



LE SFIDE DEI **BIG DATA**

tra evoluzione tecnologica, etica
e interessi collettivi

GIOVANNI BUTTARELLI

Quale quarta rivoluzione industriale, i Big Data pongono alcune sfide anche per l'esercizio di funzioni statuali e per le attività d'intelligence. Quali strategie devono sostenere il ragionevole riutilizzo a fini collettivi delle informazioni in mano privata? È configurabile una politica di sostegno di indipendenti Big Data in mano pubblica, e con quali obiettivi, garanzie e prospettive di successo? Mercato, competizione economica, sovranità statale ed etica rappresentano alcuni importanti fattori di analisi, insieme alle nuove norme europee sulla protezione dei dati personali.

È opinione diffusa che il mondo moderno sia stato interessato da tre grandi rivoluzioni industriali. Se così è, possiamo dire che un'ulteriore, la quarta, inizi a interessare la realtà tecnologica, l'economia e il futuro modo di esercizio dei poteri pubblici su scala planetaria. Come altre rivoluzioni industriali, il suo sviluppo è rapido e invisibile, specie inizialmente. I suoi primi passi inducono a ritenere che, al pari della seconda – evolutasi a partire dal 1870 grazie alla diffusione dell'elettricità – essa cambierà rapidamente e incisivamente le modalità di produrre, commerciare e amministrare la cosa pubblica, sia in paesi democratici che totalitari; avrà effetti profondi sui valori anche etici a fondamento della società contemporanea; inciderà sul concetto stesso di sovranità statale. Eppure, in un mondo costretto a individuare altre contingenti priorità, il tema non è ancora sufficientemente al centro dell'agenda politica.



Il fenomeno, che si basa su una nuova generazione di tecnologie e su una metodologia d'impiego delle informazioni decisamente innovativa, è comunemente definito come Big Data, due parole che, al netto delle definizioni di dettaglio già coniate, restituiscono immediatamente il senso:

- della centralità dell'accumulo di notizie e informazioni su scala planetaria;
- della circostanza che il diretto profitto a scopo privato e pubblico dell'uso di una quantità inimmaginabile e illimitata di dati potrà essere a beneficio, finché non interverranno fattori correttivi, solo di pochi soggetti privati in grado di impiegare strumenti informatici, software e algoritmi di straordinarie capacità, di cui la stragrande maggioranza degli operatori (privati e pubblici) non può e, probabilmente, non potrà a lungo disporre.

Quali sono le sfide che tutto ciò pone, anche in relazione all'esercizio di funzioni statuali e le attività d'intelligence?

Nel libro sui Big Data edito nel 2013, *Big Data: A revolution that will transform how we live, work and think*, Viktor Mayer-Schönberger e Kenneth Cukier hanno evidenziato come nel 2009 lo statunitense Center for Disease Control and Prevention abbia potuto prevedere le aree di sviluppo del nuovo virus dell'H1N1 e arginarne la possibile diffusione solo grazie ai 50 milioni di dati connessi alle parole di ricerca utilizzate da cittadini americani, ansiosi d'individuare i sintomi del virus, estratte da Google Inc. dal proprio motore di ricerca, elaborate in base a 450 milioni di modelli matematici dagli ingegneri della società e fatte poi interagire con i pochi dati a disposizione del Centro, in base ai metodi tradizionali di raccolta delle informazioni in ambito sanitario. È questo approccio di dipendenza pressoché integrale da un soggetto privato il futuro schema di lavoro degli organi pubblici? Il diritto europeo conosce già norme per garantire a tutti il riuso aperto delle informazioni in mano pubblica. Quali strategie, invece, devono sostenere il ragionevole riuso a fini collettivi delle informazioni in mano privata? È configurabile una politica di sostegno d'indipendenti Big Data in mano pubblica, e con quali obiettivi, garanzie e prospettive di successo?

MERCATO, COMPETIZIONE ECONOMICA E SOVRANITÀ STATALE

Una prima sfida deriva dall'affinamento delle tecnologie di raccolta e di elaborazione delle informazioni, che ha conosciuto uno straordinario salto di qualità e che permette – accanto all'ammasso più capillare e sistematico di notizie e dati con maggiore contenuto informativo – l'ela-

borazione esponenziale e infinitesimale di illimitate microinformazioni che, a prima vista, sembrano non avere un immediato valore conoscitivo. Si accumulano informazioni anche inutili perché il loro valore aggiunto emergerà domani, o perché ciò che inizia a contare di più è l'analisi aggregata di materiale grezzo.

In realtà, molti settori economici e della cosa pubblica conoscono già il fenomeno dello studio settoriale d'informazioni aggregate, utilissime a fini statistici e di ricerca, di marketing o di pianificazione delle attività pubbliche. Tuttavia, nulla di tutto ciò è paragonabile alle opportunità dei Big Data che conseguono alla fusione, in una prospettiva di lungo termine, d'informazioni disperse, di tracce elettroniche lasciate in rete da moltitudini di persone volutamente o inconsapevolmente, dall'uso intensivo dei dati immagazzinati dai motori di ricerca e dai social network, come pure dalle applicazioni installate su terminali mobili e dalla crescente diffusione dell'internet delle cose. Contribuiscono ad accrescere questo immenso patrimonio informativo i metadata ovvero, per dirlo in chiave assai sintetica, «dati che esprimono insiemi di dati», molti dei quali provenienti dalla miriade d'informazioni accessorie che circondano le comunicazioni elettroniche.

Un giusto approccio al tema dovrebbe evitare qualsivoglia visione luddista, volta a frenare lo sviluppo di nuove tecnologie che possano essere meglio indirizzate al servizio dell'uomo, delle sue comunità, della scienza e dell'economia.

Un corretto sviluppo orientato dei Big Data, se intrapreso per tempo su scala globale prima che sia troppo tardi, contribuirebbe incisivamente al benessere collettivo, alla prosperità economica e alla sicurezza pubblica. Ma, come evidenziato in un rapporto del febbraio 2015 commissionato dal Presidente Usa (*Big Data, Seizing Opportunities, Preserving Values*), vi sono anche rischi distorsivi e di discriminazione cui prestare attenzione. In un mondo interessato da diverse dinamiche regolatorie in materia di energia, ambiente, scambi commerciali, proliferazione delle armi e lotta al crimine, ora specie informatico, perché mai sulla costruzione delle società tecnologiche del futuro si dovrebbe seguire una logica d'integrale *laissez faire*?

Per l'Europa abbiamo una presenza predominante di piccole e medie imprese e un'industria manifatturiera che senza investimenti innovativi rischia di essere marginalizzata dall'intelligenza artificiale e dalla robotica. Inoltre, come evidenziato dalla Commissione europea nella Comunicazione del 2014 (*Towards a thriving data-driven economy*), soltanto due su venti dei (già allora) Big Data player sono di



matrice europea e dislocati nell'Ue, in un'area peraltro non all'avanguardia tecnologica, come il *cloud computing*. La concentrazione del potere informativo nelle mani di pochi soggetti, destinati a ridursi numericamente specie per fusioni, e per lo più dislocati solo in una o due aree geografiche nel mondo, pone diversi interrogativi, in particolare:

- sulle politiche a tutela dei consumatori;
- sulla necessaria modernizzazione delle discipline antitrust a salvaguardia della competizione in ambito economico, messe a dura prova dall'integrazione multimediale, dalle ripetute fusioni di operatori rapidamente dominanti e dalle norme di rapporti commerciali che vengono meno, dove beni e servizi erano prestati unicamente contro un corrispettivo economicamente valutabile;
- sull'effettiva efficacia e capacità di resistenza delle odierne norme a tutela dei diritti e delle libertà fondamentali in rete, aggiornate a seguito del Trattato di Lisbona e del nuovo valore cogente della Carta dei diritti e delle libertà fondamentali;
- sul riuso dei Big Data a fini pubblici, di ricerca scientifica e sulla legittimazione e capacità tecnica degli organi preposti al mantenimento della sicurezza e alla prevenzione, accertamento e repressione del crimine a impiegare a tali fini queste stesse informazioni, in conformità a un quadro trasparente di regole e garanzie, in ossequio a principi di necessità e proporzionalità.

Oggi, come dimostrano due recenti iniziative legislative presentate dalla Commissione europea il 9 dicembre 2015 – sulla fornitura di contenuti digitali e sulle nuove regole contrattuali per la vendita online di beni tangibili, volte a dare maggiori tutele a utenti e consumatori che usufruiscono di prestazioni per gli stessi apparentemente gratuite, ovvero monetariamente non onerose – gli interessati 'pagano' sempre più attraverso un altro tipo di moneta, che non è il virtuale Bitcoin, ma qualcosa di economicamente più prezioso per le imprese: i dati personali. Tali informazioni rappresentano il nuovo valore di scambio, la moneta del futuro, anzi del presente. Sono crescentemente appetibili per fornitori di beni e servizi perché il loro valore aggiunto, in ragione della possibilità di studiarne le interazioni una volta aggregate su larga scala, va ben oltre il ricavo che se ne può dedurre nell'ambito di una relazione contrattuale.

Le correnti pratiche commerciali di fidelizzazione business-to-consumer, di promozione commerciale diretta e di profilazione bilaterale della clientela continueranno a esistere su piccola e media scala, ma la vera partita della supremazia informativa si gioca già oggi su grande scala. Il potere del futuro, in ambito privato e pubblico, ruota largamente sul possesso esclusivo e aggregato di una moltitudine d'informazioni che permetteranno di conoscere i comportamenti di singoli individui e per segmenti in modo granulare, di intuire gusti e propensioni di acquisto, di profilare, di prevedere comportamenti in rete, d'investire e di pianificare in maniera straordinariamente efficace: «The Winner will take it all» si usa dire. Gli algoritmi e l'intelligenza artificiale consentiranno di individualizzare meglio il carattere e le abitudini delle persone e di costruirne un profilo attendibile, magari più efficace della stessa abilità degli interessati a individuare i connotati della propria personalità.

Già oggi numerose transazioni commerciali in rete generano informazioni all'insaputa degli interessati. L'internet delle cose faciliterà, a nostra eventuale insaputa, il dialogo diretto d'informazioni tra cose e cose, non necessariamente più tra loro e gli individui. Questa possibile opacità, e il conseguente sbilanciamento che si determina nei rapporti economici, potranno aumentare notevolmente fino al punto di rendere occulti luoghi e identità di chi gestirà le leve del potere informativo e i parametri utilizzati per personalizzare offerte commerciali individualizzate.

Tutto ciò pone anche interrogativi sull'integrità e manipolabilità dei dati, rendendo evidente che anche le attività di prevenzione e repressione del crimine, a tutela della sicurezza e a fini d'intelligence potranno, a seconda delle linee politiche delineate, trarre beneficio dai patrimoni informativi aggregati in misura più o meno consistente.

PRIVACY E PROTEZIONE DEI DATI

Sebbene riferita al circoscritto ambito della tutela di diritti e libertà fondamentali – in primo luogo, ma non solo, la riservatezza e la protezione dei dati personali – la nuova disciplina europea post-Lisbona può dare un contributo significativo al temperamento di diritti e d'interessi in materia. Da almeno un quadriennio la privacy è al centro dell'agenda politico-istituzionale dell'Europa che ha una straordinaria opportunità per orientare il dibattito a livello globale. Il 'pacchetto' del 2012, uno dei più complessi e dibattuti, ha ricevuto fermo soste-



gno politico in due vertici dei capi di stato e di governo che ne hanno incoraggiato l'approvazione definitiva dopo un intenso negoziato che ha coinvolto le tre principali istituzioni europee, assistite dal Garante che ha svolto un importante ruolo consultivo.

Il pilastro principale, il Regolamento europeo n. 679/2016 pubblicato sulla Gazzetta ufficiale del 4 maggio 2016, è già in vigore e avrà integrale applicazione anche in chiave di enforcement a partire dal 25 maggio 2018. Altre importanti misure complementari aggiorneranno presto i suoi principi per adattarli al settore delle comunicazioni elettroniche, come pure in tema di funzionamento degli organi, uffici, agenzie e istituzioni dell'Unione e di grandi basi di dati europee in ambito d'immigrazione, sicurezza, amministrazione delle frontiere, asilo, visti, cooperazione di polizia e antifrode.

Una connessa Direttiva europea (n. 680/2016) conforma altri dettagli del regolamento in relazione alle attività di polizia e giudiziarie, e dovrà essere trasposta nell'ordinamento degli Stati membri entro il 6 maggio 2018.

L'Europa si cimenta con questo ambizioso 'pacchetto' per far fronte:

- all'esigenza di armonizzare meglio e presto le normative dei 28 stati membri. Continuiamo a registrare una marcata diversità di norme e di livelli di tutela, non più giustificabile alla luce delle pur esistenti specificità culturali, politiche e normative. L'attuale quadro di asimmetrie di tutela in Europa determina incertezze e inconsistenze, come pure difficoltà per le imprese che operano su scala mondiale. Occorre un salto di qualità perché le sfide globali non consentono più all'Europa di porsi con una normativa così frammentata. Il citato Regolamento ha raccolto la sfida di introdurre una fonte normativa, per quanto possibile, unica;
- all'incessante e frenetico sviluppo di nuove tecnologie che cambia in radice le nostre società. Il legislatore non dovrebbe inseguire tale evoluzione con norme dettagliate che divengono rapidamente obsolete e pongono problemi di neutralità tecnologica. Tuttavia, l'evoluzione di internet e delle grandi reti, gli enormi flussi d'informazioni sull'intero pianeta, l'outsourcing con partner localizzati ovunque nel mondo, il cloud computing, i social network, i motori di ricerca e, da ultimo, il fenomeno dei Big Data e le nuove tecniche di sorveglianza di massa hanno evidenziato tutti i limiti dell'attuale disciplina europea;
- al nuovo quadro giuridico derivante dal Trattato di Lisbona. Introdurre una disciplina per tutelare efficacemente tutti gli indi-

vidui (non solo europei) rispetto al trattamento dei dati che li riguardano, è divenuto un vero e proprio obbligo giuridico per l'Unione. Il Trattato e la Carta dei diritti fondamentali hanno elevato il diritto alla protezione dei dati al rango di diritto fondamentale, separato dal tradizionale diritto alla tutela della sfera privata.

Il Regolamento europeo n. 679/2016 si applicherà a chiunque profili sulla rete – indipendentemente dalla località in cui sia stabilito nel mondo, anche a distanza – l'attività di cittadini dell'Unione o offra agli stessi beni e servizi. Questo riguarderà anche i Big Data?

Oggi, alcune norme europee in materia sono cogenti anche per colossi dell'informazione stabiliti fuori dell'Ue. Con il nuovo Regolamento, la 'giurisdizione' sugli Over the Top si farà più netta e chiara. Sebbene, come si è accennato, solo due dei venti Big Data player attivi nel mondo abbiano oggi il proprio centro di gravità in Europa, quest'ultima si accinge a imporre efficacia extra-europea alle proprie norme che nella società dell'informazione globale non possono avere più una dimensione solo locale, condizionata da un diritto di stabilimento di comodo o dalla dislocazione di convenienza di uffici o server. I giganti dei bit – cui affidiamo sempre più la nostra intera sfera privata che amministriamo nella vita quotidiana tramite pc, smartphone e tablet – dovranno loro malgrado conformarsi a una disciplina regionale (quella europea) che supplirà alle inerzie che si registrano ancora a livello federale statunitense e in altre aree, come nei paesi dell'Asia-Pacific Economic Cooperation (Apec).

Per le molte altre attività cross-border di trattamento delle informazioni personali, il cittadino vedrà assicurata una certa 'prossimità' per quanto riguarda l'esercizio dei diritti, mentre il meccanismo per l'assunzione delle decisioni di fondo – nei confronti d'impresa globali – dovrà essere concordato tra le varie autorità della protezione dei dati e, infine, gestito da una lead authority. Si comprende come in materia si confronti, da un lato, l'esigenza di porsi di fronte ai giganti dell'informazione con un'unica voce europea e, dall'altro, il rischio di accentramento in un solo altro paese (magari competente in base a uno 'stabilimento' di comodo di natura fiscale) delle competenze decisorie su profili crescentemente rilevanti per la tutela dei diritti fondamentali di tutti i cittadini europei.



I Big Data porranno sfide importanti a concetti e principi-cardine della protezione dei dati, come quello di 'dato personale' (diverremo sempre più identificabili o re-identificabili, con un'erosione della definizione di dato anonimo), di 'scopo del dato' (i dati sono riutilizzabili per infinite finalità), di 'titolarità del trattamento' (l'accentramento dei dati moltiplicherà i possibili gestori delle informazioni), di 'gestione limitata nel tempo' ecc. Tuttavia, le norme di nuovo conio in materia di protezione dei dati potranno raggiungere egualmente il loro obiettivo, a condizione che prevalga una visione innovativa e dinamica nella tutela degli individui. Un importante contributo potrà anche venire dall'esortazione del Garante europeo di far interagire più efficacemente queste norme con le discipline a tutela dei consumatori e in materia antitrust.

Va in questo senso l'iniziativa dello stesso Garante di insediare una Digital Clearing House che riunirà, su base volontaria, competenti autorità regolatorie in una rete informale per lo scambio di esperienze e informazioni.

Queste discipline settoriali non possono comunque fornire tutte le risposte alle sfide dei Big Data se non si avvierà anche una riflessione sui valori etici che, in ambito pubblico e privato, si debbono porre a fondamento della collettività del futuro, sul ruolo che l'individuo e la sua dignità avranno in una società basata sul monitoraggio costante dei comportamenti e sul profitto occulto dallo sfruttamento delle informazioni altrui.

Non tutto ciò che è tecnologicamente fattibile è moralmente sostenibile. Si avverte l'esigenza di una riflessione sulla praticabilità di una compensazione su scala etica degli squilibri che si possono determinare nei rapporti economici e in quello stato-cittadino. Per comprendere se, al pari di quanto avviene in alcuni ambiti medici e della genetica, vi sia spazio per:

- la codificazione in chiave evolutiva di principi orizzontali o settoriali;
- l'individuazione di soggetti preposti alla loro enucleazione (i gestori stessi delle informazioni, oppure organi pubblici, autorità preposte o entità 'paritetiche');
- l'attribuzione agli stessi di un qualche valore cogente oppure basato sull'autodisciplina;
- la comprensione di se e come, anche per gli organismi pubblici e di enforcement, sia utile fare riferimento a tali valori.

Per contribuire a questo dibattito, anche sulla base della consultazione pubblica sui risultati preliminari di un alto Gruppo etico consultivo costituito presso la propria istituzione, il Garante europeo ha ricevuto l'incarico dalla Conferenza mondiale delle autorità a tutela della riservatezza e in materia di trasparenza, di organizzare la 40^a edizione (a Bruxelles, nell'ottobre del 2018, presso il Parlamento europeo) la cui sessione pubblica sarà dedicata all'etica e al concetto moderno di dignità applicata alle nuove tecnologie. Un appuntamento pubblico di interesse orizzontale per lo studio delle future dinamiche della gestione e disponibilità delle informazioni.

Le tecnologie non sono mai interamente automatizzate. Il loro sviluppo può essere meglio orientato al servizio dell'uomo, della sua moderna dignità e del benessere collettivo, al di là di quanto si dovrà fare per legge, dal maggio del 2018, per rispettare i nuovi principi giuridici del regolamento sui *privacy by design* e *privacy by default*



BIBLIOGRAFIA

- Article 29 Data Protection Working Party, *Statement 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*, Brussels 2014.
- G. BUTTARELLI, *Speech to Vienna Parliamentary Forum on Intelligence-Security*, Vienna Hofburg, 6 May 2015.
- European Data Protection Supervisor, *Preliminary Opinion on Privacy and Competitiveness in the Age of Big Data, The interplay between data protection, competition law and consumer protection in the Digital Economy*, Brussels 2014.
- European Data Protection Supervisor, *Meeting the challenges of Big Data, Opinion 7/2015*, Brussels 2015.
- European Data Protection Supervisor, *Dissemination and use of intrusive surveillance technologies, Opinion 8/2015*, Brussels 2015.
- European Data Protection Supervisor, *Coherent Enforcement of Fundamental Rights in the Age of Big Data, Opinion 8/2016*, Brussels 2016.
- J. LANIER, *Who Owns the Future?*, San José 2013.
- D. LYON, *Surveillance, Snowden, and Big Data: Capacities, consequences, critique*, Kingston 2014.
- B. SCHNEIER, *Data and Goliath, the hidden battles to collect your data and to control your world*, W.W. Norton & Company, 2015.