media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 06/2017

ELISABETTA NUNZIANTE

Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali.

I dati sono stati definiti come il «*nuovo petrolio*»[1]. L'innovazione corre sempre più, infatti, sul filo dei dati e del loro costante (ri)utilizzo. In effetti, la crescita esponenziale dei meccanismi di raccolta dei dati (che promette di non rallentare con il consolidarsi dell'Internet of things) associata all'aumento della potenzialità di calcolo e manipolazione degli strumenti di analisi permettono e permetteranno, in sempre maggiori campi, di avere a disposizioni informazioni aggregate su larga scala[2]. E' questo il mondo dei Big Data, usati sempre di più in contesti quali servizi finanziari, assicurativi, sanitari, di trasporti sia in

[1] L'espressione è riportata in WORLD ECONOMIC FORUM, *Personal Data: the emergence of a new asset class*, 2011 p. 5 Molteplici sono stati i tentati paragoni volti a definire l'importanza che i dati assumono nella Società dell'Informazione. Qualcuno ne ha paragonato la natura alla seta per la sua capacità di accumularsi come fili nel cyberspazio e di intrecciarsi fino a formare <<*un arazzo della personalità online dell'utente*>> C. MARSDEN, I. BROWN, "*Regulating Code*", Boston, 2011. L'OECD ne ha invece sottolineato la natura di infrastruttura per la loro capacità di acquistare valore ogni qual volta riutilizzati e di servire scopi differenti. OECD, *Data-driven innovation: Big Data for growth and well-being*, Paris, 2015.

[2] Si prenda in considerazione la legge di Moore, principio dell'informatica che afferma: << la complessità di un microcircuito, misurata ad esempio tramite il numero di transistori per chip, raddoppia ogni 18 mesi (e quadruplica quindi ogni 3 anni). »

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

ambito pubblico che privato. I Big Data sono definiti dalla Commissione Europea come «*una grande quantità di tipi diversi di dati prodotti con un'alta velocità da un grande numero di fonti di diverso tipo. La gestione di tali aggregati di dati richiede oggi nuovi strumenti e metodi, come processori potenti, software e algoritmi*»[3]. Il valore delle informazioni non è dunque intrinseco ma dato dalla capacità di organizzarle, analizzarle, misurarle e conseguentemente ricavarne fattori e decisioni. Ciò significa che le attività di analisi dei Big Data riposano su due piani: software e algoritmi per l'analisi, da un lato, e l'insieme dei dati raccolti e aggregati, dall'altro.

Due sono le domande da porsi: se e come proteggere i Big Data, al fine anche di incentivarne lo sviluppo, e come proteggerci da essi e dalle loro applicazioni. I due temi sono, infatti, due facce della stessa medaglia che si influenzano e interagiscono. Il problema è come regolamentare l'informazione nella sua dimensione più pura e nelle sue applicazioni più avanzate, assicurando il giusto equilibrio tra esclusione e accesso[4].

La natura puramente informativa di tali strumenti rende la loro protezione e la loro regolamentazione ardua. Il mondo dei Big Data va quindi valutato sulla base dei due piani su cui esso si fonda: gli strumenti di analytics e i dati.

Il primo piano è quello relativo alle strutture necessarie per poter efficacemente svolgere le attività di analisi: infrastrutture fisiche e non fisiche tra le quali assumono particolare rilevanza, come detto, i software e gli algoritmi. Sorge a questo punto la difficoltà del verificare se e a che livello sia possibile configurare diritti di proprietà intellettuale su questi ultimi elementi, proteggendo il vantaggio competitivo degli operatori e allo stesso tempo stimolando lo sviluppo del settore.

---

[3] *Towards a thriving data-driven economy* (COM(2014) 442 Final) p. 4

[4] Si veda G. GHIDINI, «Exclusion and Access in Copyright Law: the Unbalanced features of the European Directive of Information Society (INFOSOC)», in *Dir. Ind.* 2013 p. 6 nota 6, dove, con riferimento al diritto d'autore, accesso e esclusione vengono definiti come "gemelli siamesi" reciprocamente dipendenti.

Per quanto riguarda i programmi per elaboratori, la protezione principale è assicurata dal diritto d'autore. La tutela di per sé si presenta come particolarmente forte: erga omnes, automatica e di lunga durata. Tuttavia, essa non offre una notevole stabilità, richiedendo la sussistenza di un requisito di originalità (inteso in UE come *author's own intellectual creation* e negli US, dopo la sentenza *Feist*, come *modicum* di creatività) che facilmente può essere negato, ogni qualvolta le istruzioni presenti nel codice siano necessitate dalla funzione[5].

Nell'ambito degli Stati Uniti, si è dunque guardato con attenzione alla disciplina brevettuale.

A differenza di quanto previsto in Europa, infatti, gli Stati Uniti consentono la protezione dei cosiddetti *business method* che potrebbero ricomprendere le combinazioni di algoritmi e programmi per elaboratore. Anche in questo senso la strada si presenta in salita. Nel *leading case Alice*, la Supreme Court ha stabilito che le condizioni che consentono la brevettabilità di tali oggetti sono due: l'invenzione non deve essere solo un'idea astratta e qualora sia tale deve mostrare un passo inventivo ulteriore che applichi tale idea[6]. La case law statunitense ci mostra che è sempre più difficile la soddisfazione di tali requisiti. In particolare, nella sentenza *Content Extractio*, la *Federal Circuit*, applicando il test di *Alice* e dichiarando l'invalidità del brevetto in questione a causa del suo oggetto astratto, così si esprime: «*The*

[5] Il principio dell'*author own intellectual creation* è stabilito nelle direttive dell'UE con specifico riferimento a *computer programs* (dir. 91/250/CE poi modificata da dir. 2009/24/CE) e *database* (dir.96/9/CE). Tuttavia è bene sottolineare che a seguito della sentenza INFOPAQ (ECJ C-5/08) il criterio deve ritenersi applicabile a tutte le opere di ingegno, in lettura congiunta con la direttiva INFOSOC (dir. 2001/29/CE). Negli USA nella sentenza *Feist* la *Supreme Court* ha innalzato il livello di creatività richiesto nella disciplina statunitense superando l'angolosassone approccio dello *sweat of the brow (Feist Publications, Inc., v. Rural Telephone Service Co.*, 499 U.S. 340 (1991))
Tuttavia, si potrebbe ritenere che una forma di protezione potrebbe sorgere in UK, laddove il CDPA sec. 3(1)(a) conserva, nonostante l'intervenuta direttiva a livello europeo, protezione per "a *table of compilations other than a database*" . Con riferimento a queste ultime, si è sostenuto che la differenza rispetto ai database sia proprio nel livello di originalità richiesto. Le *table of compilations* conserverebbero, sotto questo punto di vista, la possibilità di applicazione del vecchio approccio cd. *sweat of the brow* che richiede al fine di stabilimento della tutela la mera presenza *skill, labour and judgement* (alternativamente). Si veda relativamente alla giurisdizione inglese: T. APLIN, J. DAVID, "*Intellectual Property Law: Text, Cases and materials*", 2009, Oxford pp. 201 ss.

[6] *Alice Corp. v. CLS Bank International*, 573 U.S. 134 S. Ct. 2347 (2014).

concept of data collection, recognition, and storage is undisputedly well-known. Indeed, humans have always performed these functions»[7]. D'altra parte, l'applicazione della disciplina brevettuale agli strumenti analitici, pur se riconosciuta, risulterebbe probabilmente inidonea a garantire un effettivo livello di protezione. Il brevetto è, infatti, un diritto di proprietà intellettuale "statico" che, cioè, cristallizza l'invenzione nella sua descrizione. Al contrario, gli strumenti di data analytics, sono tanto più efficaci quanto più in grado di evolversi e di adattarsi nel tempo.

La protezione di tali strumenti, tuttavia, può efficacemente basarsi su due tutele diverse: la tutela del segreto industriale e quella contrattuale. Queste ultime hanno entrambe il difetto di essere relative: diritti *in personam* e non *in rem*.

In particolare, moltissimi dubbi possono essere sollevati rispetto all'efficacia del primo metodo. La tutela del *trade secret*, ancorché capace di coprire sia source code che algoritmi, incontra infatti dei limiti: la necessità di provare l'applicazione di misure efficaci per garantire la segretezza (difficile da raggiungere, in un mondo interconnesso e aperto come quelli dei Big Data) e l'impossibilità di proteggersi da atti indipendenti di terzi o da pratiche di *reverse engineering*[8]. In aggiunta, la tutela dei *trade secret* si presenta, più degli altri strumenti di proprietà intellettuale, come fortemente frammentata nei diversi paesi (nonostante la recente direttiva UE che è principalmente volta a garantire l'effettività dei rimedi più che ad armonizzare). In alcuni paesi, il segreto industriale è, infatti, protetto mediante previsioni legislative (in Italia artt. 98 e 99 c.p.i.) mentre in altri (si veda la Germania) esso è ricondotto alla più ampia disciplina dalla concorrenza sleale.

Analoga problematica di protezione della proprietà intellettuale, può essere sollevata con riguardo ai dataset: l'insieme aggregato dei dati sulla base del quale operano le attività di analisi dei Big Data.

---

[7] *Content Extraction v. Well Fargo Bank* 776 F.3d 1343, 1347 (Fed. Cir. 2014).

[8] D. PRANGE, "*Navigating the protection of Big Data* in *Intellectual Property Magazine*", 7/12/2016 disponibile on-line: (http://www.intellectualpropertymagazine.com/patent/navigating-the-protection-of-big-data-121248.htm) (ultimo accesso: 5 feb 17)

Questi, infatti, potrebbero essere categorizzati come database e quindi soggetti, nell'Unione Europea, al doppio livello di protezione del diritto d'autore e del diritto sui generis.

Quanto al primo, è ardua la possibilità di configurare la presenza di un livello di originalità tale da poter attrarre la protezione del copyright. Ciò è vero in particolare con riguardo a quell'insieme di dati dove, giacché sia le fonti sia l'organizzazione sono date da attività automatizzate, sembra difficile poter configurare la presenza di un autore[9]. Ancora, il diritto d'autore assicurerebbe protezione dalla sola copia esatta del database (o di parte di esso) come tale. Più appropriato sembra invece il diritto sui generis, sia nella sua costruzione sia nella sua portata. Esso, infatti, sorge a seguito di un sostanziale investimento nell'ottenimento, verificazione e presentazione dei contenuti

e permette di proteggere il database dall'estrazione dalla riutilizzazione dei dati[10]. Qualche problematica sembra sorgere rispetto all'aggettivo "sostanziale" che non è stato adeguatamente definito né dalla direttiva né dalle corti e che potrebbe limitare l'applicazione del diritto[11]. D'altra parte, anche tale tutela rischia di rivelarsi inefficace. La Corte di giustizia ha, infatti, significativamente ristretto la sua applicazione, operando una complicata distinzione tra "dati generati" e "dati raccolti", escludendo i primi dall'applicazione della direttiva e pertanto negando protezione ai database cd. spin-off[12].

---

[9] A. WIEBE, «Protection of industrial data: a new property right for the digital economy?» in *JIPLP* 2016/12 vol. 1, OUP, pp.62-77

[10] La tutela autoriale offre protezione alla selezione e all'organizzazione mentre l'ambito di protezione del diritto *sui generis* si focalizza sul contenuto.

[11] E. DERCLAYE, «The Court of Justice inteprets the database sui generis right fot the first time» in *E.L. Rev.* (2005), p. 429-430; il problema delle difficoltà interpretative relative al termine sostanziale sono state sottolineate,peraltro, anche dalla commissione in "*DG INTERNAL MARKET AND SERVICES WORKING PAPER: First evaluation of Directive 96/9/EC on the legal protection of databases*" (Brussels, 12 dicembre 2005) (disponibile on-line http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf) (ultimo accesso: 5 feb 17)

[12] *The British Horseracing Board Ltd e altri contro William Hill Organization Ltd* (ECJ C-203/2002); *Fixtures Marketing Ltd contro Svenska Spel AB* (ECJ C-338/02); *Fixtures Marketing Ltd contro Organismos*

Ancora, è bene sottolineare che, anche quando operativo, il diritto sui generis proteggerebbe i dati solo quando aggregati all'interno del dataset, lasciando in ogni caso scoperta la fase precedente che intercorre tra la creazione/raccolta di dati e la loro organizzazione/analisi[13].

D'altra parte, l'informazione allo stato puro è sempre esclusa dal raggio di azione delle privative (nel diritto d'autore con l'applicazione della teoria della dicotomia idea/espressione, nella tutela brevettuale con l'esclusione delle idee astratte, dei principi e degli algoritmi e anche nel diritto sui generis con l'attenzione rivolta alle azioni compiute rispetto all'informazione).

Nonostante qualcuno abbia valutato la proposta di pensare a un altro diritto sui generis specifico per la protezione dei Big Data, non sembrerebbe auspicabile un intervento sul *numerus clausus*[14]. La creazione di una nuova figura giuridica risulterebbe, infatti, problematica non soltanto nella definizione di requisiti e portata ma anche nell'allocazione dei diritti (chi genera i dati? chi effettua l'investimento per la loro analisi?)[15].

Per proteggere i dataset di informazioni rimasti al di fuori dell'applicazione dei diritti di proprietà intellettuale elencati dobbiamo, dunque, rivolgerci ancora una volta alle tutele relative del *trade secret* e del contratto.

Quest'ultima strada ha visto la sua consacrazione in una recente sentenza della Corte di giustizia. Nel caso Ryanair, la Corte ha, infatti, implicitamente convenuto che il database non riconosciuto come tale né dal diritto d'autore né dal diritto sui generis può trovare protezione nell'autonomia contrattuale[16].

La protezione degli asset che si pongono alla base degli strumenti dei Big Data è dunque principalmente fondata su tutele di tipo relativo. La desiderabilità di tale quadro di sistema

---

prognostikon agonon podosfairou AE (OPAP) (ECJ C-444/02); *Fixtures Marketing Ltd contro Oy Veikkaus Ab*.(ECJ C-46/02);

[13] A. WIEBE, *op. cit.*

[14] *ibidem*

[15] *ibidem*

[16] *Ryanair Ltd. Contro PR Aviation Bp* (ECJ C-30/14)

deve essere valutata risalendo alla radice delle giustificazioni della proprietà intellettuale e dell'insieme del sistema giuridico.

Se, infatti, da un lato, si potrebbe argomentare che la proprietà intellettuale riposa su una questione "morale" e quindi sulla volontà di proteggere l'autore/inventore assicurandogli la possibilità di trarre i frutti della sua opera di ingegno, dall'altro la configurazione di tali diritti dice altro. I diritti di proprietà intellettuale si caratterizzano, infatti, per un costante bilanciamento interno tra accesso ed esclusione, volto a garantire lo sviluppo della creatività e solo strumentalmente, come forma di "incentivo", la protezione del creatore.

L'individuazione di modelli di protezione degli strumenti relativi ai Big Data sembrerebbe assumere importanza in molteplici contesti commerciali (si pensi tra gli altri, a titolo di esempio, alle acquisizioni o alla tutela di tali strumenti rispetto ai propri stessi lavoratori, soprattutto a seguito della cessazione del contratto di lavoro).

Allo stesso tempo, tuttavia, una forma troppo forte di *enclosure*, rischierebbe di apporsi sull'informazione in quanto tale, bloccando il flusso delle informazioni (necessario affinché le industrie dell'innovazione possano svilupparsi) e rischiando di collidere, financo, con diritti della personalità.

Con riferimento a questi ultimi, affrontate le problematiche relative alla esclusione, è opportuno valutare il profilo dell'accesso.

Alle valutazioni relative alla protezione dei Big data si oppone, infatti, la necessità di ragionare sulle modalità mediante le quali proteggerci dai Big Data.

E', infatti, possibile che gli strumenti analitici dei Big Data (ed in particolare gli strumenti predittivi) si pongano come lesivi della dignità dell'individuo. Attraverso la profilazione e la categorizzazione degli individui all'interno di parametri precostituiti si rischia, infatti, di porre in essere pratiche discriminatorie[17]. Il pericolo è evidente in presenza di dati sensibili

[17] O. TENE, J. POLONETSKY, «Big Data for All: Privacy and Use Control in the Age of Analytics» in *Northwestern Journal of Technology and Intellectual Property* vol. 11 n. 5, 2013 p. 252 ss.

(che, infatti, godono di protezione più forte) ma, a causa del potenziale dell'aggregato, riguarda anche altre tipologie di dati personali.

Si pensi, ad esempio, a come tali pratiche possano porsi come lesive dell'individuo nel contesto del lavoro subordinato, quando, mettendo in rapporto poche caratteristiche di un lavoratore e paragonandole ad un pattern, possono essere tratte conclusioni relativamente alla sua condotta sulla base di elementi puramente probabilistici.

Ancora, si veda il rischio di colpire la persona nella sua dimensione di consumatore ponendo in essere politiche di discriminazione dei prezzi sulla base delle enormi quantità di dati raccolti.

E' evidente che il fiorire di business legati ai Big Data si ponga in primo luogo come una minaccia per la protezione dei dati personali e dei principi che si pongono alla base di essa.

I Big Data si inquadrano, infatti, all'interno di un contesto sociale e economico nel quale il meccanismo informazione/consenso mostra sempre più la sua fragilità.

A fronte di forte asimmetrie informative, di una scarsa consapevolezza e dell'urgenza di accedere ai servizi, l'interessato fornisce un consenso la cui natura libera e informata è sempre più questionabile. Dall'altro lato, le stesse imprese, diffidenti della giustificazione del trattamento basato sul consenso, inquadrano sempre più le loro attività in altre condizioni legittimanti[18].

In primo luogo, la raccolta e analisi di enormi quantità di dati rischia di minacciare il principio di *data minimization*, laddove anche dati non necessari possono rivelarsi di grande impatto nell'insieme aggregato.

In secundis, la raccolta di grandi quantità di dati rischia di avvenire a spese del principio di accuratezza dei dati.

[18] Ci si riferisce qui in particolare alle condizioni previste dall'art. 6 co. 1 lett. b) e f) del nuovo Regolamento (Reg. EU 2016/679) e cioè il trattamento necessario per l'esecuzione di un contratto ovvero di misure precontrattuali e il trattamento giustificato da legittimi interessi (in particolare, quest'ultima disposizione si pone come sufficientemente vaga da poter dar luogo ad abusi oltre ad essere contestata per la scelta di porre sullo stesso piano di valutazione interessi e diritti)

In terzo luogo, come sottolineato dall'ART.29 WP, è necessario assicurarsi che anche nel contesto dei Big Data sia rispettato il principio di finalità, garantendo cioè che gli scopi per i quali i dati sono trattati rientrino nell'ambito delle aspettative dei *data subject*[19]. In questo senso, bisogna accogliere con favore il nuovo GDPR che, con riferimento ai trattamenti ulteriori sembra adottare un approccio più rigido di compatibilità trai fini[20].

La necessità di garantire che il principio di finalità sia rispettato anche nell'ambiente dei Big Data si pone in linea con le due grandi sostanziali giustificazioni della disciplina stessa della protezione dei dati personali.

Da un lato, infatti, tale limitazione garantisce il rispetto dell'individuo e dell'esercizio della sua autonoma volontà sui dati che lo riguardano dando attuazione alle istanze di tutela dei diritti umani che connotano l'approccio europeo, soprattutto a seguito dell'implementazione del Trattato di Lisbona.

Dall'altro lato, il principio di limitazione dei fini si pone nel mercato, come sottolineato sempre dal ART.29 WP, come limite all'instaurazione di monopoli e posizioni dominanti nell'ambito dell'analisi dei dati, accomodando la visione di *free flow* dei dati non estranea all'Unione Europea e, allo stesso tempo, adatta a incontrare il fondamento logico della data protection statunitense, cioè la necessità di tutelare la posizione del soggetto dei dati personali nell'ambito del mercato.

---

[19] Art. 29 WP *"Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU"*, WP 221, 16/09/2012 (disponibile on-line: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf) (ultimo accesso: 5 feb 17)

[20] Tale conclusione può essere raggiunta confrontando i preamboli della direttiva (95/46/CE) e del nuovo regolamento (Reg. EU 2016/679). Il considerando 28 della direttiva affermava <<*the purposes of processing further to collection shall* not be incompatible *with the purposes as they were originally specified*>> mentre il considerando 50 della nuova direttiva così si pronuncia sulla questione dei successivi trattamenti : <<*The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing* is compatible *with the purposes for which the personal data were initially collected*>> (enfasi aggiunta). Mostrando che se nella valutazione interpretativa era prima sufficiente che i fini fossero meramente "non incompatibili", con il regolamento lo stesso termine utilizzato nell'art. 5 sembra essere soggetto a una valutazione di compatibilità dei fini.

Il mondo dei Big Data mostra ancora una volta la natura bifronte dei dati personali: da un lato, diretti prodotti della persona e dall'altro, asset dal valore commerciale, capaci di essere scambiati e commercializzati. Si ripropone, dunque, ancora una volta nell'Information Society, la questione della progressiva reificazione del dato personale e della configurabilità di quest'ultimo come bene giuridico[21]. Che si riconosca o meno l'ascrivibilità del dato personale (o di alcune tipologie di dati personali) alla più ampia categoria di bene giuridico, non si può certamente negare che la protezione di esso sia da considerarsi come diritto fondamentale, sia alla luce della disciplina Europea che alla luce della nostra carta costituzionale. Poiché non è possibile negare che il dato personale (anche quando inserito all'interno di modalità circolatorie) mantiene un indissolubile legame con il soggetto a cui si riferisce, è necessario che l'assetto normativo si ponga come scopo primario quello di evitare che i diritti della personalità dell'individuo siano colpiti nel loro nucleo fondamentale.

Lo scopo deve essere dunque duplice: proteggere la dignità dell'individuo e renderlo partecipe del valore che viene tratto dall'utilizzo dei suoi dati. La tutela del soggetto di diritto nell'ambito dei Big Data deve dunque valorizzare il suo rapporto diretto con i dati personali ma deve anche essere tale da assicurargli la possibilità di essere parte stessa del mercato che egli alimenta[22]. Anziché porsi in contrasto, questi due aspetti possono essere ricondotti a un unico principio e cioè la garanzia dell'autonomia dell'individuo rispetto all'utilizzo dei suoi dati personali.

---

[21] Esiste sulla questione un'ampia letteratura che non si limita alla mera contrapposizione tra contrari e favorevoli ma vede declinarsi diverse posizioni e interpretazioni. Si citano qui, tra gli altri, a mero titolo di riferimento L. MORMILE, "*Lo statuto giuridico dei dati personali*" in R. PANETTA (a cura di) "*Libera circolazione e protezione dei dati personali*", 2006, p.531 e ss. A. MANTELERO, "*Il costo della privacy tra valore della persona e ragione di impresa*", 2007 p.570 ss. In senso più ampio, sull'informazione come bene giuridico: P. PERLINGIERI, «L'informazione come bene giuridico» in *Rass.dir.civ.* 1990 e P. CATALA, "*Ebauche d'une teorie jurirdique des productions immatérielles*" in "*L'appropriation de l'information*", 1986

[22] O. TENE, J. POLONETSKY, *op. cit.* p.263, si veda anche W. KERBER, "*Digital Markets, Data and Privacy: Competition Law, Consumer Law, and Data Protection* in *Joint discussion Paper Series in Economics*, 14 (2016) p. 10 dove l'A. sottolinea che la *data portability* ha la capacità di assicurare anche un'effettiva concorrenza tra le diverse piattaforme.

Le modalità che possono essere utilizzate per proteggere l'individuo dall'implementazione dei Big Data possono essere diverse.

Tralasciando l'imposizione di obblighi di sicurezza e sulla necessità che siano applicati standard elaborati esternamente, al fine di garantire che i dati personali non siano soggetti ad accessi o intrusioni anomali, ci si sofferma su quelle soluzioni che intervengono direttamente sul rapporto impresa-dato-soggetto.

L'anonimizzazione dei dati si pone come la soluzione più semplice dal punto di vista delle imprese. Il processo che consente di rendere il dato non più identificativo dell'individuo (e, quindi, non più dato personale) permette ai controllori dei dati di sottrarsi, almeno parzialmente, dagli obblighi scaturenti dalla tutela dei dati personali. Esso non solleva, tuttavia, le imprese dei Big Data da ogni onere. E', infatti, necessario accertarsi che l'anonimizzazione non sia facilmente reversibile. Giacché la reversibilità di tali processi è solitamente possibile, bisognerà valutare con particolare attenzione il requisito "facilmente", particolarmente elastico e mutevole con l'evolversi della tecnologia.

Dall'altro lato, un ulteriore strumento, utilizzabile per proteggere il *data subject* e per attribuirgli dei poteri nell'ambito della gestione dei dati, è la cosiddetta *data portability*, ora parte del GDPR[23].

Attribuendo cioè copia intellegibile dei propri dati raccolti, l'individuo acquista consapevolezza di quanto di proprio è nelle mani del controllore e allo stesso tempo ha facoltà di utilizzarlo come meglio ritiene, esercitando la sua autonomia e partecipando dunque del valore creato dai suoi dati[24].

Perché ciò si realizzi nell'interesse del soggetto è necessario che a ciò si aggiunga un'effettività del principio di trasparenza (la cui importanza è stata, ancora una volta, sottolineata dal nuovo Regolamento UE). Quest'ultimo deve essere visto in senso ampio e, in particolare, in modo tale da investire due differenti profili. Il primo è relativo alla necessità

[23] Regolamento (UE) 2016/679 art. 20
[24] O. TENE, J. POLONETSKY, *op. cit.* p.263

di garantire al soggetto conoscenza su chi sia effettivamente in possesso dei dati personali e sulle modalità con le quali essi sono stati acquisiti, anche e soprattutto quando sono intervenuti scambi con terze parti. Il soggetto dovrebbe (ma ciò non è sempre facile nella pratica) essere in grado di risalire la catena dei passaggi che coinvolgono i suoi dati al fine di poter esercitare i suoi diritti. Dall'altro lato, è necessario che la trasparenza investa anche le modalità con la quale i dati sono trattati e, conseguentemente, gli algoritmi che sottendono l'analisi di essi.

Le ultime due soluzioni potrebbero però essere antitetiche alla prima. Le imprese operanti nel settore dei Big Data potrebbero, infatti, opporre che una volta anonimizzati e messi in sicurezza i dati, gli obblighi di garantire *data portability*, accesso completo e trasparenza si porrebbero come particolarmente onerosi.

Nell'ambito dei Big Data, dunque, si palesano le contraddizioni intrinseche dell'informazione. Il flusso dei dati, infatti, è connotato da una costante tensione tra accesso ed esclusione. Ambedue i poli devono essere valutati da due prospettive, portatrici di interessi contrapposti: le imprese e i soggetti[25].

Il bilanciamento tra chiusura e apertura è tema fondante delle analisi che investono la Società dell'informazione e, in essa, il fenomeno dei Big Data. Al fine garantire un corretto equilibrio è necessario tornare, dunque, ai principi e analizzare le varie discipline in conformità ad essi.

Se è vero che la protezione degli asset dei business dei Big Data può garantire la posizione di mercato e assicurare controllo su quanto da loro prodotto, è allo stesso tempo vero che gli interessi economici non possono in nessun caso prevalere sulla garanzia dei diritti umani e della dignità dell'individuo. Essi sono sempre remissivi, ogni qual volta l'individuo e i suoi diritti sono a rischio.

Per questo motivo, giacché una tutela *erga omnes* ed *in rem* degli strumenti e delle risorse che consentono l'utilizzo dei Big data si potrebbe porre in contrasto con il rispetto della vita

[25] Si veda in questo senso OECD, *Data-driven innovation: Big Data for growth and well-being*, Paris, 2015

privata e con il diritto al controllo dei dati personali del soggetto, non sembra irragionevole lasciare che tali prerogative siano esercitate con il ricorso a strumenti di tutela relativa ed *in personam*. Difatti, consentire una privativa troppo forte su gli strumenti analitici e allo stesso tempo sull'aggregato dei dati, rischierebbe di minare l'esercizio del diritto all'accesso e alla trasparenza, a detrimento dell'individuo. Una tale impostazione sembra essere stata recepita nell'Unione Europea con l'emanazione del GDPR che, letto in connessione con la Carta Fondamentale dei diritti, è espressione dell'esigenza di garantire il primario rispetto dei diritti fondamentali nell'ambito del flusso dei dati.

Sembra dunque ragionevole, da un lato, impedire alle imprese di acquisire un potere eccessivo sugli strumenti che consentono l'utilizzo dei Big Data e, dall'altro, rendere maggiormente effettivi i diritti di controllo e di scelta autonoma sui propri dati, in un'ottica di autodeterminazione degli individui[26].

Su un piano subordinato, la valutazione della tutela delle informazioni nei rapporti tra le diverse imprese operanti nel settore deve essere valutato alla luce del diritto alla libertà d'impresa (fondamentale, ancorché economica e dunque subordinata ai diritti della personalità). Alla luce di quest'ultima sembra evidente che l'esigenza di garantire forme di protezione sia bilanciata con l'esigenza di promuovere lo sviluppo dell'innovazione e della creatività. Pertanto, si dovrebbe evitare una *enclosure* dei flussi dell'informazione privilegiando, al contrario, un'interpretazione delle forme di protezione disponibili che sia coerente con i fini che esse perseguono.

L'equilibrio tra accesso e chiusura è il vero tema alla base dei Big Data e della rivoluzione informatica, dove l'informazione assume allo stesso il ruolo di motore dell'economia e di strumento per l'espansione dell'autonomia dell'individuo.

[26] E' questo il concetto di autodeterminazione che emerge dalla disciplina europea dei dati personali e che ha trovato consacrazione in Germania con la pronuncia della Corte Costituzionale Federale (*BVerfGE 65, 1*).