati»[802]. Ne consegue che le banche dati *sole-source* non rientrino nel campo di applicazione della Direttiva 96/9/CE, dal momento che gli investimenti del costitutore si limitino alla produzione degli elementi della banca dati. Tale impostazione ermeneutica, in linea con l'art. 102 TFUE, impedisce ai titolari del diritto di avere un vantaggio competitivo insormontabile dagli altri agenti economici, rappresentato da un «*near-absolute downstream information monopoly in derivative information products or services*»[803]. Più recentemente, dopo alcuni anni di stasi, sono riemerse nuove questioni relative alle banche dati *single-source*. La CGUE, nel caso *Ryanair*[804], pur non modificando l'orientamento adottato in precedenza, ha specificato che le eccezioni e le limitazioni al diritto d'autore e al diritto *sui generis* si applicano alle sole banche dati protette da tali istituti giuridici. In particolare, se la banca dati non gode né della tutela giuridica di diritto d'autore, né di quella di diritto *sui generis*, l'autore-costitutore della stessa non è soggetto ai limiti previsti dal par. I dell'art. 6, dall'art. 8 e dall'art. 15 della Direttiva 96/9/CE[805]. Perciò, tale soggetto gode di piena libertà contrattuale e può imporre a terzi notevoli restrizioni all'accesso al materiale del *database* nei limiti stabiliti dal diritto interno degli Stati membri. Tuttavia, com'è noto, «*contract law has not been harmonised throughout Europe and this can create discrepancies as to the level of protection afforded to such databases among the various Member States*»[806]. Tale conclusione risulta particolarmente pericolosa per le banche dati *single source*, i cui costitutori, non godendo di alcuna tutela giuridica ai sensi della Direttiva 96/9/CE, potrebbero comunque monopolizzare le informazioni contenute[807].

Gli scenari di raccolta e archiviazione di ingenti quantità di dati pongono nuove sfide alla Direttiva 96/9/CE, che, a più di vent'anni dall'entrata in vigore,

---

[802] CGUE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd., par. 31.
[803] P. HUGENHOLTZ, *Abuse of Database Right. Sole-source information banks under the EU Database Directive*, in F. LÉVÊQUE – H. SHELANSKI (CUR.), *Antitrust, Patents and Copyright: EU and US Perspectives*, Cheltenham, 2005, 203.
[804] CGUE 15 gennaio 2015 (Seconda Sezione), causa C-30/14, Ryanair Ltd c. PR Aviation BV.
[805] CGUE 15 gennaio 2015 (Seconda Sezione), causa C-30/14, Ryanair Ltd c. PR Aviation BV, parte dispositiva.
[806] M. BORGHI – S. KARAPAPA, *op. cit.*
[807] M. MYŠKA – J. HARAŠTA, *Less is more? Protecting Databases in the EU After Ryanair*, in 10(2) *Masaryk University Journal of Law and Technology*, 2016, 187.

mostra notevoli segni di invecchiamento. Infatti, dal 31 maggio al 30 agosto 2017, la Direttiva 96/9/CE è stata oggetto di una consultazione pubblica condotta dalla Commissione per raccogliere le istanze dei principali *stakeholders* in merito al testo normativo e capire se la stessa «*still fulfils its policy goals and is fit-for-purpose in a digital, data-driven economy*»[808].

I regimi di tutela delle banche dati, l'uno autorale, l'altro *sui generis*, non forniscono adeguata protezione dei soggetti che controllano i *datasets* di grandi dimensioni.

Anzitutto, al momento della stesura del testo, il legislatore europeo ha considerato come paradigma di *database* le *directories* e gli elenchi il cui assemblaggio richiede l'intervento di una mente umana. Alla fine degli anni Novanta del secolo scorso, la rivoluzione digitale si era appena affacciata nella realtà delle cose. Oggi i soggetti economici hanno patrimoni incalcolabili di informazioni e utilizzano algoritmi e tecniche automatizzate di raccolta, selezione e analisi dei dati basati sull'autoapprendimento (*machine learning*). La nozione stessa di *database*, che appare troppo statica per rispondere alle esigenze di acquisizione dei dati in tempo reale, pare essere sotto assedio. L'ampia definizione del par. II dell'art. 1 della Direttiva 96/9/CE comunque comprende i *datasets* composti da elementi incalcolabili alla mente umana[809]. Tuttavia, l'automatizzazione dei processi di acquisizione e immagazzinamento implica che il costitutore di tali banche dati non possa accedere alla tutela giuridica di diritto d'autore, prevista dagli artt. 3 ss. della Direttiva 96/9/CE, giacché la scelta e la disposizione degli elementi del *database* non possono essere considerati una creazione dell'ingegno del costitutore[810]. In definitiva, l'unica tutela cui si può ricorrere in tali casi può essere quella del diritto *sui generis* ai sensi degli artt. 7 ss. della Direttiva 96/9/CE.

In secondo luogo, secondo l'interpretazione restrittiva della CGUE, il diritto *sui generis* non spetta nemmeno ai costitutori che non destinano un investimento rilevante direttamente alla costituzione della base di dati, ma creano banche dati

---

[808] *Public consultation on the database directive: application and impact*, in *European Commission* (http://ec.europa.eu/info/consultations/public-consultation-database-directive-application-and-impact-0_en, ultimo accesso 26 agosto 2017).
[809] H. ZECH, *Data as a Tradeable Commodity*, *op. cit.*, 70; J. DREXL, *op. cit.*, 20-21.
[810] H. ZECH, *Data as a Tradeable Commodity*, *op. loc. cit.* Si confronti il § 5.1.

come sottoprodotti di altre attività (c.d. *spin-off doctrine*[811]). Com'è noto, le tecnologie di acquisizione dei dati non richiedono costi elevati per le imprese di maggiori dimensioni, che «*raccolgono i dati come un sottoprodotto di altre attività produttive*»[812]. Dal momento che i processi di acquisizione dei dati sono operazioni economiche che non richiedono ingenti investimenti, pochi soggetti possono raggiungere la soglia della rilevanza dell'investimento ai sensi del par. I dell'art. 7 della Direttiva 96/9/CE.

In terzo luogo, come si è visto nei precedenti capitoli, le imprese operanti nei sottomercati dei *Big Data* non raccolgono i dati da altre fonti, ma li producono direttamente – si pensi, per esempio, alla creazione dei dati mediante i sensori degli oggetti interconnessi dell'Internet delle Cose[813]. Finanche questa circostanza osta all'accesso alla tutela di diritto *sui generis*, giacché l'impresa impegna investimenti nella produzione dei singoli dati, e non nella raccolta da altre fonti. Lo stesso ragionamento valga per i *databases* che contengono le informazioni di valore ottenute dall'analisi dei dati non strutturati ricavati da varie fonti. Tali basi di dati sono inquadrabili nella tipologia delle *single-source*, i cui costitutori, pur avendo ampie facoltà in materia contrattuale e potendo impedire l'accesso ai dati ai terzi alla luce del già citato caso *Ryanair*, non godono della tutela del diritto *sui generis*.

Infine, come già accennato *supra*, il diritto *sui generis* non si estende ai singoli dati. Le nozioni di estrazione e reimpiego, che coinvolgono solo porzioni sostanziali della banca dati, appaiono totalmente superate dalla prassi: «*in particular, Big Data analyses whereby the 'code comes to the data' in order to generate new information will not lead to any 'extraction' since there will be no "permanent or temporary transfer of all or a substantial part of the contents of a database to another medium"*»[814].

---

[811] Questa interpretazione restrittiva, adottata dalla giurisprudenza olandese all'inizio degli anni Duemila, ha influenzato la CGUE nelle decisioni successive sopracitate. Vedasi P. HUGENHOLTZ, *op. cit.*, 203 ss.
[812] D.L. RUBINFELD – M.S. GAL, *Access Barriers to Big Data*, in 59 *Arizona Law Review*, 2017, 377; D. S. TUCKER – H. B. WELLFORD, *Big Mistakes Regarding Big Data*, in *The Antitrust Source*, 2014, 3. Vedasi, più nello specifico, § 2.2.1 del capitolo secondo.
[813] J. DREXL, *op. cit.*, 21. Vedasi § 2.1 e 2.2 del capitolo secondo.
[814] J. DREXL, *op. cit.*, 21-22 (il virgolettato è la versione inglese del par. II art. 7 Direttiva 96/9/CE).

Per queste ragioni, i soggetti che controllano i *dataset* non godono della tutela accordata dalla Direttiva 96/9/CE.

5.3. La tutela brevettuale

Com'è noto, la tutela brevettuale fa riferimento a tre categorie di invenzioni industriali: le invenzioni di procedimento, di prodotto e d'uso. In taluni casi, la materia *de qua* potrebbe ricondursi alla prima categoria in due circostanze; nondimeno, come si vedrà, difficilmente la protezione brevettuale può offrire una tutela rilevante per i soggetti controllori dei dati. Tuttavia, è probabile che le tecnologie dell'Internet delle Cose diventino oggetto di protezione esclusiva in quanto riconducibili alle cc.dd. *computer-implemented inventions* (CII)[815], che sono invenzioni «*which involve the use of a computer, computer network or other programmable apparatus, where one or more features are realised wholly or partly by means of a computer program*»[816]. Occorre soffermarsi su ciascuna di queste tre circostanze.

In primo luogo, se il brevetto riguarda un procedimento di produzione industriale, il suo titolare ha il diritto di vietare ai terzi che non hanno il suo consenso non solo di applicare il processo, ma anche di utilizzare e immettere sul mercato i prodotti ottenuti da tale processo[817]. Si potrebbero considerare i *datasets* ottenuti da processi industriali brevettati alla stregua di un prodotto che rientri nella privativa del titolare. Un siffatto scenario è assai verosimile nei contesti economici dell'Industria 4.0 e nel settore medico[818], in cui i dati sono generati come sottoprodotti di altre attività produttive. Tuttavia, le elaborazioni giurisprudenziali sul punto sono assai limitate e di senso opposto. Nel 2010, la Corte distrettuale di Düsseldorf ha asserito che l'informazione semantica (nel caso in questione, i risultati di un test genetico per cani) non può essere equiparata a un prodotto di un brevetto[819].

---

[815] G. NOTO LA DIEGA, *Software Patents and the Internet of Things in Europe, the United States and India*, in 39(3) *European Intellectual Property Review*, 2017, 173 ss.
[816] *Patents for Software? European Law and Practice*, in *European Patent Office* (www.epo.org/news-issues/issues/software.html, ultimo accesso 27 settembre 2017).
[817] Art. 64 par. I e II Convenzione sulla Concessione dei Brevetti Europei (*European Patent Convention*, EPC); art. 25 lett. c Accordo su un tribunale unificato dei brevetti, G.U. n. C. 175 del 20/6/2013 (non ancora entrato in vigore).
[818] J. DREXL, *op. cit.*, 24-25.
[819] Landgericht Düsseldorf, 16 febbraio 2010, caso 4b 0 247/09 *Hunde-Gentest*.

In secondo luogo, più complessa appare la configurazione delle attività di analisi e organizzazione condotte dalle imprese come invenzioni di procedimento[820]. Le maglie di taluni requisiti di proteggibilità delle invenzioni, *id est* la novità (art. 54 EPC) e l'attività inventiva (art. 56 EPC), appaiono troppo strette per conferire tutela giuridica a tali pratiche[821].

In terzo luogo, occorre considerare il caso delle CII. Tali invenzioni si distinguono dal programma per elaboratore in sé, che, com'è noto, è oggetto di tutela autorale[822]. Le CII quali le tecnologie dell'Internet delle Cose saranno oggetto di probabili operazioni di proprietarizzazione in tempi futuri. Lo sviluppo dell'insieme di tecnologie dell'Internet delle Cose determinerà la crescita di domande di brevetto riguardanti gli oggetti *smart*, col rischio di un «*surreptitious generalised grant of patents for computer programs as such*»[823] e dell'affossamento della questione dell'interoperabilità dei sistemi[824].

Infine, la teoria economica si oppone alla preferibilità della tutela brevettuale rispetto agli altri sistemi di protezione giuridica negli scenari di sfruttamento dei *Big Data*, ammesso che questi ultimi conferiscano tutela ai soggetti controllori dei dati. Com'è noto, accedere alla tutela brevettuale comporta costi notevoli. David Friedman, William Landes e Richard Posner, confrontando la tutela del segreto commerciale coi brevetti, hanno notato che è preferibile ricorrere alla prima se la protezione brevettuale è troppo costosa rispetto al valore dell'informazione o se quest'ultima conferisce una rendita sostanzialmente più bassa del valore della creazione intellettuale a contenuto tecnologico[825]. Quest'ultima variante può ben configurarsi quando «*an invention could easily be kept secret for a period of time longer than it would take other inventors to come up with the idea on their own*»[826]. Perciò, la tutela accordata dal segreto commerciale è consigliabile qualora il costo

---

[820] Si rimanda all'esame della catena del valore dei *Big Data* del capitolo secondo.
[821] F. SARTORE, *Big Data: Privacy and Intellectual Property in a Comparative Perspective*, Trento Law and Technology Research Group Student Paper n. 26, 2016, 91.
[822] Direttiva 2009/24/CE.
[823] G. NOTO LA DIEGA, *op. cit.*, 173.
[824] G. NOTO LA DIEGA, *op. cit.*, 183. Sulle problematiche riguardanti gli *standard* tecnici e l'interoperabilità, si veda il § 7.
[825] D. FRIEDMAN ET AL., *Some Economics of Trade Secret Law*, in 5(1) *The Journal of Economic Perspectives*, 1991, 61 ss.
[826] M. MATTIOLI, *Disclosing Big Data*, in 99 *Minnesota Law Review*, 2014, 555.

necessario a ottenere un brevetto appaia maggiore di ogni valore conseguibile dal procedimento[827].

Come si è visto, tranne che nel caso delle tecnologie dell'Internet delle Cose, la tutela brevettuale non si estende agli scenari di sfruttamento economico dei *Big Data*. Occorre ora passare all'analisi della protezione giuridica del segreto commerciale nel versante europeo.

5.4. Il segreto commerciale: la Direttiva (UE) 2016/943

Taluni autori hanno opportunamente fatto notare che la protezione giuridica del segreto commerciale (*trade secret*) è complementare e residuale a quella fornita dagli altri diritti di proprietà intellettuale. Da una parte, la tutela del segreto coinvolge non tanto un'opera o un'invenzione in quanto tali, bensì il processo creativo mediante il quale si perviene al prodotto finale, a patto che la fase di creazione sia tenuta segreta; dall'altra, il segreto commerciale si estende ai casi in cui non si può invocare la protezione di alcun'altra privativa intellettuale[828]. Se la tutela dei *trade secrets* fosse troppo forte, essa costituirebbe in capo al titolare del diritto un monopolio di fatto «*potenzialmente perpetuo*»[829], che distorcerebbe la concorrenza del mercato e impedirebbe il raggiungimento da parte degli agenti economici dell'allocazione ottimale delle risorse e, quindi, dell'efficienza paretiana[830]. Al fine di ridurre tali rischi, nella maggior parte degli ordinamenti giuridici il detentore del segreto commerciale non è titolare di un vero e proprio diritto esclusivo, ma è tutelato mediante regole di responsabilità (*liability rules*[831]) riguardanti l'acquisizione, l'utilizzo e la divulgazione illeciti delle informazioni segrete[832]. La tutela giuridica del

---

[827] M. MATTIOLI, *op. cit.*, 556.
[828] D. ARCIDIACONO, *The Trade Secrets Directive in the International Legal Framework*, in 1(3) *European Papers*, 2016, 1074.
[829] P. AUTERI ET AL., *op. cit.*, 23.
[830] Per un'analisi esaustiva e dettagliata, si veda G. SURBLYTĖ, *The Refusal to Disclose Trade Secrets as an Abuse of Market Dominance – Microsoft and Beyond*, Stämpfli, 2011.
[831] G. CALABRESI – A.D. MELAMED, *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, in 85(6) *Harvard Law Review*, 1972, 1089 ss.
[832] Tuttavia, in alcuni ordinamenti, come quello italiano, il segreto commerciale è stato oggetto di un processo di "proprietarizzazione" (P. AUTERI ET AL., *op. cit.*, 212; vedasi più nel dettaglio *infra*).

segreto commerciale dà origine a un potere di fatto sulle informazioni segrete, equiparabile al concetto civilistico di possesso[833]. Per queste ragioni, il segreto commerciale si è guadagnato l'appellativo di "Cenerentola" dei diritti di proprietà intellettuale[834].

La protezione giuridica del segreto commerciale ha fatto la sua comparsa nel diritto secondario europeo nel 2016, con l'entrata in vigore della Direttiva (UE) 2016/943, che risolve l'annosa questione di un quadro giuridico estremamente frammentato e non armonizzato a livello europeo in materia[835]. In alcuni Paesi dell'Unione (Austria, Bulgaria, Repubblica Ceca, Germania, Danimarca, Estonia, Grecia, Spagna, Finlandia, Ungheria, Lettonia, Lituania, Polonia, Romania, Slovenia e Slovacchia) la disciplina del segreto commerciale rientra espressamente nelle regole riguardanti la concorrenza sleale, secondo il paradigma incardinato nell'art. 39 dell'Accordo TRIPs[836]; a tali norme, poi, si accostano quelle generali in materia di responsabilità extracontrattuale. In un gruppo più ristretto di Stati membri, non vi è una disciplina specifica concernente il segreto commerciale: la tutela si fonda sui principi della responsabilità aquiliana (Belgio, Francia, Lussemburgo, Paesi Bassi) o sull'elaborazione giurisprudenziale in materia di *breach of confidence* (Irlanda e Regno Unito). In Svezia, Italia e Portogallo, il legislatore ha scelto di conferire una protezione giuridica più forte al segreto commerciale, prevedendo norme specifiche nei codici di proprietà intellettuale nazionali o in atti normativi *ad hoc*[837].

---

[833] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 63-64. Sul possesso dei *datasets*, vedasi *infra*, § 5.5.

[834] S.K. SANDEEN, *The Cinderella of Intellectual Property Law: Trade Secrets*, in P.K. YU (CUR.), *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age*, Praeger, 2007, 399 ss.

[835] Cons. 6-8 Direttiva (UE) 2016/943. COMMISSIONE EUROPEA, *Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 2013, 181.

[836] Accordo sugli aspetti commerciali dei diritti di proprietà intellettuale (*The Agreement on Trade Related Aspects of Intellectual Property Rights*, comunente detto Accordo TRIPs). L'art. 39 Accordo TRIPs preferisce il nominativo di "informazioni non divulgate" (*undisclosed information*) a quello di segreto commerciale (*trade secret*).

[837] In Italia, fino al 2005, la fattispecie dell'abuso del segreto commerciale era una *species* della disciplina in materia di concorrenza sleale (art. 6-*bis* Regio Decreto 29 giugno 1939 n. 1127, c.d. Legge-Invenzioni). In seguito, la disciplina del segreto commerciale è confluita negli artt. 98-99 Codice della Proprietà Industriale (C.P.I., Decreto legislativo 10 febbraio 2005 n. 30), che, dopo la modifica apportata dal Decreto legislativo 13 agosto 2010 n. 131 (Decreto correttivo) conferiscono al segreto commerciale le sembianze di un vero e proprio diritto di proprietà intellettuale, tutelabile

La mancanza di una tutela giuridica unitaria a livello europeo ha due effetti negativi sulle attività economiche europee[838]. Da un lato, gli incentivi alla conduzione di attività di innovazione a livello transfrontaliero sono scarsi, poiché il rischio di acquisizione e divulgazione illecite dei segreti commerciali aumentano negli Stati membri in cui il livello di tutela giuridica è basso; dall'altro, una protezione giuridica inadeguata del segreto commerciale riduce la competitività delle imprese, dal momento che «*businesses will lose competitive advantages if their trade secrets are misappropriated*»[839].

Come è stato svolto per gli altri regimi di tutela esistenti a livello europeo, occorre soffermarsi maggiormente sul testo normativo europeo e, in seguito, sulla configurabilità applicativa dei *trade secrets* ai grandi *datasets*.

Stando al testo della Direttiva (UE) 2016/943, la nozione di segreto commerciale, che ricalca l'art. 39 dell'accordo TRIPs, comprende le informazioni che rispondono cumulativamente ai seguenti requisiti: «*a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; b) hanno valore commerciale in quanto segrete; c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete*»[840]. La persona fisica o giuridica che controlla legittimamente un segreto commerciale è denominata «*detentore del segreto commerciale*»[841]. I requisiti del n. 1 dell'art. 2 (lett. a, b e c) sono fondamentali per capire la delicatezza della tecnica giuridica del *trade secret*. Anzitutto, le informazioni coperte dal segreto godono

---

erga omnes (P. AUTERI, *op. cit.*, 212). Tale impostazione è stata oggetto di critiche da parte di alcuni commentatori (V. FALCE – G. GHIDINI, *Trade Secrets as Intellectual Property Rights: A Disgraceful Upgrading – Notes on an Italian 'Reform'*, in R.C. DREYFUSS – K.J. STRANDBURG (CUR.), *The Law And Theory Of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, 2011, 140 ss.; V. FALCE, *Trade Secret Protection in the Innovation Union. From the Italian approach to the UE solution*, in 4 *Mercato, concorrenza e regole*, 2013, 20 ss.)

[838] COMMISSIONE EUROPEA, *Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 2013, 28-38.

[839] T. APLIN, *A Critical Evaluation of the Proposed EU Trade Secrets Directive*, King's College London Dickson Poon School of Law Legal Studies Research Paper n. 2014-25, 2014, 4.

[840] Art. 2 n. 1 Direttiva (UE) 2016/943.

[841] Art. 2 n. 2 Direttiva (UE) 2016/943.

della protezione in quanto e finché sono accessibili al ristretto numero di persone che ne hanno il legittimo controllo. In altri termini, la tutela si estingue non alla scadenza di un termine, come accade per gli altri diritti di proprietà intellettuale, bensì al verificarsi della condizione (risolutiva) dello svelamento delle informazioni. In seguito, il segreto commerciale si estingue, e le informazioni rientrano nel pubblico dominio. Si è detto, a ragione, che tale presupposto comporta che la protezione giuridica prevista dalla Direttiva (UE) 2016/943 accordata non abbia carattere assoluto, bensì relativo, giacché dipende soprattutto da «*technical, organizational, as well as contractual measures sufficient to preserve the confidential nature of the information*»[842].

Il Capo II della Direttiva (UE) 2016/943 distingue due scenari di acquisizione, utilizzo e divulgazione dei segreti commerciali. Il par. I dell'art. 3 elenca le modalità con cui tali pratiche sono considerate lecite. Tali modalità sono:

i. la scoperta o la creazione indipendente;
ii. l'osservazione, lo studio, lo smontaggio o la prova di un prodotto o di un oggetto messo a disposizione del pubblico o lecitamente in possesso del soggetto che acquisisce le informazioni, il quale è libero da qualsiasi obbligo giuridicamente valido di imporre restrizioni all'acquisizione del segreto commerciale (c.d. *reverse engineering*);
iii. l'esercizio del diritto all'informazione e alla consultazione da parte di lavoratori o rappresentanti dei lavoratori, in conformità del diritto e delle prassi dell'Unione e nazionali;
iv. qualsiasi altra pratica che, secondo le circostanze, è conforme a leali pratiche commerciali.

L'art. 4 enumera le ipotesi di modalità illecite. L'acquisizione di un segreto commerciale senza il consenso del detentore è illecita qualora compiuta in uno dei seguenti modi:

---

[842] A. WIEBE, *op. cit.*, 65. Nello stesso senso, G. SURBLYTĖ, *Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy*, Max Planck Institute for Innovation and Competition Research Paper n. 16-03, 2016, 9.

i. l'accesso non autorizzato, l'appropriazione o la copia non autorizzate di documenti, oggetti, materiali, sostanze o *files* sottoposti al lecito controllo del detentore del segreto commerciale, che contengono il segreto commerciale o dai quali il segreto commerciale può essere desunto;

ii. qualsiasi altra condotta che, secondo le circostanze, è considerata contraria a leali pratiche commerciali[843].

Poi, l'utilizzo o la divulgazione di un segreto commerciale sono da considerarsi illeciti se posti in essere senza il consenso del detentore del segreto commerciale da una persona che:

i. ha acquisito il segreto commerciale illecitamente;

ii. viola un accordo di riservatezza o qualsiasi altro obbligo di non divulgare il segreto commerciale;

iii. viola un obbligo contrattuale o di altra natura che impone limiti all'utilizzo del segreto commerciale[844].

Altre ipotesi di illiceità dell'acquisizione, dell'utilizzo e della divulgazione del segreto sono previste ai par. IV e V dell'art. 4 della Direttiva (UE) 943/2016.

L'art. 5 della Direttiva (UE) 2016/943, stabilisce poi talune eccezioni alla tutela giuridica delineata dai precedenti articoli.

Numerosi punti della normativa europea rendono il segreto commerciale uno strumento giuridico inadeguato rispetto alle attività di sfruttamento dei *Big Data*. Il legislatore europeo, infatti, non aveva in mente tali scenari economici al momento della stesura delle disposizioni[845].

In primo luogo, a differenza della tutela giuridica delle banche dati, la protezione si estende sia ai singoli dati[846], sia, come si desume dal n. 1 dell'art. 2 della

---

[843] Art. 4 par. II Direttiva (UE) 943/2016.
[844] Art. 4 par. III Direttiva (UE) 943/2016.
[845] A. WIEBE, *op. cit.*, 65.
[846] J. DREXL, *op. cit.*, 23; H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 62.

Direttiva (UE) 2016/943[847], all'insieme dei dati in quanto tale[848]. Il segreto commerciale tutela l'informazione semantica e quella sintattica[849]. Per accedere alla tutela, i singoli dati o i *datasets* non devono necessariamente rispondere a requisiti di originalità, ma è sufficiente che riguardino attività commerciali[850] e, quindi, siano raccolti e archiviati come parte di dette attività[851]. Tuttavia, appare difficile conciliare i singoli dati con il presupposto del valore commerciale stabilito dalla Direttiva (UE) 2016/943[852]: secondo il dettato normativo, «*la definizione di segreto commerciale esclude le informazioni trascurabili*»[853]. Nella catena del valore dei *Big Data* il singolo dato non detiene, di per sé, un valore commerciale[854]; al contrario, a questo requisito rispondono più verosimilmente le correlazioni fra i dati di un *dataset*[855] e, di conseguenza, gli insiemi di dati e le informazioni di valore ottenute mediante la sottoposizione del *dataset* stesso ai processi automatizzati di analisi[856]. Secondo un'altra lettura della norma, negli scenari di sfruttamento economico dei *Big Data*, nessun dato può essere considerato trascurabile, e, di conseguenza, «*there may no longer be any trivial information that would fall outside the scope of protection*»[857].

In secondo luogo, taluni punti della disciplina europea del segreto commerciale paiono assai difficilmente conciliabili con gli scenari di raccolta dei dati nell'Internet delle Cose. A ben vedere, il requisito di segretezza stabilito dal par. I dell'art. 2 (lett. a) non può essere facilmente applicato al contesto di produzione dei dati mediante i sensori di cui sono dotati gli oggetti *smart* (quali *wearables*, automobili, tostapane, termostati…), giacché, «*while the secrecy could be confirmed for data that is produced by the machines inside a factory, data collected by smart cars on freely accessible roads could be collected by the cars of many*

---

[847] L'art. 2 della Direttiva (UE) 2016/943 parla di informazioni «*nel loro insieme o nella precisa configurazione e combinazione dei loro elementi*».
[848] G. SURBLYTĖ, *Data As a Digital Resource*, Max Planck Institute for Innovation and Competition Research Paper n. 16-12, 2016, 9.
[849] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 62.
[850] H. ZECH, *Data As a Tradeable Commodity*, *op. loc. cit.*
[851] H. ZECH, *Data As a Tradeable Commodity*, *op. loc. cit.*; G. SURBLYTĖ, *Data As a Digital Resource*, *op. cit.*, 11.
[852] Art. 2 n. 1 lett. b Direttiva (UE) 2016/943.
[853] Cons. 14 Direttiva (UE) 2016/943.
[854] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 63.
[855] J. DREXL, *op. cit.*, 23.
[856] G. SURBLYTĖ, *Data As a Digital Resource*, *op. loc. cit.*
[857] A. WIEBE, *op. loc. cit.*

manufacturers and, hence, will not fulfil this requirement»[858]. Inoltre, la Direttiva (UE) 943/2016 non spiega quali siano le "misure ragionevoli" che il detentore del segreto deve porre in essere per soddisfare il requisito in questione[859].

In terzo luogo, l'individuazione del detentore del segreto è una questione particolarmente spinosa negli scenari di sfruttamento dei *Big Data*. Come già detto *supra*, il detentore del segreto è in una posizione di potere fattuale: egli, analogamente al possessore di una cosa, «*controlla legittimamente*»[860] i dati segreti in via esclusiva[861]. A differenza della figura civilistica del possessore, il detentore del segreto deve possedere legittimamente la risorsa, e non può averla acquisita in modo illecito, violando i diritti di altri soggetti[862]. Almeno per i singoli dati di un *datasets*, inoltre, è difficile stabilire se un soggetto abbia acquisito lecitamente o illecitamente i dati coperti dal segreto di un detentore (per esempio, stabilire se il soggetto abbia raccolto i dati secondo una "scoperta indipendente" o mediante un "accesso non autorizzato"). Nei contesti dell'Industria 4.0 e dell'Internet delle Cose, la determinazione del soggetto tutelato dà luogo a notevoli incertezze[863]. Si pensi, per esempio, all'utilizzo di una macchina utilizzata nel settore manifatturiero[864]. Ai dati prodotti dal congegno potrebbe accedere solo il suo costruttore, qualora quest'ultimo lo abbia progettato in modo tale che gli altri soggetti siano esclusi dall'accesso a tali risorse. In un'ipotesi del genere, il detentore del segreto commerciale sui dati in questione sarebbe il costruttore. Ma qualora sia l'utilizzatore che il costruttore del dispositivo siano in grado di accedere ai dati raccolti, sarebbe problematico stabilire chi dei due abbia il controllo legittimo su tali dati, cioè chi sia il detentore del segreto[865]. Si potrebbe addirittura concludere che non sussista il requisito di segretezza, e, quindi, alcun soggetto possa accedere alla tutela giuridica dei *trade secrets*.

---

[858] J. DREXL, *op. loc. cit.*
[859] A. WIEBE, *op. loc. cit.*; J. DREXL, *op. loc. cit.*
[860] Art. 2 n. 2 Direttiva (UE) 2016/943.
[861] H. ZECH, *op. cit.*, 64.
[862] Com'è noto, non sempre il possesso civilistico corrisponde all'esercizio del diritto di proprietà sulla cosa.
[863] J. DREXL, *op. loc. cit.*
[864] *Industria 4.0, la nuova era del manifatturiero*, in *Digital 4 Executive*, 2 luglio 2015 (www.digital4.biz/executive/approfondimenti/industria-40-la-nuova-era-del-manifatturiero_43672155526.htm, ultimo accesso 29 agosto 2017).
[865] H. ZECH, *op. loc. cit.* Sui conflitti di diritti sui grandi *datasets*, vedasi più nello specifico *infra*, § 6.

In quarto luogo, come già affermato, la tutela giuridica del segreto commerciale non dà origine a un diritto soggettivo di carattere reale e assoluto che si estende a ogni uso altrui[866], ma a una posizione protetta solo in ragione delle pratiche illecite stabilite dalla Direttiva (UE) 2016/943[867].

Infine, sussiste il rischio che il recepimento della Direttiva (UE) 2016/943 nel diritto interno degli Stati membri non porti ai risultati di armonizzazione sperati[868], e che le differenze di tutela accordata viste all'inizio del presente paragrafo creino ulteriore incertezza nell'ambito delle attività di innovazione transfrontaliera, comprese quelle che concernono lo sfruttamento dei *Big Data*.

5.5. Il paradigma della proprietà "fisica" civilistica

Secondo alcuni commentatori, la diffusione di nuove forme di ricchezza immateriale, di cui i *Big Data* sono una *species*, richiede l'allargamento di talune categorie del diritto civile, e cioè, *in primis*, delle nozioni di proprietà privata e di bene[869]. Questi tentativi si scontrano con un'impostazione granitica, che scoraggia il legislatore dall'introdurre il discorso civilistico-dominicale nell'allocazione giuridica delle nuove risorse intangibili. Secondo tale impostazione dominante nel sistema giuridico di *civil law*, la proprietà privata riguarda solo i beni materiali (si parla opportunamente di nozione "fisicista" e "terragna" della proprietà[870]), e la decisione sull'allargamento dell'oggetto del diritto di proprietà spetta unicamente al legislatore. Tuttavia, in anni recenti una parte recessiva della dottrina ha tentato di superare l'approccio tradizionale. Nel 2016, i giuristi e gli operatori del diritto riuniti nel *Deutsche Juristentag*, importante *forum* sulle riforme del diritto della

---

[866] H. ZECH, *op. cit.*, 63. *Contra* J. DREXL, *op. cit.*, 24, per il quale tale sistema di regole di responsabilità «*can be considered as better suited to serve the purposes of the data economy, by focussing on the particular way in which a third party has in particular acquired access to the data instead of granting exclusive protection against the use of data*».

[867] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, Macie Discussion Paper n. 3-2016, 2016, 5.

[868] G. SURBLYTĖ, *op. cit.*, 9.

[869] A. GAMBARO, *Dai beni immobili ai beni virtuali*, in *Enciclopedia Treccani* (http://www.treccani.it/enciclopedia/dai-beni-immobili-ai-beni-virtuali_%28XXI-Secolo%29/, ultimo accesso 30 agosto 2017); G. RESTA (CUR.), *Diritti esclusivi e nuovi beni immateriali*, Utet Giuridica, 2011.

[870] U. MATTEI, *op. cit.*, *passim*.

Germania, hanno dibattuto sulla necessità di un "aggiornamento alle nuove istanze digitali" (*digital update*) del codice civile tedesco (*BGB*[871]).

Occorre ora seguire il percorso di analisi già utilizzato per altri regimi di tutela. Prima, si analizzeranno più dettagliatamente le caratteristiche ("prerogative") della proprietà privata; in seguito, si cercherà di capire se tale opzione giuridica possa considerarsi adeguata a fornire tutela ai controllori dei grandi *datasets*.

Al di là delle differenze dei vari ordinamenti giuridici e delle tassonomie, importa notare che i beni sono strettamente connessi all'uso che i soggetti ne fanno. «*A good is the sum of its possible uses*»[872]. Tali "possibili usi" di un bene sono ben rappresentati, nella realtà giuridica, dalla costruzione del diritto di proprietà come fascio di prerogative del suo proprietario (*bundle of rights*[873]). Tale impostazione, il cui sviluppo concettuale si deve ai lavori di Wesley N. Hohfeld[874] e, soprattutto, di Antony (Tony) M. Honoré[875], ha riscosso successo dapprima nella tradizione giuridica anglo-americana, e, in seguito, si è diffusa anche negli ordinamenti di *civil law*[876]. Secondo Honoré, romanista e comparatista dell'Università di Oxford, il diritto di proprietà[877] può essere scomposto in un fascio di undici elementi costitutivi (*incidents*), che costituiscono le prerogative del titolare del diritto. Tali prerogative non si limitano alla realtà delle cose materiali. Come fa notare Honoré, «*we are left not with an inclination to adopt a terminology which confines ownership to material objects, but with an understanding of a certain shift in meaning as ownership is applied to different classes of things owned*»[878].

Tali prerogative sono:

i. il diritto al possesso esclusivo;

---

[871] J. DREXL, *op. cit.*, 26-27.
[872] H. ZECH, *Data as a Tradeable Commodity*, *op. cit.*, 56.
[873] J.E. PENNER, *The "Bundle of Rights" Picture of Property*, in 43 *UCLA Law Review*, 1996, 711 ss.; S. MUNZER, *A Theory of Property*, Cambridge University Press, 1990.
[874] W.N. HOHFELD, *Fundamental Legal Conceptions as Applied in Judicial Reasoning*, in 26(8) *Yale Law Journal*, 1917, 710 ss.
[875] A.M. HONORÉ, *Ownership*, in A.G. GUEST (CUR.), *Oxford Essays in Jurisprudence*, Oxford University Press, 1961, 107 ss.
[876] U. MATTEI, *La proprietà*, *op. cit.*, 145 ss.
[877] Non a caso, Honoré parla di *ownership*, e non di *property*, dal momento che quest'ultimo termine designa una pluralità di situazioni giuridiche diverse che, al di fuori della tradizione di *common law*, non sono per nulla riconducibili al diritto di proprietà.
[878] T. HONORÉ, *op. cit.*, 133.

ii. il diritto al godimento personale;
iii. il diritto alla gestione della risorsa;
iv. il diritto alla rendita derivante dall'uso da parte di altri;
v. il diritto sul valore del capitale;
vi. il diritto alla sicurezza della situazione proprietaria;
vii. il diritto alla trasmissione gratuita *inter vivos* o *mortis causa*;
viii. l'assenza di termini;
ix. il dovere di usare la risorsa scarsa in modo da non danneggiare gli altri;
x. l'esposizione della risorsa all'esecuzione forzata per il pagamento dei debiti;
xi. i diritti residuali dovuti all'elasticità del dominio.

Queste qualità rispondono a un'esigenza descrittiva con vocazione generale, «*collocata, cioè, oltre le specificità del singolo ordinamento positivo*»[879]. Lo schema concettuale, quindi, ha valenza euristica, e serve a inquadrare la situazione giuridica soggettiva del titolare del diritto di proprietà.

In primo luogo, il titolare del diritto di proprietà ha il diritto di possedere esclusivamente il bene (i). Secondo la tradizione giuridica romanistica, il possesso è una posizione di controllo e di disponibilità della cosa oggetto del diritto[880]. Come afferma Honoré, possedere una cosa significa «*to have exclusive physical control of a thing, or to have such control as the nature of the thing admits*»[881]. Chiaramente, il possesso di un *dataset*, e, in generale, di un'utilità incorporea differisce dalla situazione di controllo di un *asset* corporeo-tangibile. Il possesso dei dati e delle informazioni corrisponde alla possibilità di accedere a questi e controllarli[882]. Come si è notato per i dati personali[883], l'accesso consente al titolare del diritto di porre in essere altre attività tipiche della sfera giuridica del proprietario, come, per esempio, utilizzare la risorsa[884].

---

[879] U. MATTEI, *La proprietà*, *op. cit.*, 147.
[880] Secondo il co. I dell'art. 1140 cod. civ. italiano, «*il possesso è il potere sulla cosa che si manifesta in un'attività corrispondente all'esercizio della proprietà o di altro diritto reale*».
[881] T. HONORÉ, *op. cit.*, 113.
[882] Così J. RIFKIN, *L'era dell'accesso, La rivoluzione della new economy*, Mondadori, 2000, *passim*.
[883] Vedasi § 4.3.1 del capitolo terzo.
[884] H. ZECH, *Data as a Tradeable Commodity*, *op. cit.*, 56.

In secondo luogo, al titolare è allocato un diritto all'uso della risorsa, che si compone di due elementi: un diritto al godimento e all'uso personale (che Honoré chiama, in senso stretto, *right to use*) (ii), e un diritto alla gestione della risorsa (iii). Quest'ultima prerogativa implica che il proprietario possa decidere chi possa usare il bene e in quali modalità possa utilizzarlo.

In terzo luogo, il diritto alla rendita derivante dall'uso da parte di altri (*right to income*) (iv). Il proprietario gode di una rendita sulla base di un'obbligazione o di un diritto reale minore di un altro soggetto.

In quarto luogo, il diritto sul valore del capitale (*right to the capital*) (v) consiste nel potere di alienare, di consumare e di distruggere l'intero bene o alcune parti di esso[885]. A differenza dei beni tangibili, i dati non possono consumarsi. I *datasets* possono certamente essere alienati[886] e distrutti. L'alienazione di un *dataset*, nondimeno, non implica che il titolare originario del bene perda il proprio diritto di proprietà, giacché le risorse digitali non sono scarse, bensì sono riproducibili illimitatamente, a costo marginale zero. La distruzione dei dati si distingue a seconda che si incida sul livello sintattico, fisico-strutturale o semantico dell'informazione. Sul piano sintattico, un dato può essere distrutto mediante l'alterazione o la cancellazione del codice che lo rappresenta. Sul piano fisico-strutturale, la distruzione dei dati avviene se si sottopone il supporto su cui sono scritti a un'irreparabile danneggiamento. Infine, sul piano semantico, i dati possono essere distrutti solo mediante la falsificazione delle stesse[887].

---

[885] T. HONORÉ, *op. cit.*, 118.

[886] Si vedano il § 3 del presente capitolo e il § 5 del capitolo secondo. In quest'ultimo paragrafo si era detto che, nella catena del valore dei *Big Data*, l'anello dell'utilizzo dei *Big Data* comprende la possibilità di utilizzare i *datasets* ai propri fini, allo scopo di operare scelte strategiche sul mercato, ovvero di cederli a terzi. In quell'occasione, il termine "utilizzo" è stato usato in senso economico e ampio. Honoré, invece, distingue tre tipologie di utilizzo (in senso economico): il godimento personale, la gestione e l'alienamento del bene.

[887] Nondimeno, se una persona conosce un'informazione, questa non può essere distrutta, «*or at least it cannot be destroyed without violating the integrity of the persons who have access to it*» (H. ZECH, *Data As A Tradeable Commodity*, *op. cit.*, 57).

In quinto luogo, il diritto alla sicurezza della situazione proprietaria (vi) comporta che il titolare «*should be able to look forward to remaining owner indefinitely if he so chooses and he remains solvent*»[888]. Questa prerogativa fa da contraltare al potere dell'autorità pubblica, limitando i trasferimenti non consensuali della proprietà o altro diritto reale sulla cosa ai casi in cui prevalgano ragioni di interesse pubblico (espropriazione per pubblica utilità) ovvero il titolare si sia reso insolvente (espropriazione forzata). Si può facilmente avvicinare la seconda ipotesi all'oggetto *de quo*: nel diritto italiano, per esempio, si ammette generalmente la pignorabilità di beni immateriali quali partecipazioni sociali, brevetti, e, da ultimo, il dominio *Internet*[889]. Inoltre, la sicurezza della situazione proprietaria trova il corrispondente simmetrico nell'esposizione della risorsa all'esecuzione forzata per il pagamento dei debiti (*liability to execution*[890]) (x).

In sesto luogo, il diritto del proprietario ha una durata illimitata nel tempo. Tale prerogativa si estrinseca in due elementi: da una parte, nella titolarità del diritto del *de cuius* subentrano i suoi successori al momento della morte (vii); dall'altra, nell'assenza di termini di durata determinati per legge (viii). Il secondo elemento si contrappone alla limitata estensione temporale dei diritti di proprietà intellettuale: com'è noto, il brevetto dura vent'anni dal deposito dalla domanda[891]; i diritti di utilizzazione economica di un'opera dell'ingegno durano tutta la vita dell'autore e sino al termine del settantesimo anno dopo la sua morte indipendentemente dal momento in cui l'opera è stata resa lecitamente accessibile al pubblico[892]. Come si vedrà, la previsione di un diritto di proprietà sui *datasets* di grandi dimensioni senza estensioni temporali pone seri limiti all'accesso alle informazioni[893].

---

[888] T. HONORÉ, *op. cit.*, 119.
[889] V. GATTULLO ET AL., *Nuove frontiere dell'espropriazione mobiliare: Il pignoramento del dominio internet*, in *FILODiritto*, 16 settembre 2014 (www.filodiritto.com/articoli/2014/09/nuove-frontiere-dellespropriazione-mobiliare-il-pignoramento-del-dominio-internet.html, ultimo accesso 31 agosto 2017).
[890] T. HONORÉ, *op. cit.*, 123.
[891] Art. 63 Convenzione sulla Concessione dei Brevetti Europei (*European Patent Convention*, EPC).
[892] Art. 1 par. I Direttiva 2006/116/CE del Parlamento Europeo e del Consiglio del 12 dicembre 2006 concernente la durata di protezione del diritto d'autore e di alcuni diritti connessi, G.U. n. L. 372 del 27/12/2006.
[893] Vedasi *infra* in questo stesso paragrafo e § 6 e 7.

In settimo luogo, il dovere di usare la risorsa in modo da non danneggiare gli altri (ix) si traduce, nella teoria economica, nella limitazione delle esternalità negative, che determinano malfunzionamenti del mercato e corrispondono nella realtà giuridica alla nozione di immissione (*nuisance*). Tale dovere comporta che il proprietario, per esempio, limiti le immissioni (quali rumori, fumo ecc.) a quelle normalmente tollerabili. Le immissioni si distinguono in immissioni di natura pubblica e di natura privata in base al numero di consociati colpiti dall'esternalità negativa[894]. Si è già detto nel capitolo precedente che l'utilizzo di algoritmi per analizzare quantità di dati incalcolabili alla mente umana provoca una serie di esternalità negative (di natura pubblica) che si ripercuotono sulla sfera giuridica dei consumatori[895] anche nel caso in cui siano sottoposti ad analisi dati anonimizzati, che, com'è noto, non rientrano nella tutela fornita dal Regolamento (UE) 2016/679[896].

Infine, il titolare ha diritti residuali sul bene di cui è proprietario, nel senso che, quando una posizione giuridica di un altro soggetto sul bene, sia essa di natura reale o personale, si estingue, il titolare del diritto di proprietà (ri)acquisisce il corrispondente diritto[897]. Per citare un esempio, alla scadenza di un contratto di locazione di un immobile, il locatore-proprietario (ri)acquisisce il godimento e l'utilizzo del bene. Eguali scenari si prospettano nel campo della proprietà immateriale: si pensi, per esempio, alla scadenza del termine del contratto di licenza di brevetto.

È necessario ora capire se la tutela accordata dal diritto di proprietà "fisica", a prescindere dalla configurabilità astratta nel mondo dell'immateriale, conferisca protezione ai soggetti che controllano i *Big Data*.

Tale analisi potrebbe esaurirsi anzitempo considerando che, al momento della stesura di questo lavoro, in nessun Paese europeo le proposte di "digitalizzazione" della proprietà fisica hanno avuto realizzazione. Dunque, le ragioni che

---

[894] Si veda più nel dettaglio il discorso sui *public bads* del § 6.2 del capitolo terzo.
[895] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione).
[896] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (d'ora in poi: Regolamento (UE) 2016/679), G.U. n. L. 119 del 4/5/2016.
[897] M.E. BAYLES, *Principles of Law: A Normative Analysis*, Springer, 1987, 87.

fanno propendere per l'inadeguatezza di un regime dominicale sono da trovarsi solamente in prospettive *de iure condendo* e *policies*.

L'equiparazione dei beni intangibili, quali i *datasets* di grandi dimensioni, alle risorse corporali oggetto del diritto di proprietà privata "fisica" implica una serie di problematiche e distorsioni che è difficile dirimere[898]. In primo luogo, le questioni più spinose sono legate alle qualità economiche dei beni informazionali: a differenza dei beni materiali, oggetto della proprietà privata, che sono risorse scarse e rivali, i dati sono *assets* (tendenzialmente) non rivali. Per i primi, lo *jus excludendi alios* è lo strumento di allocazione che impedisce che le risorse scarse siano preda di comportamenti idiosincratici di un'intera comunità. L'istituzione della proprietà privata frena l'abuso (cioè l'uso eccessivo) di una risorsa naturale scarsa (c.d. "tragedia dei (beni) comuni", *tragedy of the commons*[899]). Per i secondi, questo dispositivo euristico non funziona[900], perché l'uso di un soggetto non espone la risorsa all'esaurimento e non interferisce con l'utilizzo altrui, che avviene a costo marginale zero[901]: «*indeed, copying information actually multiplies the available resources* […] *The result is that rather than a tragedy, an information commons is a "comedy" in which everyone benefits*»[902].

In secondo luogo, la quasi totalità delle prerogative caratterizzanti il diritto di proprietà fisica sono incorporate altresì, *mutatis mutandis*, negli istituti di esclusiva intellettuale visti in precedenza, tranne l'assenza di un termine di durata della protezione. L'estensione temporale illimitata di un diritto esclusivo sul bene avrebbe effetti distorsivi e oltremodo anticoncorrenziali[903], e «*would amount to a very powerful intellectual property right that would have the potential of undermining the free flow of information*»[904].

---

[898] J. DREXL, *op. cit.*, 27 ss.
[899] G. HARDIN, *The Tragedy of the Commons*, in 162 *Science*, 1968, 1243 ss.; U. MATTEI, *op. cit.*, 8-10.
[900] C.M. ROSE, *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, in 66 *Law & Contemporary Problems*, 2003, 89 ss.; M. LEMLEY, *Property, Intellectual Property, and Free Riding*, John M. Olin Program in Law and Economics Working Paper n. 291, 2004, 25.
[901] G. MAZZIOTTI, *EU Digital Copyright Law and the End-User*, Springer, 2008, 16.
[902] M. LEMLEY, *Property, Intellectual Property, and Free Riding*, *op. cit.*, 26.
[903] Vedasi § 2.2.1 del capitolo secondo e D.L. RUBINFELD – M.S. GAL, *op. cit.*, 1 ss.
[904] J. DREXL, *op. cit.*, 28.

6. L'istituzione di un nuovo diritto esclusivo sui dati non personali

Dall'analisi condotta nei paragrafi precedenti, si è visto che i regimi di tutela esistenti a livello europeo non sono adeguati a fornire protezione ai soggetti che controllano e sfruttano economicamente i *datasets*[905]. Le carenze e le insufficienze del quadro giuridico hanno fatto sorgere alcune voci a favore della delineazione di una posizione giuridica esclusiva sull'utilizzo dei grandi *datasets*[906] che consenta di superare le ristrettezze del quadro giuridico.

6.1. Il nuovo diritto esclusivo sui dati non personali

La costruzione di un diritto esclusivo sui dati non personali è una questione alquanto complessa, dal momento che concerne l'economia digitale, un contesto dinamico e sottoposto a cambiamenti continui. La Commissione[907] e taluni commentatori europei[908] hanno cercato di elaborare una soluzione giuridica che tenga conto di questo fondamentale accorgimento[909].

Secondo la proposta della Commissione e degli autori, la nuova posizione giuridica sui *datasets* ha natura reale e può farsi valere nei confronti della collettività (*erga omnes*). Un tale riconoscimento giuridico estenderebbe il *numerus clausus* dei diritti di proprietà intellettuale[910].

Il titolare è, in prima battuta, il produttore del *dataset*, cui è assegnato il diritto di utilizzo esclusivo. Il produttore è la persona fisica o giuridica che è il

---

[905] Solo la tutela brevettuale delle tecnologie dell'Internet delle Cose sembra essere uno scenario probabile.
[906] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017; T.J. FARKAS, *op. cit.*; W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*; A. WIEBE, *op. cit.*; H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*
[907] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 33 ss.
[908] J. DREXL, *op. cit.*, 38 ss.; H. ZECH, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, *op. cit.*, 460 ss.; H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 74 ss.
[909] Per le giustificazioni di un nuovo diritto esclusivo sui dati non personali, si rimanda al paragrafo successivo.
[910] Vedasi *supra*, § 4.

soggetto "economicamente responsabile" dei dispositivi che generano i dati[911], tenendo conto degli investimenti e delle risorse allocate nella creazione dei dati[912]. Tuttavia, come si è già detto riguardo alla determinazione del detentore del segreto commerciale[913], in taluni casi l'individuazione del titolare può risultare difficoltosa, dato che investimenti sostanziali nella produzione dei dati sono compiuti sia dal costruttore dei dispositivi dotati di sensori, sia dall'utilizzatore di tali congegni. Quando la creazione dei dati è frutto di investimenti e risorse di più persone o enti, si delinea un regime di contitolarità sui *datasets*. Il titolare del diritto, inoltre, può concederlo in licenza o trasferirlo a un'altra persona fisica o giuridica.

L'oggetto del diritto in questione sono i dati intesi come sequenza di *bits* (*machine-readable coded information*[914]) non strutturati[915]. In altri termini, la tutela riguarda unicamente il piano sintattico dell'informazione, giacché la protezione dei *datasets* a livello semantico avrebbe effetti molto negativi sulla libera circolazione delle informazioni, costituendo una sorta di iper-esclusiva che determinerebbe l'uscita di numerose risorse informative dal pubblico dominio[916]. I dati non personali sono tutelati a prescindere dalla modalità con cui sono prodotti: può trattarsi di dati raccolti mediante l'utilizzo di dispositivi muniti di sensori degli oggetti dell'Internet delle Cose, oppure raccolti su *Internet*[917]. I metadati, cioè i dati che descrivono un altro insieme di dati, sono inclusi nella protezione giuridica in questione[918]. Rimarrebbero esclusi, invece, i dati prodotti nuovamente in seguito a una nuova rilevazione[919].

---

[911] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 75. Riguardo ai dati anonimizzati, il soggetto che ha proceduto alla raccolta è il titolare.
[912] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 35.
[913] Vedasi *supra*, § 5.2.
[914] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 74.
[915] Tuttavia, come si è fatto notare sopra, la nozione di "banca dati" della Direttiva 96/9/CE è sufficientemente ampia da accogliere anche i *datasets* non strutturati. Vedasi *supra*, § 5.1.
[916] H. ZECH, *Information as Property*, *op. cit.*, 196.
[917] Solo i dati dei consumatori sottoposti a processi di anonimizzazione sono oggetto della tutela. Nondimeno, se dalle combinazioni dei *datasets* emergono profili individualizzati, le informazioni di valore che si ottengono mediante l'analisi sono sottoposte alla disciplina dei dati personali. Si rimanda al capitolo terzo.
[918] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 34.
[919] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 75.

Il requisito per accedere alla tutela è la mera produzione del dato «*through automated measurement processes, intellectual activity or simple computing power*»[920].

Il diritto esclusivo è sottoposto a una serie di eccezioni e limitazioni. Vi è il rischio che una protezione giuridica troppo forte, pur concernendo il piano sintattico delle informazioni, vada a eccessivo nocumento della libera circolazione delle informazioni. Perciò, la tutela ha necessariamente un'estensione temporale limitata e deve escludersi allorché il riuso dei dati da parte di terzi avvenga per finalità non commerciali[921]. Inoltre, il titolare del diritto dev'essere soggetto all'obbligo di consentire l'accesso ai dati ai terzi in una serie di ipotesi[922].

i. Se il diritto è allocato all'utilizzatore del dispositivo che produce i dati (*machine-generated*), è prevista un'eccezione a favore del costruttore del congegno di produzione del dato. Infatti, «*the manufacturer may not only have a legitimate interest to use such data for the purposes of further improving product design, but also may have a legal obligation to monitor the behaviour of his products on the market*»[923].

ii. Le autorità pubbliche possono richiedere l'accesso a certe tipologie di dati per fini di interesse pubblico. Come si è visto in precedenza, anche la disciplina dei dati personali trova ampie limitazioni se la raccolta e il trattamento hanno scopi di pubblica sicurezza. Analogamente, l'accesso delle autorità pubbliche ai dati non personali statistici e ambientali risponde a finalità di pubblica utilità.

iii. Infine, libero accesso ai dati è consentito a studiosi e ricercatori che operano in strutture interamente o prevalentemente finanziate dal denaro pubblico.

---

[920] H. ZECH, *Data As a Tradeable Commodity*, *op. cit.*, 74.
[921] Si confronti l'art. 27 lett. a Accordo su un tribunale unificato dei brevetti, G.U. n. C. 175 del 20/6/2013.
[922] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 35-36.
[923] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 35.

6.2. Le ragioni giustificatrici: un'analisi economica

Alla luce della proposta di un nuovo strumento di esclusiva, occorre ora interrogarsi sull'opportunità di una siffatta posizione giuridica ricorrendo agli strumenti di analisi delle scienze economiche.

I giuristi e gli economisti (soprattutto quelli di provenienza nordamericana) hanno posto i diritti di proprietà intellettuale sotto la lente di ingrandimento dell'analisi economica per trovarne le *rationes*. L'influenza della dottrina giuseconomica ha determinato il sorgere di una vera e propria "teoria economico-utilitaristica" della proprietà intellettuale, che affonda le sue radici nei lavori di Jeremy Bentham e John Stuart Mill[924].

Le giustificazioni tradizionali della proprietà intellettuale sono di due diversi ordini. Anzitutto, l'esclusiva serve a bilanciare il celebre *trade-off* fra incentivo alla creazione (*incentive*) e accesso alle informazioni (*access*). Da una parte, i creatori non hanno sufficienti incentivi allo sviluppo di prodotti e opere innovativi in assenza di una tutela giuridica esclusiva, poiché i beni immateriali possono essere facilmente copiati dai concorrenti che non hanno sopportato i costi di creazione[925]. Come si è già affrontato in precedenza[926], questo elemento dipende dalla natura pubblica (in senso economico) dei beni immateriali, cioè dalla non-rivalità e non-escludibilità nel consumo. In assenza di uno strumento di esclusiva che rende scarso un bene altrimenti in condizione di *commons*, gli investimenti del creatore non sarebbero adeguatamente remunerati, e, di conseguenza, il bene sarebbe prodotto in maniera insufficiente. Dall'altra parte, l'istituzione di una tutela troppo forte, consentendo al creatore di imporre un prezzo per fruire del prodotto creativo, ostacolerebbe l'accesso al bene immateriale e limiterebbe la libera circolazione della conoscenza nella realtà sociale. I due problemi sono risolti mediante la previsione di due fasi temporalmente distinte. In un primo tempo, la privativa rende il bene escludibile per un periodo di tempo limitato. Dopo il passaggio del termine di durata

---

[924] W. FISHER, *Theories of Intellectual Property*, in S.R. MUNZER (CUR.), *New Essays in the Legal and Political Theory of Property*, Cambridge Studies in Philosophy and Law, 2001.
[925] W. LANDES – R. POSNER, *The Economic Structure of Intellectual Property Law*, Harvard University Press, 2003.
[926] Vedasi § 5.6.

della privativa, l'accesso al bene diviene libero e passa, quindi, nel pubblico dominio[927].

In secondo luogo, l'introduzione di diritti di proprietà intellettuale serve a facilitare e incentivare la commercializzazione e l'uso dei beni immateriali da parte dei soggetti diversi dal titolare del diritto (per esempio, mediante i contratti di licenza[928]). Per agevolare effettivamente la circolazione di tali beni, occorre che la privativa sia chiaramente definita e il soggetto cui è allocata sia adeguatamente individuato.

Occorre chiedersi se un nuovo diritto esclusivo sui *datasets* di grandi dimensioni trovi queste giustificazioni o si spieghi in base a ulteriori *rationes*.

6.2.1. Fra incentivo alla creazione e accesso alle informazioni

Se analizzato in rapporto ai *datasets* di grandi dimensioni, il *trade-off* incentivo alla creazione – accesso alle informazioni è fortemente condizionato da due dati empirici. Da un lato, la produzione di quantità sterminate di dati (non personali) avviene su larga scala, a costi bassissimi, spesso come sotto-prodotto di altre attività produttive[929]. L'uso di sensori degli oggetti dell'Internet delle Cose segna una crescita esponenziale della massa di dati. Dall'altro, le barriere all'entrata nei vari sotto-mercati dei *Big Data*[930] e le tecnologie di sicurezza ostacolano l'accesso alle risorse informative.

Prendendo in considerazione la prima variabile, risulta chiaro che il problema di sotto-produzione per mancanza di incentivi, caratterizzante i beni immateriali "tradizionali" (opere dell'ingegno, invenzioni ecc.), non può estendersi agli scenari di sfruttamento economico dei dati. A differenza degli altri beni incorporei, «*data typically involve complex assignment of different rights across different data*

---

[927] F. LÉVÊQUE – Y. MÉNIÈRE, *The Economics of Patents and Copyright*, Berkeley University Press, 2004, 5; A. IANNARELLI, *"Proprietà", "immateriale", "atipicità": i nuovi scenari di tutela*, in G. RESTA (CUR.), *Diritti esclusivi e nuovi beni immateriali*, Utet Giuridica, 2011, 97 ss.
[928] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*, 8; F. LÉVÊQUE – Y. MÉNIÈRE, *op. cit.*, 11 ss.
[929] Vedasi capitolo secondo.
[930] Vedasi capitolo secondo.

stakeholders»[931], che, come visto, sono i soggetti operanti nei diversi anelli della catena del valore dei *Big Data.* L'indagine sulla necessità di un diritto di privativa per ciascuno di questi dimostra che a nessuna categoria sia necessaria una tutela esclusiva che operi come incentivo alla produzione, alla raccolta, all'archiviazione, all'analisi e al riutilizzo dei dati, giacché tali attività sono insite nel modello di *business* degli agenti economici[932]. Perciò, questi ultimi conducono attività di produzione e sfruttamento dei dati anche in assenza dell'allocazione di un diritto esclusivo, controllando *de facto* tali utilità ed escludendo i terzi dalla fruizione delle risorse digitali[933].

Riguardo alla seconda variabile, occorre notare che i dati sono resi facilmente escludibili mediante tecnologie di sicurezza (per esempio, la cifratura e la crittografia[934]) che li rendono segreti potenzialmente per sempre. «*So far the large data holders as Google, Facebook, and others do not seem to suffer from a vast copying and leaking of their huge amounts of collected data*»[935]. Chiaramente, questa circostanza ha conseguenze anti-concorrenziali sul mercato, dal momento che pochi soggetti acquisiscono un potere di mercato che incide negativamente sugli attori privati minori, quali le piccole e medie imprese (PMI[936]).

In conclusione, riguardo agli scenari di sfruttamento dei *Big Data*, nel bilanciamento del *trade-off* incentivo alla creazione – accesso alle informazioni, la variabile dell'accesso dovrebbe senz'altro prevalere sulla prima, dal momento che le attività di produzione e acquisizione dei dati non hanno bisogno di ulteriori incentivi giuridici.

---

[931] OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being,* 2015, 100.
[932] J. DREXL, *op. cit.*, 30-33. Sul punto, si rimanda al § 7.1.
[933] A. WIEBE, *op. cit.*, 67. Il punto sarà oggetto di una trattazione specifica nel § 7.
[934] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*, 9-10.
[935] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. loc. cit.*
[936] Si rimanda al capitolo secondo e al § 7.

6.2.2. Agevolazione del commercio dei *datasets*

Un ulteriore argomento a favore dell'istituzione di un diritto di proprietà intellettuale sui dati è l'incentivazione e la facilitazione della commercializzazione di tali risorse. A prima vista, «*the allocation of a right could bring some order into a market that now looks more like the wild west*»[937]. Come per la risoluzione del *trade off* incentivo alla creazione-accesso alle informazioni, occorre chiedersi se la mancanza di uno strumento giuridico esclusivo esponga il mercato a malfunzionamenti legati agli scambi dei dati. Le disfunzioni dei mercati dell'informazione sono ravvisabili principalmente in due scenari[938].

Il primo è comunemente conosciuto come paradosso dell'informazione di Arrow, per il quale un compratore non può adeguatamente valutare la sua disponibilità a pagare per l'informazione ignorandone il contenuto, ma se il venditore gliela rivelasse prima della conclusione del contratto, di fatto costui la cederebbe a titolo gratuito[939]. L'allocazione di una privativa consente al compratore di conoscere in anticipo il contenuto dell'informazione, ma non di poterla utilizzare senza il consenso del venditore. In realtà, quello che interessa ai compratori dei sottomercati dei *Big Data* non è il contenuto dei singoli dati, bensì le informazioni ricavate dall'analisi dei *datasets* o l'accesso ai dati non strutturati per sottoporli ai procedimenti di analisi.

Il secondo problema inerisce alla possibilità che il primo compratore dei *datasets*, rivendendoli ad altri soggetti, comprometta il benessere del venditore. Tuttavia, «*there is not any particular risk that the data will be copied by competitors for the purpose of substituting the data holder's offer, nor does the grant of access to the data to others, such as Big Data analysts, involve particular investment by the data holders*»[940]. In prima istanza, il rischio di pratiche di *free riding* è facil-

---

[937] A. WIEBE, *op. loc. cit.*
[938] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*, 12 ss.
[939] K. ARROW, *Economic welfare and the allocation of resources for inventions*, in R.R. NELSON (CUR.), *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton University Press, 1962, 609 ss.
[940] J. DREXL, *op. cit.*, 34.

mente eluso mediante il ricorso a clausole contrattuali o a tecnologie (il cui funzionamento ricalca i *Digital Rights Management* per il diritto d'autore) che limitano o rendono impossibile la cessione a terzi dei dati. *In secundis*, i modelli di *business* di imprese quali le piattaforme digitali si basano su un uso "indiretto" dei *datasets*, cioè sulla fornitura di servizi basati sulle risorse informative, che non postula la rivelazione dei dati raccolti[941].

L'istituzione di un diritto esclusivo non trova adeguata giustificazione nemmeno sotto i profili presentati pocanzi. Tuttavia, le attività dei *data brokers* potrebbero costituire una parziale eccezione a tale conclusione: la tutela proprietaria sui dati potrebbe stabilizzare le loro attività, basate fondamentalmente sulla compravendita di *datasets*. In ogni caso, le maglie strette della disciplina europea sulla protezione dei dati personali[942] e la preferenza degli strumenti contrattuali rendono siffatta previsione di scarsa portata operativa.

6.2.3. Altre possibili giustificazioni di un nuovo diritto esclusivo sui *datasets*

Oltre alle giustificazioni di cui si è detto, tradizionalmente addotte riguardo alla proprietà intellettuale, se ne potrebbero aggiungere due ulteriori specifiche per i *datasets* non personali.

Anzitutto, un elemento giustificatorio si può ravvisare nella chiara assegnazione dei benefici che scaturiscono dalle attività di sfruttamento dei dati. L'attribuzione di assetti proprietari, quindi, risponderebbe alla necessità di una maggiore certezza del diritto[943]. Tale esigenza discende dalla sempre più intensa integrazione e compenetrazione delle imprese in *value networks*[944], che rendono più difficile l'allocazione delle risorse digitali: «*in these networks firms have different opinions about who should hold these data and the right to use them commercially, and that a clear assignment of property would resolve conflicts and thus contribute to the*

---

[941] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*, 13.
[942] Si rimanda la trattazione al capitolo terzo.
[943] J. DREXL, *op. cit.*, 35.
[944] Vedasi capitolo primo; J. DREXL, *op. cit.*, 16-18.

order of the market»[945]. In realtà, per ovvia eterogenesi dei fini, pare ben più probabile che il riconoscimento di assetti esclusivi apporti notevole incertezza del diritto alla materia *de qua*[946]. L'elefantiasi dei diritti di privativa di diversi titolari sul medesimo *datasets* può comportare le note conseguenze nefaste in materia di benessere allocativo (tragedia degli anticomuni[947]). L'assegnazione dei diritti di proprietà potrebbe essere apprezzata dalle piccole e medie imprese (PMI), che vedrebbero remunerati più adeguatamente gli sforzi economici. Tuttavia, gli attori privati già risolvono i problemi di attribuzione ricorrendo agli strumenti contrattuali, prevedendo un'esclusività *de facto* dei *datasets* in capo a certi contraenti. Questa opzione, più flessibile e dinamica, pare più adatta agli scenari dell'economia digitale, ma lascia irrisolto il problema dell'influenza che gli agenti economici più potenti possono esercitare su quelli minori. Il diritto dei contratti e la disciplina sulla concorrenza possono fornire strumenti di *governance* dei *datasets* migliore di quella fornita da un assetto esclusivo[948].

In secondo luogo, il riconoscimento della proprietà sui *datasets* può essere uno strumento utile a rafforzare l'accesso ai dati se sono previste limitazioni ed eccezioni obbligatorie alla situazione giuridica soggettiva[949]. Un sistema di eccezioni inderogabili dalle parti, limitando il principio della libertà contrattuale, potrebbe eliminare il rischio di atteggiamenti abusivi di quelle più potenti nei confronti delle più deboli. Nondimeno, lo stesso obiettivo può perseguirsi mediante la legislazione settoriale e specifica, come dimostrano peraltro i recenti interventi normativi del legislatore europeo[950]. Andando nello stesso senso, in altre circostanze

---

[945] W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, *op. cit.*, 15.
[946] S. STALLA-BOURDILLON ET AL., *Building the European Data Economy: Position Paper on the Proposal for a New Right in Non-Personal Data*, 2017.
[947] M. HELLER, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, in 111(3) *Harvard Law Review*, 1998, 621 ss.
[948] Vedasi § 7.
[949] J. DREXL, *op. cit.*, 36 ss.
[950] Si pensi, per esempio, alla Direttiva 2009/72/CE del Parlamento europeo e del Consiglio, del 13 luglio 2009, relativa a norme comuni per il mercato interno dell'energia elettrica e che abroga la direttiva 2003/54/CE, G.U. n. L. 211 del 14/8/2009, che prevede il libero accesso ai dati dei consumatori raccolti dai sistemi di telegestione dei contatori elettrici (c.d. *smart meters*). Sulla legislazione specifica in tema di accesso ai dati, si veda più nel dettaglio COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 25 ss.

la Commissione ha proposto di incentivare l'accesso ai dati mediante l'istituzione di un'eccezione al diritto d'autore «*per le riproduzioni e le estrazioni effettuate da organismi di ricerca ai fini dell'estrazione di testo e di dati* [*text and data mining*] *da opere o altro materiale cui essi hanno legalmente accesso per scopi di ricerca scientifica*»[951].

6.2.4. La sconvenienza di una nuova privativa intellettuale

Dall'esame condotto nei precedenti paragrafi, emerge chiaramente che tutte le *rationes* su cui ci si è concentrati pocanzi non paiono determinanti a far propendere per l'assegnazione di un nuovo strumento di esclusiva sui *datasets*. L'istituzione di un diritto esclusivo sui *datasets* avrebbe ripercussioni pregiudizievoli sulla nascente economia dei *Big Data*, rafforzando la concentrazione delle risorse digitali nelle mani di pochi agenti economici[952], fenomeno già particolarmente presente nei mercati dei *Big Data*[953]. La previsione di una nuova privativa intellettuale limiterebbe notevolmente il libero flusso dei dati e delle informazioni (*free flow of data*), principio ispiratore di politiche condotte a livello internazionale negli ultimi trent'anni. Già nel 1985 i governi degli Stati membri dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) hanno dichiarato l'importanza di abbattere le barriere alla libera circolazione dei dati in formato elettronico fra i diversi Stati membri dell'Organizzazione[954]. Nel 2017, la Commissione europea è pervenuta a soluzioni simili, asserendo che, per sfruttare appieno il potenziale dell'economia dei dati europea, gli interventi delle autorità nazionali degli Stati membri concernenti le attività di raccolta, archiviazione, analisi e riutilizzo dei dati devono essere ispirate a un principio di libera circolazione dei dati all'interno

---

[951] Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale*, 2016, art. 3 par. I.
[952] M. RICOLFI, *IoT and the Ages of Antitrust*, paper inedito fornito dall'autore, 2017, 13.
[953] Si rimanda al capitolo secondo.
[954] Dichiarazione sui flussi di dati transfrontalieri dell'OCSE del 1985 (*OECD Declaration on Transborder Data Flows*).

dell'Unione, che discende dalla libera circolazione dei servizi e dalla libertà di stabilimento previsti nel diritto europeo primario e secondario[955].

Negli scenari economici *data-driven*, segnati da forte dinamicità e dall'abbondanza di risorse digitali, altri strumenti giuridici sono preferibili alla tutela proprietaria, che, come si è visto, non risponde alle tradizionali giustificazioni economiche[956] e finirebbe per rappresentare un'ulteriore barriera all'entrata nel mercato della raccolta dei *Big Data*[957]. La flessibilità e la capacità di adattamento ai diversi settori economici rendono il diritto dei contratti un campo più adeguato all'economia dei dati, caratterizzata da una forte dinamicità[958]. Com'è noto, le imprese trasferiscono i diritti di sfruttamento economico attraverso lo strumento duttile della licenza a prescindere dall'esistenza di un istituto di privativa[959]. Inoltre, come già spiegato, gli attori privati sogliono limitare l'accesso ai dati mediante strumenti tecnici anche in assenza di una tutela giuridica: «*factual exclusivity has the potential of forcing parties into negotiations and can trigger transactions in very similar ways as in the case of intellectual property*»[960].

Come già fatto presente in precedenza[961], l'esclusività *de facto* comporta però problema di accesso alle risorse digitali, che sono controllate da un numero limitato di soggetti economici. È quindi opportuno affrontare il problema della *governance* dei dati da un'altra prospettiva, *id est* intervenire in materia di regolamentazione dell'accesso ai dati ricorrendo ad altri campi del diritto[962]. Nel paragrafo successivo si tenterà di gettare luce su tale questione.

---

[955] Comunicazione della Commissione *Building a European Data Economy*, 2017, 6. Si vedano gli artt. 49-55 e 56-62 TFUE. Si noti che, nello stesso documento, la Commissione ha proposto un ventaglio di soluzioni (legislative e non) per dirimere le questioni della nascente *data economy*.
[956] Vedasi *supra*, § 6.2 e *infra*, § 7.1.
[957] D.L. RUBINFELD – M.S. GAL, *op. cit.*, 361-62.
[958] J. DREXL, *op. cit.*, 40-41.
[959] Vedasi *supra*, § 4.
[960] J. DREXL, *op. cit.*, 29. Vedasi *supra* § 6.2.1.
[961] Si rimanda al § 1 del capitolo secondo e al § 6.2.1 del presente capitolo.
[962] W. KERBER, *Governance of Data: Exclusive Property vs. Access*, *op. cit.*, 761.

7. La regolamentazione dell'accesso ai dati: una questione aperta

7.1. Abbondanza e controllo *de facto*

In un articolo che ha suscitato un vivace dibattito, Mark Lemley, *William H. Neukom Professor* nell'Università di Stanford, ha delineato il ruolo dei diritti di proprietà intellettuale nei nuovi scenari economici[963]. Il contributo del giurista americano ha dato nuova linfa al più ampio dibattito intorno alla c.d. economia della post-scarsità (o dell'abbondanza), per la quale, da una parte, la produzione di taluni beni avviene a un costo marginale zero e, dall'altra, i costi fissi iniziali di produzione diminuiscono in modo vertiginoso[964]. La tesi principale del brillante lavoro di Lemley verte sull'idea che, come *Internet* ha azzerato i costi di riproduzione e distribuzione delle opere dell'ingegno e ha abbassato quelli di realizzazione del contenuto creativo[965], così i recenti cambiamenti tecnologici segneranno la fine della scarsità di numerosi beni materiali e servizi. In particolare, tre nuove tecnologie (attualmente a uno stadio iniziale di sviluppo) trasformeranno radicalmente l'offerta di beni e servizi, abbassandone i costi: la stampa 3D, la biologia di sintesi e la robotica[966]. Lo strumento dell'esclusiva intellettuale, creato in un mondo di risorse scarse, ha avuto la principale funzione di incentivare la creatività e l'innovazione poiché, come si è visto, rende artificialmente scarsi i beni immateriali "tradizionali", che di per sé sono beni pubblici[967]. Questo discorso però non trova più riscontro nell'attuale realtà economica, in cui «*people* […] *create when given the opportunity to do so, even without effective IP protection*»[968]. Nemmeno le ulteriori giustificazioni della proprietà intellettuale, quale l'agevolazione della circolazione dei beni immateriali, paiono più adeguate ai nuovi scenari economici[969].

---

[963] Ci si riferisce a M. LEMLEY, *IP In a World Without Scarcity*, in 90(2) *New York University Law Review*, 2015, 460 ss.
[964] M. GAL, *Competition and Innovation in the Digital Environment*, in G. COLANGELO – V. FALCE (CUR.), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Il Mulino, 2017, 14; S.K. MEHRA, *Competition Law for a Post-Scarcity World*, in 4 *Texas A&M Law Review*, 2016, 1 ss.
[965] Nello stesso senso, S.K. MEHRA, *op. cit.*, 13.
[966] M. LEMLEY, *IP In a World Without Scarcity*, *op. cit.*, 471 ss.
[967] Si rimanda al § 6.2.
[968] M. LEMLEY, *IP In a World Without Scarcity*, *op. cit.*, 515.
[969] M. LEMLEY, *IP In a World Without Scarcity*, *op. cit.*, 463 ss.

Benché l'eccellente analisi di Lemley non tocchi i recenti *trend* evolutivi segnati dalla comparsa sul mercato delle tecnologie dei *Big Data*, dell'Internet delle Cose e dell'intelligenza artificiale, le conclusioni svolte in quella sede sono rilevanti anche per i tre fenomeni appena menzionati, che si fondano sull'abbondanza delle risorse digitali e «*are responsible for an unprecedented flourishing and innovation, which no longer requires outside incentives*»[970]. Infatti, come si è visto in precedenza[971], tali ricavati tecnologici «*increase living standards by lowering costs and improving quality* […] [and] *make economic growth less dependent upon capital and raw material inputs*»[972].

Nel capitolo secondo, si è indagata a fondo la struttura dei mercati dei *Big Data*[973]. Si è visto che tali mercati hanno effetti negativi sulla concorrenza e sul benessere dei soggetti economici[974]. L'accumulo e il controllo di imponenti patrimoni di dati, infatti, comporta l'insorgere di un notevole vantaggio concorrenziale basato su un controllo *de facto*, e non sull'allocazione di un'esclusiva intellettuale[975]. I soggetti economici che detengono tale potenza sono i cc.dd. "signori dei dati" (Google, Amazon, Facebook, Apple), cioè le poche grandi piattaforme digitali che, sfruttando questo potere, escludono gli altri agenti economici dall'accesso ai dati[976] e contribuiscono alla creazione di un vero e proprio "feudalesimo informazionale[977]". Grazie alle attività di acquisizione di dati condotte su larga scala, tali attori privati comprendono le preferenze dei consumatori, e, se un nuovo prodotto o servizio ha successo, lo copiano tempestivamente[978] o acquisiscono il *newcomer*

---

[970] M. RICOLFI, *Beyond Intellectual Property: the Perils of Abundance*, paper inedito fornito dall'autore, 2017, 4.
[971] Vedasi capitolo secondo.
[972] INDEPENDENT STRATEGY, *Global Markets: A short paper on everything*, 2015 (www.instrategy.com/download/Reports/A-short-paper-on-everything-231015.pdf, ultimo accesso 26 settembre 2017).
[973] Si rimanda al capitolo secondo e a D. RUBINFELD – M. GAL, *op. cit.*, 339 ss.
[974] M. GAL, *op. cit.*, 20.
[975] M. RICOLFI, *Beyond Intellectual Property: the Perils of Abundance*, *op. loc. cit.*
[976] Si rimanda all'analisi delle barriere all'ingresso nei sottomercati dei *Big Data* del capitolo secondo.
[977] L'espressione è di P. DRAHOS – J. BRAITHWAITE, *Information Feudalism: Who Owns the Knowledge Economy?*, Earthscan Publications Ltd, 2002.
[978] Si pensi alle cc.dd. "storie" (contenuti audiovisivi, quali fotografie e video, pubblicati su un *social* che scompaiono dopo un certo intervallo di tempo), servizio creato da *Snapchat* e puntualmente copiato da *Instagram*, *Facebook* e *Whatsapp* (*Le Storie di Instagram crescono e Snapchat accusa il colpo*, Wired.it, 31 gennaio 2017 (https://www.wired.it/internet/social-network/2017/01/31/storie-

che ha commercializzato i nuovi prodotti e servizi[979]. Inoltre, i soggetti egemoni non detengono un mero potere di mercato, bensì un vero e proprio potere politico[980].

Alla luce di queste considerazioni, occorre identificare strumenti giuridici che riescano a bilanciare più adeguatamente gli interessi dei diversi *stakeholders*. Come si vedrà, alcuni settori del diritto della concorrenza, pur sembrando adeguati agli scenari di sfruttamento dei *Big Data*, si rivelano di scarsa utilità allo stato attuale delle cose. Il diritto dei consumatori potrebbe offrire una qualche altra soluzione migliore. In assenza di un quadro giuridico soddisfacente, occorre delineare le *policies* e le linee di intervento del legislatore.

7.2. La regolazione dell'accesso ai *Big Data* nel diritto della concorrenza

Numerosi autori hanno posto le attività di sfruttamento economico dei *Big Data* condotte dagli operatori economici al vaglio del diritto della concorrenza, soprattutto in riferimento alle attività condotte dalle piattaforme digitali[981]. Lo strumentario del diritto *antitrust*, a ben vedere, può essere certamente utile a dirimere questioni di regolamentazione dell'accesso ai dati, poiché si adegua alla totalità dei settori economici. Tuttavia, esso è limitato ai soli scenari in cui si possono riscontrare le violazioni delle regole in materia come tipizzate nei vari istituti[982].

Fra le varie fattispecie, ci si concentrerà su quelle rilevanti ai fini del presente lavoro. In particolare,

---

snapchat-instagram, ultimo accesso 3 giugno 2017). Si rimanda alle considerazioni svolte nel § 2.2.4 del capitolo secondo.

[979] Si pensi, per esempio, all'acquisizione della *startup* DeepMind da parte di Google nel 2014. Sul punto, si rimanda a M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 8-9.

[980] M. RICOLFI, *Beyond Intellectual Property: the Perils of Abundance*, *op. cit.*, 6.

[981] Si vedano, *inter alios*, AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *Competition Law and Data*, 2015 (autorità della concorrenza francese e tedesca); G. COLANGELO, *Big Data, piattaforme digitali e antitrust*, in *Mercato concorrenza regole*, 3, 2016, 425 ss.; J. DREXL, *op. cit.*, 42 ss.; A. LERNER, *The Role of "Big Data" in Online Platform Competition*, in *Online Platform Competition*, SSRN library, 2014, 20 ss. (www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780, ultimo accesso 3 giugno 2017); B. LUNDQVIST, *Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. The Issue of Accessing Data*, Faculty of Law, University of Stockholm Research Paper n. 1, 2016; M.E. STUCKE – A.P. GRUNES, *Big Data and Competition Policy*, Oxford University Press, 2016.

[982] Cioè le concentrazioni, le intese restrittive e l'abuso di posizione dominante. Vedasi J. DREXL, *op. cit.*, 42.

i. la dottrina delle infrastrutture essenziali (*essential facilities doctrine*) può essere rilevante per imporre l'accesso ai *datasets* controllati dall'impresa egemone in modo esclusivo;
ii. negli scenari di sfruttamento dei dati raccolti dagli oggetti dell'Internet delle Cose, si delineano accordi di esclusiva che possono esaminarsi sia come condotta unilaterale posta in essere da un'impresa egemone[983], sia alla luce della disciplina delle intese anticoncorrenziali[984].

Prima di considerare queste due situazioni, occorre dedicare alcune considerazioni alla nozione di abuso di posizione dominante.

7.2.1. I *Big Data* come infrastruttura essenziale

7.2.1.1. L'abuso di posizione dominante

Com'è noto, la figura dell'abuso di posizione dominante richiede l'accertamento di due condizioni:

i. *in primis*, occorre verificare l'esistenza di una posizione dominante (art. 102 TFUE);
ii. in secondo luogo, è necessario dimostrare l'abuso, cioè il comportamento dell'agente economico monopolista che pregiudica la posizione dei concorrenti.

In un caso risalente, il concetto di posizione dominante è stato definito dalla CGCE come «*situazione di potenza economica grazie alla quale l'impresa che la detiene è in grado di ostacolare la persistenza di una concorrenza effettiva sul mercato di cui trattasi ed ha la possibilità di tenere comportamenti alquanto indipendenti nei confronti dei suoi concorrenti, dei suoi clienti e, in ultima analisi, dei consumatori*»[985]. Questa nozione è stata presto tacciata di scarsa utilità; in seguito, gli interpreti hanno preferito far riferimento a parametri quantitativi delle teorie

[983] Com'è noto, si tratta della figura dell'abuso di posizione dominante (art. 102 TFUE).
[984] G. COLANGELO, *op. cit.*, 444 ss.; M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 4 e 7-8.
[985] CGCE 13 febbraio 1979, causa 85/76, Hoffmann-La Roche & Co. AG c. Commissione delle Comunità europee, massima.

economiche per misurare il potere di mercato di un'impresa[986]. Al fine di valutare l'esistenza della posizione dominante, occorre far riferimento a una serie di indicatori.

Anzitutto, occorre individuare il mercato rilevante, riconducibile a due variabili, il mercato del prodotto e il mercato geografico. La Commissione ha dato una definizione di tali entità in una Comunicazione del 1997. La prima «*comprende tutti i prodotti e/o servizi che sono considerati intercambiabili o sostituibili dal consumatore, in ragione delle caratteristiche dei prodotti, dei loro prezzi e dell'uso al quale sono destinati*». La seconda «*comprende l'area in cui le imprese interessate forniscono o acquistano prodotti o servizi, nella quale le condizioni di concorrenza sono sufficientemente omogenee*»[987].

Tali nozioni mostrano gravi insufficienze nei contesti economici dominati dalle tecnologie dei *Big Data*[988].

In primo luogo, nei mercati dominati dalle interazioni nelle piattaforme multiversante[989], è addirittura difficile scorgere l'esistenza di un mercato secondo i criteri tradizionali dell'*antitrust*, dal momento che le piattaforme offrono servizi ai consumatori a titolo gratuito e non si ravvisano la domanda e l'offerta[990]. L'ipotesi di uno scambio economico imperniato sui dati dei consumatori, considerati come prodotti, pare poco convincente[991]. Secondo alcuni, inoltre, nei mercati multiversante è necessario tenere in considerazione le esternalità di rete e gli effetti *feedback*[992] che congiungono i diversi versanti delle piattaforme: «*in the present context of organic search and search advertising* [...] *it is clear that these feedback effects are highly significant and, indeed, vital to the viability of the search-advertising*

---

[986] P. AUTERI ET AL., *op. cit.*, 481.
[987] Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza, G.U. n. C. 372 del 09/12/1997.
[988] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 5; G. COLANGELO, *op. cit.*, 439 ss.
[989] Si vedano, più nel dettaglio, i § 2.2.5 e 6.3 del capitolo secondo.
[990] G. COLANGELO, *op. loc. cit.*
[991] Tale idea è avanzata da BUNDESKARTELLAMT, *The Market Power of Platforms and Networks: Executive Summary*, 2016, 8. *Contra*, G. COLANGELO, *op. cit.*, 440.
[992] Si rimanda al § 2.2.3 del capitolo secondo.

platform, because organic search offered to consumers for free would not be a viable standalone business»[993].

In secundis, la nozione di sostituibilità mostra numerose ristrettezze negli scenari di sfruttamento dei *Big Data*. Secondo alcuni, per valutare opportunamente la sostituibilità dei *datasets* occorre far riferimento alle diverse tipologie di dati che «*satisfy different needs of different companies*»[994], con particolare riguardo ai servizi offerti dalle imprese sulle basi di questi[995]. Maggiori incertezze si ravvisano riguardo alle ingenti quantità di dati raccolti dagli oggetti dell'Internet delle Cose. Come fa notare Drexl, i dati sono beni tendenzialmente non rivali, e, in presenza di numerose fonti, succedanei, cioè sostituibili da dati analoghi provenienti da fonti alternative. Il parametro della sostituibilità è difficilmente applicabile agli scenari di sfruttamento di *datasets* di grandi dimensioni, poiché «*even the petitioner for access, such as a Big Data analyst, will often only have a vague understanding about the kind of data contained in the dataset and about which data will produce the most valuable new information based on observable correlations*»[996]. Tale considerazione è particolarmente rilevante per l'esame della nota e controversa dottrina delle infrastrutture essenziali (*essential facilities doctrine*) che ci si appresta a svolgere.

7.2.1.2. I dati come infrastrutture essenziali

La dottrina delle infrastrutture essenziali ha conosciuto alterne fortune nei versanti europeo e statunitense[997]. Nel primo, essa è stata estesa a una pluralità di contesti (quale quello della proprietà intellettuale) grazie al lavoro interpretativo dei

---

[993] J. RATLIFF – D. RUBINFELD, *Is there a market for organic search engine results and can their manipulation give rise to antitrust liability?*, in 10(3) *Journal of Competition Law and Economics*, 2014, 519.
[994] G. PITRUZZELLA, *Big Data, Competition and Privacy: A Look from the Antitrust Perspective*, in 23 *Concorrenza e mercato*, 2016, 20.
[995] G. PITRUZZELLA, *Big Data And Antitrust Enforcement*, in 1 *Rivista italiana di Antitrust*, 2017, 79-80. Nello stesso senso, I. GRAEF, *Market definition and market power in data: the case of online platforms*, in 38(4) *World Competition Law and Economics*, 2015, 473 ss.
[996] J. DREXL, *op. cit.*, 46-47.
[997] Per un inquadramento della dottrina nei vari ordinamenti giuridici, vedasi S. WEBER WALLER – W. TASCH, *Harmonizing Essential Facilities*, in 76(3) *Antitrust Law Journal*, 2010, 741 ss.

giudici della CGCE (poi CGUE), in particolare nelle sentenze *Magill*[998], *Bronner*[999], *IMS Health*[1000] e *Microsoft*[1001]. La giurisprudenza europea ha conferito al requisito dell'essenzialità infrastrutturale una lettura molto ampia, «*dovendosi con ciò intendere che l'accesso ai* data *interessati è indispensabile per l'esercizio di una determinata attività in quanto non esiste rispetto ad essi alcuna alternativa potenziale realistica, senza che possa a tal fine ritenersi sufficiente sostenere che le eventuali alternative sono meno vantaggiose*»[1002].

Se si prende in considerazione il livello semantico dell'informazione, sembra facile soddisfare il requisito di indispensabilità dell'infrastruttura. Nei casi *Magill* e *Microsoft*, infatti, la Corte di giustizia ha affermato che il rifiuto di concedere l'accesso a informazioni di base, quali quelle relative rispettivamente ai palinsesti televisivi e alla documentazione informatica, che costituiscono un'unica fonte, consiste in un abuso di posizione dominante[1003]. Come è emerso nel caso *Microsoft*, inoltre, non necessariamente il *dominium* deriva da una posizione giuridica esclusiva detenuta dall'impresa dominante, ma anche dalla mera disponibilità di una risorsa che diviene essenziale nella prassi (*standard*[1004]): ciò può rivelarsi di fondamentale importanza per gli scenari di sfruttamento dei *datasets* di grandi dimensioni, per cui l'allocazione giuridica della privativa è ancora a uno stadio di discussione, e, com'è ormai noto, non è la cosa consigliabile[1005].

---

[998] CGCE 6 aprile 1995, cause C-241/91 e C-242/91, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) c. Commissione.
[999] CGCE 26 novembre 1998 (Sesta Sezione), causa C-7/97, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG.
[1000] CGCE 26 aprile 2004 (Quinta Sezione), causa C-418/04, IMS Health GmbH & Co. OHG c. NDC Health GmbH & Co. KG.
[1001] CGCE 17 settembre 2007 (Grande Sezione), causa T-201/04, Microsoft Corp. v Commissione.
[1002] G. COLANGELO, *op. cit.*, 447-48.
[1003] Si vedano, più in particolare, S. MARCO COLINO, *Competition Law of the Eu and UK*, Oxford University Press, 2011, 440 ss.; R. WHISH – D. BAILEY, *Competition Law: Seventh Edition*, Oxford University Press, 2012, 798 ss.
[1004] Altro esempio di *standard* è la divisione del territorio in segmenti (*bricks*) utilizzata nel caso *IMS Health*. Per un'analisi approfondita sul caso *Microsoft*, si veda C. AHLBORN – D.S. EVANS, *The Microsoft Judgment and its Implications for Competition Policy towards Dominant Firms in Europe*, in 75(3) *Antitrust Law Journal*, 2009, 887 ss.
[1005] Come affermato *supra*, § 4, lo strumento flessibile della licenza è utilizzato anche in contesti in cui, pur non sussistendo un diritto di esclusiva su un bene, la parte voglia attribuire a un terzo i diritti di sfruttamento economico.

Si delineano diversi problemi per l'applicazione del principio degli scenari economici *data-driven*. Si pensi, per esempio, a un'impresa che svolge attività di analisi e vuole accedere ai dati raccolti e anonimizzati da una piattaforma digitale o ai dati non personali raccolti da un'impresa che raccoglie i dati prodotti da automobili *smart*. Anzitutto, vi sono numerosi dubbi che i *datasets* rispondano al criterio di essenzialità per competere nel mercato collegato (a valle). La presenza di numerosi agenti, quali i *data brokers* e le imprese dell'Industria 4.0, e l'economicità dell'acquisizione dei dati, che sono spesso generati come un sottoprodotto (*by-product*) di altre attività produttive, fanno propendere per una risposta negativa al quesito[1006]. In secondo luogo, come è stato opportunamente fatto notare, non si comprende come un concorrente possa ambire alla produzione di un nuovo prodotto per il quale richiede accesso ai dati controllati dall'impresa egemone «*if she cannot even begin to fathom what the new product may be until she had access to such data*»[1007]. In terzo luogo, non è chiaro se l'accesso debba essere garantito solo a una parte o alla totalità dei dati di cui l'impresa dominante dispone, e come l'accesso debba essere organizzato nel tempo (per esempio, in un momento determinato, in modo continuativo, in tempo reale[1008]?).

In conclusione, alla luce dell'analisi condotta, allo stato delle cose la dottrina delle infrastrutture essenziali pare difficilmente applicabile al fine di migliorare l'accesso ai *Big Data.*

7.2.2. Gli accordi di esclusiva fra le intese restrittive della concorrenza e l'abuso di posizione dominante

Negli scenari economici caratterizzati dall'utilizzo delle tecnologie dei *Big Data* e dell'Internet delle cose, si possono individuare accordi mediante i quali i

[1006] G. COLANGELO, *op. cit.*, 448.
[1007] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 6.
[1008] M. GAL, *op. cit.*, 22.

soggetti interessati pongono limiti all'accesso ai *datasets*. Come si è detto, tali accordi di esclusiva possono essere analizzati sia alla luce delle intese restrittive della concorrenza, sia dell'abuso di posizione dominante[1009].

La nozione di abuso di posizione dominante è già stata esaminata in precedenza[1010]. Riguardo alle intese anticoncorrenziali[1011], sussistono notevoli dubbi su come possano essere considerati il pregiudizio sensibile (alla luce del principio *de minimis* stabilito dalla Commissione[1012]) e il mercato rilevante[1013] ai fini dell'applicazione della norma.

Vi sono almeno due scenari riconducibili alla materia *de qua*, e, in particolare, al modello di *business* basati sui cc.dd. *product-service systems* (PSS), cioè *set* di prodotti e servizi che soddisfano congiuntamente i bisogni dell'utente[1014]. Com'è noto, grazie all'integrazione di *software* e sensori, gli oggetti dell'Internet delle Cose dispongono di ampie funzionalità. I sensori del dispositivo *smart* raccolgono dati, che sono successivamente archiviati e analizzati e, sulla base dei risultati dell'analisi, l'apparecchiatura modifica la sua funzionalità automaticamente mediante gli attuatori attivati da remoto; inoltre, i dati raccolti da una parte sono utili al funzionamento della macchina, dall'altra sono riutilizzabili per altri scopi. Si possono immaginare diversi scenari. Si pensi, per esempio[1015],

i. alle clausole contrattuali di esclusività inserite nei contratti di cessione dei dati;
ii. alle restrizioni contrattuali che proibiscono il c.d. *reverse engineering* da parte dell'utilizzatore del *software* in un oggetto dell'Internet delle Cose;

[1009] G. COLANGELO, *op. cit.*, 444; RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 4 e 7-8.
[1010] § 7.2.1.1.
[1011] Art. 101 TFUE.
[1012] Comunicazione relativa agli accordi di importanza minore che non determinano restrizioni sensibili della concorrenza ai sensi dell'articolo 101, paragrafo 1, del trattato sul funzionamento dell'Unione europea (comunicazione «de minimis»), G.U. n. 2014/C 291/01 del 30/08/2014.
[1013] Si rimanda alle considerazioni fatte *supra*, § 7.2.1.1, con la precisazione che «*sulla nozione in esame si sono consolidate prassi standardizzate di volta in volta appena corrette dagli adattamenti richiesti dallo specifico settore preso in considerazione*» (P. AUTERI ET AL., *op. cit.*, 455).
[1014] C. VAN HALEN ET AL., *Methodology for Product Service System Innovation*, Uitgeverij Van Gorcum, 2005, 21.
[1015] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 7.

iii. alle restrizioni inserite negli accordi contrattuali fra un soggetto controllore e un terzo concernenti il riuso dei *datasets*;

iv. alla restrizione della portabilità dei dati di un soggetto economico allorché decide di interrompere il rapporto con l'impresa che fornisce tali risorse e passare a un altro *provider*.

In queste ipotesi, nel caso in cui il compratore e il venditore stipulano un contratto, si configura la fattispecie dell'intesa anticoncorrenziale (verticale) se ai concorrenti è precluso l'accesso ai mercati della riparazione dell'oggetto *smart*, ovvero se le clausole contrattuali impediscono al compratore di condividere i dati prodotti dall'apparecchiatura in questione[1016]. Tuttavia, a ben vedere, negli accordi presi in esame non rileva tanto il contenuto dell'accordo, quanto la «*de facto position of the supplier, who may well be the only business in a position to provide the service (for "products as a service") and to distill information form the data gathered from the Thing*»[1017]. La fattispecie di abuso di posizione dominante rileva allorché si integrino le situazioni sopra descritte non in presenza di strumenti contrattuali, ma di misure tecniche e di controllo tecnologico *de facto* che, escludendo di fatto uno o più concorrenti dal mercato interessato, hanno effetti anticoncorrenziali. Tuttavia, come già fatto presente *supra*, le problematiche relative alla definizione del mercato rilevante ostano all'applicazione delle norme a tutela della concorrenza, e, in definitiva, rendono il diritto *antitrust* un campo non particolarmente adeguato a risolvere le questioni inerenti all'accesso ai *Big Data* allo stato delle cose.

7.3. Il diritto dei consumatori… a tutela delle imprese: la Direttiva 93/13/CEE

Nei casi in cui sia stipulato un contratto di fornitura di dati non personali (*data trading*), il soggetto economico dotato di maggiore potere contrattuale può esercitare un'influenza notevole nella conduzione delle trattative, imponendo clausole lesive dei diritti dell'altro contraente. Le norme inserite nella Direttiva

[1016] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 4.
[1017] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. loc. cit.*

93/13/CEE, che rispondono alla *ratio* di tutela dei consumatori, possono essere rilevanti per redistribuire il potere contrattuale fra le due parti negli scenari di sfruttamento dei *Big Data*, cioè, in particolare, riguardo ai contratti di fornitura di dati (non personali) acquisiti dagli oggetti dell'Internet delle Cose.

In particolare, ai sensi del par. I dell'art. 3 della Direttiva 93/13/CEE, «*una clausola contrattuale, che non è stata oggetto di negoziato individuale, si considera abusiva se, malgrado il requisito della buona fede, determina, a danno del consumatore, un significativo squilibrio dei diritti e degli obblighi delle parti derivanti dal* contratto»[1018]. L'applicazione della normativa ai contesti sopracitati desta talune problematiche di non facile risoluzione: da una parte, non sono previste linee guida nella valutazione delle clausole in materia di raccolta e utilizzo dei dati; dall'altra, il campo di applicazione della Direttiva 93/13/CEE è limitato ai soli rapporti fra le imprese e i consumatori (B2C[1019]).

Occorre notare che alcuni Stati membri dell'Unione hanno esteso la normativa anche alle relazioni fra più imprese (B2B[1020]): a ben vedere, i quattro scenari prospettati nel paragrafo precedente potrebbero essere risolti facendo ricorso a tali norme (per esempio mediante la previsione della nullità della clausola o del contratto). Tuttavia, l'assenza di armonizzazione implica una sostanziale incertezza del diritto, e postula la necessità di un'estensione da parte del legislatore sopra descritta anche ai contesti B2B in ogni Stato membro.

7.4. Prospettive *de iure condendo* e *policies*: vie d'uscita

Le soluzioni esistenti nell'ordinamento europeo non sono sufficienti a garantire un accesso diffuso ai *datasets*. In particolare, come si è visto, sia il diritto della concorrenza, sia la disciplina a tutela dei consumatori mostrano insufficienze difficilmente risolvibili ricorrendo alle norme e agli istituti attualmente disponibili. Inoltre, si pone una problematica ulteriore, che potenzialmente vanifica gli sforzi di

---

[1018] Direttiva 93/13/CEE del Consiglio del 5 aprile 1993 concernente le clausole abusive nei contratti stipulati con i consumatori, G.U. n. L. 095 del 21/04/1993.
[1019] J. DREXL, *op. cit.*, 56.
[1020] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 21.

garantire l'accesso: una volta che a un'impresa è consentito di accedere alle risorse digitali, essa non potrebbe comunque fruirne se i formati digitali dei *datasets* non sono compatibili con le tecnologie utilizzate. In altri termini, l'assenza di *standard* aperti dei formati e di interoperabilità dei sistemi pongono un limite ulteriore all'accessibilità dei dati[1021].

Occorre quindi vedere quali sono le vie d'uscita dalle carenze indicate nei paragrafi precedenti.

7.4.1. Le proposte della Commissione: norme dispositive e accesso dietro corrispettivo

La Commissione ha delineato una serie di approcci legislativi che possono migliorare l'accesso ai *datasets*[1022].

Una prima proposta prevede una serie di norme dispositive per le licenze dei *datasets*. Tali regole, potendo comunque essere facilmente derogate dalle parti[1023], difficilmente porterebbero ai risultati sperati.

In secondo luogo, come si è visto, consentire alle parti contraenti di "fare da sé" può comportare che quelle più forti impongano condizioni lesive dei diritti di quelle più deboli: se non si applicano correttivi al *laissez-faire* degli agenti economici, un ristretto numero di attori privati pone limiti all'accesso al patrimonio informativo a detrimento degli altri agenti economici[1024]. Dato che in numerosi casi il vantaggio concorrenziale di un soggetto economico è determinato non dal controllo sui dati in sé, ma da capacità di analisi più efficienti, secondo la Commissione si dovrebbe stabilire l'accesso dietro corrispettivo a certe tipologie di dati agli agenti economici che operano in un mercato diverso da quello del possessore dei

---

[1021] U. PAGALLO ET AL., *What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT*, in R. LEENES ET AL. (CUR.), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017, 74-76.
[1022] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 31 ss.
[1023] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 31-32.
[1024] Vedasi capitolo secondo.

datasets[1025] mediante la previsione di una licenza obbligatoria[1026], come è stato stabilito in alcuni interventi normativi europei di carattere settoriale[1027]. Gli operatori economici dovrebbero poter accedere a questi *datasets*, detti "dati comuni" (*data commons*[1028]), a condizioni eque, ragionevoli e non discriminatorie (*Fair, Reasonable And Non-Discriminatory*, FRAND[1029]), come è previsto per le licenze dei SEPs (*Standard Essential Patents*).

7.4.2. Il diritto di portabilità dei dati non personali

Il diritto di portabilità dei dati ha a che fare con la facoltà del titolare di disporne e trasferirli. Il Regolamento (UE) 2016/679 prevede che l'interessato abbia il diritto di portabilità dei dati personali, cioè di «*ricevere in un formato strutturato, di uso comune e leggibile da dispositivo*» o di «*trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti*»[1030]. Come si è detto nel precedente capitolo, la portabilità risponde a una fondamentale esigenza di tutela del consumatore, giacché consente di abbattere i costi di transizione (*switching costs*) e di diminuire gli effetti di *lock-in*[1031]: i consumatori possono passare da un servizio *online* offerto da un'impresa a

---

[1025] Questi soggetti, quindi, non sono concorrenti. «*Certain types of data could possibly be identified to which access to third parties can be given with welfare-enhancing effects without impinging on the economic interests of the player that has invested into the data collecting capabilities*» (COMMISSIONE EUROPEA*, Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 36 ss.).

[1026] COMMISSIONE EUROPEA*, Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 37-38.

[1027] Si vedano gli artt. 27 e 30 Regolamento 1907/2006 (CE) del Parlamento europeo e del Consiglio del 18 dicembre 2006 concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE, G.U. n. L. 396 del 30/12/2006, per i quali le imprese sono tenute a fornire l'accesso ai dati.

[1028] Occorre non confondere i dati comuni coi dati aperti (*open data*), sui quali si è detto a proposito delle autorità del settore pubblico: vedasi § 6.1 del capitolo secondo.

[1029] Y. MÉNIÈRE – N. THUMM, *Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept*, JRC Science and Policy Report, 2015.

[1030] Art. 20 par. I Regolamento (UE) 2016/679. Sul diritto di portabilità dei dati (personali) vedasi nello specifico § 4.3.3 del capitolo terzo.

[1031] Vedasi J. DREXL. *op. cit.*, 56-57. Per una definizione, si veda, in particolare, il § 3.4 del capitolo secondo.

uno simile fornito da un'altra anche se ciò non è espressamente previsto dalle condizioni contrattuali.

Il diritto secondario europeo non prescrive particolari obblighi che impongono un livello minimo di portabilità dei dati non personali. «*This is partly because the requirements for implementing data portability can be technically demanding and costly, as different providers of the same services may store data differently*»[1032]. Secondo la Commissione, ci sono ottime ragioni per estendere il diritto di portabilità anche ai dati non personali e alle relazioni contrattuali fra più imprese (*business to business*, B2B). In modo analogo a quanto accade per i consumatori, un'impresa che si avvale di un servizio offerto da un altro agente economico incontra notevoli costi di transizione al momento del cambiamento dell'operatore, se non è prevista la possibilità di trasferire i dati. Per esempio, «*a lock-in problem can* […] *arise with regard to industrial data where suppliers want to take data with them concerning the quality and longevity of their parts after the termination of the supply contract with the manufacturer of the final product*»[1033]. Nella prassi, le compagnie inseriscono clausole contrattuali che regolano (e spesso negano) la possibilità di trasferire i dati non personali a terzi, col rischio che gli attori privati più grandi impongano condizioni sfavorevoli alle imprese minori (PMI[1034]). Un diritto di portabilità dei dati non personali garantirebbe l'accesso al patrimonio informativo a un numero più elevato di soggetti, rafforzando la concorrenza sul mercato, e, nel contempo, non avrebbe gli effetti negativi di un diritto di esclusiva come quelli analizzati nei paragrafi precedenti.

La Commissione si è impegnata a promuovere un dibattito fra i diversi *stakeholders* sulla possibilità di estendere il diritto di portabilità ai dati non personali nei contratti riguardanti alcuni servizi *online*, tenendo conto degli effetti che una tale allocazione avrebbe sul mercato[1035].

[1032] Comunicazione della Commissione *Building a European Data Economy*, 2017, 12.
[1033] J. DREXL, *op. cit.*, 57.
[1034] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 47. Sul potere contrattuale asimmetrico, vedasi § 7.3.
[1035] COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 48-49.

7.4.3. Le nuove sfide del diritto della concorrenza

Nei paragrafi precedenti si è visto che il diritto *antitrust* mostra notevoli ristrettezze nella regolamentazione dell'accesso ai *datasets* e, in generale, nella risoluzione delle più ampie problematiche che derivano dallo sfruttamento dei *Big Data* e dell'insieme di tecnologie dell'Internet delle Cose[1036]. In particolare, per frenare la tendenza alla concentrazione del patrimonio digitale in capo a pochi soggetti, è necessario che il diritto della concorrenza si rinnovi su due fronti.

In primo luogo, finora pochi autori hanno indagato le problematiche relative all'identificazione della giurisdizione adeguata alla regolamentazione dell'accesso ai dati[1037]. Il diritto *antitrust*, sia al di là, sia al di qua dell'Atlantico, ha sviluppato una dimensione prevalentemente territoriale[1038]. Com'è noto, il fenomeno dei *Big Data* non conosce confini spaziali ed ha, perciò, un'entità globale. In un siffatto scenario, il livello dello sforzo regolatore dovrebbe collocarsi su un piano internazionale, o perlomeno le giurisdizioni dovrebbero coordinare i rimedi alla concentrazione del potere in capo a poche piattaforme digitali[1039]. I tentativi di sviluppo di un diritto della concorrenza su scala internazionale non hanno avuto molto successo nel passato, benché la scienza politica abbia offerto già da tempo numerosi contributi per il superamento della dimensione nazionale[1040]. Tuttavia, gli Stati potrebbero concertare un piano d'azione in sedi internazionali, quale l'Unione internazionale delle telecomunicazioni (*International Telecommunication Union*, ITU); inoltre, anche l'operato di organizzazioni non governative quale il *World Wide Web Consortium* (W3C) potrebbe rivelarsi utile ad affrontare adeguatamente le questioni della regolamentazione dell'accesso ai dati.

[1036] Si pensi, *inter alia*, alla discriminazione perfetta mediante prezzi personalizzati per i singoli consumatori (M. MAGGIOLINO, *Big Data e prezzi personalizzati*, in 23 *Concorrenza e mercato*, 2016, 95 ss.) e agli accordi collusivi sulla base del controllo dell'andamento del mercato mediante strumenti di *Big Data analytics* (G. COLANGELO, *op. cit.*, 449-50).
[1037] M.S. GAL, *op. cit.*, 22; D.L. RUBINFELD – M.S. GAL, *op. cit.*, 379 ss.; M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 11-12.
[1038] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 10. Negli Stati Uniti, per esempio, secondo la c.d. *effects doctrine*, i rimedi *antitrust* si estendono a imprese straniere solo se gli effetti economici della condotta anticoncorrenziale si verificano nel mercato interno (A. PARRISH, *The Effects Test: Extraterritoriality's Fifth Business*, in 61(5) *Vanderbilt Law Review*, 2008, 1455 ss.).
[1039] M.S. GAL, *op. cit.*, 22.
[1040] J. BRAITHWAITE – P. DRAHOS, *Global Business Regulation*, Cambridge University Press, 2000.

In secondo luogo, l'orientamento esclusivamente economico del diritto *antitrust*, basato sulle teorizzazioni della Scuola di Chicago[1041], che ha posto al centro dell'analisi dell'*antitrust* l'efficienza globale del sistema economico (o efficienza allocativa[1042]), limita notevolmente l'adeguatezza di questo campo del diritto alla materia *de qua*. Come si è già affermato, il potere detenuto dalle grandi piattaforme sopra menzionate non ha solamente una dimensione economica, ma anche una dimensione politica. Perciò, da una parte, il diritto della concorrenza deve recuperare un approccio multiruolo che consenta la gestione del potere economico per ragioni di sovranità, come avanzato dal Senatore Sherman nel discorso tenuto in occasione dell'approvazione della celebre legge che porta il suo nome[1043], e persegua il raggiungimento di un grado elevato di democrazia economica[1044]; dall'altra, deve tornare a promuovere «*la difesa dei contraenti più deboli, individuati sia nelle imprese di piccole-medie dimensioni* [quali le *startup* innovative]*, sia nei consumatori*»[1045]. In questo senso, l'utilizzo di rimedi a tutela dei consumatori per le finalità del diritto della concorrenza potrebbe rappresentare una buona soluzione[1046]; inoltre, lo sviluppo di *standard* tecnici aperti dei formati e dell'interoperabilità favorirebbe la diffusione dei *datasets* come beni comuni della conoscenza[1047], contrasterebbe la concentrazione delle risorse digitali nelle mani di pochi soggetti e promuoverebbe la decentralizzazione dei dati. Tuttavia, la questione rimane aperta – perché, a ben vedere, si è appena all'inizio di rivoluzione dell'informazione che trasformerà il mondo sempre più profondamente e porrà sfide sempre più complesse al diritto.

[1041] R. BORK, *The Antitrust Paradox*, Free Press, 1978.
[1042] P. AUTERI ET AL., *op. cit.*, 433.
[1043] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 3. Ci si riferisce chiaramente allo Sherman Act del 1890.
[1044] N. ABRIANI ET AL., *Diritto industriale*, in *Trattato di Diritto Commerciale*, diretto da G. COTTINO, Cedam, 2001, 529.
[1045] P. AUTERI ET AL., *op. loc. cit.*; G. AMATO, *Il potere e l'antitrust*, Il Mulino, 1998, 93.
[1046] M. RICOLFI, *IoT and the Ages of Antitrust*, *op. cit.*, 14 («*Empowering users, by helping them to overcome informational and power asymmetries* […] *may* […] *reduce the rate of lock-in and advance transparency, to the benefit of competitive openness*»).
[1047] C. HESS – E. OSTROM (CUR.), *Understanding Knowledge as a Commons*, MIT Press, 2007.

CONSIDERAZIONI FINALI

Nel presente lavoro, si è analizzata la questione dell'accesso ai *Big Data* da una prospettiva giuridico-economica.

Come si è potuto notare nel capitolo primo, i *Big Data* hanno una rilevanza fondamentale negli odierni scenari economici. In seguito, nel capitolo secondo, si è visto che talune barriere limitano l'entrata nei sottomercati dei *Big Data* corrispondenti ai diversi anelli della catena del valore di tali utilità (raccolta, archiviazione, analisi e uso). Tali barriere all'ingresso costituiscono limiti all'accesso alle risorse digitali, e sono di tipologia differente (tecnologica, giuridica ecc.). Fra quelle di natura tecnologica, si è visto che soprattutto le esternalità di rete, le economie di scala, di gamma e di velocità, i mercati multi-versante, i costi di transizione (*switching costs*) consentono a uno scarso numero di soggetti economici di raggiungere un notevole vantaggio competitivo determinato dalla concentrazione del potere informativo digitale[1048], che ha effetti negativi sul benessere sociale e sul funzionamento dei vari sottomercati dei *Big Data*. Ulteriori barriere di carattere giuridico, quali quelle relative alla sicurezza dei sistemi di immagazzinamento (che riguardano l'anello dell'archiviazione dei dati) e quelle inerenti a questioni di *privacy* informazionale e protezione dei dati personali (concernenti le fasi della raccolta, dell'analisi e dell'uso dei dati), sono state erette dal legislatore per perseguire determinate finalità sociali, quale la tutela degli interessi degli utenti-consumatori.

Nel capitolo terzo, i *Big Data* sono stati passati al vaglio della *privacy* informazionale e della protezione dei dati personali, che riguardano rispettivamente il versante americano e quello europeo. A differenza del primo, il legislatore europeo ha recentemente stabilito limiti sostanziali all'accesso ai *Big Data* da parte delle imprese e, nel contempo, ha arricchito il novero dei diritti degli interessati, rafforzando, fra gli altri, il diritto di accesso e il diritto alla cancellazione, nonché stabilendo un nuovo diritto alla portabilità dei dati personali. Si è dato conto, inoltre, dei

[1048] A. MANTELERO, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in 1 *Diritto dell'informazione e dell'informatica*, 2012, 135 ss.

recenti *trends* di commodificazione dei dati personali: benché nessuno dei due ordinamenti presi in esame riconosca un diritto di proprietà su tali utilità, negli Stati Uniti, da un lato, numerosi autori hanno proposto di considerare le informazioni personali al pari di *assets* strategici al fine di regolarizzare il mercato; nell'Unione europea, dall'altro, la protezione dei dati personali non può prescindere dal rango di diritto fondamentale almeno "sulla carta", anche se in alcune norme del Regolamento 679/2016 si ravvisano i germi di una tutela proprietaria. Le barriere giuridiche all'analisi dei dati personali, riguardanti le attività di utilizzo di algoritmi e sistemi di intelligenza artificiale, costituiscono una questione particolarmente spinosa. Un influente autore statunitense ha proposto di considerare le esternalità negative degli algoritmi alla stregua di immissioni (*nuisances*) di cui gli attori privati che utilizzano le tecniche di analisi dovrebbero farsi carico[1049]. Le considerazioni di politica legislativa non possono prescindere, ad avviso di chi scrive, da un così importante contributo. Nel versante europeo, si dibatte sulle esigenze di tutela dei gruppi di interessati formati sulla base dell'analisi dei dati personali (*group privacy*); inoltre, talune regole del Regolamento (UE) 2016/679 prevedono un diritto alla spiegazione del procedimento decisionale automatizzato.

Un ulteriore limite giuridico all'accesso ai *Big Data* discende dalle questioni di appartenenza inerenti ai dati non personali prodotti dai sensori degli oggetti dell'Internet delle Cose, come si è visto nel capitolo quarto (la c.d. *data ownership*). Giacché i regimi esistenti non garantiscono un'adeguata tutela ai *datasets* di ingenti dimensioni, secondo parte della dottrina europea è necessario istituire un nuovo diritto esclusivo su tali *assets*. Nondimeno, come si è ampiamente analizzato nel corso del capitolo, una siffatta allocazione giuridica non trova adeguate giustificazioni economiche. Anzi, la previsione di una privativa sui *datasets* finirebbe per rafforzare la posizione di potere (di mercato e politico) di poche piattaforme digitali (quali *Google*, *Amazon*, *Facebook* e *Apple*), basata attualmente sul controllo *de facto* di immensi patrimoni informativi digitali, e pregiudicherebbe l'accesso ai *newcomers* nei sottomercati dei *Big Data*. In questo scenario, occorre promuovere

[1049] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione), 1 ss.

azioni di decentramento delle risorse digitali. È preferibile, dunque, spostare l'attenzione sulla tematica della regolamentazione dell'accesso ai *datasets* mediante altri campi del diritto, quale lo strumentario dell'*antitrust* e la tutela dei consumatori, che però devono "reinventarsi" per raccogliere le sfide imposte dai *Big Data*. Particolarmente ragionevoli paiono le proposte della Commissione di estendere il diritto di portabilità ai dati non personali e prevedere un accesso dietro corrispettivo ai *datasets* mediante la concessione di una licenza obbligatoria a condizioni eque, ragionevoli e non discriminatorie (*Fair, Reasonable And Non-Discriminatory*, FRAND).

Come afferma opportunamente Michal Gal, «*we live in formative times*»[1050]. Al giurista sarà richiesto un compito difficile in futuro, che vada al di là della mera strategia dello struzzo e consenta di riconquistare gli orizzonti perduti: «*l'innovazione non guarderà indietro; sarà necessario capirne i nessi reali, come pure la loro ricaduta sul piano pratico-applicativo*»[1051].

[1050] M. GAL, *Competition and Innovation in the Digital Environment*, in G. COLANGELO – V. FALCE (CUR.), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Il Mulino, 2017, 11.
[1051] R. PARDOLESI, *Prefazione*, in G. COLANGELO – V. FALCE (CUR.), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Il Mulino, 2017, 10.

BIBLIOGRAFIA

Articoli, monografie, volumi collettanei e working papers

AARON R. ET AL., *Data Brokers In An Open Society*, Open Society Foundations Report, 2016.

ABRIANI N. ET AL., *Diritto industriale*, in *Trattato di Diritto Commerciale*, diretto da COTTINO G., Cedam, 2001.

AMATO G., *Il potere e l'antitrust*, Il Mulino, 1998.

ANDREJEVIC M., *iSpy: Surveillance and Power in the Interactive Era*, University Press of Kansas, 2007.

ANGIULI O. ET AL., *How to De-Identify Your Data. Balancing statistical accuracy and subject privacy in large social-science data sets*, in 13(8) *ACM Queue*, 2015, 1 ss.

APLIN T., *A Critical Evaluation of the Proposed EU Trade Secrets Directive*, King's College London Dickson Poon School of Law Legal Studies Research Paper n. 2014-25, 2014, 1 ss.

ARCIDIACONO D., *The Trade Secrets Directive in the International Legal Framework*, in 1(3) *European Papers*, 2016, 1073 ss.

ARMSTRONG M., *Competition in Two-Sided Markets*, in 37(3) *Rand Journal Of Economics*, 2006, 668 ss.

ARVIDSSON A. – BONINI T., *Valuing Audience Passions: From Smythe to Tarde*, in 18(2) *European Journal of Cultural Studies*, 2015, 158 ss.

AUTERI P. ET AL., *Diritto industriale: proprietà intellettuale e concorrenza*, Giappichelli, 2016.

BAGNOLI V., *The Big Data relevant market*, in *Concorrenza e Mercato*, 23, 2016, 73 ss.

BALGANESH S., *Quasi-property: like, but not quite property*, in 160 *University of Pennsylvania Law Review*, 2012, 1889 ss.

BALKIN J.M., *Information Fiduciaries and the First Amendment*, in 49(4) *U.C. Davis Law Review*, 2016, 1183 ss.

BALKIN J.M., *The Three Laws of Robotics in the Age of Big Data*, in 78 *Ohio State Law Journal*, 2017 (in corso di pubblicazione), 1 ss.

BARNEY D. ET AL. (CUR.), *The Participatory Condition in the digital age*, University of Minnesota Press, 2016.

BAUMAN Z. – LYON D., *Liquid Surveillance: A Conversation*, Polity Press, 2012.

BAYLES M.E., *Principles of Law: A Normative Analysis*, Springer, 1987.

BENKLER Y., *Degrees of Freedom, Dimensions of Power*, in 145 *Daedalus*, 2016, 18 ss.

BENKLER Y., *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, in 52 *Federal Communications Law Journal*, 2000, 561 ss.

BERGELSON V., *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, in 37 *University of California Davis Law Review*, 2003, 379 ss.

BESANKO D. – BRAEUTIGAM R.R., *Microeconomics*, Wiley & Sons, 2014.

BEVYERS E. ET AL. (CUR.), *Räume und Kulturen des Privaten*, Springer, 2017.

BINNS R., *Data protection impact assessments: a meta-regulatory approach*, in 7(1) *International Data Privacy Law*, 2017, 22 ss.

BLAIR R.D. – SOKOL D. (CUR.), *Cambridge Handbook of Antitrust, Intellectual Property and High Tech*, Cambridge University Press, in corso di pubblicazione.

BLOUSTEIN E.J., *Group privacy: The right to huddle*, in 8(2) *Rutgers Camden Law Journal*, 1977, 219 ss.

BORGHI M. – KARAPAPA S., *Contractual restrictions on lawful use of information: sole-source databases protected by the back door?*, in 37(8) European Intellectual Property Review, 2015, 505 ss.

BORK R., *The Antitrust Paradox*, Free Press, 1978.

BRAITHWAITE J. – DRAHOS P., *Global Business Regulation*, Cambridge University Press, 2000.

BRANDIMARTE L. ET AL., *Misplaced Confidences: Privacy and the Control Paradox*, in 4(3) *Social Psychological and Personality Science*, 2012, 340 ss.

BUZZACCHI C., *La politica europea per i Big Data e la logica del single market: prospettive di maggiore concorrenza?*, in 23 *Concorrenza e mercato*, 2016, 155 ss.

BOYD D. – CRAWFORD K., *Critical Questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon*, in 15(5) *Information, Communication & Society*, 2012, 662 ss.

BURRELL J., *How the machine 'thinks': Understanding opacity in machine learning algorithms*, in 3(1) *Big Data & Society*, 2016, 1 ss.

CALABRESI G. – MELAMED A.D., *Property Rules, Liability Rules and Inalienability: One View of the Cathedral*, in 85(6) *Harvard Law Review*, 1972, 1089 ss.

CASTELLS M., *The Information Age: Economy, Society and Culture. Volume I: The Rise of the Network Society*, Wiley Blackwell, 2010.

CASTELLS M., *The Information Age: Economy, Society and Culture. Volume II: The Power of Identity*, Wiley Blackwell, 2009.

CASTELLS M., *The Information Age: Economy, Society and Culture. Volume III: End of Millennium*, Wiley Blackwell, 2010.

CATE F.H. – MAYER-SCHÖNBERGER V., *Notice and consent in a world of Big Data*, in 3(2) *International Data Privacy Law*, 2013, 67 ss.

CAVANILLAS J.M. – CURRY E. – WAHLSTER W. (CUR.), *New Horizons for a Data-Driven Economy. A roadmap for Usage and Exploitation of Big Data in Europe*, Springer, 2016.

CHANDLER A.D., JR., *The Visible Hand. The Managerial Revolution in American Business*, Harvard University Press, 1977.

CHANDLER A.D., JR., *Scale and Scope. The Dynamics of Industrial Capitalism*, Harvard University Press, 1990.

CHEN H. – CHIANG R.H.L. – STOREY V.C., *Business Intelligence And Analytics: From Big Data To Big Impact*, in 36(4) *MIS Quaterly*, 2012, 1167.

CHEN M. ET AL., *Big Data: Related Technologies, Challenges and Future Prospects*, Springer, 2014.

COASE R.H., *The Nature of the Firm,* in 4(16) *Economica, New Series*, 1937, 386 ss.

COASE R.H., *The problem of social cost*, in 3 *Journal of Law & Economics*, 1960, 1 ss.

CODD E.F., *A Relational Model of Data for Large Shared Data Banks*, Addison Wesley, 1970.

COHEN J., *Examined Lives: Informational Privacy and the Subject as Object*, in 52(5) *Stanford Law Review*, 2000, 1373 ss.

COHEN J., *What Privacy is For*, in 126(4) *Harvard Law Review*, 2013, 1904 ss.

COLANGELO G., *Big Data, piattaforme digitali e antitrust*, in *Mercato concorrenza regole*, 3*,* 2016, 425 ss.

COLANGELO G. – FALCE V. (CUR.), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione*, Il Mulino, 2017.

COOLEY T., *A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract*, Callaghan, 1888.

COOTER R. – ULEN T., *Law & Economics*, Addison-Wesley, 2012.

CHRISTIAN B. – GRIFFITHS T., *Algorithms to live by*, William Collins, 2016.

CRAIN M., *The limits of transparency: Data brokers and commodification*, City University of New York (CUNY) Academic Works, 2017.

DAVENPORT T.H. – BECK J.C., *The Attention Economy: Understanding The New Currency Of Business*, Harvard Business School Press, 2001.

DAVIS K. – PATTERSON D., *Ethics of Big Data*, O'Reilly, 2012.

DAVISON M., *The Legal Protection of Databases*, Cambridge University Press, 2003.

DE FRANCESCHI A. (CUR.), *European Contract Law and the Digital Single Market: The Implications of the Digital Revolution*, Intersentia, 2016.

DE FRANCESCHI A. – LEHMANN M., *Data as Tradeable Commodity and New Measures for their Protection*, in 1(1) *Italian Law Journal*, 2015, 51 ss.

DE HERT P. – PAPAKOSTANTINOU V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*, in 28 *Computer Law & Security Review*, 2012, 130 ss.

DE MAURO A. ET AL., *A formal definition of Big Data based on its essential features*, in 65(3) *Library Review*, 2016, 122 ss.

DE MONTJOYE Y. ET AL., *Unique in the Crowd: The privacy bounds of human mobility*, in 3 *Scientific Reports*, 2013, 1 ss.

DERCLAYE E., *The Legal Protection of Databases: A Comparative Analysis*, Edward Elgar, 2008.

DOURISH P., *Algorithms and their others: Algorithmic culture in context*, in 3(2) *Big Data & Society*, 2016, 1 ss.

DRAHOS P. – BRAITHWAITE J., *Information Feudalism: Who Owns the Knowledge Economy?*, Earthscan Publications Ltd, 2002.

DREIER T., *Online and Its Effect on the "Goods" Versus "Services" Distinction*, in 44 *International Review of Intellectual Property and Competition Law*, 2013, 137 ss.

DREXL J., *Designing competitive markets for industrial data - Between Propertisation and Access*, Max Planck Institute for Innovation and Competition Research Paper n. 16-13, 2016, 1 ss.

DREXL J., *Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics*, Max Planck Institute for Innovation and Competition Research Paper n. 16-16, 2016, 1 ss.

DREXL J. ET AL., *Data Ownership and Accesso to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the*

Current European Debate, Max Planck Institute for Innovation and Competition Research Paper n. 16-10, 1 ss.

DREYFUSS R.C. – STRANDBURG K.J. (CUR.), *The Law And Theory Of Trade Secrecy: A Handbook of Contemporary Research*, Edward Elgar, 2011.

DUMBILL E., *Making sense of Big Data*, in 1(1) *Big Data*, 2013, 1 ss.

DURANTE M. e PAGALLO U. (CUR.), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, 2012.

DURHAM M.G. – KELLNER D.M., *Media and Cultural Studies: Keyworks*, Wiley-Blackwell, 1981.

ESTEVE A., *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in 7(1) *International Data Privacy Law*, 2017, 36 ss.

EVANS D., *Attention to Rivalry among Online Platforms and Its Implications for Antitrust Analysis*, Coase-Sandor Institute for Law & Economics Working Paper n. 627, 2013.

EVANS D. – SCHMALENSEE R., *Markets with Two-Sided Platforms*, in 1 *Issues In Competition Law And Policy*, 2008, 667.

FALCE V., *Trade Secret Protection in the Innovation Union. From the Italian approach to the UE solution*, in 4 *Mercato, concorrenza e regole*, 2013, 20 ss.

FARKAS T.J., *Data Created by the Internet of Things: The New Gold without Ownership*, in 23 *Revista La Propiedad Inmaterial*, 2017, 5 ss.

FERTIK M. – THOMPSON D., *The Reputation Economy. How To Optimise Your Digital Footprint In a World Where Your Reputation Is Your Most Valuable Asset*, Crown Business, 2015.

FLORIDI L., *Big Data and Their Epistemological Challenge*, in 25 *Philosophy and Technology*, 2012, 435 ss.

FLORIDI L., *The Ethics of Information*, Oxford University Press, 2013.

FLORIDI L. (CUR.), *Protection of Information and the Right to Privacy – A New Equilibrium?*, Springer, 2014.

FLORIDI L., *Open data, data protection, and group privacy*, in 27 *Philosophy and Technology*, 2014, 1 ss.

FLORIDI L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, 2014.

FORAY D., *L'economia della conoscenza*, Il Mulino, 2006.

FREEMAN J., *The Private Role in Public Governance*, in 75 *New York Law Review*, 2000, 543 ss.

FRIEDMAN D. ET AL., *Some Economics of Trade Secret Law*, in 5(1) *The Journal of Economic Perspectives*, 1991, 61 ss.

FRIEDMAN L.M., *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, in 30 *Hofstra Law Review*, 2002, 1093 ss.

FRIEDMAN L.M., *Guarding Life's Dark Secrets: Legal and Social Controls over Reputation, Propriety, and Privacy*, Stanford University Press, 2007.

FU W.W. ET AL., *The bandwagon effect on participation in and use of a social networking site*, in 17(5) *First Monday*, 2012 (www.firstmonday.org/ojs/index.php/fm/article/view/3971/3207#author, ultimo accesso 1° giugno 2017).

GAMBARO A., *Dai beni immobili ai beni virtuali*, in *Enciclopedia Treccani* (http://www.treccani.it/enciclopedia/dai-beni-immobili-ai-beni-virtuali_%28XXI-Secolo%29/, ultimo accesso 30 agosto 2017).

GAMBARO A., *Trattato dei diritti reali. Volume 1: proprietà e possesso*, Giuffrè, 2011.

GAVAZZI G., *Norme primarie e norme secondarie*, Giappichelli, 1967.

GELLMAN R., *Fair Information Practices: A Basic History*, in *SSRN Library*, 2017 (http://ssrn.com/abstract=2415020, ultimo accesso 18 luglio 2017).

GILBERT MILLER H. – MORK P., *From Data to Decisions: A Value Chain for Big Data*, in 15(1) IT Professional, 2013, 57 ss.

GITELMAN L. (CUR.), *"Raw Data" is an Oxymoron*, MIT Press, 2013.

GOODMAN B., *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*, 29th Conference on Neural Information Processing Systems Paper, 2016.

GOODMAN B. – FLAXMAN S., *European Union regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine*, 2017, in corso di pubblicazione.

GORZ A., *L'immateriale: Conoscenza, Valore e Capitale*, Bollati Boringhieri, 2003.

GRAEF I., *Market definition and market power in data: the case of online platforms*, in 38(4) *World Competition Law and Economics*, 2015, 473 ss.

GRAF VON DER SCHULENBURG J.M. – SKOGH G., *Law and economics and the economics of legal regulation*, Kluwer, 1986.

GRANT R.M., *Toward a knowledge-based theory of the firm*, in 17 *Strategic Management Journal*, 109 ss.

GRECO P., *I diritti sui beni immateriali*, Utet Giuridica, 1948.

GREENBERGER M. (CUR.), *Computers, Communications, And The Public Interest*, John Hopkins Press, 1971.

GRUNES A. - STUCKE M.E., *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, in *The Antitrust Source*, 2015, 1 ss.

GUEST A.G. (CUR.), *Oxford Essays in Jurisprudence*, Oxford University Press, 1961.

GURIN J., *Big Data and Open Data: How Open Will the Future Be?*, in 10 *Journal of Law and Policy for the Information Society*, 2014/2015, 691 ss.

HARDIN G., *The Tragedy of the Commons*, in 162 *Science*, 1968, 1243 ss.

HEGEL G.W.F., *Lineamenti di filosofia del diritto*, Bompiani, 2006.

HELLER M., *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, in 111(3) *Harvard Law Review*, 1998, 621 ss.

HESS C. – OSTROM E. (CUR.), *Understanding Knowledge as a Commons*, MIT Press, 2007.

HILDEBRANDT M. – DE VRIES K. (CUR.), *Privacy, Due Process and the Computational Turn-Philosophers of Law Meet Philosophers of Technology*, Routledge, 2013.

HILL R.K., *What an Algorithm Is*, in 29(1) *Philosophy & Technology*, 2016, 35 ss.

HOOFNAGLE C. – WHITTINGTON J., *Free Accounting for the Costs of the Internet's Most Popular Price*, in 61 *UCLA Law Review*, 2014, 606 ss.

HOSNI H. – VULPIANI A., *Forecasting in Light of Big Data*, in *Philosophy & Technology*, 2017, 1 ss.

HOWARD P., *Pax Technica. How the Internet of Things May Set Us Free or Lock Us Up*, Yale University Press, 2015.

HULL G., *Digital Copyright and the Possibility of Pure Law*, in 14 *Qui Parle*, 2003, 21 ss.

JAMES W., *The Principles of Psychology*, Henry Holt and Company, 1890.

KAYE L., *The proposed EU Directive for the legal protection of databases: a cornerstone of the information society?*, in 12 *European Intellectual Property Review*, 1996, 583 ss.

KERBER W., *Governance of Data: Exclusive Property vs. Access*, in 47 *IIC International Review of Intellectual Property and Competition Law*, 2016, 759 ss.

KERBER W., *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, Macie Discussion Paper n. 3-2016, 2016, 1 ss.

KERBER W., *Exhaustion of Digital Goods: An Economic Perspective*, Macie Discussion Paper n. 23-2016, 2016, 1 ss.

KIRKPATRICK D., *The Facebook effect*, Simon & Schuster, 2010.

KLIAZOVICH D. ET AL., *GreenCloud: a packet-level simulator of energy-aware cloud computing data centers*, in 3 *Journal of Supercomputing*, 2010, 1263 ss.

KLIESEN K.L. – MCCRACKEN M.W., *Tracking the U.S. Economy with Nowcasts*, in *The Regional Economist*, 2016.

KLIMAS T. – VAICIUKAITE J., *The Law of Recitals in European Community Legislation*, in 15 *ILSA Journal of International & Comparative Law*, 2008, 32 ss.

KOOMEY J.K., *Worldwide electricity used in data centers*, in 3(3) *Environmental Research Letters*, 2008, 1 ss.

KOOPS B.J., *Forgetting footprints, shunning shadows. A critical analysis of the "right to be forgotten" in Big Data practice*, in 8(3) *SCRIPTed*, 2011, 229 ss.

KOSINSKI M. ET AL., *Private traits and attributes are predictable from digital records of human behavior*, in 110(15) *PNAS*, 2013, 5802 ss.

KROLL J.A. ET AL., *Accountable Algorithms*, in 165 *University of Pennsylvania Law Review*, 2017, 633 ss.

KUEMPEL A., *The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry*, in 36(1) Northwestern Journal of International Law & Business, 2016, 207 ss.

LANDES W. – POSNER R., *The Economic Structure of Intellectual Property Law*, Harvard University Press, 2003.

LEENES R. ET AL. (CUR.), *Data Protection and Privacy: (In)visibilities and Infrastructures*, Springer, 2017.

LEMLEY M., *Private Property*, in 52(5) *Stanford Law Review*, 2000, 1545 ss.

LEMLEY M., *Property, Intellectual Property, and Free Riding*, John M. Olin Program in Law and Economics Working Paper n. 291, 2004, 1 ss.

LEMLEY M., *The Surprising Virtues of Treating Trade Secrets as IP rights*, in 61(2) *Stanford Law Review*, 2008, 311 ss.

LEMLEY M., *IP In a World Without Scarcity*, in 90(2) *New York University Law Review*, 2015, 460 ss.

LERNER A., *The Role of "Big Data" in Online Platform Competition*, in *Online Platform Competition*, SSRN library, 2014, 20 ss. (www.papers.ssrn.com/sol3/papers.cfm?abstract_id=2482780, ultimo accesso 3 giugno 2017).

LESSIG L., *Code and Other Laws of the Cyberspace*, Basic Books, 1999.

LESSIG L., *The Architecture of Privacy*, in 1 *Vanderbilt Entertainment Law and Practice*, 1999, 56 ss.

LESSIG L., *Privacy as Property*, in 69(1) *Social Research*, 2002, 247 ss.

LÉVÊQUE F. – MÉNIÈRE Y., *The Economics of Patents and Copyright*, Berkeley University Press, 2004.

LÉVÊQUE F. – SHELANSKI H. (CUR.), *Antitrust, Patents and Copyright: EU and US Perspectives*, Edward Elgar, 2005.

LITMAN J., *Information Privacy/Information Property*, in 52(5) *Stanford Law Review*, 2000, 1283 ss.

LOBEL O., *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, in 89 *Minnesota Law Review*, 2004, 342 ss.

LOOS M., *The Regulation of Digital Content B2C Contracts in CESL*, Centre for the Study of European Contract Law Working Paper Series n. 2013-10, 2013.

LUNDQVIST B., *"Turning Government Data Into Gold": The Interface Between EU Competition Law and the Public Sector Information Directive—With Some Comments on the Compass Case*, in 44 *IIC International Review of Intellectual Property and Competition Law*, 2011, 79 ss.

LUNDQVIST B., *Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. The Issue of Accessing Data*, Faculty of Law, University of Stockholm Research Paper n. 1, 2016.

LYCETT M., *"Datafication": making sense of (big) data in a complex world*, in 22(4) *European Journal of Information Systems*, 381 ss.

LYON D., *Surveillance Studies: An Overview*, Polity Press, 2007.

LYON D., *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*, in *Big Data and Society*, 2014, 1 ss.

MACNISH K.N.J., *Unblinking Eyes: The Ethics of Automated Surveillance*, in 14(2) *Ethics and Information Technology*, 2012, 151 ss.

MAGGIOLINO M., *Big Data e prezzi personalizzati*, in 23 *Concorrenza e mercato*, 2016, 95 ss.

MALGIERI G., *Trade Secrets v Personal Data: a possible solution for balancing rights*, in 6(2) *International Data Privacy Law*, 2016, 102 ss.

MANTELERO A., Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in 1 *Diritto dell'informazione e dell'informatica*, 2012, 135 ss.

MANTELERO A., *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in 32 *Computer Law & Security Review*, 2016, 238 ss.

MATTEI U., *Il modello di Common Law*, Giappichelli, 2014.

MATTEI U., *La proprietà*, in *Trattato di diritto privato*, diretto da SACCO R., 2ª ed., UTET Giuridica, 2015.

MATTIOLI M., *Disclosing Big Data*, in 99 *Minnesota Law Review*, 2014, 535 ss.

MAYER-SCHÖNBERGER V., *Delete: The virtue of forgetting in the digital age*, Princeton University Press, 2009.

MAYER-SCHÖNBERGER V. – CUKIER K., *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013.

MAYER-SCHÖNBERGER V. – PADOVA Y., *Regime Change? Enabling Big Data through Europe's new Data Protection Regulation*, in 17 *Columbia Science & Technology Law Review*, 2016, 315 ss.

MAZZIOTTI G., *EU Digital Copyright Law and the End-User*, Springer, 2008.

MCDONALD A.M. – CRANOR L.F., *The Cost of Reading Privacy Policies*, in *I/S: A Journal of Law and Policy for the Information Society*, 2008, 543 ss.

MCGUIGAN L. – MANZEROLLE V. (CUR.), *The Audience Commodity in a Digital Age: Revisiting a Critical Theory of Commercial Media*, Peter Lang, 2014.

MEHRA S.K., *Competition Law for a Post-Scarcity World*, in 4 *Texas A&M Law Review*, 2016, 1 ss.

MÉNIÈRE Y. – THUMM N., *Fair, Reasonable and Non-Discriminatory (FRAND) Licensing Terms. Research Analysis of a Controversial Concept*, JRC Science and Policy Report, 2015.

MICKLITZ N.W. – REICH N., *The Commission Proposal for a 'Regulation on a Common European Sales Law (CESL)' – Too Broad or Not Broad Enough?*, EUI Working Papers LAW n. 2012/04, 2012.

MIGLIETTI L., *Profili storico-comparativi del diritto alla privacy*, in *Rivista di diritti comparati*, 2014 (www.dirittocomparati.it/profili-storico-comparativi-del-diritto-alla-privacy, ultimo accesso 14 luglio 2017).

MYŠKA M. – HARAŠTA J., *Less is more? Protecting Databases in the EU After Ryanair*, in 10(2) *Masaryk University Journal of Law and Technology*, 2016, 170 ss.

MITTELSTADT B.D., *Auditing for Transparency in Content Personalization Systems*, in 10 *International Journal of Communication*, 2016, 12 ss.

MITTELSTADT B.D. ET AL., *The ethics of algorithms: Mapping the debate*, in 3(1) *Big Data & Society*, 2016, 3 ss.

MOLINO J.L. – SEDKAOUI S., *Big Data, Open Data and Data Development*, ISTE Ltd. and Wiley & Sons, 2016.

MUNZER S., *A Theory of Property*, Cambridge University Press, 1990.

MUNZER S. (CUR.), *New Essays in the Legal and Political Theory of Property*, Cambridge Studies in Philosophy and Law, 2001.

MURPHY R.S., *Property Rights in Personal Information: An Economic Defence of Privacy*, in 83 *Georgetown Law Journal*, 1995, 2381 ss.

NELSON R.R. (CUR.), *The Rate and Direction of Inventive Activity: Economic and Social Factors*, Princeton University Press, 1962.

NEWMAN J.M., *Antitrust in zero-price markets: Foundations*, in 164(1) *University of Pennsylvania Law Review*, 2015, 149 ss.

NEWMAN N., *Search, Antitrust and the Economics of the Control of User Data*, in 30(3) *Yale Journal on Regulation*, 2014, 1 ss.

NICITA A. ET AL., *Le opzioni nel mercato delle regole*, SIDE Working Paper, 2005.

NORDHAUS W.D., *Productivity growth and the new economy*, Brookings Papers on Economic Activity, 2002, 221 ss.

NOTO LA DIEGA G., *Software Patents and the Internet of Things in Europe, the United States and India*, in 39(3) *European Intellectual Property Review*, 2017, 173 ss.

O'BRIEN D., *The Right of Privacy*, in 2 *Columbia Law Review*, 1902, 437 ss.

OHLHORST F., *Big Data Analytics. Turning Big Data Into Big Money*, John Wiley & Sons, 2013.

OHM P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in 57 *UCLA Law Review*, 2010, 1701 ss.

OREFICE M., *I Big Data. Regole e concorrenza*, in 4 *Politica del diritto*, 2016, 697 ss.

OSTROM E., *Governing the Commons. The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990.

PAEZ M. – LA MARCA M., *The Internet Of Things: Emerging Legal Issues For Businesses*, in 43 *Northern Kentucky Law Review*, 2016, 29 ss.

PAGALLO U., *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, 2014.

PAGALLO U., *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in 1 *European Data Protection Law Review*, 2017, 36 ss.

PAGALLO U., *Algo-Rhythms and the Beat of the Legal Drum*, in *Philosophy & Technology*, 2017.

PARRISH A., *The Effects Test: Extraterritoriality's Fifth Business*, in 61(5) *Vanderbilt Law Review*, 2008, 1455 ss.

PASQUALE F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.

PAVOLOTSKY J., *Privacy in the age of Big Data*, in 69 *The Business Lawyer*, 2013, 217 ss.

PENNER J.E., *The "Bundle of Rights" Picture of Property*, in 43 *UCLA Law Review*, 1996, 711 ss.

PERZANOWSKI A. – SCHULTZ J., *Legislating Digital Exhaustion*, in 29 *Berkeley Technology Law Journal*, 2014, 1535 ss.

PITRUZZELLA G., *Big Data, Competition and Privacy: A Look from the Antitrust Perspective*, in 23 *Concorrenza e mercato*, 2016, 15 ss.

PORTER M. E., *Competitive Advantage: creating and sustaining superior Performance*, Free Press, 1985.

POUND R., *Interests of Personality*, in 28 *Harvard Law Review*, 1915, 343 ss.

PROSSER W.L., *Handbook on the Law of Torts*, West Pub. Co., 1941.

PROSSER W.L., *Privacy*, in 48 *California Law Review*, 1960, 383 ss.

PURTOVA N.N., *Property rights in personal data: Learning from the American discourse*, in 25(6) *Computer Law and Security Review*, 2009, 507 ss.

PURTOVA N.N., *Property rights in personal data: A European perspective*, BOXPress BV, 2011.

RADIN M.J., *Property and Personhood*, in 34 *Stanford Law Review*, 1982, 957 ss.

RATLIFF J. – RUBINFELD D., *Is there a market for organic search engine results and can their manipulation give rise to antitrust liability?*, in 10(3) *Journal of Competition Law and Economics*, 2014, 517 ss.

RAYPORT J.F.– SVIOKLA J.J., *Exploiting the virtual value chain*, in *Harvard Business Review*, 1995, 73 ss.

REICHMAN J.H. – SAMUELSON P., *Intellectual Property Rights in Data?*, in 50 *Vanderbilt Law Review*, 1997, 51 ss.

RESTA G. (CUR.), *Diritti esclusivi e nuovi beni immateriali*, Utet Giuridica, 2011.

RICH M.L., *Machine Learning, Automated Suspicion Algorithms, And The Fourth Amendment*, in 164 *University of Pennsylvania Law Review*, 2016, 871 ss.

RICHARDS N.M., *Intellectual Privacy*, in 87 *Texas Law Review*, 2008, 387 ss.

RICHARDS N.M., *The Limits of Tort Privacy*, in 9 *Journal of Telecommunications and High Technology Law*, 2011, 357 ss.

RICHARDS N.M., *The Dangers of Surveillance*, in 126(7) *Harvard Law Review*, 2013, 1934 ss.

RICHARDS N.M. – KING J., *Big Data Ethics*, in 49(2) *Wake Forest Law Review*, 2014, 393 ss.

RICHARDS N.M. – SOLOVE D.J., *Prosser's Privacy Law: A Mixed Legacy*, in 98 *California Law Review*, 2010, 1887 ss.

RICŒUR P., *La marque du passé*, in 1 *Revue de Métaphysique et de Morale*, 1998, 7 ss.

RICOLFI M., *Beyond Intellectual Property: the Perils of Abundance*, paper inedito fornito dall'autore, 2017.

RICOLFI M., *IoT and the Ages of Antitrust*, paper inedito fornito dall'autore, 2017.

RIFKIN J., *L'era dell'accesso, La rivoluzione della new economy*, Mondadori, 2000.

RIFKIN J., *Società a costo marginale zero*, Mondadori, 2014.

ROCHET J.C. – TIROLE J., *Platform Competition in Two-Sided Markets*, in 1 *Journal of European Economic Association*, 2003, 990 ss.

RODOTÀ S., *Intervista su privacy e libertà*, Laterza, 2005.

ROESSLER B. – MOKROSINSKA D. (CUR.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, Cambridge University Press, 2015.

ROSE C.M., *Romans, Roads, and Romantic Creators: Traditions of Public Property in the Information Age*, in 66 *Law & Contemporary Problems*, 2003, 89 ss.

ROSE-ACKERMAN S., *Inalienability and the Theory of Property Rights*, in 85 *Columbia Law Review*, 1985, 931 ss.

ROSEN J., *The right to be forgotten*, in 64 *Stanford Law Review Online*, 2012, 88 ss.

RUBINFELD D.L. – GAL M.S., *Access Barriers to Big Data*, in 59 *Arizona Law Review*, 2017, 339 ss.

RUBINSTEIN I., *Big Data: The End of Privacy or a New Beginning?*, in 3(2) *International Data Privacy Law*, 2013.

RULLANI E., *Le capitalisme cognitif: du déjà vu?*, in 2 *Multitudes*, 2000, 87 ss.

RYSMAN M., *The Economics of Two-sided Markets*, in 23(3) *Journal Of Economic Perspectives*, 2009, 125 ss.

SACCO R., *Introduzione al diritto comparato*, UTET Giuridica, 1992.

SAMUELSON P., *Privacy as Intellectual Property*, in 52(5) *Stanford Law Review*, 2000, 1125 ss.

SARTOR G., *The right to be forgotten in the Draft Data Protection Regulation*, in 5 *International Data Privacy Law*, 2015, 64 ss.

SARTOR G., *The right to be forgotten: balancing interests in the flux of time*, in 24 *International Journal of Law and Information Technology*, 2016, 72 ss.

SARTORE F., *Big Data: Privacy and Intellectual Property in a Comparative Perspective*, Trento Law and Technology Research Group Student Paper n. 26, 2016, 1 ss.

SAVIČ M., *The Legality of Resale of Digital Content after UsedSoft in Subsequent German and CJEU Case Law*, in 37(7) *European Intellectual Property Review*, 2015, 414 ss.

SCHEPP N.P. – WAMBACH A., *On Big Data and Its Relevance for Market Power Assessment*, in 7(2) *Journal of European Competition & Practice*, 2016, 120 ss.

SCHOLZ L., *Privacy as Quasi-Property*, in 101 *Iowa Law Review*, 2016, 1113 ss.

SCHWARTZ P.M., *Property, Privacy, and Personal Data*, in 117(7) *Harvard Law Review*, 2004, 2055 ss.

SCHWARTZ P.M., *The EU-U.S. privacy collision: A turn to institutions and procedures*, in 126 *Harvard Law Review*, 2013, 1966 ss.

SCHWARTZ P.M. – JANGER E.J., *Notification of data security breaches*, in 105 *Michigan Law Review*, 2007, 913 ss.

SCHWARTZ P.M. – SOLOVE D., *Reworking Information Privacy Law: A Memorandum Regarding Future ALI Projects About Information Privacy Law*, 2012.

SHELANSKI H., *Information, innovation, and competition policy for the Internet*, in 161(6) *University of Pennsylvania Law Review*, 2013, 1663 ss.

SHORT J.L., *The Paranoid Style in Regulatory Reform*, in 63 *Hastings Law Journal*, 2012, 633 ss.

SMITH E.E. – KOSSLYN S.M., *Cognitive Psychology: Mind And Brain*, Pearson, 2007.

SMYTHE D.W., *Communications: Blindspot of Western Marxism*, in 1(3) *CTheory*, 1977, 1 ss.

SOLOVE D.J., *A Taxonomy of Privacy*, in 154(3) *University of Pennsylvania Law Review*, 2006, 477 ss.

SOLOVE D.J., *Understanding Privacy*, Harvard University Press, 2008.

SOLOVE D.J., *Introduction: Privacy Self-Management and the Consent Dilemma*, in 126 *Harvard Law Review*, 2013, 1880 ss.

SOLOVE D.J. – RICHARDS N.M., *Privacy's Other Path: Recovering the Law of Confidentiality*, in 96 *Georgetown Law Journal*, 2007, 123 ss.

SOLOVE D.J. – SCHWARTZ P.M., *Information Privacy Law*, Wolters Kluwer, 2015.

SPADA P., *Conclusioni al Convegno su "IP e Costituzioni" organizzato presso l'Università di Pavia il 23 e 24 settembre 2005*, in *AIDA*, 2005.

SPIEKERMANN S. ET AL., *The challenges of personal data markets and privacy*, in 25 *Electronic Markets*, 2015, 161 ss.

STALLA-BOURDILLON S. – KNIGHT A., *Anonymous data v. Personal data–A false debate: An EU perspective on anonymisation, pseudonymisation and personal data*, in *Wisconsin International Law Review*, 2017 (in corso di pubblicazione).

STAMATOUDI I., *The EU Databases Directive: Reconceptualising Copyright and Tracing the Future of the Sui Generis Right*, in 50 *Revue hellénique de droit international*, 1997, 435 ss.

STIGLITZ J. ET AL., *The role of government in the digital age*, Report commissionato dalla *Computer & Communications Association*, 2000, 1 ss.

STOUT L., *The shareholder value myth: how putting shareholders first harms investors, corporations, and the public*, Berrett-Koehler Publisher, 2012.

STRAHILEVITZ L., *Toward a Positive Theory of Privacy Law*, in 126 *Harvard Law Review*, 2013, 2010 ss.

STUCKE M.E. – GRUNES A.P., *Big Data and Competition Policy*, Oxford University Press, 2016.

SURBLYTĖ G., *The Refusal to Disclose Trade Secrets as an Abuse of Market Dominance – Microsoft and Beyond*, Stämpfli, 2011.

SURBLYTĖ G., *Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy*, Max Planck Institute for Innovation and Competition Research Paper n. 16-03, 2016, 1 ss.

SURBLYTĖ G., *Data As a Digital Resource*, Max Planck Institute for Innovation and Competition Research Paper n. 16-12, 2016, 1 ss.

SUTHAHARAN S., *Big Data classification: problems and challenges in network intrusion prediction with machine learning*, in 41(4) *Performance Evaluation Review*, 2014, 70 ss.

TANG C., *The Data Industry. The Business and Economics of Information and Big Data*, Wiley & Sons, 2016.

TAPSCOTT D., *The Digital Economy: Promise and Peril In The Age of Networked Intelligence*, McGraw-Hill, 1994.

TAVANI H.T., *Philosophical theories of privacy: implications for an adequate online privacy policy*, in 38 *Metaphilosophy*, 2007, 1 ss.

TAYLOR L. ET AL. (CUR.), *Group Privacy: New Challenges of Data Technologies*, Springer, 2017.

TENE O. – POLONETSKY J., *Big Data for all: Privacy and user control in the age of analytics*, in 11(5) *Northwestern Journal of Technology and Intellectual Property*, 2013, 240 ss.

TORREMANS P.L.C., *Holyoak & Torremans Intellectual Property Law*, Oxford University Press, 2014.

TORREMANS P.L.C., *The Future Implications of the Usedsoft Decision*, CREATe Working Paper n. 2014/2, 2014.

TUCKER D.S. – WELLFORD H.B., *Big Mistakes Regarding Big Data*, in *The Antitrust Source*, 2014, 1 ss.

UBALDI B., *Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives*, OCSE Working Paper on Public Governance, 2013.

UBERTAZZI L.C., *Introduzione al diritto europeo della proprietà intellettuale*, in *Contratto e impresa/Europa*, 2003, 1054 ss.

VAN ALSENOY B., *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, in 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2016, 271 ss.

VAN DER SLOOT B. – VAN SCHENDEL S., *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, in 7 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2016, 110 ss.

VAN DIJCK J., *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in 12 *Surveillance and Society*, 2014, 197 ss.

VAN HALEN ET AL., *Methodology for Product Service System Innovation*, Uitgeverij Van Gorcum, 2005.

VICTOR J.M., *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, in 123(2) *Yale Law Journal*, 2013, 513 ss.

VLADECK D.C., *Charting the Course: The Federal Trade Commission's Second Hundred Years*, in 83 *George Washington Law Review*, 2015, 2101 ss.

WACHTER S. ET AL., *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*, in 7(2) *International Data Privacy Law*, 2017, 76 ss.

WALKER G. – WEBER D., *A Transaction Cost Approach to Make-or-Buy Decisions*, in 29(3) *Administrative Science Quarterly*, 1984, 373 ss.

WARREN S. – BRANDEIS L., *The Right to Privacy*, in 4(5) *Harvard Law Review*, 1890, 193 ss.

WEBER R.H., *The Right to Be Forgotten: More than a Pandora's Box?*, in 2 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2011, 120 ss.

WEBER WALLER S. – TASCH W., *Harmonizing Essential Facilities*, in 76(3) *Antitrust Law Journal*, 2010, 741 ss.

WEISER M., *Hot Topics - Ubiquitous Computing*, in 10 *Computer*, 1993, 71 ss.

WHITE G.E., *Tort Law in America: An Intellectual History*, Oxford University Press, 2003.

WIEBE A., *Protection of industrial data – a new property right for the digital economy?*, in 12(1) *Journal of Intellectual Property Law & Practice*, 2017, 62 ss.

WILLIAMSON O.E., *Markets and Hierarchies: Analysis and Antitrust Implications*, Free Press, 1975.

WU T., *Attention Markets and the Law*, in *SSRN Library*, 2017 (http://ssrn.com/abstract=2941094, ultimo accesso 27 giugno 2017).

YU P.K. (CUR.), *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age*, Praeger, 2007.

ZECH H., *Information as Property*, in 6 *Journal Of Intellectual Property, Information Technology And E-Commerce Law*, 2015, 192 ss.

ZECH H., *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, in 11 *Journal of Intellectual Property Law & Practice*, 2016, 460 ss.

ZECH H., *Building a European Data Economy*, in 48 *IIC International Review of Intellectual Property and Competition Law*, 2017, 501 ss.

Documenti

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, 2014.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on the right to data portability*, 2017.

AUTORITAT CATALANA DE LA COMPETÈNCIA, *The Data-Driven Economy. Challenges for Competition*, 2016.

AUTORITÉ DE LA CONCURRENCE – BUNDESKARTELLAMT, *Competition Law and Data*, 2015.

CAPGEMINI CONSULTING, *The Open Data Economy Unlocking Economic Value by Opening Government and Public Data*, 2013.

CENTRE FOR INFORMATION POLICY LEADERSHIP, *Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL GDPR Interpretation and Implementation Project*, 2016 (http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf, ultimo accesso 19 giugno 2017).

COMMISSIONE EUROPEA, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, 2011.

COMMISSIONE EUROPEA, *Commission Staff Working Document Impact Assessment Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 2013.

COMMISSIONE EUROPEA, *Roadmap for completing the Digital Single Market*, 2015 (http://ec.europa.eu/commission/sites/beta-political/files/roadmap_en.pdf, ultimo accesso 12 agosto 2017).

COMMISSIONE EUROPEA, *Special Eurobarometer 431: Data Protection Report*, 2015.

COMMISSIONE EUROPEA, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017.

COMPETITION AND MARKETS AUTHORITY, *The Commercial Use of Consumer Data*, 2015.

DEMOS, *The Data Dialogue*, 2012 (www.demos.co.uk/files/The_Data_Dialogue.pdf?1347544233, ultimo accesso 3 luglio 2017).

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion. Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, 2014.

FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change*, 2012.

FEDERAL TRADE COMMISSION, *Data Brokers: A Call For Transparency and Accountability*, 2014.

FEDERAL TRADE COMMISSION, *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, 2016.

IBM INSTITUTE FOR BUSINESS VALUE, *Analytics: The real-world use of Big Data. How innovative enterprises in the midmarket extract value from uncertain data*, 2013.

INDEPENDENT STRATEGY, *Global Markets: A short paper on everything*, 2015 (www.instrategy.com/download/Reports/A-short-paper-on-everything-231015.pdf, ultimo accesso 26 settembre 2017).

INFORMATION COMMISSIONER'S OFFICE, *Annual Track 2014*, 2014 (https://ico.org.uk/media/about-the-ico/documents/1043485/annual-track-september-2014-individuals.pdf, ultimo accesso 3 luglio 2017).

INFORMATION COMMISSIONER'S OFFICE, *Data Protection Rights: What the public want and what the public want from Data Protection Authorities*, 2015 (http://ico.org.uk/media/about-the-ico/documents/1431717/data-protection-rights-

what-the-public-want-and-what-the-public-want-from-data-protection-authorities.pdf, ultimo accesso 3 luglio 2017).

LANEY D., *3-D data management: controlling data volume, velocity and variety*, META Group Research Note, 2001.

MCKINSEY GLOBAL INSTITUTE, *The Internet of Things: Mapping the value beyond the hype*, 2015 (http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx, ultimo accesso 16 settembre 2017).

MELL P. – GRANCE T., *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology Special Publication 800-145, 2011 (http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, ultimo accesso 13 settembre 2017).

NEW VANTAGE PARTNERS, *Big Data Business Impact: Achieving Business Results through Innovation and Disruption*, 2017 (www.newvantage.com/wp-content/uploads/2017/01/Big-Data-Executive-Survey-2017-Executive-Summary.pdf, ultimo accesso 14 giugno 2017).

OCSE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

OCSE, *Recommendation for enhanced access and more effective use of Public Sector Information (PSI)*, 2008.

OCSE, *The OECD Privacy Framework*, 2013.

OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being: Interim Synthesis Report*, 2014.

OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being,* 2015.

OSBORNE CLARKE, *Legal study on Ownership and Access to Data*, Final Report prepared for the European Commission DG Communications Networks, Content & Technology, 2016.

PRIVACY INTERNATIONAL, *The global surveillance industry*, 2016.

ROYAL STATISTIC SOCIETY, *Public attitudes to the use and sharing of their data*, 2014 (www.statslife.org.uk/files/perceptions_of_data_privacy_charts_slides.pdf, ultimo accesso 3 luglio 2017).

STALLA-BOURDILLON S. ET AL., *Building The European Data Economy: Position Paper On The Proposal For A New Right In Non-Personal Data*, 2017.

UN GLOBAL PULSE, *Mining Indonesian Tweets to Understand Food Price Crises*, 2014 (http://www.unglobalpulse.org/sites/default/files/Global-Pulse-Mining-Indonesian-Tweets-Food-Price-Crises%20copy.pdf, ultimo accesso 18 settembre 2017).

UNITED STATES SENATE COMMITTEE COMMERCE, SCIENCE, AND TRANSPORTATION, OFFICE OF OVERSIGHT AND INVESTIGATIONS, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, 2013.

VICKERY G., *Review Of Recent Studies On Psi Re-Use And Related Market Developments*, *report* commissionato dalla Commissione europea, 2011.

WHITE HOUSE, *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*, 2012.

Diritto primario dell'Unione europea

Carta dei diritti fondamentali dell'Unione europea, G.U. n. C. 202 del 7/06/2016.

Trattato sull'Unione europea e trattato sul funzionamento dell'Unione europea (versione consolidata), G.U. n. C. 202 del 7/06/2016.

Diritto derivato dell'Unione europea

Direttiva 93/13/CEE del Consiglio del 5 aprile 1993 concernente le clausole abusive nei contratti stipulati con i consumatori, G.U. n. L. 095 del 21/04/1993.

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U. n. L. 281 del 23/11/1995.

Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, G.U. n. L. 077 del 27/03/1996.

Direttiva 2001/29/CE del Parlamento europeo e del Consiglio, del 22 maggio 2001, sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione, G.U. n. L. 167 del 22/06/2001.

Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico, G.U. n. L. 345 del 31/12/2003.

Direttiva 2006/116/CE del Parlamento Europeo e del Consiglio del 12 dicembre 2006 concernente la durata di protezione del diritto d'autore e di alcuni diritti connessi, G.U. n. L. 372 del 27/12/2006.

Direttiva 2009/24/CE del Parlamento europeo e del Consiglio del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore, G.U. n. L. 111 del 5/05/2009.

Direttiva 2009/72/CE del Parlamento europeo e del Consiglio del 13 luglio 2009, relativa a norme comuni per il mercato interno dell'energia elettrica e che abroga la direttiva 2003/54/CE, G.U. n. L. 211 del 14/8/2009.

Direttiva 2011/83/UE del Parlamento europeo e del Consiglio del 25 ottobre 2011 sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio, G.U. n. L. 304 del 22/11/2011.

Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013 che modifica la Direttiva 2003/98/CE, G.U. n. L. 175 del 27/06/2013.

Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati

personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, G.U. n. L. 119 del 4/05/2016.

Direttiva (UE) 2016/943 del Parlamento Europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, G.U. n. L. 157 del 15/6/2016.

Regolamento 1907/2006 (CE) del Parlamento europeo e del Consiglio del 18 dicembre 2006 concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche (REACH), che istituisce un'agenzia europea per le sostanze chimiche, che modifica la direttiva 1999/45/CE e che abroga il regolamento (CEE) n. 793/93 del Consiglio e il regolamento (CE) n. 1488/94 della Commissione, nonché la direttiva 76/769/CEE del Consiglio e le direttive della Commissione 91/155/CEE, 93/67/CEE, 93/105/CE e 2000/21/CE, G.U. n. L. 396 del 30/12/2006.

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), G.U. n. L. 119 del 4/5/2016.

Atti atipici dell'Unione europea

Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza, G.U. n. C. 372 del 09/12/1997.

Comunicazione della Commissione *Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti*, G.U. n. C. 45 del 24/02/2009.

Comunicazione della Commissione *Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*, 2011.

Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a un diritto comune europeo della vendita*, 2011.

Comunicazione della Commissione *Proposta di Regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, 2012.

Comunicazione della Commissione *Verso un quadro orizzontale europeo per i ricorsi collettivi*, 2013.

Comunicazione della Commissione *Verso una florida economia basata sui dati*, 2014.

Comunicazione relativa agli accordi di importanza minore che non determinano restrizioni sensibili della concorrenza ai sensi dell'articolo 101, paragrafo 1, del trattato sul funzionamento dell'Unione europea (comunicazione «de minimis»), G.U. n. 2014/C 291/01 del 30/08/2014.

Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale*, 2015.

Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di vendita online e di altri tipi di vendita a distanza di beni*, 2015.

Comunicazione della Commissione *Strategia per il mercato unico digitale in Europa*, 2015.

Comunicazione della Commissione *Proposta di Direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale*, 2016.

Comunicazione della Commissione *Building a European Data Economy*, 2017.

Raccomandazione 2013/396/UE dell'11 giugno 2013 relativa a principi comuni per i meccanismi di ricorso collettivo di natura inibitoria e risarcitoria negli Stati membri che riguardano violazioni di diritti conferiti dalle norme dell'Unione, G.U. n. L. 201 del 26/7/2013.

Giurisprudenza della Corte di giustizia dell'Unione europea

CGUE 29 ottobre 2015 (Seconda Sezione), causa C-490/14, Freistaat Bayern c. Verlag Esterbauer GmbH.

CGUE 15 gennaio 2015 (Seconda Sezione), causa C-30/14, Ryanair Ltd c. PR Aviation BV.

CGUE 3 luglio 2012 (Grande Sezione), causa C-128/11, UsedSoft GmbH c. Oracle International Corp.

CGUE 9 marzo 2012 (Grande Sezione), causa C-131/12, Google Spain c. Agencia Espanola de Protección de Datos.

CGUE 1° marzo 2012 (Terza Sezione), causa C-604/10, Football Dataco Ltd e altri c. Yahoo! UK Ltd e altri.

CGCE 7 maggio 2009 (Terza Sezione), causa C-553/07, College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer.

CGCE 17 settembre 2007 (Grande Sezione), causa T-201/04, Microsoft Corp. v Commissione.

CGCE 9 novembre 2004 (Grande Sezione), causa C-444/02, Fixtures Marketing Ltd c. Organismos prognostikon agonon podosfairou AE (OPAP).

CGCE 9 novembre 2004 (Grande Sezione), causa C-203/02, The British Horseracing Board Ltd e altri c. William Hill Organization Ltd.

CGCE 26 aprile 2004 (Quinta Sezione), causa C-418/04, IMS Health GmbH & Co. OHG c. NDC Health GmbH & Co. KG.

CGCE 26 novembre 1998 (Sesta Sezione), causa C-7/97, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG,

Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG.

CGCE 6 aprile 1995, cause C-241/91 e C-242/91, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) c. Commissione.

CGCE 13 febbraio 1979, causa 85/76, Hoffmann-La Roche & Co. AG c. Commissione delle Comunità europee.

Concentrazioni

COMMISSIONE EUROPEA, 3 ottobre 2014, caso n. COMP/M.7217 – *Facebook/Whatsapp.*

Giurisprudenza statunitense

ACLU v. Clapper, 14-42 2d Cir. (2015).

ACLU v. Clapper, 959 F. Supp. 2d 724 (2013).

Capitol Records, LLC v. ReDigi Inc., 12-0095 U.S. Dist. (2012).

Klayman v. Obama, 957 F. Supp. 2d 1 (2013).

United States v. Jones, 565 U.S. 400 (2012).

Northwest Airlines Privacy Litigation, WL 1278459 (2004).

Kyllo v. United States, 533 U.S. 27 (2001).

Boy Scouts of America v. Dale 530 U.S. 640 (2000).

U.S. News & World Report, Inc. v. Avrahami, 95-1318 Va. Cir. Ct. (1996).

Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991).

Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

Boomer v. Atlantic Cement Co., 26 N.Y.2d 219 (1970).

Katz v. United States, 389 U.S. 347 (1967).

NAACP v. Alabama, 357 U.S. 449 (1958).

Melvin v. Reid, 297 P. 91 (1931).

Brents v. Morgan, 299 S.W. 967 (1927).

Pavesich v. New England Life Insurance Co., 50 S.E. 68 (1905).

Roberson v. Rochester Folding Box Co., 64 N.E. 442 (1902).

Fonti normative di diritto italiano

Regio Decreto 29 giugno 1939 n. 1127 (Legge-Invenzioni).

Legge 22 aprile 1941 n. 633 (Legge sul diritto d'autore e su altri diritti connessi al suo esercizio).

Legge 7 agosto 1990 n. 241 (Legge sul procedimento amministrativo).

Decreto legislativo 30 giugno 2003 n. 196 (Codice della Privacy).

Decreto legislativo 10 febbraio 2005 n. 30 (Codice della Proprietà Industriale).

Decreto legislativo 13 agosto 2010 n. 131 (Decreto Correttivo del Codice della Proprietà Industriale).

Decisioni giurisprudenziali italiane

Cass., Sez. I, sentenza 24 aprile 2016, n. 13161.

Cass., Sez. III, sentenza 5 aprile 2012, n. 5525.

TAR Lazio, sede Roma, sez. III bis, sentenza 22 marzo 2017, n. 3769.

Trib. Milano 28 settembre 2016, n. 10374.

Trib. Torino (ord.) 17 luglio 1997.

Risorse web

Addio Google Glass, cancellati anche gli account sui social network, in *Wired*, 26 gennaio 2016 (www.wired.it/internet/social-network/2016/01/26/google-glass-cancellati-account-social-network, ultimo accesso 29 giugno 2017).

Android Flashlight App Developer Settles FTC Charges It Deceived Consumers, in *Federal Trade Commission*, 5 dicembre 2013 (www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived, ultimo accesso 3 luglio 2017).

«Bene», in *Enciclopedia Treccani Online* (http://www.treccani.it/enciclopedia/bene, ultimo accesso 14 agosto 2017).

Facebook, il tasto Like è una spia, in *BU ICT San Raffaele* (www.buict.sanraffaele.it/it/2012-09-28-15-27-47/21-notizie/newsflash/239-facebook-il-tasto-like-e-una-spia.html, ultimo accesso 17 luglio 2017).

ICO fines insurance firm after hacked card details used for fraud, in *Information Commissioner's Office*, 24 febbraio 2015 (http://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/02/ico-fines-insurance-firm-after-hacked-card-details-used-for-fraud, ultimo accesso 3 luglio 2017).

Industria 4.0, la nuova era del manifatturiero, in *Digital 4 Executive*, 2 luglio 2015 (www.digital4.biz/executive/approfondimenti/industria-40-la-nuova-era-del-manifatturiero_43672155526.htm, ultimo accesso 29 agosto 2017).

Le Storie di Instagram crescono e Snapchat accusa il colpo, in *Wired.it*, 2017 (www.wired.it/internet/social-network/2017/01/31/storie-snapchat-instagram, ultimo accesso 3 giugno 2017).

Legislative Train Schedule – Common European Sales Law (CESL), in *Europarl.europa.eu* (www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-common-european-sales-law, ultimo accesso 9 agosto 2017).

Patents for Software? European Law and Practice, in *European Patent Office* (www.epo.org/news-issues/issues/software.html, ultimo accesso 27 settembre 2017).

Public consultation on the database directive: application and impact, in *European Commission* (http://ec.europa.eu/info/consultations/public-consultation-database-directive-application-and-impact-0_en, ultimo accesso 26 agosto 2017).

The big bang: how the Big Data explosion is changing the world, in *Microsoft*, 11 febbraio 2013 (http://news.microsoft.com/2013/02/11/the-big-bang-how-the-big-data-explosion-is-changing-the-world, ultimo accesso 12 settembre 2017).

Transparency And Open Government. Memorandum For The Heads Of Executive Departments And Agencies, in *Obama White House*, 21 gennaio 2009 (http://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government, ultimo accesso 22 giugno 2017).

ANDERSON C., *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, in *Wired*, 23 giugno 2008 (www.uvm.edu/~cmplxsys/wordpress/wp-content/uploads/reading-group/pdfs/2008/anderson2008.pdf, ultimo accesso 19 settembre 2017).

BAWDEN T.*, Global warming: Data centres to consume three times as much energy in next decade, experts warn*, in *The Independent*, 23 gennaio 2016 (www.independent.co.uk/environment/global-warming-data-centres-to-consume-three-times-as-much-energy-in-next-decade-experts-warn-a6830086.html, ultimo accesso 27 aprile 2017).

BODE BODE A., *Open Data: a History*, in *Data.gov*, 4 aprile 2013 (www.data.gov/blog/open-data-history, ultimo accesso 22 giugno 2017).

BURRINGTON I., *The Environmental Toll of a Netflix Binge*, in *The Atlantic*, 16 dicembre 2015 (www.theatlantic.com/technology/archive/2015/12/there-are-no-clean-clouds/420744, ultimo accesso 21 giugno 2017).

CHIGNARD S., *A brief history of open data*, in *Paris Innovation Review*, 29 marzo 2013 (www.parisinnovationreview.com/2013/03/29/brief-history-open-data, ultimo accesso 22 giugno 2017).

DEMARY M. – DEMARY V., *Blockchain: cheap, fast and accurate (but consumes a huge amount of energy),* in *LSE Business Review Blog*, 19 gennaio 2017 (http://blogs.lse.ac.uk/businessreview/2017/01/19/blockchain-cheap-fast-and-accurate-but-consumes-a-huge-amount-of-energy, ultimo accesso 19 giugno 2017).

DONNELLY C. – SIMMONS G., *Small Businesses Need Big Data, Too*, in *Harvard Business Review*, 5 dicembre 2013 (www.hbr.org/2013/12/small-businesses-need-big-data-too, ultimo accesso 15 giugno 2017).

GATTULLO V. ET AL., *Nuove frontiere dell'espropriazione mobiliare: Il pignoramento del dominio internet*, in *FILODiritto*, 16 settembre 2014 (www.filodiritto.com/articoli/2014/09/nuove-frontiere-dellespropriazione-mobiliare-il-pignoramento-del-dominio-internet.html, ultimo accesso 31 agosto 2017).

GIBBS S., *Google buys UK artificial intelligence startup Deepmind for £400m*, in *The Guardian*, 27 gennaio 2014 (www.theguardian.com/technology/2014/jan/27/google-acquires-uk-artificial-intelligence-startup-deepmind, ultimo accesso 19 giugno 2017).

GILLETTE F., *The Rise and Inglorious Fall of MySpace*, in *Bloomberg Businessweek*, 23 giugno 2011 (www.bloomberg.com/news/articles/2011-06-22/the-rise-and-inglorious-fall-of-myspace, ultimo accesso 28 giugno 2017).

GRAY A., *These are the world's 10 biggest corporate giants*, in *World Economic Forum*, 16 gennaio 2017 (www.weforum.org/agenda/2017/01/worlds-biggest-corporate-giants, ultimo accesso 27 giugno 2017).

HARDESTY L., *How hard is it to 'de-anonymize' cellphone data?*, in *MIT News*, 27 marzo 2013 (http://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data, ultimo accesso 17 luglio 2017).

HICKEN M., *Find out what Big Data knows about you (it may be very wrong)*, in *CNN Money*, 5 settembre 2013 (http://money.cnn.com/2013/09/05/pf/acxiom-consumer-data/index.html, ultimo accesso 30 giugno 2017).

HOWARD A., *What is smart disclosure?*, in *Radar O'Reilly*, 1° aprile 2012 (http://radar.oreilly.com/2012/04/what-is-smart-disclosure.html, ultimo accesso 23 giugno 2017).

JOHNSON B., *Privacy's dead: Facebook chief*, in *The Sydney Morning Herald*, 19 gennaio 2010 (http://www.smh.com.au/business/privacys-dead-facebook-chief-20100118-mgs8.html, ultimo accesso 11 luglio 2017).

MEOLA A., *Wearable technology and IoT wearable devices*, in *Business Insider*, 19 dicembre 2016 (www.businessinsider.com/wearable-technology-iot-devices-2016-8?IR=T, ultimo accesso 14 giugno 2017).

MOTT N., *The FTC condemns the data brokerage industry's collection practices*, in *Pando*, 27 maggio 2014 (http://pando.com/2014/05/27/the-ftc-condemns-the-data-brokerage-industrys-collection-practices, ultimo accesso 29 giugno 2017).

NORDRUM A., *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, in *IEEE Spectrum*, 18 agosto 2016 (http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, ultimo accesso 15 settembre 2017).

O'REILLY T., *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, in *OReilly*, 30 settembre 2005 (www.oreilly.com/pub/a/web2/archive/what-is-web-20.html, ultimo accesso 29 aprile 2017).

POPPER N., *Knight Capital Says Trading Glitch Cost It $440 Million*, in *The New York Times*, 2 agosto 2012 (http://dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/?_r=0, ultimo accesso 16 giugno 2017).

RISEN J. – LICHTBLAU E., *Bush Lets U.S. Spy on Callers Without Courts*, in *New York Times*, 16 dicembre 2005 (www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html, ultimo accesso 13 luglio 2017).

ROCKEFELLER IV J.D., *What Information Do Data Brokers Have on Consumers, and How Do They Use It?*, in *US Senate Committee on Commerce, Science, & Transportation*, 18 dicembre 2013 (www.commerce.senate.gov/public/index.cfm/hearings?Id=a5c3a62c-68a6-4735-9d18-916bdbbadf01&Statement_id=A47C081A-D653-4272-8D12-D6EDC1E04DC6, ultimo accesso 30 giugno 2017).

ROSSITER J., *Keeping our Focus on What's Next*, in *Yahoo! Tumblr.com*, 28 giugno 2013 (http://yahoo.tumblr.com/post/54125001066/keeping-our-focus-on-whats-next, ultimo accesso 19 giugno 2017).

SCHMITT G., *A tale of two judges*, in *Weekly Standard*, 13 gennaio 2014 (www.weeklystandard.com/tale-two-judges/article/773264, ultimo accesso 18 luglio 2017).

SINTEF, *Big Data, for better or worse: 90% of world's data generated over last two years*, in *ScienceDaily*, 22 maggio 2013 (www.sciencedaily.com/releases/2013/05/130522085217.htm, ultimo accesso 14 giugno 2017).

SLOANE G., *New Google Ad Filter Frightens Some Publishers and Ad Tech Players*, in *AdvertisingAge*, 5 giugno 2017 (www.adage.com/article/digital/google-ad-blocker-frightens-publishers/309252, ultimo accesso 6 giugno 2017).

TASSI P., *Facebook's Advertising Is Starting To Spiral Out Of Control*, in *Forbes*, 1° luglio 2013 (www.forbes.com/sites/insertcoin/2013/07/01/facebooks-advertising-is-starting-to-spiral-out-of-control/#13ad1bcc699c, ultimo accesso 28 giugno 2017).

VAN RIJMENAM M., *Tesco and Big Data Analytics, a Recipe for Success?*, in *Datafloq*, 22 dicembre 2016 (http://datafloq.com/read/tesco-big-data-analytics-recipe-success/665, ultimo accesso 18 settembre 2017).

VARIAN H., Hal *Varian Answers Your Questions*, in *Freakonomics*, 28 febbraio 2008 (http://freakonomics.com/2008/02/25/hal-varian-answers-your-questions, ultimo accesso 29 aprile 2017).

WEAVER M., *New BT service could end nuisance phone calls*, in *The Guardian*, 16 gennaio 2017 (www.theguardian.com/money/2017/jan/16/bt-says-new-service-could-block-up-to-30m-nuisance-calls-a-week, ultimo accesso 4 luglio 2017).

ZAFFARANO F., *Whatsapp diventa gratuito, tolti i 99 cent all'anno*, in *La Stampa*, 18 gennaio 2016 (www.lastampa.it/2016/01/18/tecnologia/whatsapp-diventa-gratis-tolti-i-cent-allanno-LYzdZGYpdA22S3hGZxBE8M/pagina.html, ultimo accesso 7 luglio 2017).

ZETTER K., *World's Top Surveillance Societies – Updated with link*, in *Wired*, 31 dicembre 2007 (www.wired.com/2007/12/worlds-top-surv, ultimo accesso 12 luglio 2017).

Siti

adblockplus.org

aboutthedata.com

https://en.oxforddictionaries.com

tsaboin.com