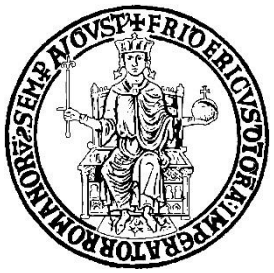
UNIVERSITÀ DEGLI STUDI DI NAPOLI "FEDERICO II"



DIPARTIMENTO DI GIURISPRUDENZA

CORSO DI DOTTORATO IN "SOVRANITÀ E GIURISDIZIONE NELLA STORIA, NELLA TEORIA E NEL DIRITTO CONTEMPORANEO" – XXIX CICLO

Tesi di Dottorato

I *BIG DATA* E GLI EFFETTI SU TRASPARENZA, *PRIVACY* E INIZIATIVA ECONOMICA

Coordinatore del Corso di Dottorato
Ch.mo Prof. Sergio Moccia

Tutor
Ch.ma Prof.ssa Giovanna De Minico

Dottoranda
Dott.ssa Maria Orefice

A mamma e papà

persiane socchiuse, porte sempre aperte.

«Il macigno rotola ancora. Lascio Sisifo ai piedi della montagna! Si ritrova sempre il proprio fardello. Ma Sisifo insegna la fedeltà superiore, che nega gli dei e solleva i macigni. Anch'egli giudica che tutto sia bene. Questo universo, ormai senza padrone, non gli appare sterile né futile. Ogni granello di quella pietra, ogni bagliore minerale di quella montagna, ammantata di notte, formano, da soli, un mondo. Anche la lotta verso la cima basta a riempire il cuore di un uomo. Bisogna immaginare Sisifo felice».

I *BIG DATA* E GLI EFFETTI SU TRASPARENZA, *PRIVACY* E INIZIATIVA ECONOMICA

Introduzione

Con il presente lavoro ci proponiamo di investigare in merito alla compatibilità del nuovo fenomeno dei *Big Data* con i diritti fondamentali, in particolare con il dovere costituzionale della trasparenza e con la *privacy*.

Analizzeremo, ancora, le intersezioni di queste raccolte massive di dati col diritto alla libera competizione, nel tentativo di rielaborare le tradizionali categorie giuridiche, alla luce delle nuove forme di diffusione e comunicazione del pensiero.

L'ambito di indagine di questa tesi è ancora poco conosciuto dalla dottrina pubblicistica italiana, ma a livello europeo - sia accademico che di Corti - è invece da tempo investigato con attenzione, ne sia prova la recente multa comminata dalla Commissione Europea a *Google* per abuso di posizione dominante sul mercato degli acquisti comparativi *online* (*http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740*) e l'indagine formale avviata, sempre nei confronti di *Google*, sul sistema operativo *Android,* oltre al programma di ricerca europea "Horizon 2020".

Esamineremo le implicazioni dei *Big Data*, nozione con la quale si intendono, secondo la descrizione fornita dall'OCSE[1], tutti i contenuti generati dagli utenti in Rete (inclusi *blog*, foto, video; dati comportamentali; dati sociali; dati di geolocalizzazione; dati demografici e dati identificativi in generale) sui seguenti profili:

a) sull'imperativo costituzionale di apertura dei dati al pubblico;
b) sul diritto fondamentale alla *privacy*;
c) sul diritto di iniziativa economica e sulla tutela della concorrenza.

I profili trattati sono evidentemente differenti, ma complementari: essi, infatti, si intersecano con il principio di uguaglianza, che è il filo conduttore delle libertà in Rete.

[1] OCSE, *Exploring the economics of personal data: a Survey of Methodologies for Mesauring Monetary Value*, in *http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en*, p. 7.

L'eguaglianza giuridica, come si vedrà nei capitoli 1 e 3 non si coniuga solo nell'uguale sottoposizione alla legge, ma anche nell'eguale garanzia dei diritti; essa rappresenta la costante tensione delle libertà e in quanto tale impone che tutti i cittadini godano pienamente e in pari misura dei diritti fondamentali.

In riferimento ad a) se gli *open data*, espressione con la quale si intendono i dati raccolti e aperti per lo più dai soggetti pubblici, relativi per esempio al servizio di trasporto o ai tassi di inquinamento delle città, diventano un faro sull'azione di governo e allo stesso tempo elemento strutturale, costitutivo del mercato, al punto che le imprese li pongono al servizio del profitto, allora essi devono essere aperti dalle PP.AA. in formati tali da assicurare a tutti la fruizione, l'utilizzo e il riutilizzo, tanto più se si considera che i dati aperti possono essere impiegati per lo sviluppo di servizi di pubblica utilità, che facilitano il godimento dei diritti fondamentali. Nel tentativo di individuare il regime giuridico più adatto alla loro *governance*, avanzeremo una serie di ipotesi sui formati e le politiche di apertura più adatte al paradigma della trasparenza.

Si aggiunga che con l'affermazione delle nuove tecnologie, la conversione della P.A. da soggetto autoritativo cartaceo a soggetto partecipativo digitale non produce solo effetti positivi in termini di riduzione dei costi, ma ha altresì effetti positivi sulla *e-democracy*, perché consente ai cittadini di partecipare attivamente e agevolmente, mediante la semplice connessione a Internet, alla gestione della *res pubblica*.

Viene esplorato il terreno dei servizi resi dalla Pubblica Amministrazione attraverso Internet e dei diritti fondamentali che la pratica degli *E-services* e dell'*Internet of Things* intercetta.

In riferimento a b) il principio di eguaglianza, sopra menzionato, si traduce nella pretesa dei cittadini di controllare e gestire i propri dati personali. Lo scopo è quello di impedire agli *Over The Top* lo sfruttamento e la monetizzazione dei *Big Data* finalizzati alla discriminazione delle offerte dei prodotti, dei rispettivi prezzi, delle notizie e delle informazioni che circolano in Rete, diverse per ogni utente profilato. La cessione dei dati agli *OTT* per finalità non meglio specificate è successiva all'installazione delle applicazioni

sui dispositivi elettronici ed è condizione necessaria per la fruizione dei servizi offerti dalle applicazioni.

Questo trasferimento, in realtà, non sarebbe libero perché il mercato non offre alternative agli utenti, i quali non hanno a disposizione un *carnet* di applicazioni con *privacy policy* differenti.

Le strategie commerciali *data driven*, i cui termini di funzionamento restano ignoti, incidono inevitabilmente sulla libera formazione dell'individuo, sulla sua capacità di autodeterminarsi, sulla sicurezza e in ultima istanza, sulla sua capacità di votare liberamente, quindi sulla democrazia.

Proprio in questo spazio si ravvisa la necessità di indagare una definizione di *privacy* più calzante alla realtà interconnessa.

A tale scopo analizzeremo l'evoluzione della nozione di riservatezza: dapprima intesa come appropriazione dominicale di uno spazio privato, in cui mettersi comodi - sicuri di non essere osservati - e poi divenuta «strumento necessario per difendere la società delle libertà e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale».

La Rete non ha soltanto accelerato e amplificato il godimento delle libertà fondamentali, ma ha anche esteso la portata del concetto di *privacy*, che ha assunto una valenza proteiforme: la *privacy* in Rete non è scomparsa, al contrario si è moltiplicata in *associational privacy*; *physical privacy*; *informational privacy*; *decisional privacy*; *intellectual privacy*. Ciascuna di queste sfere richiede una tutela specifica.

Passeremo in rassegna la giurisprudenza americana e ci chiederemo se anche i *Big Data* sono coperti dalla cd. «reasonable expectation of privacy», elaborata dalla Corte Suprema US nel 2014, e come questi dati possano essere effettivamente ed efficacemente protetti in un contesto iperconnesso. La Corte nella famosa pronuncia *Riley v. California* ha affermato che la Costituzione americana non lascia il cittadino dinanzi alla scelta di Hobson: vuoi uno *smartphone* (e con esso rinunci a ogni ragionevole aspettativa di *privacy* sulle informazioni che condividi con i terzi) oppure vuoi la ragionevole aspettativa di *privacy* (che esige che tu nasconda i dati inclusi nello *smartphone* e che presuppone un "non utilizzo" dello *smartphone*)?

La Suprema Corte in quell'occasione ha indicato una risposta, evidenziando che «the cell phones are now such a pervasive and insistent part of daily» (sent. *Riley v. California* a p. 2484), per cui utilizzando indifferentemente il servizio di posta elettronica o un'applicazione di messaggistica sullo *smarthphone* l'individuo non intende in alcun modo rinunciare alla sua *privacy*.

Il lavoro, prendendo le mosse dalla giurisprudenza americana, mostra come la condivisione dei dati con terze parti non sminuisca la ragionevole aspettativa di *privacy* protetta dal IV emendamento. Allo stesso modo il fatto che parte di questi dati siano archiviati su *server* remoti, piuttosto che sullo *smartphone*, non riduce l'aspettativa di protezione della propria riservatezza.

Lo studio prosegue con l'attento esame del contesto regolatorio europeo, precisamente con la specifica analisi delle modifiche introdotte dal nuovo Regolamento GPDP 2016/679/UE alla definizione di consenso al trattamento dei propri dati, che ha modificato la vecchia direttiva 95/46/CE.

Ci interrogheremo sul livello di protezione previsto per il trasferimento dei dati verso un paese terzo o un'organizzazione internazionale e ci chiederemo se sia sufficiente ammettere un trasferimento dei dati a un Paese terzo, se esso si limita ad assicurare garanzie adeguate (artt. 46-47 Reg. 2016/679/UE) e non equivalenti, e se questo scambio, che abbassa la protezione della *privacy,* possa tutelare efficacemente la riservatezza dei cittadini europei.

Analogamente, in riferimento a c) osserveremo che se i dati raccolti dagli OTT, diventano *asset* strategico esclusivo di pochi *players,* che li utilizzano per estendere la propria dominanza in altri settori e si fanno barriera all'ingresso per i nuovi *competitors*, ne risulta falsato il gioco della concorrenza, anche a danno del consumatore, costretto a scegliere i servizi offerti dall'operatore dominante, in assenza di una valida alternativa.

In questo modo ci renderemo conto che servizi apparentemente liberi, come la scelta di utilizzare *Gmail* per la gestione della posta elettronica, *Chrome* come *browser* di ricerca, *Youtube* per visualizzare un video, *Google maps* per navigare - non a caso tutti di proprietà

di *Google* - sono «imposti» dall'assenza di alternative o dall'utilizzo del sistema operativo *Android*.

Successivamente, approfondiremo lo studio dell'indagine aperta dalla Commissione Europea nei confronti di *Google*, conclusasi con l'accertamento dell'abuso e l'irrogazione di una multa, e avanzeremo la possibilità di un nuovo approccio nella definizione del mercato rilevante, dal quale emergerebbe *ictu oculi* la condotta abusiva del dominante su una pluralità di servizi, apparentemente operanti su mercati diversi.

Secondo l'autrice, occorrerebbe guardare non alla quota di mercato, ma al numero di utenti iscritti ai servizi *Google*. Si dovrebbe parlare di un mercato di utenti perché *Google* opererebbe come rivenditore di informazioni degli utenti sulla base di un costante *profiling*: questo dovrebbe essere il criterio rilevante per definire il mercato.

Se il mercato di riferimento non è quello della ricerca o della pubblicità, ma quello dei dati, nei rivenditori di informazioni personali si dovrebbero individuare i reali concorrenti: si pensi a *Facebook*, *Twitter*, *Instagram* e agli altri fornitori di servizi di posta elettronica, per esempio, i quali non dovrebbero sfuggire a quest'analisi.

Tutti questi soggetti inseriscono pubblicità nella pagina dei loro servizi per estrarre dati, fonte remunerativa dei loro servizi.

Dunque, la titolarità dei dati si imporrebbe come *essential facility*, di carattere immateriale, indispensabile per competere sul mercato, da ciò deriverebbe l'obbligo di aprire i dati in capo ai *Big* della Rete.

Tale imperativo produrrebbe benefici per la concorrenza in quanto favorirebbe l'innovazione tecnologica e la qualità dei servizi, mediante l'apertura a più concorrenti, i quali avrebbero accesso a tutti i dati che acquisirebbero i caratteri del bene pubblico.

Tirando le somme del ragionamento svolto, discuteremo con rigore scientifico delle problematicità connesse, rispettivamente, alle contrastanti esigenze, da una parte, di chiusura (*rectius* controllo) dei dati, dettate dalla tutela della *privacy* e, dall'altra, di apertura degli stessi, domandate dall'efficace spiegarsi del principio di trasparenza, nel tentativo di individuare una soluzione regolatoria condivisa ed efficace, indispensabile a una penetrazione di garanzie a tutti i livelli.

La ricerca condotta ha registrato, invece, *de facto* un'inversione di rotta nel perseguimento del risultato tra la diffusione indiscriminata dei dati personali, sotto forma di *big data* - i quali oggi sfuggono, come ampiamente sarà esplicato nel prosieguo, dalle mani dei loro legittimi proprietari - e la gelosa chiusura dei dati da parte delle PPAA, custode arcigna delle informazioni degli amministrati, che, proprio perché appartenenti a loro, dovrebbero essere loro restituite.

Una simile deviazione dovrebbe essere corretta dall'intervento del *policy maker*.

Il nuovo *habitat* delle libertà fondamentali invocherebbe un intervento normativo speciale che, partendo da un'interpretazione evolutiva delle Costituzioni nazionali e dalle Carte internazionali[2], recepisca i nuovi caratteri del mezzo, le nuove logiche di mercato e conseguentemente elabori nuovi paradigmi *antitrust* per consentire l'efficace tutela della concorrenza, delle libertà e della tutela del consumatore. Questo tipo di intervento eteronomo dovrebbe tenere conto delle caratteristiche del nuovo terreno di gioco delle transazioni economiche e delle libertà, nonché della posizione di chi è già in dominanza e intende rafforzarla, o lo sta già facendo per moltiplicare il suo iniziale vantaggio politico-economico, indisturbato.

I *Big Data* non sono neutrali, buoni o cattivi, ma devono essere declinati a favore dell'eguaglianza, della concorrenza per piegare, ora la loro protezione, ora il loro utilizzo ai bisogni dei più deboli, offrendo un'occasione di effettiva inclusione politica agli individui nel compimento di quella dimensione costituzionale annunciata negli artt. 2 e 3, comma 2, Cost..

Per una tutela efficace - proprio perché i vecchi rimedi si sono rivelati carenti in quanto riferiti a un mezzo i cui effetti erano limitati nello spazio – sarebbe necessario l'intervento del legislatore sovranazionale, con norme speciali, che partendo dai diritti fondamentali universalmente riconosciuti, riveda il diritto *antitrust* e la tutela dell'utente in Rete, alla luce dei cambiamenti tecnologici per definire i nuovi mercati rilevanti, su cui operano gli *Over the Top*, le responsabilità e i rimedi al ripristino della situazione *quo ante* le fratture competitive.

---

[2] A mero titolo semplificativo si richiama la Dichiarazione universale dei diritti dell'uomo, 1948, art. 19; Patto sui diritti civili e politici, 1966, art. 19; CEDU, 1950, articolo 10; TUE, art. 6,§§ 1-2 TUE; Carta dei diritti fondamentali dell'Unione Europea, 2000, artt. 11 § 2, 42.

Al fine di ristabilire la concorrenzialità del mercato sarebbero necessari una serie di aggiustamenti, volti a favorire una maggiore competitività tra le imprese.

In base all'art. 7 del Regolamento (CE) n.1/2003 la Commissione, constatata l'infrazione di cui all'articolo 102 TFUE, può obbligare, mediante decisione, a porre fine all'infrazione. A tal fine, può imporre all'impresa l'adozione di tutti i rimedi comportamentali o strutturali, proporzionati alla violazione commessa e, necessari, a far cessare effettivamente l'infrazione stessa. I rimedi strutturali possono essere imposti solo quando non esiste un rimedio comportamentale parimenti efficace o quando un rimedio comportamentale parimenti efficace sarebbe più oneroso, per l'impresa interessata, del rimedio strutturale.

I rimedi sono proposti dall'azienda ma devono essere proporzionali ed efficaci, e, se ritenuti rispondenti alle preoccupazioni espresse dalla Commissione nella sua valutazione preliminare, la Commissione può, mediante decisione, renderli obbligatori per le imprese (art. 9 del citato Regolamento).

Lo scopo che si vuole raggiungere è di ristabilire la concorrenza, far cessare la violazione e disincentivare la reiterazione dell'infrazione *pro futuro*. La concorrenza a cui si tende, non sarà una concorrenza perfetta del mercato, ma semplicemente il ripristino della situazione *quo ante*.

Non sarebbero sufficienti, stante l'ampiezza del portafogli di *Google*, i rimedi classici, quali l'azione risarcitoria, le sanzioni pecuniarie - come quella di recente irrogata in una misura pari a 2,42 miliardi di euro, seppure la più alta sanzione mai comminata dall'*Antitrust* europeo per abuso di posizione dominante - i provvedimenti a contenuto prevalentemente inibitorio o di *reductio in pristinum*. L'atto di immediata desistenza dalla condotta abusiva non sarebbe in grado di modificare la situazione di fatto che si è affermata sul mercato e, se emesso, sarebbe agevolmente eluso, date le peculiarità della Rete, terreno di ricaduta del provvedimento inibitorio. Si potrebbe subordinare, allora, l'autorizzazione a specifiche condizioni, ossia a impegni concreti dell'impresa, volti a evitare che la concorrenza venga falsata. L'impresa si potrebbe impegnare a cedere una parte della sua attività o a dare in licenza una determinata «tecnologia» a un altro operatore. Se la Commissione o l'Autorità *antitrust* nazionale è convinta che gli impegni possano

mantenere o ristabilire la concorrenza sul mercato, la autorizza, salvo verificare poi che l'impresa rispetti le condizioni concordate; in caso contrario, può prendere ulteriori provvedimenti. E, proprio in questo contesto, come anticipato, sarebbe pensabile un rimedio che consista nell'obbligo di condividere i dati con i terzi concorrenti.

A questo punto il cerchio si chiude: i dati sono polivalenti, mostrano facce diverse, e possono perseguire obiettivi contrastanti, da un lato essi sono strumento democratico perché i diritti fondamentali e le libertà costituzionali, che la loro conoscenza e il loro utilizzo consentono di esercitare in forma più piena rispetto al passato, hanno un radicamento popolare: «si riferiscono al "popolo" nella totalità dei suoi componenti ed esprimono perciò, in capo a ciascuno, un frammento di sovranità»; dall'altro essi sono informazioni personali, talora sensibili, da proteggere nonché *key asset* del *fair play* competitivo.

Allora serve una regolazione che tenga insieme questa pluralità di valenze ed esiga che a guidare l'apertura dei dati e la loro condivisione con il pubblico sia un'operazione di «minimization», che non annacqui le potenzialità dei dati, ma coniughi la loro democratizzazione con la loro anonimizzazione. Solo in questo modo avremo utilizzato appieno le opportunità delle tecnologie, a vantaggio di tutti.

Capitolo I

L'apertura dei dati al pubblico e l'imperativo costituzionale

SOMMARIO: 1. Gli *Open Data*, una declinazione dei *Big Data*: la fonte giuridica (1.1. *Esempi più significativi di uso sociale degli* Open Data - *1.2. Lo stato dell'arte*). – 2. L'*Open Data Policy* nel panorama internazionale: il modello *FOIA* (2.1. *Lettura parallela tra il recente modello italiano e il parametro del Foia statunitense*). - 3. L'accesso generalizzato e la sua logica sottesa: i *closed data* (3.1. *Le criticità del decreto legislativo 97/2016. Le eccezioni all'accesso e le Linee Guida Anac*). - 4. Le variabili di apertura dei dati: la necessità del dato grezzo – 5. Gli *open data* come ancella del mercato.

1. Gli *Open Data*, una declinazione dei *Big Data*: la fonte giuridica

La nozione di *Open Data* (*rectius Open Government Data*) viene generalmente riferita a tutti i dati detenuti e aperti dalle pubbliche amministrazioni; essa è dunque *species* del più ampio *genus* di *Big Data*[3], per quest'ultima si intende la raccolta di dati, non necessariamente aperti, aggregati da soggetti indistintamente pubblici e privati[4].

Quanto al concetto di *Open Data* non si è ancora raggiunta una posizione unanime in dottrina: infatti, per i più gli *Open Data* si riferirebbero agli *Open Government Data* e includerebbero esclusivamente i dati aperti, generati e detenuti dal governo e dalle pubbliche amministrazioni[5], la loro apertura rappresenterebbe, in altre parole, l'aspetto caratterizzante dell'*Open Government*[6]; per altri invece gli *Open Data* abbraccerebbero anche i dati generati, detenuti e pubblicati dai privati[7]. Si pensi ai dati che possono essere pubblicati in forma di *database* sui temi più disparati da Istituti e Centri di Ricerca, Ong, Associazioni *non profit*, Fondazioni, laboratori e specificamente, per esempio, ai dati scientifici condivisi tra i ricercatori per accelerare il progresso e trovare nuovi trattamenti e cure contro malattie gravi nel settore della telemedicina[8].

Nell'uno e nell'altro caso, per definire aperti i dati è necessario che posseggano alcuni requisiti: accessibili[9] attraverso la connessione a Internet, senza limitazioni collegate

---

[3] Per un approfondimento della nozione di *Open Data* ci sia consentito rinviare all'articolo pubblicato dall'autrice M. OREFICE, *Gli* open data *tra principio e azione: lo stato di avanzamento*, in www.forumcostituzionale.it, 25 maggio 2015, p. 1 ss., almeno per il ricco apparato di note.

[4] Si pensi per esempio ai dati che il governo raccoglie sugli individui per la sicurezza nazionale o che i venditori raccolgono sui loro clienti, e che forniscono a queste entità informazioni che gli individui potrebbero anche non desiderare.

[5] *Ex multis* cfr. C. ROMAN, *Open data*, in *ConLawNOW* 19, 2016 p. 19; D. RONCI, *Il Governo Aperto*, Roma, Feltrinelli, Gruppo Editoriale L'Espresso, 2015, p. 132.

[6] C. J. TOLBERT – K. MOSSBERGER, *The Effects of E-Government on Trust and Confidence in Government*, in *Public Administration Review*, May-June 2006, p. 354. Il paradigma *open* è tratto indispensabile dell'*e-government* così definito dagli autori: «E-government holds promise for improved delivery of many types of public services, including online transactions, and for disseminating information about the operation of government. It can improve communication between citizens and government through e-mail, enabling more direct participation in government decision making».

[7] Cfr. con schema di insiemi di dati proposto da Gurin in J. GURIN, *Big Data and Open Data: How Open Will the Future Be?*, in *10 ISJLP*, 691 2014-2015, p. 692 ss..

[8] Sull'applicazione del *data sharing* all'*e-health* cfr. con Rivista *MIT Technology Review*, vol. 117, n. 5.

[9] Secondo il progetto *Open Definition* di *Open Knowledge Foundation* «A piece of content or data is open if anyone is free to use, reuse, and redistribute it — subject only, at most, to the requirement to attribute and share-alike». Confronta anche con le *Ten Open data Guidelines - Transparency International Georgia* dove sono stabiliti i caratteri dei

all'identità o allo scopo dell'utente; elaborabili da un'applicazione informatica senza che sia necessaria la disponibilità di uno specifico *software*; accompagnati da licenze che non pongano restrizioni sull'uso e sul riuso[10].

La logica sottesa a questa tipologia di dati è simile a quella che ha condotto all'affermazione di sistemi aperti di condivisione della conoscenza: quali l'*open source*, l'*open access* e l'*open content*[11].

L'apertura dei dati al pubblico perseguirebbe una serie di finalità, non tanto il reperire notizie su appalti e concessioni, accedere a *curricula* e competenze di professionisti in un *click*, quanto permettere ai cittadini di conoscere l'importo esatto delle voci di spesa sopportate dal Comune di residenza - e di avere una panoramica su bilanci, rimborsi e compensi degli amministratori. Queste voci, se riferite ad anni diversi, consentono anche di confrontarle con quelle degli anni precedenti, in questo modo gli elettori possono verificare l'operato dei propri governanti e conseguentemente orientare con maggiore cognizione il proprio voto[12].

In altre parole l'apertura dei dati faciliterebbe l'esercizio dei diritti fondamentali e delle "vecchie" libertà trasferite nel nuovo *habitat* della Rete[13]:

---

dati aperti, che devono essere: 1) completi; 2) primari; 3) tempestivi; 4) accessibili; 5) leggibili dai computer; 6) in formati non proprietari; 7) liberi da licenze; 8) riutilizzabili; 9) ricercabili; 10) permanenti, in http://www.transparency.ge/en/node/1088 e con gli 8 *Open Government Data Principles* in https://public.resource.org/8_principles.html, dove è specificato che possono, tuttavia, essere consentite restrizioni ragionevoli legate alla *privacy*, alla sicurezza o a diritti proprietari e che la compatibilità deve essere aggiornabile, nonché con i principi che definiscono la conoscenza aperta, in http://opendefinition.org/od/1.0/it/, sviluppati dagli 11 principi *open source,* in https://opensource.org/osd.html.

[10] L'art. 2, lett. e), D. Lgs. 36/2006 (che riprende la direttiva relativa al riutilizzo dell'informazione del settore pubblico anche nota come Direttiva PSI), contiene la definizione di "riutilizzo": «l'uso del dato di cui è titolare una pubblica amministrazione o un organismo di diritto pubblico, da parte di persone fisiche o giuridiche, a fini commerciali o non commerciali diversi dallo scopo iniziale per il quale il documento che lo rappresenta è stato prodotto nell'ambito dei fini istituzionali». La nozione di dato pubblico, quale dato "conoscibile da chiunque", è contenuta nell'art. 2, lett. d), D. Lgs. 36/2006 (ed è ripresa nel D. Lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale).

[11] A. M. TAMMARO, Open Source*,* Open Access *ed* Open Content: *verso sistemi aperti di condivisione della conoscenza,* in Comunicazione al Convegno *Open Culture. Accessing and sharing knowledge*, tenutosi a Milano dal 27 al 29 giugno 2005, in https://www.academia.edu/3031518/Open_Source_Open_Access_ed_Open_Content_verso_sistemi_aperti_di_condivisione_della_conoscenza

[12] Si confronti con i servizi resi dalla piattaforma open source open bilanci, in *http://www.openpolis.it/progetti/openbilanci/*.

[13] Sull'esercizio delle libertà in Rete cfr. G. AZZARITI, *Internet e Costituzione*, in www.costituzionalismi.it, 6 ottobre 2011 p. 1-8; G. DE MINICO, *Antiche libertà e nuova frontiera digitale*, Giappichelli, Torino, 2016, p. 43 ss.; ID., *Tecnica e diritti sociali nella* regulation *della banda larga*, in G. DE MINICO (a cura di), *Dalla tecnica ai diritti. Il caso della banda larga*, Jovene, 2010, p. 3 ss.; T. E. FROSINI, *Liberté Egalité Internet*, Editoriale Scientifica, Napoli, 2015, *passim;* ID., *Tecnologie*

L'O*pen Data*, come l'espressione più percettibile in chiave moderna del principio di trasparenza, si farebbe «precondizione dell'effettività dei diritti fondamentali, sanciti dalla Carta costituzionale»[14] e diventerebbe strumento necessario per lo sviluppo economico, nonché amplificatore della partecipazione democratica alla *res pubblica*[15]. Una simile politica di apertura apre spazi inediti di esercizio della sovranità popolare, inaugurando un modello di cittadinanza più pervasiva ed efficace, già presente implicitamente nelle maglie larghe del dettato costituzionale[16] e contribuisce alla creazione di un modello di «*see-through society*»[17].

L'Amministrazione è pertanto chiamata a impegnarsi per favorire, da un lato, l'autonoma iniziativa del singolo liberando i dati che ella possiede, con licenza *standard* al fine di offrire i prodotti della sua funzione istituzionale[18], in ossequio al dovere di trasparenza, *ex* artt. 1, 2, 21, 48, 97[19] della Costituzione.

Dall'altro lato, la stessa sarebbe parimenti tenuta a favorire questo flusso continuativo di dati per fornire materia prima agli chi li utilizzerà; in questa seconda ipotesi l'Amministrazione agirebbe in conformità con l'articolo 41 della Cost. – come l'utilità sociale impone, nonché in ossequio al principio di sussidiarietà orizzontale.

L'articolo 118.4, Cost. delinea in capo al singolo «un diritto fondamentale, quello della persona a sostituirsi o affiancarsi all'amministrazione nel rendere un'attività di

---

e libertà costituzionali, in *Dir. Informatica*, 2003, 3, p. 487; S. NIGER, *Internet, democrazia e valori costituzionali*, in *Astrid*, 2011, p. 22 ss.; G. ABELTINO, *Internet e libertà fondamentali: trovare un* fil rouge, in O. POLLICINO - E. BERTOLINI - V. LUBELLO (a cura di), *Internet: regole e tutela dei diritti fondamentali,* Aracne, 2013, p. 71 ss.

[14] M. OREFICE, *op. cit.,* p. 3, cit.; con riferimento alla capacità dei dati di incidere sui diritti costituzionali cfr. V. MAYER-SCÖNBERGER - K. CUKIER, *Big Data. Una rivoluzione che trasformerà il modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013, p. 237 ss. ripresa dall'autrice M. OREFICE, *I Big Data. Regole e concorrenza*, in *Politica del diritto*, 4/2016, p. 711 ss.

[15] G. VILELLA, *Innovazione tecnologica e democrazia*, Pendragon, Bologna, 2015, *passim*.

[16] C. ROMANO, *Open data e riutilizzo nel decreto trasparenza: propulsore per la democrazia e lo sviluppo o sfida ulteriore per i diritti fondamentali?*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Collana Crispel, Università degli Studi Roma Tre, 2014, p. 266.

[17] J. GURIN, *op. cit.*, p. 692, cit.

[18] G. MANCOSU, *La transparence publique à l'ère de l'Open Data. Étude comparée Italie-France*, Thèse de doctorat en Droit public, Université Panthéon-Assas (Paris 2), 29 mars 2016.

[19] M. R. SPASIANO, *Il principio di buon andamento: dal metagiuridico alla logica del risultato in senso giuridico*, in *Ius Pubblicum Network Review*, aprile 2011, pp. 15 e ss; L. IANNUCCILLI - A. DE TURA, *Il principio di buon andamento dell'amministrazione nella giurisprudenza della corte costituzionale* (a cura di), in http://www.cortecostituzionale.it/documenti/convegni_seminari/STU_212.pdf.

pubblica utilità in ragione del vincolo solidaristico»[20] o ancora per migliorare e ampliare il patrimonio informativo. La stessa pubblica amministrazione sarà destinataria di quei dati che mediante l'interoperabilità, ovverosia attraverso sistemi condivisi che consentono l'accesso e l'utilizzo delle informazioni e delle funzionalità incorporate nelle piattaforme pubbliche, saranno fruibili e utilizzabili da altri uffici pubblici per l'erogazione di servizi al cittadino o la creazione di altri dati *linkati*[21].

C'è un denominatore comune tra l'art. 41 e l'art. 118.4, Cost. nello strumento del patrimonio comune dei dati utilizzabili per il perseguimento di obiettivi di utilità sociale. Nell'uno e nell'altro caso l'amministrazione è chiamata a rilasciare i dati per fare in modo che l'iniziativa economica e l'autonoma iniziativa dei cittadini, singoli e associati, si spieghino in conformità all'utilità sociale. L'*output* della p.a. (che libera i dati) si traduce in *input* per la stessa p.a. nel momento in cui la condivisione dei dati ne assicura il buon andamento, di cui all'art. 97.2, Cost.

I dati così rilasciati possono essere utilizzati in applicazioni "intelligenti" per aiutare i consumatori a fare scelte complesse[22].

Una dimostrazione emblematica di come le aziende possano tradurre in *business* le risorse racchiuse nei dati, aggiungendo valore agli stessi, è dato dalla *Climate Corporation*, che ha iniziato ad analizzare i dati aperti sul meteo per studiarne l'impatto degli agenti atmosferici sull'agricoltura e creare un sistema di vendita di assicurazioni a misura di agricoltore. Ma per farlo ha dovuto sviluppare un elevato livello di competenza per capire come le condizioni meteorologiche, il suolo e le condizioni agricole possano incidere sui raccolti e quali rischi possano causare ai raccolti.

Gli esempi sono innumerevoli[23].

---

[20] G. DE MINICO, *Gli* open data*: una politica costituzionalmente necessaria"?*, in *www.forumcostituzionale.it*, 12 giugno 2014, p. 4, cit..

[21] Per la definizione di *linked data* sia consentito il richiamo al *paper* dell'autrice M. OREFICE, *I* Big Data. *Regole e Concorrenza*, in *Politica del diritto*, 4/2016, p. 713 ss..

[22] Gurin nell'articolo citato offre l'esempio pratico della scelta di un volo aereo, l'autore sostiene che senza questi strumenti (applicazioni che usano dati aperti), sarebbe straordinariamente difficile scegliere fra le centinaia di voli ogni giorno tra Miami e Città del Messico, e trovare il volo che meglio soddisfa le proprie esigenze. Aggiunge l'esempio del servizio *GreatSchools*, che utilizza *Open Data* per aiutare i genitori a trovare scuole che saranno a misura dei loro figli. *GreatSchools* utilizza sia il *feedback* che sul sito viene rilasciato dai genitori e dagli ex studenti sia i dati derivanti da valutazioni formali a livello nazionale ed è usato dal 40% delle famiglie americane.

[23] Gli esempi sono presi in prestito a Gurin in J. GURIN, *op. cit.*, p. 694 ss..

L'applicazione *ITriage Health* consente a un viaggiatore in una città straniera, che lamenti dolore toracico, di cercare i suoi sintomi, capire se il problema ha bisogno di una cura urgente e, in caso affermativo, di trovare l'unità di pronto soccorso più vicina.

Un'altra società, *Aidin* ha sviluppato un servizio che sta utilizzando dati governativi aperti per migliorare la cura post-ospedaliera, mentre *Eviderao* utilizza dati sulla salute per predire l'efficacia dei diversi trattamenti.

Opower, una società con sede nell'area di Washington DC, combina i dati sull'efficienza energetica con i dati relativi all'utilizzo di energia di un singolo nucleo familiare e utilizza queste informazioni con lo scopo di far risparmiare corrente ai consumatori. Quest'applicazione fornisce anche un'analisi di quanta energia utilizzano i vicini, per spronare la competizione. Spingere le persone a ridurre il consumo energetico non è semplice, ma *Opower* sta riscuotendo un grande successo. Molte aziende stanno lavorando a come rendere più utili i dati di governo per altre aziende. *Enigma.io* raccoglie gli *Open Data* di fonti federali, statali e locali e li carica su una piattaforma tecnica, appositamente sviluppata, in modo che possa essere utilizzata più facilmente dal pubblico per analizzare e generare nuove intuizioni. Oltre a rendere l'accesso ai dati pubblici gratuiti sulla sua piattaforma, *Enigma.io* fornisce informazioni più approfondite dietro abbonamento ai suoi servizi alle aziende che desiderano utilizzare questi dati per le loro particolari esigenze.

Da qui emerge chiaramente che la liberazione dei dati, definita *Smart Disclosure*, non è dettata solo da esigenze di trasparenza e da ragioni di controllo dei governi, ma è definita anche e in maniera forse più preponderante, dall'esigenza di partecipare alla cosa pubblica[24], migliorare l'assistenza sanitaria, orientandola verso l'uguaglianza[25], l'istruzione, l'energia, i trasporti, i servizi finanziari e così via, o dalla semplice volontà di avviare un'attività economica, che potrebbe comunque tradursi nella fornitura di servizi utili alla

[24] *Supra* nota 15.

[25] Cfr. con la Rivista *MIT Technology Review*, vol. 117, n. 5, la quale passa in rassegna una serie di progetti alimentati dai dati e applicati alla telemedicina. Il progetto di *IBM* denominato *Watson* ha lo scopo di rendere la competenza medica oncologica una merce. Se le malattie aumentano più del numero di specialisti, questa sproporzione potrebbe ripercuotersi sulla tutela della salute perché ci saranno pochi specialisti formati ad alti livelli, alla portata dei pazienti più ricchi. Piattaforme mediche alimentate da dati aperti, rompono il monopolio degli esseri umani sulla competenza sul cancro e consentono di esercitare agevolmente diritti fondamentali.

collettività. I dati possono essere impiegati anche per rendere la città ecologica e vivibile, cioè per puntare sull'energia rinnovabile[26] mediante piattaforme alimentate dai cittadini che possono inserire autonomamente dati e segnalazioni[27] su rete elettrica, traffico, inquinamento[28], consumo idrico, illuminazione pubblica al fine di pianificare aree verdi, gestione del traffico, rendere più efficiente la fornitura di energia con lo sviluppo di soluzioni innovative anche del settore privato, non necessariamente a spese della municipalità. Per trasformare, infatti, una città in *smart* serve conoscerla.

Il radicamento costituzionale dell'apertura risiederebbe negli articoli 1, 3, 41, 32, 48, 97. Qui, preme chiarire che ciascun articolo gioca nella relazione con il principio di apertura un ruolo diverso: per esempio gli articoli 1 e 3 costituiscono la finalità dell'obbligo di apertura perché i dati si liberano per consentire ai cittadini di essere sovrani nonché tutti uguali; rispetto agli articoli 32 e 41 l'apertura è la condizione di effettività del diritto di iniziativa ivi incluso, in quanto solo se i dati sono accessibili possono essere utilizzati per la tutela della salute pubblica e lo svolgimento di un'attività di impresa seppure per fini di utilità sociale.

Si sta affermando un nuovo approccio anche nel settore scientifico, dove i dati relativi alla ricerca vengono sempre più condivisi per amplificarne le esternalità positive. Si ribalta la vecchia logica della segretezza che spingeva gli scienziati dell'industria farmaceutica a mantenere i dati per sé fino allo sviluppo di prodotti brevettabili.

Questo perché i vecchi approcci segreti non si sono rivelati favorevoli al progresso e allo sviluppo.

Al contrario, modello più collaborativo, che molti scienziati credono debba essere seguito adesso, è stato sperimentato nel Progetto Genoma Umano, che ha esemplificato un approccio che ha visto accelerare notevolmente il progresso scientifico. Allo stesso modo, diverse fondazioni biomediche, come la *Multiple Myeloma Research Foundation*, ora

---

[26] Cfr. con *Copenhaghen big data platform.*

[27] Tramite *tablet* o *smartphone* con apposita *app,* oppure con foto e *tweet,* se per esempio l'illuminazione non funziona o il riscaldamento è troppo alto.

[28] L'inquinamento uccide 8 milioni di persone nel mondo all'anno. Il software *BreezoMeter* elaborato da una *startup* fondata da alcuni israeliani consente di reperire dati su qualità dell'aria e livello di inquinamento in ogni quartiere del mondo.

richiedono ai loro concessionari di condividere i propri dati come condizione di finanziamento[29].

La condivisione dei dati produce benefici perché aiuta gli scienziati a superare gli ostacoli che si frappongono nella loro ricerca. L'approccio noto come il *crowdsourcing*[30] consente a migliaia di volontari di contribuire a rendere più utili i dati scientifici aperti, creando un nuovo modello di *open enterprise* nel *problem solving*. L'esempio è offerto dal sito *Zooniverse*, avviato da uno studente di dottorato che doveva osservare la struttura delle galassie usando immagini dal telescopio *Hubble*. A tal fine, dal momento che l'occhio umano meglio del computer si è mostrato adatto a questo tipo di analisi, lo studioso ha trovato un modo per analizzare novecentomila immagini per il suo lavoro: insieme ai suoi colleghi ha pubblicato le immagini *online*, fornendo indicazioni semplici su come identificare il particolare tipo di galassia che cercava e ha invitato il pubblico a partecipare. Decine di migliaia di persone si sono offerte volontarie. *Zooniverse* ha ora applicato lo stesso approccio a una vasta gamma di problemi scientifici, tra cui la ricerca sul cancro, problemi climatici e astrofisici. Dunque la folla (*crowd*), grazie alla Rete, contribuisce alla creazione di un'intelligenza collettiva che partendo dal basso[31] innesca un circuito produttivo di conoscenze a vantaggio dell'intera comunità. Queste iniziative sono esempi di costruzioni orizzontali del diritto che prendono avvio dalla fonte costituzionale[32] e implementano l'effettività e l'efficacia dei diritti fondamentali.

---

[29] J. GURIN, *op. cit.*, p. 696.

[30] ID., *op. cit.*, *ivi*, p. 697, cit.

[31] A Saronno c'è un sistema per monitorare in tempo reale i posti auto disponibili e trovare subito parcheggio. A Venezia la possibilità per i dipendenti comunali di denunciare in forma anonima i colleghi corrotti. A Milano una piattaforma di crowdfunding per finanziare coi fondi pubblici i progetti sociali che raccolgono almeno il 50 per cento dei contributi dai privati. Sono soltanto alcune delle idee con cui la burocrazia prova a svecchiarsi aiutata dalle nuove tecnologie. Si ascolti la puntata della trasmissione radiofonica *Eta Beta* del 22/05/2017 - *Sharing, app e crowdfunding, la burocrazia ai tempi dei social*, in *http://www.etabeta.rai.it/dl/portaleRadio/media/ContentItem-91169551-ef99-4954-bf77-20198a2677f3.html*.

[32] Articoli 118.4, 21,41,48, 97 etc.

1.1. *Esempi più significativi di uso sociale degli* Open Data

Offriamo una panoramica delle principali utilizzazioni degli *Open Data* a fini di utilità sociale, sulle quali è ampia la letteratura sociologica che non costituisce però oggetto della nostra materia di esame, ma ha costituito uno spunto illuminante per ricostruire un quadro d'insieme.

Le attività degli utenti *online* hanno creato un registro di dati su tutto, dai prodotti e servizi al consumo alle tendenze politiche: ora è possibile analizzare questi dati attraverso un nuovo approccio noto come *sentiment analysis*, che utilizza un insieme di tecniche di analisi di testo e di altre forme di dati per estrarre e analizzare opinioni e intuizioni sui prodotti, sui servizi e le tendenze.

L'analisi dell'opinione è uno strumento emergente per la strategia di *marketing* e *business* e può essere utilizzato anche per il bene sociale. A Washington, DC in due anni, l'Ufficio del Sindaco ha utilizzato la *sentiment analysis*[33] per valutare e analizzare ciò che le persone dicono sui *social media* delle agenzie governative, come il *Department of Motor Vehicles*. Il sistema di *feedback* si è rivelato un modo per migliorare le azioni di governo.

Gli *Open Data* alimentano anche le *Smart Cities*[34] perché i dati possono aiutare le città a conoscere i suoi punti di debolezza e di forza e a gestirsi meglio. Diversi centri di ricerca in tutto il mondo, tra cui il *Center for Urban Science and Progress* di New York[35], stanno analizzando i diversi tipi di fenomeni urbani, che vanno dai dati raccolti dal governo agli studi sui modelli di traffico e sui cambiamenti ambientali, misurati dai sensori nelle città. Questi dati aperti possono essere utilizzati per ottimizzare gli interventi nelle città, monitorare le infrastrutture e migliorare la salute pubblica, la gestione delle emergenze e altro ancora.

Una delle prime applicazioni sviluppate ha riguardato il trasporto pubblico: *Nextbus*[36] indica quando arriva il bus, in questo modo non si dovrà aspettare sotto la pioggia, per esempio, perché si viene informati anche se il bus tarderà e di quanti minuti. Poiché

---

[33] ID., *op. cit.*, *ibidem*.

[34] ID., *op. cit.*, 698, cit.

[35] in http://cusp.nyu.edu/.

[36] in *http://cts.cubic.com/en-us/solutions/real-timepassengerinformation/nextbus,inc.aspx*.

Nextbus ha iniziato a sviluppare applicazioni anche per altre città, le città stesse hanno ritenuto utile impegnarsi per aprire i dati di trasporto in un formato *standard* al fine di rendere più agevole per l'azienda fornire questo servizio. Si afferma un nuovo tipo di solidarietà collettiva, alimentata dai dati.

OpenGov[37] ha sviluppato una piattaforma che consente a qualsiasi città del paese di mettere i propri dati finanziari in un semplice grafico. I *budget* della città sono generalmente conservati in fogli di calcolo difficili da leggere. La piattaforma *OpenGov* ha aperto quei dati in un modo più trasparente per i cittadini, ma consente anche ai sindaci di confrontarli con quelli delle città vicine su dimensioni come la *performance* finanziaria o le ore di lavoro extra della polizia[38], innescando un circolo virtuoso di efficienza.

Dunque, il modello *open* incentiverebbe oltre l'economia immateriale, anche l'innovazione civica[39], mediante il *civic hacking*[40], legato al modello dell'*innovation without permission*. Si tratta di un approccio fondamentale per la sperimentazione di soluzioni alternative, libere da processi e procedure burocratiche, che si muovono nella direzione della *mission* sociale della nostra Repubblica, spesso carente. Questo tipo di iniziativa avvantaggerebbe l'intera comunità e promuoverebbe un sistema di inclusione perché eliminerebbe le barriere allo sviluppo della cultura e al godimento dei diritti, trasformando «i tradizionali paradigmi di gestione della cosa pubblica, avviando processi di cambiamento culturale sia all'interno che all'esterno degli uffici, mettendo in relazione cittadini e rappresentanti»[41].

Pro Publica, un'organizzazione che non persegue scopi di lucro, ha sviluppato un approccio molto efficace e basato sui dati aperti per alimentare il giornalismo d'inchiesta e mettere luce su fatti di pubblico interesse che in altri modi sarebbe impossibile. La Fondazione *Sunlight* ha lavorato per il Congresso e la campagna elettorale, utilizzando dati pubblici per rendere i problemi trasparenti al pubblico.

---

[37] in *https://www.opengov.com/*.

[38] J. GURIN, *op. cit.*, *ibidem*.

[39] La definizione è di Alex Howard: «a new idea, technology or methodology that challenges and improves upon existing processes and systems, thereby improving the lives of citizens or the function of the society that they live within» in *http://gov20.govfresh.com/defining-civic-innovation-definition-open-government/*, March 16th, 2012.

[40] J. TAUBERER, *Open Government Data*, self-published, *passim,* 2014.

[41] D. ZAVETTIERI, Civic hacking*: innovare senza permesso*, in *www.innovatoripa.it*, 16 ottobre 2015.

Un'altra tendenza che si sta sviluppando è quella di rendere *open i* reclami dei consumatori allo scopo di responsabilizzare le aziende verso il pubblico. L'Ufficio di tutela dei consumatori finanziari, per esempio, ha creato un *database* di reclami su carte di credito, mutui e altri tipi di servizi finanziari. Dall'analisi di queste denunce, reclami, valutazioni delle banche e delle istituzioni finanziarie è emerso che tali istituzioni migliorano significativamente il loro servizio clienti. Altre agenzie governative, tra cui la *Consumer Product Safety Commission*, stanno raccogliendo i reclami dei consumatori per renderli pubblici. Allo stesso modo, le sei agenzie federali che gestiscono i reclami dei prodotti stanno coordinando i loro dati su un unico portale migliorare il livello di informazioni ai consumatori e incrementare la responsabilità aziendale per garantire la sicurezza dei prodotti.

Gli investitori, i sostenitori e i consumatori stanno ora richiedendo informazioni più approfondite sulla responsabilità delle imprese. Una società chiamata *GoodGuide* analizza circa 1500 *set* di dati per fornire ai consumatori e alle stesse società approfondimenti sull'impatto ambientale e sulla sostenibilità di un'ampia gamma di prodotti di consumo. Il progetto *Carbon Disclosure* raccoglie dati sull'impronta di carbonio di diverse società e lo mette a disposizione degli investitori istituzionali che gestiscono collettivamente oltre 90 trilioni di dollari negli *asset*. Alla responsabilità delle imprese si affianca un Rapporto ambientale/sociale/governativo, detto ESG[42]. Qui le aziende riportano specifiche metriche che descrivono come le loro operazioni influenzano l'ambiente, le comunità locali e le preoccupazioni sociali.

La trasparenza non accenderebbe più i riflettori solo sui governi e sulle pubbliche amministrazioni ma anche sui privati, spronandoli alla sana competitività declinabile *in melius*.

Alcuni dei Rapporti ESG sono volontari, e alcuni sono ora istituzionalizzati a livello di governo. La *Securities and Exchange Commission* ora richiede alle società pubbliche di riferire sull'utilizzo di minerali di conflitto, minerali trovati in molti prodotti elettronici estratti in condizioni disumane nella Repubblica del Congo. Le grandi aziende e i loro

[42] J. GURIN, *op. cit., ivi*, p.702 ss..

lobbisti hanno mostrato resistenze nei confronti di proposte di leggi iniziative di *advocacy*[43] orientate verso una maggiore trasparenza. Alcune di queste resistenze sono dettate da una logica di conservazione delle informazioni proprietarie, mentre alcune sono inquadrate come un'obiezione contro la regolamentazione in generale.

L'apertura dei dati favorirebbe un nuovo tipo di responsabilità sociale, migliorerebbe la competizione tra le aziende e la qualità dei prodotti e dei servizi.

Ma da sola non basta: dovrebbe aggiungersi un obbligo di pubblicazione periodica di *report* con dati aggiornati e autentici[44].

Gli *Open Data* andrebbero trattati come *commons*[45], beni comuni appartenenti al genere umano.

Le limitazioni sui dati e sul loro riutilizzo limitano lo sviluppo della comunità. Per questo è essenziale che i dati scientifici siano resi aperti per fare in modo che la scienza progredisca e la società ottenga il massimo beneficio dalle ricerche scientifiche. I dati cartografici, le istituzioni pubbliche sono necessari per agevolare l'esecuzione di comuni attività umane. I dati che sarebbero prodotti dalla pubblica amministrazione, ma finanziati dal denaro pubblico, o comunque ceduti alla stessa affinché eroghi dei servizi devono tornare ai loro legittimi proprietari e alla comunità in generale, sotto forma di dati aperti e universalmente disponibili. L'informazione, creata dall'amministrazione con i dati forniti dai cittadini, a loro spese, è acquisita al concetto di bene comune e richiede una pubblicazione *ex se*. Dunque, il suo regime giuridico dovrà essere quello *open* per diffondere

---

[43] Si ripropone quanto sostenuto da Gurin in J. GURIN, *op. cit.*, p. 702.

[44] Infra § 4. del presente capitolo.

[45] E. OSTROM, *Governare i beni collettivi*, Venezia, Marsilio, 2006, *passim*; P. BARNES, *Capitalismo 3.0*, Milano, Egea Università Bocconi editore, 2006, *passim*; C. HESS - E. OSTROM - P. FERRI - I. KATERINOV (a cura di), *La conoscenza come bene comune. Dalla teoria alla pratica*, Milano, Mondadori, 2009, *passim* e J. STIGLITZ, *Knowledge as a Global Public Good*, New York, Oxford University Press, 1999, *passim*; J. L. CONTRERAS - J. H. REICHMAN, *Sharing by design: Data and decentralized commons*, 350 Science 1312, *University of Utah College of Law Research Paper No. 172,* available at *SSRN: https://ssrn.com/abstract=2799306,* December 11th, 2015, p. 1 ss.. Gli autori affermano: « A rich literature beginning with the work of Ostrom addresses the organization and governance of common pool resources shared by communities of users in contexts ranging from the global environment to communal living spaces. More recent work has expanded these principles to knowledge commons: collections of intangible resources, such as digital libraries, scholarly publications, and scientific data. Responding to calls for increased international scientific collaboration, several expert bodies have developed high-level principles for transborder data sharing. Although these efforts lay the groundwork for broad data-pooling initiatives, critical design decisions must be made before addressing larger issues of governance and operation». Nel settore dell'*e-health* cfr. con B. J. EVANS, *Barbarians at the Gate: Consumer-Driven Health Data Commons and the Transformation of Citizen Science*, in *American Journal of Law and Medicine*, Vol. 42, Issue 4, 2016, p. 3 ss..

la conoscenza a favore di tutti, mettendo in chiaro i processi decisionali, risparmiando denaro[46] e responsabilizzando funzionari e amministratori.

1.2. *Lo stato dell'arte*

Qui per stato dell'arte intendiamo la descrizione dello stato di recepimento del paradigma *open* nel nostro ordinamento, ci chiederemo se è la legge a dover essere esibita come fonte normativa dell'obbligo di aprire i dati in capo all'amministrazione.

Partiamo da una breve premessa sull'individuazione degli specifici titoli normativi *sub*-costituzionali che, pur lasciando all'amministrazione la facoltà di pubblicare o meno i dati[47], le impongono di pubblicarli nel modo più aperto possibile nel caso in cui optasse per renderle aperte.

Nel quadro sopra descritto si è mosso il legislatore italiano che, accogliendo parte dei principi[48] elaborati dai movimenti di sostegno all'apertura dei dati, è intervenuto nella definizione di «dato di tipo aperto» con la Legge 17 dicembre 2012, n. 221[49], inserendola nell'art. 68 del Codice dell'Amministrazione Digitale[50]. Secondo la previsione di cui all'art. 68.3: «agli effetti del presente Codice si intende per:

---

[46] A tal proposito, rileva l'azione di apertura dei dati in ambito europeo mediante il portale *European Open Data Portal (in https://open-data.europa.eu/en/data/*, inaugurato a novembre 2015. Si tratta di una raccolta di dati (240.000 *dataset* divisi in 13 categorie, dalla salute all'istruzione, si tratta di dati aperti a tutti e utilizzabili da tutti per i più disparati scopi) prodotti dalle istituzioni e dagli organi UE (provenienti da 34 paesi europei). L'impiego di tali dati potrebbe far risparmiare 629 milioni di ore di attesa su strade europee e le PP.AA. che utilizzano dati aperti potrebbero risparmiare nel 2020 fino a 1,7 miliardi di euro. Si deve però trattare di dati maturi cioè utili, è per questo che l'UE ha lanciato questo portale.

[47] Qui ci riferiamo a quei dati che non rientrano in quelli su cui vi è obbligo di pubblicazione ai sensi dell'art. 14 del d. lgs. 33/2013.

[48] *Supra* nota 8.

[49] Legge 17 dicembre 2012, n. 221 Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese. (12G0244) (GU Serie Generale n.294 del 18-12-2012 - Suppl. Ordinario n. 208), in *http://www.gazzettaufficiale.it/eli/id/2012/12/18/012G0244/sg*.

[50] Decreto legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale. (GU Serie Generale n.112 del 16-05-2005 - Suppl. Ordinario n. 93), in *http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104*.

a) formato dei dati di tipo aperto, un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;
b) dati di tipo aperto, i dati che presentano le seguenti caratteristiche:
    1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
    2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;
    3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione, salvo i casi previsti dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36, e secondo le tariffe determinate con le modalità di cui al medesimo articolo».

Tale definizione, in coordinamento con quanto disposto dall'articolo 52 dello stesso Codice rappresenta la base del principio dell'*open by default*, che oggi trova posto nell'ordinamento italiano, e che è anche la base, seppure in termini opposti, di chiusura, al principio del *data protection by default* accolto dall'articolo 25, paragrafo 2 del Regolamento UE 2016/679[51], che contrariamente al primo vuole che per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone senza il consenso della persona stessa[52]. Il principio dell'*open by default*, diretta emanazione del brocardo «quae lex non prohibet debent permissa videri», vuole che l'apertura dei dati delle pubbliche

[51] In *http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT*.

[52] «such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons».

amministrazioni sia predefinita, appunto, "in linea di principio", ovviamente, nel caso in cui non siano specificati particolari termini di uso.

L'articolo 7 del Decreto legislativo 14 marzo 2013, n. 33[53], in materia di «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni», cd. Decreto Trasparenza, ha confermato il principio dell'*open by default*, rafforzandolo nella precisazione che i dati e i documenti soggetti a pubblicazione *online* obbligatoria non possono avere alcuna licenza che vada oltre l'obbligo di citare la fonte e rispettarne l'integrità[54].

In occasione del trentanovesimo vertice del G8, tenutosi il 18 giugno 2013 in Irlanda del Nord, i *leader* del G8 hanno firmato l'*Open Data Charter*[55], con cui hanno individuato i 6 principi strategici, per rendere il proprio patrimonio informativo pubblico, nell'*open by default*; *timely and comprehensive; accessible and usable; comparable and interoperable; for improved governance and citizen engagement*; *for Inclusive Development and Innovation.* Successivamente nell'ottobre del 2015, durante l'incontro globale sull'*Open Government Partnership*[56] a Città del Messico, un gruppo di 17 governi[57] ha sottoscritto la Carta internazionale dei dati aperti per definire i principi e le buone pratiche per il rilascio dei dati a governativi.

A simili iniziative legislative e di *soft law*, tuttavia non sono seguite azioni tese a rendere effettivi i propositi espressi in punto di diritto e che richiedono necessariamente come punto di avvio politiche di digitalizzazione ovvero la trasformazione di documenti,

---

[53] Decreto legislativo 14 marzo 2013, n. 33 Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni. (13G00076) (GU Serie Generale n.80 del 05-04-2013), in *http://www.gazzettaufficiale.it/eli/id/2013/04/05/13G00076/sg*.

[54] la Presidenza del Consiglio dei Ministri ha ribadito che la Direttiva PSI obbliga la Pubblica Amministrazione italiana a rendere riutilizzabili gratuitamente tutti i documenti in suo possesso, compresi i documenti i cui diritti di proprietà intellettuale siano detenuti da biblioteche, da musei e da archivi.

[55] In *http://opendatacharter.net/principles/*.

[56] L'*Open Government Partnership* (OGP) è un'iniziativa internazionale che mira a ottenere impegni concreti dai Governi in termini di promozione della trasparenza, di sostegno alla partecipazione civica, di lotta alla corruzione e di diffusione, dentro e fuori le Pubbliche Amministrazioni, di nuove tecnologie a sostegno dell'innovazione.
L'*Open Government* Partnership è stata lanciata ufficialmente il 20 settembre 2011 da otto Paesi (Brasile, Gran Bretagna, Indonesia, Messico, Norvegia, Repubblica delle Filippine, Sudafrica e Stati Uniti): da allora il numero di Paesi aderenti è cresciuto costantemente fino a includere 70 membri, in *http://open.gov.it/open-government-partnership/come-funziona-ogp/*.

[57] La Carta è stata sottoscritta da Cile, Corea del Sud, Guatemala, Filippine Francia, Italia, Messico, Regno Unito e Uruguay, oltre che dalle città di Buenos Aires, Minatitlán, Puebla, Veracruz, Montevideo, Reynosa, Xalapa e lo stato messicano di Morelos.

immagini in un formato digitale, leggibile da una macchina e la dematerializzazione di atti e documenti di aziende e pubbliche amministrazioni.

Alla trasformazione digitale della pubblica amministrazione mancherebbe, infatti il pezzo centrale e cioè l'Anagrafe nazionale della popolazione residente: è quanto è emerso dalle audizioni svolte dalla Commissione parlamentare di inchiesta sul livello di innovazione della P.A..

Solo 4[58] dei 7.981 Comuni sono entrati nella banca unica digitale[59].

Senza l'Anagrafe unica, neanche *spid*, il Sistema Pubblico di Identità Digitale[60], che permette di accedere a tutti i servizi *online* della pubblica amministrazione con un'unica Identità Digitale (*username* e *password*) utilizzabile da computer, *tablet* e *smartphone* ha buone probabilità di decollare.

Si sono susseguiti finora ritardi, proroghe, costi imprevisti e complessità tecnologiche.

Introdotto dal decreto legge 18 ottobre 2012, n. 179[61] l'obiettivo della nuova Anagrafe nazionale della popolazione residente era previsto per il 2016.

L'Anagrafe centrale avrebbe preso il posto delle oltre ottomila anagrafi dei Comuni, avrebbe assorbito l'Indice nazionale delle anagrafi (*Ina*) e l'Anagrafe della popolazione italiana residente all'estero (*Aire*). Tale sistema, contenente anche l'archivio nazionale informatizzato dei registri di Stato civile e i dati delle liste di leva, avrebbe consentito al cittadino di accedere alle sue informazioni anagrafiche con l'identità elettronica *spid* e a tutti i soggetti aventi diritto di consultare le informazioni ivi contenute, sgravando i Comuni dalla gestione delle richieste. L'incrocio dei dati toponomastici avrebbe permesso anche di concretizzare l'Anagrafe nazionale dei numeri civici e delle strade urbane

---

[58] Sono i Comuni di Lavagna, Bagnocavallo, Sant' Agata sul Santerno e Cesena.

[59] D. COLOMBO – C. FOTINA, Se alla PA manca ancora l'Anagrafe digitale, in *Il sole 24 ore*, 29 aprile 2017, n. 112.

[60] In *https://www.spid.gov.it/*.

[61] Testo del decreto legge 18 ottobre 2012, n. 179 (pubblicato nel supplemento ordinario n. 194/L alla Gazzetta Ufficiale 19 ottobre 2012, n. 245), coordinato con la legge di conversione 17 dicembre 2012, n. 221 (in questo stesso supplemento ordinario alla pag. 1), recante: «Ulteriori misure urgenti per la crescita del Paese.». (12A13277) (GU Serie Generale n.294 del 18-12-2012 - Suppl. Ordinario n. 208), in *http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2012-12-18&atto.codiceRedazionale=12A13277*.

(*Anncsu*), strumento necessario a completare la riforma del Catasto, ma l'obiettivo è stato prorogato di due anni.

I Comuni hanno dovuto sopportare costi non previsti per passare al nuovo sistema Sogei e abbandonare i *software* proprietari finora in uso per le funzioni demografiche.

Spid conta, ad oggi 3.720 amministrazioni attive[62] ma i servizi offerti sono inutili senza i Comuni in Rete. Persino l'Inps ha incontrato non poche difficoltà nello *switch* dal *pin* allo *spid*, perché regole di sicurezza e sistemi di autenticazione non sono compatibili. È chiaro che la generazione di nuovi *spid* è direttamente proporzionale alla domanda legata ai servizi. Secondo uno studio della Commissione Europea (DESI), nel 2017[63] l'Italia occupa il venticinquesimo posto nell'utilizzazione di servizi di *E-Government* con una percentuale del 16%. Con riguardo all'indice di digitalizzazione dell'economia e della società (DESI) nella classifica del 2017, l'Italia è al terzultimo posto prima di Romania, Bulgaria e Grecia.

Inoltre, da quanto emerge dal censimento delle imprese italiane che utilizzano *Open Data* nella loro attività, progetto avviato con il progetto *Open Data 200* Italia[64] nel nostro Paese il mercato appare ancora immaturo e pressoché scarsa la qualità dei dati pubblicati dalle imprese.

Se la modernizzazione della pubblica amministrazione, come riportato dal Rapporto OCSE 2017[65], sarebbe in grado di incrementare dell'1% il PIL appare evidente che anche il futuro economico della società dipenderà in gran parte da come si svilupperanno i *Big Data* e gli *Open Data*, intendendo per primi, per lo più, i dati raccolti utilizzati, archiviati e incrociati anche per scopi ignoti da soggetti pubblici e privati e per i secondi la parte di *Big Data* aperti. Un mondo in cui si svilupperanno solo i primi sempre più grandi dati verranno raccolti e detenuti da piccoli e potenti gruppi, una simile prospettiva realizzerà un futuro

---

[62] ID., *ibidem*.

[63] The Digital Economy and Society Index (DESI) 2017, in *https://ec.europa.eu/digital-single-market/en/desi*.

[64] Sviluppato dalla Fondazione Bruno Kessler, sul modello dell'americano *Open Data 500* del *GovLab – New York University*, in fase di pubblicazione. Cfr. L. INDEMINI, *Open Data 200: il censimento delle imprese italiane che utilizzano open data*, in *La Stampa*, 26 aprile 2017. L'Italia è salita dal venticinquesimo è salita al diciassettesimo posto guadagnando otto posizioni nel ranking del *Global Open Data Index 2015*, ovvero la classifica mondiale che misura la quantità e la qualità dei dati rilasciati dagli Stati. La Gran Bretagna è al primo posto, seguono Danimarca e Francia. Dopo l'Italia, invece, Svizzera e Brasile. Una posizione condivisa con Canada, Spagna e India. La vetta della classifica è occupata da Taiwan. Sul podio anche il Regno Unito e a seguire la Danimarca. Prima dell'Italia, tra le nazioni europee, si piazzano la Finlandia al 5° posto, l'Olanda all'8°, Norvegia e Francia al 10°, la Romania al 13° e la Bulgaria al 16°.

[65] *In https://www.oecd.org/eco/surveys/italy-2017-OECD-economic-survey-overview-italian.pdf.*

orwelliano[66]. Al contrario, se anche i *Big Data* diventeranno *Open*, i rischi saranno più piccoli, i vantaggi potenziali saranno maggiori e per tutti. È tuttavia necessario che si sviluppino strutture tecnologicamente in grado di accogliere i cambiamenti imposti dal progresso della tecnica, la quale facilita il godimento delle libertà e l'effettività dei principi democratici.

2. L'*Open Data policy* nel panorama internazionale: il modello FOIA

L'ordinamento statunitense nel 2009 è stato il primo[67] ad aprire al pubblico un catalogo di *Open Government Data* che oggi offre centinaia di migliaia di *dataset*.

Non è possibile predire il valore dei dati finché non vengono rilasciati in formato *open*. L'amministrazione Obama, come un numero crescente di governi in tutto il mondo, ha voluto aprire i dati governativi a tutti i livelli e ne ha mostrato il valore. Nel maggio 2013, attraverso un Ordine Esecutivo[68] e una nota *dell'Office of Management and Budget*[69], l'Amministrazione ha istituito «the Open Data Policy, stating that all federal data should be made open and easily usable unless there is an express reason not to»[70].

Nell'annunciare l'*Open Data policy*, il presidente Obama ha affermato che gli *Open Data* «going to help launch more startups. It's going to help launch more businesses...It's going to help more entrepreneurs come up with products and services that we haven't even

---

66 G. ORWELL, *1984*, Harvill Secker, London, 1949, *passim*.

67 Attraverso il portale *www.data.gov* B. OBAMA, *Memorandum for the Heads of Executive Departments and Agencies on Transparency and Open Government*, 2009, in *http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf*.

68 B. OBAMA, *Executive Order*, *Making Open and Machine Readable the New Default for Government Information*, May 9th, 2013, in *https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-* .

69 SYLVIA M. BURWELL ET AL., *Memorandum for the Heads of Executive Departments and Agencies, Open Data Policy - Managing Information as an Asset*, May 9th, 2013, *http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf*.

70 J. GURIN, *op. cit.*, *ivi*, p. 699, cit.

imagined yet»[71]. Questa politica di apertura è stata progettata appositamente per rendere i dati del governo più utili al settore privato, rafforzare la democrazia e promuovere l'efficienza e l'efficacia nelle azioni di governo. Obiettivi questi, che, come detto in precedenza, rappresentano lo scopo comune di ogni *policy* di apertura.

Il portale *data.gov* ha sviluppato un sistema bidirezionale di *feedback*, suggerimenti e richieste di aprire determinate categorie di dati. Tuttavia, la mancanza di un formato *standard* ha posto non pochi problemi. Negli Stati Uniti ci sono circa 10.000 sistemi di informazione federali diversi e ciascuno di questi ha un formato diverso. Sono, per lo più, sistemi ereditati, malfunzionanti tecnologicamente e non interoperabili[72].

Ad esempio, l'*Occupational Safety and Health Administration* e l'*Environmental Protection Agency* gestiscono entrambi un certo numero di dati, l'OSHA fornisce servizi per la sicurezza sul lavoro, l'EPA per la lotta all'inquinamento. Non è possibile, tuttavia sfruttare in modo incrociato questi due *set* di dati perché operano in modi diversi[73].

Per avere la misura di quanto l'apertura dei dati possa incidere sulla politica di governo e caratterizzarla in termini di inclusione, democraticità e partecipazione è sufficiente fare cenno agli effetti dell'inversione di rotta della politica statunitense in materia di trasparenza. Il 21 gennaio 2017 l'Amministrazione Trump, poco dopo la cerimonia del giuramento del nuovo Presidente, ha rimosso tutte le pagine *web* che citavano l'«Open Government» dal sito della Casa Bianca. Questi spazi in rete non contenevano più parole come «Open Government» o «Open Data», nemmeno nella «Issues tab», limitata alle questioni relative all'energia, alla politica estera, alla crescita del lavoro, alle forze militari, all'applicazione della legge e al commercio[74]. I siti dedicati all'iniziativa governativa di apertura dei dati di Obama, sopra citata, restituivano l'errore «404 Page Not Found» e il messaggio «Sorry, the page you're looking for can't be found.

---

[71] B. OBAMA, *Remarks by the President at Applied Materials*, Inc.-Austin, TX, May 9th, 2014, transcript, *http://www.whitehouse.gov/the-press-office/2013/05/09/remarkspresident-applied-materials-inc-austin-tx*.

[72] Infra § 4 del presente capitolo.

[73] J. GURIN, *op. cit.*, *ivi*, p. 700.

[74] A. WITZE, *Trump removes "Open Government" from White House website*, January 21st, 2017, in *https://g0v.news/trump-removes-open-government-from-white-house-website-5f7c4feb7c18*; A. TARANTOLA, *Trump administration is killing its open data portal*, April 14th, 2017, in *https://www.engadget.com/2017/04/14/trump-admin-killing-open-data-portal/*.

Here are some useful pages». Di conseguenza, il contenuto dell'iniziativa di Obama era stato archiviato[75].

Questa improvvisa chiusura non era inaspettata. La rimozione era stata prevista nel dicembre 2016 e aveva già provocato un'azione collettiva di *backup*[76].

Le città, invece, non hanno seguito la politica di chiusura, infatti hanno reagito implementando la loro partecipazione agli eventi dedicati all'apertura dei dati al pubblico[77], che nel 2016 avevano registrato una diminuzione delle adesioni da 21 a 16, salite nel 2017 inaspettatamente a 36.

«President Trump's anemic approach to truth and transparency is a danger to open data, while his bigoted and sexist worldview is a warning signal of how he might use government collected data to harm vulnerable groups»[78] è il motivo principale che ha scatenato la reazione popolare[79], al punto che nel corso dell'*Open Data Day 2017* in NYCWright è stato avviato un programma di salvataggio dei dati, chiamato «Data Refuge», con lo scopo di scaricare, copiare e archiviare quei *Sensitive Government Data* in pericolo di essere eliminati dall'attuale amministrazione statunitense in nome dell'interesse pubblico[80]. Gli organizzatori degli eventi *Open Data Day* hanno insegnato ai partecipanti a estrapolare dati e a creare *metadata*. Di conseguenza, su Twitter sono stati scaricati più di 9 *gigabyte* di dati dalla pagina *web* della Casa Bianca di Obama e 40 *terabyte* di *data.gov*. Questi dati sono stati caricati sul sito di *DatProject*[81] e su *GitHub*.

---

[75] In *https://obamawhitehouse.archives.gov/*.

[76] BRADY DENNIS, *Energy and Environment Scientists are frantically copying U.S. climate data, fearing it might vanish under Trump*, in *Washington Post*, available at *https://www.washingtonpost.com/news/energy-environment/wp/2016/12/13/scientists-are-frantically-copying-u-s-climate-data-fearing-it-might-vanish-under-trump/?postshare=3751481645413207&tid=ss_tw&utm_term=.b83bd6ff8812*; J. LAUSSON, *Face à Trump, Internet Archive a copié 200 To de données gouvernementales au cas où*, 11 mai 2017, in *http://www.numerama.com/politique/256838-face-a-trump-internet-archive-a-copie-200-to-de-donnees-gouvernementales-au-cas-ou.html* .

[77] A. WITZE, *Trump Presidency Sees Spike in "Open Data Day" Events Across US Cities*, April, 19th, 2017, in *https://g0v.news/trump-presidency-sees-spike-in-open-data-day-events-across-us-cities-7d331439a9c5*.

[78] Le parole sono di Max Ogden, programmatore e organizzatore del *Portland event* in *https://g0v.news/trump-presidency-sees-spike-in-open-data-day-events-across-us-cities-7d331439a9c5*.

[79] B. DENNIS, *Scientists are frantically copying U.S. climate data, fearing it might vanish under Trump*, in *The Washington Post*, December 13, 2016. In questo articolo le preoccupazioni che hanno spinto a una vera e propria *"guerrilla archiving" event in Toronto* sono state determinate dalle dichiarazioni del Presidente, le quali hanno preoccupato la comunità scientifica. Trump ha asserito che il cambiamento climatico è "una frottola" dell'uomo e ha promesso di invertire le politiche ambientali messe in atto dal presidente Obama. Si è temuto che il nuovo Presidente potesse modificare o smantellare parti il database federale di dati su tutto, dal crescente livello del mare al numero di incendi nel paese.

[80] A. WITZE, *Trump Presidency Sees Spike in "Open Data Day" Events Across US Cities*, *ibidem*.

[81] Maggiori informazioni sul sito *https://datproject.org/*.

La mobilitazione popolare in difesa dei dati sottende un concetto «as a political right, and not just as a means to solve problems in your community»[82] perché «a popular government without popular information or the means of acquiring it, is but a prologue to a farce, or a tragedy, or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives»[83].

Questo cambio di rotta che assume il dato come «arm themselves with the power which knowledge gives»[84] sottolinea che essi sono elementi caratterizzanti politiche trasparenti, mentre la loro chiusura è sintomo di un atteggiamento della pubblica autorità dispotico e intollerante.

La posizione degli Stati Uniti non è rimasta isolata come dimostra il fatto che anche il Regno Unito, benché con modalità diverse, ha utilizzato tecnologie *linked data* con *www.data.gov.uk*. Questo tipo di tecnologie consente la pubblicazione dei dati sul *web* in una modalità *machine readable*[85] e favorisce l'interoperabilità tra *dataset,* cioè consente a terzi di utilizzare *dataset* differenti, a prescindere da chi li abbia pubblicati e di combinarli tra loro con lo scopo di incrementare il loro valore[86].

A partire dal 2011 il governo del Canada[87] ha lanciato un piano per la pubblicazione dei dati aperti delle amministrazioni canadesi. Il portale dei dati aperti è stato avviato nel 2013 e il 9 ottobre 2014 il governo canadese ha emanato la Direttiva sul Governo Aperto[88] con lo scopo di disciplinare il riuso dei documenti e dati governativi, che ha portato successivamente all'apertura del portale *Gouvernement ouvert du Canada.*

---

[82] A. WITZE, *Trump Presidency Sees Spike in "Open Data Day" Events Across US Cities*, *ibidem*.

[83] J. MADISON, *letter to W. T. Barry*, August 4, 1822. The Writings of James Madison, ed. Gaillard Hunt, vol. 9, p. 103 (1910), cit..

[84] *Ibid.*

[85] M. GUERRINI - T. POSSEMATO, *Linked data: un nuovo alfabeto del web semantico*, in *http://www.bibliotecheoggi.it/content/201200300701.pdf*, aprile 2012, p. 7, cit.

[86] M. OREFICE, *Gli open data tra principio e azione: lo stato di avanzamento*, p. 3, cit..

[87] In *http://open.canada.ca/en/open-data*.

[88] In *https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28108*.

Tra i precursori dell'*Open data policy* anche i governi australiano e neozelandese, in particolare, *data.govt.nz* ha offerto il collegamento ai *dataset* contenuti in altri siti governativi[89].

Negli ordinamenti anglosassoni il rapporto cittadino-pubblica amministrazione è stato fin da subito impostato in termini di generalizzata accessibilità, tanto che «any person has a right, enforceable in court, to obtain access to federal agency records»[90].

Nel nostro ordinamento, invece, l'accesso cd. documentale[91] è stato storicamente subordinato dalla l. 241 del 1990, art. 22 e ss. alla lesione di «un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso».

Questo tipo di accesso è legato al concetto di appropriazione dominicale dell'amministrazione che veicola un'informazione tirannica e restituisce una conoscenza frammentata, ponendosi in netto contrasto con la natura di Internet che invece aprirebbe all'inedita idea di una proprietà indivisa, ampliando la portata dell'articolo 97.

Il "buon andamento" della pubblica amministrazione, principio costituzionale «cardine della vita amministrativa e quindi condizione dello svolgimento ordinato della vita sociale»[92] prescriverebbe l'esigenza di un'amministrazione efficace, efficiente ed economica[93], parametri giuridici dell'attività e dell'organizzazione amministrativa.

2.1. *Lettura parallela tra il recente modello italiano e il parametro del Foia statunitense*

La costruzione giuridica dell'accesso come diritto condizionato sospensivamente ha finito per paralizzare il rapporto tra il cittadino e l'amministrazione, in aperta violazione

---

[89] In *https://data.govt.nz/*.

[90] *Foia*, 4 giugno 1966, in http://www.Foia.gov/index.html.

[91] L'accesso documentale si distingue dall'accesso civico semplice, previsto dal primo comma dell'art. 5 del d. lgs. 14 marzo 2013, n. 33 trasparenza. A seguito dell'approvazione del d. lgs. 97/2013 si è aggiunto un terzo tipo di accesso ai due già riconosciuti dal nostro ordinamento: l'accesso generalizzato.

[92] Corte. Cost. del 9 dicembre 1968, n. 123, in http://www.giurcost.org/decisioni/1968/0123s-68.html.

[93] E. CASETTA, *Manuale di diritto amministrativo*, 2011, Milano, 2011, p. 52 e ss.; G. CORSO, *Manuale di diritto amministrativo*, Torino, 2013, p. 158 e ss.

dell'articolo 97 della nostra Costituzione, che come detto nei paragrafi che precedono, riconosce il diritto alla trasparenza[94], come valore intrinseco e integrante del diritto all'informazione e alla buona amministrazione[95].

L'amministrazione non dovrebbe agire in regime di assoluta libertà e autonomia, ma è obbligata a rispettare regole e vincoli diretti a consentire che tutto il suo agire sia preordinato al raggiungimento di quegli scopi di pubblico interesse per i quali è stata appositamente istituita.

Ad adiuvandum, sul piano internazionale l'articolo 41[96] della Carta dei diritti fondamentali dell'Unione europea interviene sul medesimo tema e riconosce nell'articolo 42 riconosce «ad ogni cittadino dell'Unione e ad ogni persona fisica o giuridica che risieda o abbia la propria sede sociale in uno Stato membro il diritto di accedere ai documenti del Parlamento europeo, del Consiglio e della Commissione»[97].

Tuttavia, in spregio alle disposizioni citate, la chiusura alla trasparenza del nostro ordinamento è confermata dal comma 3 dell'art. 24 della stessa legge 241/90, secondo il quale «non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni».

Il d. lgs. 14 marzo 2013, n. 33 ha introdotto un secondo tipo di accesso civico nel nostro ordinamento, cd. semplice, correlato ai soli atti e informazioni oggetto di obblighi di pubblicazione; tale accesso ha assegnato a chiunque il diritto di richiedere detti atti nei soli casi di omessa pubblicazione. Si tratta, dunque, di un rimedio alla violazione degli obblighi di pubblicazione imposti dalla legge alla pubblica amministrazione[98], esperibile

---

[94] M. VIGGIANO, *I limiti alla pubblicità dell'azione amministrativa per finalità di trasparenza derivanti dalla protezione dei dati personali*, in L. CALIFANO - C. COLAPIETRO (a cura di), *op. cit.*, *ivi*, p. 228; M. LUCIANI, *Nuovi diritti fondamentali e nuovi rapporti tra cittadino e pubblica amministrazione*, in *Riv Critica dir. priv.*, 1985, p. 61; M.R. SPASIANI, *Il principio di buon andamento: dal metagiuridico alla logica del risultato in senso giuridico*, in *iuspubblicum.com*, aprile 2011; R. VILLATA, *La trasparenza dell'azione amministrativa*, in *Dir. Proc. Amm.*, 1987, p. 528.

[95] Artt. 21-97-98-118.4, della Costituzione Italiana. R. CARIDÀ *Principi costituzionali e pubblica amministrazione*, in *www.giurcost.org*, p. 11 ss.; A. D'ATENA, *Il principio di sussidiarietà nella Costituzione italiana*, in *Riv. it. dir. pub. com.*, 1997, p. 603 ss.; V. C. JAMBRENGHI, *Buon andamento dei pubblici uffici e garanzie costituzionali degli interessi coinvolti*, in *http://www.consiglionazionaleforense.it/site/home/agenda/docCat.2335.1.30.2.C.html*, Roma, marzo 2014, p. 9 e ss.

[96] *ex pluris* artt. 10-11.

[97] Per avere una panoramica della regolazione europea in materia, si rinvia allo scritto M. OREFICE, Open Data *tra principio e azione: lo stato di avanzamento*, p. 4 ss.

[98] Esempi di obblighi di pubblicazione: *curricula* dei titolari di posizioni organizzative redatti in conformità al vigente modello europeo; compensi dirigenti uffici pubblici; elenco incarichi conferiti o autorizzati a ciascun dipendente, con l'indicazione dell'oggetto, della durata e del compenso spettante per ogni incarico; etc.

dal *quivis de populo*, che infatti non dovrà dimostrare di essere titolare di un interesse diretto, concreto e attuale alla tutela di una situazione giuridica qualificata[99].

In un intervento legislativo quasi convulso un altro tipo di accesso si è aggiunto ai primi due: quello generalizzato, introdotto dal d. lgs. 25 maggio 2016, n. 97[100], tendente a «favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e promuovere la partecipazione al dibattito pubblico»[101]. A tali fini è disposto che «chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione»[102].

L'accesso generalizzato è dunque autonomo e indipendente dall'obbligo di pubblicazione, che invece è il presupposto dell'accesso civico «semplice».

Esso incontra come limiti, da una parte, il rispetto della tutela degli interessi pubblici e privati indicati (all'art. 5-bis, commi 1 e 2), e dall'altra, il rispetto delle norme che prevedono specifiche esclusioni (previste dall'art. 5-bis, comma 3)[103].

Le due forme di accesso civico regolate dal c.d. decreto trasparenza hanno natura, presupposti ed oggetto differenti dal diritto di accesso di cui agli artt. 22 e seguenti, legge n. 241/1990, meglio noto come «accesso documentale».

Si osserva che tali ultime disposizioni assumono carattere di specialità - accesso ai documenti amministrativi - rispetto alle norme del decreto trasparenza afferenti le modalità di accesso a qualsivoglia documento, atto o informazione detenuta dalla PA. La finalità dell'accesso documentale, si precisa, è quella di porre i soggetti interessati in condizione di esercitare al meglio le facoltà che l'ordinamento attribuisce loro, a tutela delle proprie posizioni giuridiche. Il richiedente deve infatti dimostrare di essere titolare di

---

[99] Tra gli esempi di obblighi di pubblicazione: *Curricula* dei titolari di posizioni organizzative redatti in conformità al vigente modello europeo; compensi dirigenti uffici pubblici; elenco incarichi conferiti o autorizzati a ciascun dipendente, con l'indicazione dell'oggetto, della durata e del compenso spettante per ogni incarico; etc.

[100] Il decreto lgs. ha novellato l'art. 5, comma 2 del d. lgs. n. 33/2013. Decreto legislativo 25 maggio 2016, n. 97 Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche. (16G00108) (GU Serie Generale n.132 del 08-06-2016), in *http://www.gazzettaufficiale.it/eli/id/2016/06/08/16G00108/sg*.

[101] Art. 6, comma 2 del d. lgs. 97/2016 che modifica l'articolo 5 del d. lgs. 33/2013.

[102] *ibidem*.

[103] Infra § 3.1. del presente capitolo.

un «interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso»; in funzione di tale interesse la domanda di accesso deve essere opportunamente motivata.

La legittimazione all'accesso ai documenti amministrativi (*rectius* documentale) va così riconosciuta a chiunque può dimostrare che gli atti oggetto della domanda di ostensione hanno spiegato o sono idonei a spiegare effetti diretti o indiretti nei propri confronti, indipendentemente dalla lesione di una posizione giuridica.

Pertanto, le ricordate limitazioni hanno spinto il legislatore a introdurre questo terzo tipo di accesso per inserire nel nostro ordinamento un meccanismo analogo a quello anglosassone del c.d. *Foia - Freedom Of Information Act*, il quale però ha una matrice diversa e deriva da un contesto storico[104] ben più complesso. A questo punto riteniamo necessario un rapido *excursus* storico sulle origini del *Foia*, visto che esso rappresenta il modello al quale il recente legislatore italiano ha guardato.

L'istituto statunitense nasceva nel 1966 per offrire effettività alla garanzia del *right to know*[105], emanazione del *freedoom of speech* e soprattutto del *freedom of information*[106], ma essenzialmente rivendicava il diritto di contestare «arbitrary political power, preparing the way for the revolutionary concepts of popular sovereignty and the people's right to know, which were eventually embodied in the American Constitution»[107] e quindi di opporsi al «crime of seditious libel»[108], risultato della lotta del popolo inglese «to establish and preserve the right (...) to full information in respect of the doings or misdoings of their government»[109]. Sebbene, prevalente dottrina sottolinei che i Padri fondatori consideravano il diritto di conoscere fondamento della democrazia degli Stati Uniti

---

104 Sin da quando gli USA erano una colonia britannica, ma anche dopo la dichiarazione di indipendenza e l'adozione della Costituzione, l'imposizione delle politiche di governo e l'applicazione e da parte delle Corti continuò ad essere amplissima e perdurò sino almeno al 1925

105 L'espressione è stata coniata da K. COOPER, The Right to Know: An Exposi1ion of the Evils of News Suppression and Propaganda, New York, 1956; H.L. CROSS, The Right to Know: Legal Access to Public Records and Proceedings, New York, 1953.

106 H.N. FOERSTEL, *Freedom of information and the right to know*, Greenwood press, Westport, Connecticut, 1999, p. 3. ss.. L'autore descrive il contesto come permeato da un «official desire to maintain an ignorant public and a shackled press» (p. 3).

107 ID., *op. cit., ivi*, p. 8, cit.

108 Che puniva penalmente «any speech that criticized the government, its officials, or its generai authority» a prescindere dalla veridicità o meno dell'informazione in ID., *op. cit., ivi,* p. 4, cit.

109 *Grosjean v. American Press Association*, 297.S. 233 (1936).

d'America, la fonte legale sulla base della quale i tribunali e la Corte Suprema avrebbero dovuto decidere i casi è mancata, anche se indubbiamente il richiamo al *right to know* è venuto spesso in soccorso del giudice[110]. Questa è la ragione che ha spinto il Congresso statunitense ad adottare un atto legislativo, il *Freedom of Information Act - Foia* del 1966 che andasse a correggere il *Federal Administrative Procedure Act* – APA del 1946, il quale seppure nato con lo scopo di favorire la diffusione delle informazioni e riempire la lacuna costituzionale, aveva in via di fatto, a causa della formulazione troppo vaga delle eccezioni previste rispetto all'obbligo di *Public information*, legittimato la pratica del segreto da parte delle agenzie federali come gestione ordinaria delle richieste di accesso.

Il *Foia*, allora, introduceva una disciplina normativa autonoma e separata, recuperando e ampliando quanto statuito dalla sezione 3 dell'APA. Inoltre, nella sua versione originaria prevedeva che ogni persona avesse diritto di richiedere l'accesso ai *record*[111], quindi le informazioni contenute nei documenti, posseduti dalle agenzie federali, salvo i casi in cui sussistessero le nove esenzioni[112] o una delle tre speciali clausole di esenzione previste in favore di FBI e delle forze di sicurezza. Non erano previsti né un termine ragionevole per rispondere alla richiesta di accesso, né sanzioni per il caso di violazioni e neanche la gratuità.

Dopo lo scandalo *Watergate*, nel 1975 il *Foia* è stato revisionato[113] e prevista la possibilità di un accesso gratuito per i documenti richiesti nell'interesse pubblico; quindi introdotto l'accesso parziale, ampliati i poteri del giudice a fronte del rifiuto d'accesso e la definizione di "agenzia".

Queste modifiche sono state ampiamente criticate dal giudice Antonin Scalia che sul punto ha osservato che «the amendments have significantly reduced the privacy, and hence

---

[110] *Ex multis* in *Whitney v. California* 274 U.S. 357 (1927) il giudice ha evidenziato la necessità di una cittadinanza informata.

[111] infatti «data will only become information or knowledge when they are interpreted by human beings» in N. KOCK, *Systems Analysis & Design Fundamentals: A Business Process Redesign Approach*, SAGE Publications, Thousand Oaks. 2006, p. 4.

[112] l. classified information for national defence or foreign policy; 2. intern al personnel rules and practices; 3. information that is exempt under other laws; 4. trade secrets and confidential business information; 5. inter-agency or intra-agency memoranda or letters that are protected by legal privileges; 6. personnel and medical files; 7. law enforcement records or information; 8. information concerning bank supervision; 9. geological and geophysical information.

[113] Le modifiche furono fortemente criticate da A. SCALIA, *The Freedom of Information Act Has No clothes*, in *AEJ Journal on Governmnent and Society Regulation*, March/April 1982, p. 14 ss.

the autonomy, of all our nongovernmental institutions – corporations, labor, unions, universities, churches, political and social clubs – all those private associations that form, as Tocqueville observed, diverse centers of power apart from what would otherwise be the all-powerful democratic state»[114].

La scarsa applicazione del *Foia* condusse alla *openness initiative* della Presidenza Clinton, culminata nell'adozione, nel 1996, dell'*Electronic Freedom of Information Act* - E-*Foia*[115]. L'E-*Foia*[116] ha introdotto una *proactive disclosure*, imponendo[117] alle agenzie federali l'apertura *online* nelle c.d. *Reading Rooms* dei documenti già oggetto di richieste e la fornitura di appositi indici per guidare gli istanti a formulare le proprie richieste.

Nel 2009, quando il livello di effettiva attuazione del *Foia* da parte delle agenzie federali statunitensi era pressoché scarso[118], è stata la Presidenza Obama a intervenire nel settore per garantire maggiore trasparenza ed effettività al *Foia* prima con il *Memorandum* sul *Freedom of lnformation Act* e successivamente, nel 2016, con il *Foia Improvement Act*[119]. In particolare, l'emendamento del 2016 ha imposto alle agenzie di lavorare, *pro futuro*, nella prospettiva di una *presumption of openness*. Il diniego dovrà quindi avvenire solo in presenza di un espresso divieto normativo o dinanzi alla sussistenza di un interesse protetto dalle cause di esenzione del *Foia*[120]. Le agenzie dovranno in questi casi motivare accuratamente rispetto al potenziale danno per l'interesse tutelato che l'evasione della richiesta di accesso, in concreto, causerebbe.

---

114 A. CALIA, *op. cit*, p. 18, cit.

115 In vigore sin dal 31 marzo 1997.

116 L'E-*Foia* ha modificato termini e procedure per agevolare e accelerare il trattamento delle richieste di accesso.

117 Dal 1° novembre 1997.

118 D. R. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in *Riv. Ital. Dir. Pubbl. Communitario*, 2016. L'autrice a p. 30 sostiene che « Da un'analisi approfondita della situazione risulta infatti che - anche se esisteva ed esiste tuttora, senza dubbio, un atteggiamento di ostilità (o quantomeno di scarso entusiasmo) da parte della burocrazia delle agenzie nei confronti della sottostante idea di trasparenza e delle sue implicazioni - , in prevalenza, i ritardi nelle risposte a richieste di accesso ai sensi del *FOIA* sono inerenti alla natura stessa del lavoro richiesto per evaderle, a fronte dell'inadeguatezza del personale e del cronicamente inadeguato finanziamento previsto per le relative attività».

119 *FOIA Improvement Act* of 2016, firmato dal Presidente Obama il 30 giugno 2016 (Public Law No. 114-185).

120 La Section 552 del Titolo 5 prevede ora infatti che (A) An agency shall— (i) withhold information under this section only if— (I) the agency reasonably foresees that disclosure would harm an interest protected by an exemption described in subsection (b); or (II) disclosure is prohibited by law; and (ii) (I) consider whether partial disclosure of information is possible whenever the agency determines that a full disclosure of a requested record is not possible; and (II) take reasonable steps necessary to segregate and release nonexempt information.

In sintesi, il sistema statunitense operante a livello federale è quello che impone all'amministrazione l'obbligo generalizzato di rilasciare i documenti richiesti da chiunque e conseguentemente, e cioè solo dopo solo la richiesta del soggetto, di pubblicarli nella *reading room*; questo sistema contempla eccezioni all'obbligo di rilascio e pubblicazione di stretta interpretazione, il che impedisce di convertire la regola generale della *disclosure* in quella della oscurità.

Ora, l'accesso generalizzato italiano, da ultimo introdotto, che sembrerebbe ispirarsi al *Foia* nella sua versione embrionale e non nel suo più recente sviluppo, consente ai cittadini di richiedere anche dati e documenti che le pubbliche amministrazioni non hanno l'obbligo di pubblicare, senza alcuna limitazione quanto alla legittimazione soggettiva del richiedente[121].

Quindi, il sistema italiano condivide del *Foia* la sua filosofia di fondo: l'amministrazione non deve rendere visibile *motu proprio* ciò che possiede, ma solo su richiesta del *quivis de populo*. Il nuovo accesso, pertanto, non la incoraggia ad aprire tutti i documenti in suo possesso, perché si accontenta di un'amministrazione *friendly and transparent* su domanda del cittadino[122].

Tuttavia, l'insufficienza della legge non sarebbe un valido alibi per l'amministrazione e ciò perché l'obbligo di apertura non dovrebbe esibire la legge come suo titolo giustificativo, bensì l'articolo 97 della Costituzione, almeno secondo una parte della dottrina[123]. Ci sia consentita ancora una riflessione: sarebbe riduttivo far coincidere la *policy* di apertura col diritto di chiedere i documenti, perché se il dovere di trasparenza si risolve anche nella visibilità delle azioni governative, allora esso comporta l'inevitabile esibizione dei dati[124].

In conclusione, la precettività dell'art. 97[125] consente al legislatore di intervenire per specificare, secondo quanto l'aggiornamento tecnologico impone, le modalità attuative di

---

121 G. DE MINICO, *La trasparenza della PA costruita sull'asimmetria*, in *il Sole 24 ore*, 21 maggio 2017, p. 13.

122 C. J. TOLBERT - KAREN MOSSBERGER, *op. cit., ibidem,* 2006.

123 G. DE MINICO, *op cit*., p. 3.

124 Si è già espressa in termini analoghi la prof.ssa De Minico in G. DE MINICO, *op cit*., p. 3.

125 «La giuridicità dell'art. 97 si risolve in un dover essere della p.a. che implica un valore precettivo inteso come azione e impone al legislatore di realizzare una organizzazione degli uffici tale da garantire l'effettiva tutela della "superiore esigenza" del buon andamento. Resta ferma la discrezionalità di cui gode il legislatore in ordine alle scelte concernenti la struttura e la gestione degli uffici, ma restano altrettanto fermi i parametri di logicità, non

un obbligo già posto nel dettato costituzionale, e quindi al tempo stesso gli vieta di attenuare o addirittura azzerare detto obbligo, come invece sembra fare il nostro legislatore.

3. L'accesso generalizzato e la sua logica sottesa: i *closed data*

Il Decreto legislativo del 25 maggio 2016, n. 97, come anticipato, ha introdotto nel nostro ordinamento il cosiddetto accesso generalizzato.

L'articolo 3, comma 1 del suddetto d. lgs.[126] ha riconosciuto una «libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione».

Come ampiamente descritto nel § 2.1., l'accesso generalizzato così configurato resta subordinato alla previa richiesta dell'utente. Questo nuovo strumento, infatti, ha poco di nuovo perché si aggiunge a due tipi di accesso e prevede una sorta di richiesta di accesso a quei dati che potremmo definire i *closed data* della P.A.

«The process of drafting and submitting *FOIA* requests and then waiting for the agency's response» - scrive David C. Vladeck - «is a breeding ground for delay and cynicism over the Act's efficacy Under *FOIA*, there is no centralized "reading room": each agency must create its own website and post only those documents that are the result of three or more *FOIA* requests»[127].

---

arbitrarietà, ragionevolezza e adeguatezza alla luce dei quali occorre valutare, caso per caso, la rispondenza della scelta legislativa al canone del buon andamento» in M. OREFICE, *op. cit.*, p. 10 cit.. Sulla precettività delle norme costituzionali. Cfr. A. AMORTH, *Il contenuto giuridico della Costituzione. Discorso inaugurale*, Società tipografica modenese, Modena, 1946, p. 41 e ss. Sul contenuto precettivo dell'art. 97, primo comma, Cost. si richiama la sentenza n. 14 del 1962 della Corte Costituzionale.

126 Suddetto articolo ha modificato l'articolo 2 del d. lgs. 33/2013.

127 B.S. NOVECK, *Is Open Data the Death of FOIA?*, in *Yale L.J. F.* 273 2016

Si tratta di un mezzo di trasparenza ancora *peer to peer*[128], non a carattere diffuso perché subordinato a una richiesta di accesso ai dati e alle informazioni della p.a. che mantiene una posizione di diffidenza rispetto a quella del cittadino ficcanaso[129].

L'accesso generalizzato così si differenzia e prende le distanze dalla *open data policy* e dalla trasparenza *tout court*[130], intesa come massima espressione della democrazia; secondo quest'ultima accezione la trasparenza sarebbe strettamente connessa all'esercizio del diritto politico (artt. 1-48) perché consentirebbe al cittadino di vedere sotto una lente tutto quello che riguarda la cosa pubblica e di conseguenza di votare consapevolmente (*rectius* liberamente). La trasparenza allora non può essere resa a singhiozzo, secondo un andamento a intermittenza, essa su Internet si arma degli *open data* per facilitare l'esercizio dei diritti politici in Internet e incentivare la partecipazione democratica dei cittadini alla vita del Paese, per esempio attraverso le consultazioni su progetti di legge.

Una piena trasparenza implica un'apertura svincolata a preliminari richieste di accesso: in altre parole il cittadino dovrebbe sapere, senza fare domanda, come vengono spesi i suoi soldi, quali giudici hanno ricevuto un provvedimento disciplinare; presso quale azienda si rifornisce la mensa scolastica e così via.

Un obbligo di trasparenza rimanda all'esistenza di un correlativo diritto al suo adempimento, diritto questo, che spetterà a chiunque di *default*.

L'accesso generalizzato introdurrebbe, invece la possibilità di chiedere alle PP.AA. di visionare quei dati e quelle informazioni ancora chiuse.

Con una metafora il cittadino dovrebbe ancora bussare alla porta di casa sua per entrare «in the era of big data technologies, when information storage is cheap and plentiful, if the goal is to promote greater transparency, it is hard to imagine why we should continue to invest in the legal framework and its attendant practices for demanding data after the fact when, instead, we can build the platforms and policies to ensure proactive and prospective publication of government information in reusable formats online […] By contrast, with open data, technology helps to transform information transparency from

---

[128] L'espressione è presa in prestito alla prof.ssa De Minico, che gentilmente ne ha discusso con l'autrice.

[129] Così la prof.ssa De Minico nell'articolo *La trasparenza della PA costruita sull'asimmetria*, pubblicato su *Il sole 24 ore* del 21 maggio 2017, p. 13.

[130] L. CALIFANO - C. COLAPIETRO (a cura di), *op. cit.*, *ivi*, p. 297 e ss.

a legal principle into a practical reality. In essence, whereas *FOIA* is a legal regime, open data is a set of technology standards and practices»[131].

Il *Foia* italiano legittimerebbe l'interesse all'oscurità delle pubbliche amministrazioni, non solo subordinando l'accesso alla richiesta secondo il binomio "request-respond", ma anche attraverso la sovra-classificazione di eccezioni[132] che vanificano la finalità originaria del *Foia* di memoria statunitense, oramai emancipato verso un modello *open data*, che sta interessando anche i privati che iniziano a sperimentare i benefici del *data sharing*[133]. Un esempio chiarirà questo aspetto. Il paradigma "chiedi e avrai" ben si adatta all'interesse alla chiusura delle cause farmaceutiche in riferimento al processo regolativo, a cui possono avere accesso "senza che gli altri sappiano", in un sistema in cui l'informazione diventa elitaria e antidemocratica[134]. Le stesse case farmaceutiche, grazie a questo modello, potrebbero agevolmente "beneficiare" dell'occultamento dei dati negativi che potrebbero non essere inclini agli affari aziendali. La vocazione democratica dell'informazione richiederebbe che l'apertura di dati e informazioni al pubblico diventasse la regola generale: una trasparenza *ex officio*. E allora quelle case farmaceutiche sarebbero costrette ad aprire i dati sia positivi che negativi contrastando anche casi di ciarlataneria medica[135].

Si badi bene, un sistema che tende all'oscurità incentiverebbe lo spionaggio industriale e politico[136]. Una impostazione di chiusura di *default* mina le più basilari regole di democrazia fino a deformare i risultati elettorali[137], a insaputa degli elettori[138].

Il vecchio modello del 1966 che ha ispirato il nuovo *Foia* italiano del 2016 obbliga l'amministrazione a comunicare al cittadino le informazioni richieste, scoprendo i dati e i

---

131 B. S. NOVECK, *Is Open Data the Death of FOIA?*, in *Yale L.J. F.* 273 2016, p. 280.

132 Infra § 2.1

133 Il gigante farmaceutico britannico GlaxoSmithKline ha annunciato nell'ottobre 2012 di aprire i dati scientifici e condividerli rinunciando al sistema di segretezza dei dati che lo ha reso una delle più grandi aziende farmaceutiche a livello mondiale, con vendite di 43,6 miliardi di dollari nel 2013. Cfr. con Rivista MIT *Technology Review*, *ibidem.*

134 L'esempio è offerto dalla prof.ssa De Minico nella conversazione del 20 marzo 2017.

135 Si pensi ai recentissimi casi di false cure e terapie Hamer e Di Bella.

136 J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in *Max Planck Institute for Innovation and Competition Research Paper*, No. 16-16 , p. 3 ss.

137 G. MONBIOT, *Big data's power is terrifying. That could be good news for democracy*, in *The Guardian*, March 6, 2017: «Online information already lends itself to manipulation and political abuse, and the age of big data has scarcely begun. In combination with advances in cognitive linguistics and neuroscience, this data could become a powerful tool for changing the electoral decisions we make. Our capacity to resist manipulation is limited. Even the crudest forms of subliminal advertising swerve past our capacity for reason and make critical thinking impossible».

138 ID., *ibid.*

documenti da lui richiesti, ma fa gravare l'onere di attivarsi sul cittadino, sollecitando atteggiamenti avversariali contro l'amministrazione[139].

Il *Foia* italiano, in linea con quello americano, afferma una forma reazionaria di trasparenza nel senso formale e procedurale perché risponde a richieste *ad hoc* di documenti e informazioni e in senso sostanziale, politico perché indebolisce la capacità di regolamentazione; distribuisce i beni delle pp.aa. in maniera non ugualitaria: solo a chi chiede; e contribuisce ad una cultura di antagonismo e derisione che circonda la burocrazia politica interna, mentre isola ancora di più le agenzie di sicurezza nazionale, così come le aziende, in circostanze simili[140].

L'estensione del diritto di accesso a "qualsiasi persona" (comprese le persone giuridiche e gli stranieri) lo rende un "sussidio"[141], senza criteri di ammissibilità.

Di conseguenza, l'efficacia della legge dipenderebbe dall'apporto costante di richiedenti tenaci che sanno cosa cercare[142]. La dipendenza del *Foia* alle previe richieste, non è solo "contenziosa e richiede tempo", ma stabilisce anche la "non divulgazione" come la norma di *default*, in assenza di una richiesta formale di informazioni e di un corrispondente *record*[143].

Nel modello *Foia* il richiedente non ha l'obbligo di spiegare il motivo per cui cerca i documenti o di pubblicizzarli una volta ottenuti. La trasparenza del governo verrebbe in questi termini inquadrata come un diritto individuale in possesso solo del richiedente[144].

Il *Foia* non si limita a tradire le sue stesse aspirazioni di trasparenza e responsabilità; esso distorce sistematicamente la produzione di informazioni verso interessi commerciali e facilita potenti agende anti-regolatorie. La domanda strutturale che richiede la nostra

---

139 G. DE MINICO, *La trasparenza della PA costruita sull'asimmetria*, cit.

140 B. S. NOVECK, *op. cit.*, p. 274.

141 ID., *op. cit.,* p. 3, cit.: «*FOIA*'s extension of access rights to "any person" (including legal persons and foreigners) makes it an entitlement program with no eligibility criteria».

142 ID., *ivi*, p. 3. cit.: « The law's efficacy depends on a steady supply of tenacious requesters who know what to look for; in practice, corporate lawyers, information resellers, and other private rent-seekers use it most».

143 ID., *ibid.*

144 ID., *ivi,* p.6, cit.: «Government transparency is thus framed as an individual right held by the requester alone».

attenzione è se il *Foia* equivale ad un impedimento a lungo termine per la capacità amministrativa, per la fiducia nel governo, e per una democrazia egualitaria[145].

Da ciò deriva che al *Foia* e agli *Open Data* sono sottese logiche diverse, perché gli stessi perseguono fini opposti: 1) il primo è attivato dal richiedente a suo vantaggio, la *disclosure* generalizzata nell'oggetto è, invece, ad operatività automatica a beneficio del *quivis de populo*, con effetti *erga omnes*; 2) con il *Foia* l'informazione non è utilizzabile da tutti, con la logica *open* è utilizzabile per ulteriori fini; 3) il *Foia* opera *ex post*, gli *Open Data ex ante*. La politica del *Foia* è incompatibile con quella *open* e ne è onnivora. L'*open data* dovrebbe allora costituire la regola generale, il *Foia* l'eccezione tesa a verificare i dati nascosti in cassaforte, qualora lo richiedano le esigenze democratiche.

3.1. *Le criticità del decreto legislativo 97/2016. Le eccezioni all'accesso e le Linee Guida Anac*

Il d. lgs. 97/2016 ha mantenuto ferma una contraddizione: il novellato art. 5, comma 2, del d. lgs. n. 33/2013, che introduce l'accesso "generalizzato" allo «scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico» convive con il comma 3 dell'art. 24 della legge 241/90, secondo il quale «non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni»[146].

Nonostante la sua apparente filosofia di *full agency disclosure* già il *Foia* statunitense, che lo ispira, avrebbe potuto mostrare tutti i suoi limiti, quindi la direzione che il *Foia* italiano avrebbe dovuto evitare nonché la filosofia da preferire. Esso si è mostrato permeato di deroghe. Poiché esso stava diventando un simbolo sempre più decantato come garanzia di *right to know* negli ultimi cinque anni, la quantità dei segreti di sicurezza nazionale è cresciuta sempre di più per contenere la portata degli effetti dell'apertura. Guardando alla

---

[145] ID., *ivi*, p. 56, cit. : «The structural question that demands our attention is whether *FOIA* amounts to a long-term impediment to administrative capacity, trust in government, and an egalitarian democracy».

[146] Tale limite si riferisce sì all'accesso documentale, ma come si concilia con quello generalizzato?

sua applicazione pratica si sarebbe già potuto scoprire il peggiore dei risultati: il *Foia* perseguiva *de facto* la finalità opposta a quella fissata *de iure,* legittimando il segreto di governo, e allo stesso tempo delegittimando e debilitando il governo stesso[147].

Gli studi hanno costantemente dimostrato che la maggior parte delle richieste *Foia* sono avviate da imprese interessate al perseguimento dei propri interessi commerciali desiderosi di imparare dai concorrenti, dagli avversari, o dal contesto regolativo. Al di là di imprese e gruppi commerciali, altre classi significative di utenti *Foia* hanno incluso individui alla ricerca di documenti relativi ai servizi di governo o alle loro procedure di immigrazione, così come oppositori politici intenzionati a sommergere il sistema con ripetute richieste pretestuose. La struttura *request-driven* del *Foia* ha incanalato le risorse pubbliche verso l'industria privata, creando possibilità di arbitrio informativo, aumentando il peso delle imprese nel corso del contenzioso e dei negoziati, e compromettendo il carattere partecipativo della legge.

Così il decreto legislativo 97, nonostante le modifiche intervenute rispetto alla bozza di decreto[148], ha conservato la eccessiva discrezionalità nella individuazione dell'interesse

---

147 ID., *ivi*, p. 4, cit.: «one might find that *Foia* ultimately serves to legitimate the lion's share of government secrecy while delegitimating and debilitating government itself».

148 Si sottolinea che sulla bozza di decreto attuativo sono intervenute diverse critiche da parte delle Associazioni di categoria (FOIA4Italy) - i fautori di un più ampio *Freedom of Information Act* italiano, i quali si erano mobilitati e avevano raccolto firme sono stati ascoltati dalla Commissione Affari Costituzionali il 7 aprile 2016 - e da parte di altri esperti (cfr. Audizioni Presidente *ANAC*, Raffaele Cantone del 30 marzo 2016 e del Garante per la protezione dei dati personali, Antonello Soro del 6 aprile 2016). Si è altresì pronunciato il Consiglio di Stato con il parere n. 343/2016 del 18 febbraio 2016 nel quale il Supremo Organo della Giustizia Amministrativa ha espresso una serie di considerazioni sulla necessità di una "riforma organica" della pubblica amministrazione e di una 'visione nuova' della stessa. In particolare il Consiglio di Stato ha insistito su:

• rilevanza cruciale dell'implementazione della riforma, anche dopo l'approvazione dei decreti attuativi;

• importanza, in particolare, della creazione di una cabina di regia per l'attuazione "in concreto", che curi anche gli strumenti "non normativi" di intervento (quali: la formazione dei dipendenti incaricati dell'attuazione, la comunicazione istituzionale a cittadini e imprese sui loro nuovi diritti, l'adeguata informatizzazione dei procedimenti, etc.);

• importanza della "manutenzione" della riforma, attraverso una fase di monitoraggio e verifica dell'impatto delle nuove regole, nonché con la definizione, se del caso, di decreti correttivi, o di quesiti attuativi da porre al Consiglio di Stato. (Nel suo parere, il Consiglio di Stato si è, dunque mostrato assai critico sullo schema di decreto legislativo. Si è citato Norberto Bobbio, «l'aspirazione a una democrazia intesa come regime del potere visibile». Si è sottolineato come la trasparenza sia «una forma di prevenzione dei fenomeni corruttivi». Ma senza semplicità nell'accesso ai dati e con troppe eccezioni, è tutto inutile. Il silenzio-rigetto, decorsi i 30 giorni dalla richiesta, realizzerebbe poi «il paradosso che un provvedimento in tema di trasparenza neghi all'istante di conoscere in maniera trasparente gli argomenti in base ai quali la pubblica amministrazione non gli accorda l'accesso richiesto»).

La commissione Affari costituzionali, chiamata a rendere un parere obbligatorio, ma non vincolante sul decreto in esame, ha accolto i rilievi espressi dai tecnici e il legislatore, conformandosi ad essi, ha recepito alcune delle indicazioni ivi contenute mediante l'introduzione delle seguenti modifiche al testo originario:

rilevante[149] - anche il diritto d'autore può esserlo[150]- in base al quale l'amministrazione può rifiutare l'istanza di accesso.

L'articolo 6, comma 2 del d. lgs. 97/2016 che introduce nel decreto Trasparenza l'articolo 5 bis, al comma 1 stabilisce i limiti all'accesso e recita: «l'accesso civico di cui all'articolo 5, comma 2, è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici inerenti a:

a) la sicurezza pubblica e l'ordine pubblico;

b) la sicurezza nazionale;

c) la difesa e le questioni militari;

d) le relazioni internazionali;

e) la politica e la stabilità finanziaria ed economica dello Stato;

f) la conduzione di indagini sui reati e il loro perseguimento;

g) il regolare svolgimento di attività ispettive.

L'accesso di cui all'articolo 5, comma 2, è altresì rifiutatosi il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

A. La previsione di un obbligo di motivazione in caso di rigetto (era inizialmente previsto, in caso di mancata risposta dopo trenta giorni dalla domanda di un singolo cittadino, una sorta di "silenzio-rigetto" della P.A. privo di motivazione e di un presidio sanzionatorio, in caso di illegittimità del rifiuto);

B. La definizione di linee guida sulle eccezioni all'accoglimento delle richieste di accesso, rimessa all'*ANAC* che ha pubblicato le Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013 oggetto di consultazione fino al 28 novembre 2016. Le censure mosse alle eccezioni all'accesso hanno riguardato il fatto che oltre a essere numerose e vaghe non elencavano i criteri ex ante sulla base dei quali l'amministrazione può rifiutare l'accesso e creano non pochi problemi non solo per i cittadini, ma anche per le amministrazioni;

C. La definizione di un potere sanzionatorio, oggetto del Regolamento in materia di esercizio del potere sanzionatorio ai sensi dell'articolo 47 del decreto legislativo 14 marzo 2013, n. 33, come modificato dal decreto legislativo 25 maggio 2016, n. 97 (inizialmente non erano previste sanzioni. L'amministrazione che negasse illegittimamente l'accesso non era sanzionata, nemmeno a seguito di un giudizio soccombente);

D. La previsione della gratuità dell'accesso, prima sottoposta a un costo non meglio definito;

E. La possibilità di ricorrere oltre al TAR (in caso di contestazione del rigetto) al riesame del responsabile della prevenzione della corruzione e della trasparenza (la previsione iniziale del solo ricorso al TAR, eccessivamente oneroso - il costo del contributo unificato è di 500 euro - aveva il chiaro scopo di dissuadere il cittadino ad agire in giudizio in difesa dei suoi diritti). Qualora si tratti di atti delle amministrazioni delle regioni degli enti locali, il richiedente può altresì presentare ricorso al difensore civico competente per ambito territoriale

[149] L'articolo 6, comma 1 del d. lgs. 97/2016 che modifica l'articolo 5 del d.lgs. 33/2013 stabilisce che «Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis».

[150] Il novellato articolo lett. 5 bis, comma 2, lett. c) del d.lgs. 33/2013.

a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia;

b) la libertà e la segretezza della corrispondenza;

c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali».

Viene richiesta una valutazione del pregiudizio "verosimile" secondo un criterio soggettivo rimesso alla discrezionalità del dirigente.

Occorre rilevare, inoltre, che l'interesse all'apertura del dato non va, secondo quanto stabilito dal decreto in esame nella sua versione definitiva, di volta in volta valutato e bilanciato con un interesse di pari livello, ma sacrificato *tout court*, qualora "pregiudichi" uno degli ambiti richiamati dal decreto n. 97/2016.

Il decreto, infatti non fissa i criteri *ex ante* in base ai quali dovranno essere decise le eccezioni, a tal fine è intervenuta un'appendice regolatoria, fonte di *soft law*: le linee guida *Anac*. L'articolo 6, comma 2 del decreto ha previsto che «ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità nazionale anticorruzione, d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni operative».

L'*Anac* è stata chiamata a fornire alle amministrazioni, *ex* art. 6, comma 2 del d. lgs. 97, nella cornice fissata dallo stesso d. lgs. 97/2016, elementi per la valutazione dell'esistenza di pregiudizi agli interessi tutelati dall'art. 5 co. 1 e 2 del del d.lgs. 33/2013. Tali pregiudizi in caso di diniego dovranno essere dimostrati come probabili e concreti ai sensi della disciplina sull'accesso generalizzato e mai assunti presuntivamente.

Il 28 dicembre 2016, con Determinazione n. 1309 sono state approvate in via definitiva le Linee guida operative che definiscono le esclusioni e i limiti al neo accesso civico "generalizzato" di cui all'art. 5 co.2 del d.lgs. 33/2013, relative ai dati, informazioni e documenti "aggiuntivi" rispetto a quelli a pubblicazione obbligatoria, quest'ultimi già vigenti dal 21 aprile 2013, giorno di entrata in vigore del previgente del d.lgs. 33/2013 e aggiornati sempre a fine di quest'anno.

Si ritiene opportuno svolgere alcune considerazioni in punto di domanda:

1) Le linee guida in apertura specificano le differenze tra le tre tipologie di accesso e precisano che «l'accesso agli atti di cui alla l. 241/90 continua certamente a sussistere, ma parallelamente all'accesso civico (generalizzato e non), operando sulla base di norme e presupposti diversi. Tenere ben distinte le due fattispecie è essenziale per calibrare i diversi interessi in gioco allorché si renda necessario un bilanciamento caso per caso. Tale bilanciamento è, infatti, ben diverso nel caso dell'accesso documentale dove la tutela può consentire un accesso più in profondità e, nel caso dell'accesso generalizzato, dove le esigenze di controllo diffuso del cittadino devono consentire un accesso meno in profondità (se del caso, in relazione all'operatività dei limiti) ma più esteso, avendo presente che l'accesso in questo caso comporta, di fatto, una larga conoscibilità (e diffusione) di dati, documenti e informazioni»[151].

Ci chiediamo perché l'accesso generalizzato sarebbe un accesso meno in profondità rispetto a quello documentale. Se volessimo conoscere l'operato della P.a. dovremmo fermarmi in superficie? Oppure dovremmo essere titolari di una situazione giuridica soggettiva? Se così fosse, cosa sarebbe cambiato, rispetto alla l. 241 del 1990?

2) L'*Anac* invita i soggetti tenuti all'applicazione del Decreto trasparenza ad adottare regolamenti interni sull'accesso per fornire un quadro organico e differenziare i tre tipi di accesso[152]. Non si rischia in questo modo di incentivare la proliferazione di documenti difformi e quindi la frammentarietà?

3) L'*Anac* definisce l'ambito soggettivo e oggettivo di applicazione del d. lgs.[153] L'*Anac* interpreta estensivamente i soggetti passivi (a chi si può inoltrare la richiesta di accesso) indicati dall'articolo 2 del d. lgs. 33/2013 e stabilisce che non sono esclusi i soggetti di cui ai punti 2 e 3 solo perché la disciplina vi si applica «in quanto compatibile» in quanto il principio della compatibilità (…) concerne la sola necessità

---

[151] Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013, Art. 5- bis, comma 6, del d.lgs. n. 33 del 14/03/2013 recante «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni». Delibera n. 1309 del 28 dicembre 2016, in *http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666*, p. 7.

[152] *Ibidem.*

[153] Pubbliche amministrazioni, enti pubblici economici, ordini professionali, società in controllo pubblico ed altri enti di diritto privati assimilati, società in partecipazione pubblica ed altri enti di diritto privato assimilati.

di trovare adattamenti agli obblighi di pubblicazione in ragione delle caratteristiche organizzative e funzionali dei citati soggetti. Non è invece operante per quel concerne l'accesso generalizzato, stante la *ratio* e la funzione dell'accesso generalizzato descritta nel primo paragrafo delle presenti linee guida. L'accesso generalizzato, pertanto, è da ritenersi senza dubbio un istituto «compatibile» con la natura e le finalità dei soggetti sopra elencati ai punti 2 e 3, considerato che l'attività svolta da tali soggetti è volta alla cura di interessi pubblici.

Analogamente l'*Anac* non riduce il campo di applicazione dell'istituto per i soggetti indicati al comma 3 dell'art. 2 bis del decreto trasparenza ai soli dati e documenti inerenti all'attività di pubblico interesse. In merito, l'Autorità chiarisce che «l'intento del legislatore è quello di garantire che la cura concreta di interessi della collettività, anche ove affidati a soggetti esterni all'apparato amministrativo vero e proprio, rispondano comunque a principi di imparzialità, del buon andamento e della trasparenza», e che, pertanto, devono considerarsi ricomprese anche «le attività che pur non costituendo diretta esplicazione della funzione o del servizio pubblico svolti sono ad esse strumentali».

Nella definizione dell'ambito oggettivo[154] delle Linee Guida l'A*nac* specifica che non è ammissibile una richiesta di accesso meramente esplorativa (generica), volta a scoprire di quali informazioni l'amministrazione dispone.

4) Le richieste non devono essere generiche, ma consentire l'individuazione del dato[155]. Il cittadino dovrebbe sapere specificamente quello che chiede, se così fosse non avrebbe già la risposta che cerca?

Tale esternazione contrasta con i rilievi del Consiglio di Stato[156], nel parere reso sul testo del decreto, che aveva ritenuto «incongruo che l'istanza di accesso civico, considerati i suoi presupposti e le sue finalità, debba essere già in grado di identificare «chiaramente» i dati, le informazioni o i documenti richiesti»[157]. Il dettaglio di quanto richiesto talvolta può non essere specificamente noto all'istante prima dell'accesso.

---

[154] p. 10.

[155] Si richiama in nota il parere del Consiglio di Stato del 18.2.2016.

[156] Consiglio di Stato con il parere n. 343/2016 del 18 febbraio 2016.

[157] *Ibid.*

L'*Anac* precisa che non è inoltre ammessa «una domanda di accesso per un numero irragionevole di documenti imponendo così un carico di lavoro tale da paralizzare, in modo molto sostanziale, il buon funzionamento dell'amministrazione, la stessa può ponderare da un lato, l'interesse dell'accesso del pubblico ai documenti e, dall'altro, il carico di lavoro che ne deriverebbe, al fine di salvaguardare, in questi casi particolari e distretta interpretazione»[158].

Il «carico di lavoro» viene bilanciato con l'interesse alla trasparenza e quindi elevato a diritto? Chi valuta la manifesta irragionevolezza del numero di documenti? E in base a che cosa? È una via di fuga per le amministrazioni inoperose? Chi stabilisce quando un numero è irragionevole? Se lo fa il dipendente della P.A. sulla base delle sue competenze la valutazione potrebbe non essere oggettiva. Non è forse l'inverso e cioè l'interesse all'accesso e conseguentemente la gestione di una pluralità di domande, ovviamente purché non pretestuose, a rispondere al principio di buon andamento della pubblica amministrazione, *ex* articolo 97 Cost.?

5) L'*Anac* stabilisce che per informazioni si intende «la rielaborazione di dati detenuti dalle amministrazioni effettuate per propri fini contenuti in distinti documenti» e che la p.a. non ha l'obbligo di rielaborare i dati ai fini dell'accesso generalizzato, ma solo di consentire l'accesso. L'amministrazione non sarebbe tenuta a raccogliere, elaborare dati che non siano già in suo possesso.

La P.A. aprirebbe dati manipolati o elaborati e non dati grezzi? Non dovrebbe fornire una doppia o triplice versione degli stessi, in modo che il cittadino possa incrociarli e verificare in base a quali criteri sono stati elaborati?[159]

Quali sono i criteri sulla base dei quali vengono raccolti i dati, quali i criteri di elaborazione? Una manipolazione potrebbe alterare il dato. Come già esplicitato nei paragrafi che precedono, servirebbero parametri *standard* pubblici che dettino criteri di raccolta dei dati e delle informazioni della PP.AA.

Qualora i dati richiesti non fossero nelle disponibilità dell'amministrazione, la stessa non si dovrebbe invece attivare per produrli o per fornirli mediante

[158] Si richiama sentenza del Tribunale Prima Sezione ampliata 13 aprile 2005 causa T 2/03.

[159] *Supra* § 4.

piattaforme interoperabili o il cittadino dovrebbe accettare l'inerzia della p.a. inoperosa?

6) L'*Anac* ha definito l'ambito di applicazione delle eccezioni assolute e dei limiti. Ha ampliato l'estensione delle eccezioni anziché circoscriverle, l'Autorità richiama una vasta serie di norme e sentenze che ben potranno fornire ai funzionari pubblici motivi di rigetto per l'astratta ricorrenza di una delle fattispecie esposte nelle Linee Guida.

In riferimento alle eccezioni assolute per le quali il bilanciamento è effettuato a monte dal legislatore- Segreto di Stato e divieto di divulgazione - sulla base di una valutazione preventiva e generale. Dunque l'accesso generalizzato è escluso da quelle fonti di rango legislativo che tutelano questi interessi prioritari e fondamentali, vengono individuati:

A) il Segreto di Stato[160].
B) Altri casi previsti dalla legge e limiti di cui all'art. 24, comma 1 della legge n. 241/90[161].

Si badi bene, sono previste ulteriori limitazioni alla conoscibilità previste da normative di settore (es. archivi di Stato e altri Archivi disciplinati dal Codice dei beni culturali e del paesaggio).

In riferimento alle eccezioni relative, ovvero eccezioni relative o qualificate, il legislatore non opera, come per le eccezioni assolute, una generale e preventiva individuazione di esclusioni all'accesso generalizzato, ma rimanda all'attività valutativa delle amministrazioni mediante uno pseudo-bilanciamento, caso per caso, tra l'interesse pubblico all'apertura dei dati e la tutela di altrettanti rilevanti interessi considerati tali dall'ordinamento. La disciplina non chiarisce l'atteggiarsi in concreto della ricorrenza di ipotesi di eccezione. La valutazione è rimessa all'amministrazione che dovrà valutare caso

---

[160] Oltre alla definizione generale di cui all'art. 39 della legge n. 124/2007, altre ipotesi di segreto sono quello statistico, sulla corrispondenza, sui pareri professionali, sui dati sensibili – art. 7 e 26, co 4 d. lgs. 33/2013.

[161] Il diritto di accesso è escluso: a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo; b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano; c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione; d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

per caso se l'interessa all'apertura prevale sulla tutela di altri validi interessi tutelati dall'ordinamento. Deve sussistere un nesso di causalità tra accesso e pregiudizio concreto valutato sulla base di un evento probabile e non solo possibile.

Ne deriva che la trasparenza retrocede ogni volta che possa risultare scalfito un altro interesse tutelato dal nostro ordinamento in nome, oltretutto, di normative spesso vetuste. E in risposta alla discrezionalità senza criteri prestabiliti ex ante dal legislatore si avranno soluzioni diverse sul territorio nazionale a seconda della sensibilità e operosità dell'amministrazione coinvolta.

L'amministrazione dovrà agire in negativo verificando prima l'assenza di eccezioni assolute poi la presenza o meno di eccezioni relative, ed eventualmente indicare chiaramente quale – tra gli interessi elencati all'art. 5, co. 1 e 2 – viene pregiudicato; dimostrare che il pregiudizio prefigurato dipende direttamente dalla *disclosure* dell'informazione richiesta; dimostrare che il pregiudizio conseguente alla *disclosure* è un evento altamente probabile, e non soltanto possibile.

Non si forniscono, in questo modo, indicazioni certe a un personale che non ha neanche un'adeguata formazione. In virtù della clausola di invarianza finanziaria, deve provvedersi «con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente». L'*Anac*, inoltre riconosce la temporaneità delle indicazioni contenute dichiarando soggette a continua interpretazione evolutiva.

Il decreto che avrebbe dovuto sancire la prevalenza della trasparenza come attività necessaria al corretto ed efficace agire della P.A., finisce per consacrarne la limitazione.

Per esempio: con riguardo alle richieste aventi ad oggetto la stabilità finanziaria ed economica dello Stato, l'*Anac* pone all'attenzione delle stesse PP.AA. gli "effetti di contagio" e le "ripercussioni rilevanti" che potrebbero derivare dalla divulgazione di informazioni in materia di banche, assicurazioni e affini, incentivando il funzionario a rigettare la domanda di accesso. A rendere ancora più plausibile una tale soluzione è la sanzione minore prevista per il diniego scarsamente motivato rispetto a quella prevista per la violazione di segreto/riservatezza.

Altri esempi di rigetti all'accesso generalizzato saranno chiarificatori:

- il CSM ha negato l'accesso all'elenco dei magistrati nei confronti dei quali si era concluso un procedimento disciplinare secondo la motivazione che tali procedimenti hanno natura giurisdizionale. Ci chiediamo se un procedimento sanzionatorio possa definirsi giudiziario. Sarebbero allora equiparabili ai procedimenti penali? Se il Garante *Privacy* ha specificato che i provvedimenti disciplinari contro i professionisti devono essere resi pubblici[162] perché l'utente ha il diritto di conoscere, allora perché la regola di trasparenza non varrebbe per i magistrati?

«La legge n. 675/1996 non ha modificato la disciplina legislativa sulla pubblicità degli albi professionali, i quali, anche in ragione della tutela dei diritti di coloro che, a vario titolo, intrattengono rapporti con gli iscritti, sono funzionalmente soggetti ad un regime di piena pubblicità, che si estende anche ai provvedimenti di carattere disciplinare. Detto regime di conoscibilità dei provvedimenti disciplinari, che si fonda su rilevanti motivi di interesse pubblico, deve ritenersi prevalente rispetto all'interesse alla riservatezza del singolo professionista destinatario della sanzione disciplinare, purché la menzione del relativo provvedimento applicativo avvenga in modo corretto e in termini esatti e completi. Ne consegue la liceità della divulgazione di detti provvedimenti tramite riviste o notiziari curati dai Consigli dell'Ordine, la cui pubblicazione è riconducibile all'ampia nozione di trattamento di dati personali finalizzato alla pubblicazione o diffusione occasionale di articoli, saggi o altre manifestazioni del pensiero, cui è applicabile la disciplina prevista dall'art. 25 delle legge n. 675/1996 in tema di attività giornalistica e di informazione». E ancora il Garante[163] «Detti principi operano anche nel caso della ripubblicazione della notizia dell'irrogazione della sanzione – nella specie, la sospensione per sei mesi dall'esercizio della professione – nel corso della sua esecuzione, non assumendo alcuna rilevanza che la

[162] Così il Gpdp 29 marzo 2001, in *Bollettino,* n. 18, pag. 20 [doc. web n. 39536].

[163] Gpdp 25 settembre 2002, in *Bollettino*, n. 31, pag. 55 [doc. web n. 1066212].

rivista giunga ai destinatari in un tempo di poco successivo alla cessazione della sospensione». Aprire questi dati esporrebbe i giudici ad azioni intimidatorie? Nascondere i dati o aprire i dati risponderebbe alla tutela del buon andamento della giustizia? Posto che bisognerebbe verificare lo stadio del procedimento – si dovrebbero pubblicare solo i dati relativi a procedimenti chiusi – occorre capire se rendere accessibile queste informazioni risponde all'interesse di garantire l'imparzialità della giustizia.

- Alcuni comuni, nei confronti dei quali era stata avanzata domanda, hanno negato l'accesso al carteggio istituzionale[164] tra sindaco e assessori. In particolare un Comune ha negato l'accesso in virtù della segretezza *ex* art. 15 (limite relativo), un altro ha motivato il rigetto con la mancata indicazione delle mail specifiche di cui si chiedeva visione.

Dagli interrogativi posti si evince chiaramente che l'accesso legittima la chiusura, offrendo una serie di eccezioni in cui l'amministrazione potrà nascondere la ragione della propria diffidenza e mantenere avversariale il rapporto con il cittadino, rinunciando a qualsiasi forma di collaborazione.

4. Le variabili di apertura dei dati: la necessità del dato grezzo

A questo punto dell'esame ci sembra opportuno analizzare i diversi modi di essere del dato, a tal fine proveremo a linearizzare nella descrizione fenomeni che presentano un'indubbia specificità tecnica.

Partiamo dalla definizione di dato.

I dati sono descrizioni di fatti potenzialmente riproducibili, parte di strutture informative più vaste.

[164] occorrerebbe qui verificare più che dall'indirizzo e-mail utilizzato, dal tenore della conversazione se la mail è privata o istituzionale.

Il dato è di per sé neutro[165], diventa informazione quando viene creato, estratto, elaborato e utilizzato per determinate finalità. L'apparato di informazioni, formato da dati di uno stesso tipo o di tipo diverso, costituisce un "dataset" e diventa conoscenza quando viene interpretato attraverso strumenti quali applicazioni, indicatori, metodi, incroci.

La conoscenza prodotta dai dati si eleva a consapevolezza quando è in grado di influire sulla realtà, migliorandola, al punto che essi divengono, nel caso specifico degli *Open Data*, bene comune[166].

Affinché i dati sviluppino tutto il loro potenziale in termini di utilità è necessario che l'informazione che essi contengono venga rilasciata, come più volte evidenziato, in formati di *file machine-readable*.

I dati si possono aprire utilizzando una grande varietà di formati, ma va tenuto presente che non tutti questi formati rispondono ai requisiti necessari per essere definiti "aperti"; si vuole qui dire che non è sufficiente pubblicare un dato perché sia "aperto". Un esempio può servire a linearizzare questo concetto tecnico: la pubblicazione di un formato immagine (es. jpeg) non è un dato aperto perché per come esso si presenta non è riutilizzabile agevolmente da chiunque, ma è solo scaricabile e visibile. In sintesi: un dato è aperto se è generativo in via incrementale di altri dati grazie all'apporto conoscitivo chi viene dopo colui che immesso per rimo il dato di partenza.

Il formato in cui i dati sono pubblicati, ossia la fonte digitale in cui sono memorizzati può essere aperta o chiusa. È aperta se le specifiche per il *software* sono a disposizione di chiunque, che può utilizzarle gratuitamente, senza alcuna limitazione di riuso determinata da diritti di proprietà intellettuale. Diversamente è chiusa se il formato è proprietario e le caratteristiche tecniche non sono pubblicamente disponibili, o se il riutilizzo è limitato.

Da questa descrizione risulta evidente che il fine ultimo dell'apertura è rappresentato dall'interoperabilità. In altre parole essa rappresenta «la capacità di diversi sistemi e organizzazioni di lavorare insieme […] di combinare una base di dati (*database*) con altre. L'interoperabilità è la chiave per realizzare il principale vantaggio pratico dell'apertura:

---

[165] Cfr. con articolo 68.3, CAD. Cfr anche con *Breve guida agli* open data, in *http://www.ascuoladiopencoesione.it/wp-content/uploads/2016/01/2.3-Breve-Guida-Open-Data.pdf*.

[166] *ibid.*

aumentare in modo esponenziale la possibilità di combinare diverse basi di dati, e quindi sviluppare nuovi e migliori prodotti e servizi»[167].

Non solo l'apertura consente il riutilizzo e lo sviluppo delle informazioni, ma annulla i costi che potrebbero essere imposti da dati pubblicati in formati proprietari, leggibili soltanto utilizzando un determinato *software* che potrebbe avere costi proibitivi o cadere in disuso. Si distinguono diversi tipi di formati che per ragioni di praticità tratteremo superficialmente, semplificandone la definizione tecnica. Ci avvarremo di una schematizzazione che è quella proposta da Tim Berners-Lee.

Uno dei formati disponibili è il CSV (*Comma Separated Values*) formato di *file* compatti utile a riunire insiemi di dati a base testuale, facilmente importabili ed esportabili verso fogli di calcolo e *database*. Questo formato però è così grezzo che senza documentazione, metadati, rende i dati inutili, dal momento che diventa complicato identificare il significato delle diverse colonne. I fogli di calcolo, come *Excel* utilizzabili unitamente alle descrizioni delle colonne potrebbero contenere funzioni e formule non facilmente gestibili. I *database* consentono un accesso diretto ai dati, estraibili in forma isolata, in ragione dell'interesse legato all'utilizzo, la loro adozione comporta alcuni problemi di sicurezza nell'estrazione remota e l'accesso ai casi in cui le tabelle siano ben documentate. Il formato RDF (*Resource Description Frame*work) definisce in che modo le informazioni devono essere rappresentate *online*. RDF associa dati a informazioni diverse, consentendo di estrarne contenuti permettono l'integrazione con altri e l'interoperabilità tra più applicazioni. Il formato HTML (*Hyper-Text Markup Language*) permette di descrivere la formattazione di un documento *web*, attraverso il protocollo HTTP. Con questo formato si possono generare collegamenti a diversi *file*, consentendo l'organizzazione e la costruzione di ipertesti. Il formato XML (*eXtensible Markup Language*) è un linguaggio flessibile utilizzato per lo scambio dei dati, di cui conserva la struttura dei dati, integrabile con altri dati senza che si interferisca con la loro lettura. Il formato JSON è di semplice lettura per tutti i linguaggi di programmazione. Il documento di testo come *Word* o *PDF* mostra facilmente dati, è condivisibile ma non è adatto all'inserimento automatico di dati. Il testo semplice è facilmente leggibile anche se senza informazioni strutturali è necessario un analizzatore

[167] *Breve guida agli* open data, p. 3, cit.

per interpretare ogni documento. L'immagine acquisita da *scanner* è il formato meno adatto alla fruibilità, ciò nonostante questo tipo di formato può aiutare a visualizzare le immagini dei dati nativi analogici.

Infine vi sono i formati proprietari, il cui utilizzo è limitabile ai casi in si prevede un utilizzo successivo in un sistema simile a quello che li ha generati[168].

Tuttavia, nel caso in cui si dovesse scegliere se pubblicare i dati *no machine readable* o non pubblicarli, la logica dell'*Open Data* propende verso la prima soluzione. È questa la ragione che ha guidato il movimento *Raw Data Now!*[169] avviato da Tim Berners-Lee: avere dati non aperti, ma distribuiti in formato *raw* è preferibile a non averli affatto perché sarà poi la comunità degli utenti – qualora ne ravvisi l'utilità - a elaborarli e a convertirli in *open data* mediante tecniche di *data scraping*. Tim Berners-Lee ha proposto un modello di classificazione dei dati per distinguere i diversi formati utilizzabili nella codifica dei *set,* attribuendo ad essi un numero di stelle da uno a cinque, che corrispondono ai gradi di apertura. I dati con una sola stella sono quelli sì disponibili, leggibili, archiviabili, pubblicabili e stampabili ma che rappresentano il livello base di dati non strutturati, non elaborabili (formati come *.gif*, *.jpg*, *.png*, *.docx*, *.pdf*). I dati con due stelle sono quelli codificati con un formato proprietario, non aperto ma comunque convertibili in dati aperti proprio perché strutturati (es. *Microsoft Excel*). I dati con tre stelle sono strutturati e codificati in un formato non proprietario, si tratta di dati aperti semplici che è possibile elaborare senza utilizzare *software* proprietari (es. *.csv*). I dati con quattro stelle indicano i dati strutturati e codificati in un formato non proprietario, utilizzabili direttamente *online* (es. si pensi ai dati relativi agli indirizzi delle fermate del *bus*, opportunamente codificati, da qualsiasi *browser* è possibile georeferenziarli su una mappa). Infine i dati con cinque stelle sono i *Linked Open Data* (LOD)[170], quei dati aperti, cioè, dati strutturati e codificati in un formato non proprietario, utilizzabili direttamente online e che presentano anche, nella struttura del *dataset*, collegamenti ad altri *dataset*. In altri termini, è possibile collegare dinamicamente tra

---

168 *Breve guida agli* open data, pp. 3-5, cit.

169 "*Raw data now!*" di *Tim Berners-Lee e il Web prossimo venturo*, *in* https://www.ted.com/talks/tim_berners_lee_on_the_next_web, nel marzo 2009.

170 M. OREFICE, *op. cit.,* p. 713 ss.

loro più *dataset*, incrociando così informazioni provenienti da fonti diverse, eventualmente gestite da diverse Amministrazioni o Enti Privati.

Tanto premesso, per ridurre il rischio di comportamenti di diffusione strategica dei dati, sarebbe opportuno che il legislatore specificasse non solo la tempistica del rilascio, ma anche il formato, così come la sostanza degli obblighi di pubblicazione di base. Gli *standard* di temporalità e di formattazione servono a facilitare l'analisi e soprattutto la supervisione. Essi, infatti, stabiliti i criteri generali sulla base dei quali i documenti andrebbero rilasciati *rectius* aperti, possono anche rendere più difficile per le agenzie rilasciare il materiale in modo parziale o opportunistico, e quindi falsato, cioè in modo da avvantaggiare certe agende politiche o interessi particolari, o in un modo progettato per nascondere gli elementi controversi del "flusso" di informazioni[171].

In questa sede analizzeremo una serie di modalità di *disclosure* per avanzare una specifica proposta di apertura cioè l'analisi che seguirà è preordinata alla seguente domanda: in quale formato è più utile per gli utenti - cittadini che i dati vengano pubblicati?

a) Una modalità potrebbe essere quella consistente nel rendere disponibili i dati nella loro forma grezza[172], quindi dati non necessariamente *open*[173], questi dati sono caricati in un formato non necessariamente fruibile ma convertibile, non sono necessariamente completi, ma integrabili. Questo è il modo di procedere dell'amministrazione italiana che rende visibile meno del minimo indispensabile (per lo più) formati a due stelle. In riferimento a questa modalità ci chiediamo: il fatto che siano grezzi dà la garanzia della neutralità, cioè è sufficiente a definire i dati non manipolati?;
b) Un'altra modalità potrebbe essere quella di "aprire" i dati *linked*, cioè collegati con altri *dataset*, i dati cd. "a cinque stelle" nella classificazione di Tim Berners-

[171] «They can also make it harder for agencies to release material in a biased or opportunistic manner, so as to benefit certain political agendas or special interests, or in a manner designed to hide controversial items in a "flood" of information». Id, *op. cit.*, pp. 51-52, cit..

[172] Cfr. discorso su "*Raw data now*!" di *Tim Berners-Lee e il Web prossimo venturo*.; A. COURMONT, *Open data et recomposition du gouvernement urbain: de la donnée comme instrument à la donnée comme enjeu politique*, in *Informations sociales*, 2015/5 (n° 191), p. 43 ss.

[173] *Supra* nota 9.

Lee, dati multi-contenutistici[174], potenziabili nei futuri sviluppi e strumentali al diritto di iniziativa economica. Anche qui ci chiediamo il collegamento è neutrale, o dipende dalle intenzioni di chi lo effettua?;

c) Un'altra modalità potrebbe essere quella del dato non solo *linkato,* ma volontariamente manipolato dall'amministrazione che lo detiene e lo rende pubblico per una determinata finalità. Questa modalità pone, in forma più chiara rispetto alle altre, una serie di questioni relative all'attendibilità e genuinità dei dati. Se da una parte il dato elaborato è un dato più utile, perché iper-collegato; dall'altra l'interesse a manipolare i dati per finalità specifiche potrebbe adulterare i dati, per esempio per nascondere delle inottemperanze o una mala gestione. Allora, ci chiederemo: chi effettua la manipolazione deve dichiararne anche la finalità? Chi la controlla? L'amministrazione stessa? Un ufficio *ad hoc* o l'Ufficio a cui o alla cui attività quei dati si riferiscono? Occorrerebbe, forse, in prima battuta, definire l'Autorità chiamata a effettuare questa manipolazione; in seconda battuta, il criterio in base al quale è stata resa o dovrebbe essere resa. Quindi ci chiediamo se debba essere comune o possa essere mutuato a seconda dell'Autorità di controllo interessata per definire, infine, l'Autorità chiamata a verificare la conformità delle manipolazioni ai criteri pubblicati.

Per capire quale delle tre modalità è quella più adatta al cittadino è necessario fare luce sulle finalità del processo di apertura dei dati.

Come ampiamente anticipato nel paragrafo 1, il singolo può utilizzare i dati per avviare un'attività commerciale o sviluppare un'applicazione per fini lucrativi, svolgere un'attività autonoma di interesse generale, anche in forma associata, sulla base del

---

[174] Così si è espresso *Tim Berners-Lee,* in *https://www.ted.com/talks/tim_berners_lee_on_the_next_web, nel marzo 2009*: "[…] quando ricavo tali informazioni non avrò solo l'altezza, il peso o la data di nascita di qualcuno, ma otterrò relazioni. I dati sono relazioni […]. La tal persona è nata a Berlino, Berlino è in Germania. E quando ci sono delle relazioni, ogni volta che c'è una relazione l'altro dato a cui è relazionato riceve anch'esso uno di quei nomi che iniziano con HTTP. Quindi posso continuare e consultare questo nuovo dato. Così [se] cerco una persona -- posso vedere la città in cui è nata posso vedere la regione in cui si trova, in che città, quale sia la popolazione di questa città, e così via. Così posso scorrere tutte queste informazioni". Cfr. con J. GURIN, *Open Data Now The Secret to Hot Startups, Smart Investing, Savvy Marketing, and Fast Innovation*, 2014, pp. 1-21.

principio di sussidiarietà orizzontale, sostituendosi ai pubblici poteri tenuti[175] a favorire l'autonoma iniziativa dei privati.

Dal ragionamento svolto, risulta chiaro che gli *Open Data* si elevano a *Super Data*[176] cioè raggiungono l'apice della loro utilità, quando si aprono a tutti i loro possibili sviluppi, cioè quando diventano aperti a tutti i potenziali utilizzatori e si possono leggere facilmente perché hanno un formato *standard*, agevolmente apribile da qualsiasi terminale e soprattutto quando sono collegati ad altri dati, ad altri *dataset*.

Stante questa finalità, non escludiamo l'ipotesi di una modalità inedita, vale a dire che non rientra in nessuna delle tre sopra indicate. La nostra proposta è la seguente.

Di ogni dato dovrebbe essere pubblicata una triplice versione, in formato grezzo, assunto che sia neutrale[177], e in formato *linkato* con manipolazione, in modo tale da garantire al suo potenziale fruitore la possibilità di incrociare quel dato e verificare così i criteri attraverso i quali esso è stato prodotto, selezionato ed eventualmente elaborato.

Questa modalità impedirebbe altresì le possibili manipolazioni, ovvero la manomissione dei dati, finalizzata al perseguimento di interessi privati o meglio consentirebbe di verificare se il dato è stato orientato per la finalità, preventivamente dichiarata[178]. Restano alcune domande: in questo caso il cittadino-sentinella si sostituirebbe al verificatore o sarebbe comunque necessaria un'Autorità preposta al controllo?

A fini esemplificativi, assumiamo che i laboratori che effettuano le analisi delle acque si occupino anche delle operazioni di depurazione, essi potrebbero avere interesse a manipolare i risultati così ottenuti - dai quali si potrebbe desumere l'alto tasso di inquinamento delle acque - applicando criteri utili a nascondere il superamento di

---

175 art. 118.4, cfr. G. DE MINICO, *Gli open data verso una politica costituzionalmente necessaria?*, in *www.forumcostituzionale.it,* 2014, p. 4; G. ARENA, *Il principio di sussidiarietà orizzontale nell'art. 118 u. c. della Costituzione*, in *AA. VV.*, *Studi in onore di Giorgio Berti*, Napoli, 2005, vol. 1, p. 179 e ss.; G. BERTI, *Sussidiarietà e organizzazione dinamica*, in *Jus*, 2004, p. 171 e ss.; V. CERULLI IRELLI, *voce sussidiarietà* (dir. amm.), in *Enc. Giur.*, agg. XII, 2004; G. LOMBARDI–L. ANTONINI, *Principio di sussidiarietà e democrazia sostanziale: profili costituzionali della libertà di scelta*, in *Dir. soc.*, 2003, p. 155 e ss.

176 M. OREFICE, *op. cit.*, 713 e ss.

177 Qui la garanzia della neutralità dovrebbe risiedere nella responsabilità dell'amministrazione che pubblica il dato, chiamata a rispondere della sua autenticità.

178 M. VILLONE nella conversazione tenuta il 13 febbraio 2017; D. POZEN, *Freedom of Information Beyond the Freedom of Information Act*, in *Columbia Public Law*, Research Paper No. 14-541 February 1, 2017, p. 51 ss.; C. ROMAN, *Open data,* in *ConLawNOW,* 19, 2016, p. 24 ss.

determinati valori-limite, o al contrario a mostrare l'inquinamento ma solo per ottenere l'affidamento del servizio di depurazione.

Ne consegue l'evidente opportunità di incrociare i dati manipolati con il dato grezzo, che da statico e inutile in forma isolata, anche se, resta ben inteso, preferibile rispetto alla chiusura, diventerebbe la garanzia dell'autenticità del dato. Affinché il dato grezzo possa conservare la sua funzione di garanzia, è necessaria, ma non sufficiente la sua pubblicazione unitamente a quella dei criteri per la lettura. Un esempio sarà chiarificatore: se nel caso già esaminato il dato non fosse collegato a una tabella dei parametri microbiologici[179], dove sono determinati i valori-limite previsti dalla normativa sulle acque di balneazione, vigente in Italia, quindi con la specificazione di quali valori risultano "fortemente inquinati", non sarebbe possibile effettuare la verifica incrociata dei dati, al fine di accertarne la "bontà".

La nostra proposta come sopra illustrata prevede la triplice pubblicazione[180] dei dati nella versione grezza, in quella elaborata dal soggetto pubblicante, e infine, nel formato arricchito dai principi, dalle finalità e dai criteri di elaborazione dei dati grezzi.

Questa soluzione non è però immune da critiche, alcune delle quali sono state anticipate nell'elencazione delle possibilità di accesso ai dati.

La prima criticità attiene alla valutazione dell'opportunità di enucleare una serie di criteri pubblici oggettivi, che fungano da linee guida nella elaborazione dei dati. In merito a tali linee guida ci chiediamo se esse debbano essere predeterminate e fisse, oppure generiche e mutuabili dalle singole amministrazioni. Quest'ultima opzione si giustificherebbe in quanto consentirebbe maggiore elasticità nell'elaborare il dato[181], nell'individuare i criteri per la sua determinazione, e infine nell'imputare la responsabilità per l'autenticità del dato[182].

---

179 Altri dati grezzi ma linkati secondo la classificazione a cinque stelle di Tim Berners-Lee.

180 La professoressa Giovanna De Minico, in uno scambio dialogico del 20 marzo 2017 ha profilato la possibilità di una triplice pubblicazione, che comprenda oltre ai due *set* (dati grezzi e dati elaborati) la pubblicazione dei principi e dei criteri in base ai quali i dati grezzi sono stati elaborati e per quali finalità).

181 D. POZEN, *op. cit.* 2017 p. 51 ss.; C. ROMAN, *op. cit.,* 2016, p. 24 ss.

182 Il problema della responsabilità va almeno accennato, esso comporta che il soggetto responsabile si assuma ogni incombenza, che lo chiamerà a risponderne qualora l'informazione, divenuta fonte di *n* servizi e applicazioni, dovesse rivelarsi in futuro inesatta oppure obsoleta.

La seconda critica riguarda l'individuazione del soggetto tenuto a dettare i principi in base ai quali i dati devono essere collegati e manipolati; questa questione potrebbe condurre a istituire un'Autorità *ad hoc*, la quale non dovrebbe essere la mera ripetizione di un'Autorità Indipendente, perché il neo soggetto diversamente dal modello richiamato sarebbe titolare di uno degli interessi in gioco, e quindi mancherebbe di quell'indispensabile requisito di terzietà, che caratterizza l'universo delle A.I.

Propendiamo tra le due opzioni, linee guida fisse o variabili, per la prima a condizione di intendere l'aggettivo fisso nei limiti del minimo indispensabile: vale a dire, queste linee dovrebbero prescrivere soltanto formati di dati aperti e interoperabili, nonché anche l'indicazione del soggetto responsabile dell'autenticità del dato.

5. Gli *open data* come ancella del mercato

Risulta di plastica evidenza che gli *Open Data* non coprono solo i dati relativi all'operato del governo («the working of government»), ma includono anche il valore supremo dell'informazione che può essere usata «to increase agency accountability and responsiveness; improve public knowledge of the agency and its operations; further the core mission of the agency; create economic opportunity; or respond to need and demand as identified through public consultation»[183]. In questo senso diventa «a means to solve social problems, create jobs, and generate entrepreneurship».

La domanda di accesso, che nel nostro ordinamento rappresenta l'unico strumento per avere i dati e le informazioni in chiaro, invece, ha una natura litigiosa «giving rise to litigation when the government refuses a request and perversely reinforcing a culture of closed-door governing»[184], tant'è che l'apertura dell'amministrazione, in caso di

[183] B. S. NOVECK, *ivi*, p. 275.
[184] ID., *ivi*, p. 280.

accoglimento della domanda è provocata ed è rivolta al singolo e non alla comunità di utenti.

La richiesta di accesso adotta una «nondisclosure as the default norm»[185], in questo modo il *Foia* alimenta un *cat-and mouse process* per cui la sua principale limitazione sta proprio nell'assenza di una responsabilità proattiva delle pubbliche amministrazioni, «in particular, (a) it does not require agencies to generate information, and (b) it imposes only minimal (and frequently disregarded) obligations to disseminate information without being asked[186]».

Il paradigma *open*, invece, alimenta una rete di condivisione, interoperabilità e riutilizzo. Diversi sono i benefici connessi alla logica di *disclosure*: a) consente di oscurare *ab origine* i dati personali mediante programmi di criptazione, in tal modo non è necessario intervenire nuovamente sul testo con dispendio di tempo e di risorse e con maggiori rischi per la tutela effettiva della *privacy*; b) permette la creazione di documenti nativi digitali, senza che ci sia bisogno di produrre copie di carta ai fini del rilascio, a vantaggio della riutilizzabilità di quei dati per gli scopi sopra elencati; c) alimenta un flusso informativo sempre crescente e innesca un circolo virtuoso di produzione di benefici sociali.

Gli *Open Data* rappresenterebbero allora l'evoluzione del *Foia* perché ne superano l'efficacia. Il regime del *Foia,* in un simile contesto, si inserirebbe come un supplemento, o meglio una *extrema* ratio, in caso di *gaps* del regime *open*. Vi sarebbe dunque la possibilità di ricorrere a un simile istituto, nel caso in cui il cittadino dovesse scontrarsi con la chiusura della p.a.[187].

Nell'esperienza americana, cui ha guardato il legislatore italiano, a sette anni di distanza dall'avvento di un sistema *open* le richieste di accesso sono cresciute da 600.000 a

---

185 D. POZEN, *ivi,* p. 3.

186 H. MICHAEL, *Law Lags Behind: FOIA and Affirmative Disclosure of Information*, 7, *CARDOZO PUB. L. POL'Y & ETHICS J.* 577, 578-79 2009.

187 G. DE MINICO, *La trasparenza della PA costruita sull'asimmetria*, in *il Sole 24 ore*, 21 maggio 2017, p. 13: « […] Il tempo di internet ha suggerito agli americani la filosofia più avanzata dell'*open data*. Con essa l'informazione, creata dall'amministrazione con i dati forniti dai cittadini, è acquisita al concetto di bene comune: un *asset* condiviso e condivisibile tra cittadini e amministrazione. Pertanto, il suo regime giuridico non segue più il modello del Foia, e quindi nonne ripropone l'inconveniente di un'informazione tirannica e singolarmente privilegiata. Si risolve nel semplice obbligo per l'amministrazione di pubblicare ex se ogni dato in suo possesso, e a questo dovere generalizzato per oggetto e destinatario corrisponde un vero e proprio diritto di chiunque alla conoscenza del patrimonio informativo del soggetto pubblico, con eccezione dei vari segreti di Stato e simili».

700.000[188]. Ne sia prova il fatto che incentiva le richieste di accesso hanno completato il quadro normativo esistente, sollecitando il rilascio delle informazioni in tutti i campi e innescando un circolo virtuoso di apertura, che stimola il dibattito tra pubblico e privato su cosa pubblicare, con quale frequenza e in quale formato, ben potendo evolvere nell'articolazione di Linee Guida su cosa, come e quando pubblicare finalizzate al miglioramento della qualità dei dati.

Ma «naked disclosures alone are not enough; rather, change depends upon the actions that are taken following the publication of data». È necessario che si accompagni all'apertura una politica del riutilizzo e un sistema di controllo dei dati basato sul "data about data", cioè sulla diffusione di informazioni sui dati, che spesso sono non richiesti, non conosciuti o non utilizzati.

La prevalenza del regime *open* su quello di accesso fa in modo che la trasparenza non sia un obbligo da soddisfare, ma una politica di collaborazione democratica «rooted in a theory about government effectiveness whereas *FOIA* is grounded in a theory of governmental legitimacy»[189].

Una lente sull'agire pubblico risponde all'evoluzione della società tecnologica che offre nuovi strumenti di partecipazione e controllo alla cosa pubblica e segna la fine dell'era della carta, a cui invece è ancora ancorato il regime dell'accesso, tradizionalmente collegato alla distribuzione di copie di carta e alla gelosa custodia e conservazione di dati.

«Open data emphasizes the instrumental value of information as an asset for evidence-based decisionmaking, service delivery, and economic growth»[190].

La spinta finale per la trasparenza, proprio perché connessa all'esercizio dei diritti fondamentali e alla partecipazione democratica, dovrebbe derivare dai governi oltre che dai sostenitori dell'approccio *open*, ma *de facto* essa sembra che stia diventando la scelta economica degli investitori. Un numero crescente di investitori sta ora cercando società "sostenibili", ovvero aziende che seguono buone prassi ambientali e sociali e che permettano loro di avere successo e incrementare gli introiti nel lungo periodo. Per gli

---

188 D. POZEN, *ivi*, p. 6.

189 B. S. NOVECK, ivi, p. 284.

190 D. POZEN, *ivi,* p. 4, cit..

investitori, la sostenibilità può essere semplicemente un indicatore di buona *corporate governance*: le aziende sostenibili hanno maggiori probabilità di essere preparate per i mandati ambientali dei governi, più possibilità di operare in modi che non contrastino con le amministrazioni locali e meno occasioni di causare catastrofi ambientali o altri scandali che possono danneggiare la loro reputazione[191]. Sembrerebbe che la critica più autentica alla illegittima chiusura delle amministrazioni venga proprio dal mercato: sono le aziende private che vedono negli *open data* un elemento strutturale, costitutivo del mercato, e li pongono al servizio del profitto, dal momento che essi rappresentano un fattore in grado di generare ricchezza.

L'apertura dei dati incontra l'approvazione del mercato che *ex se* supererebbe l'atavico contrasto con l'uguaglianza. Il mercato cancellerebbe le vecchie posizioni asimmetriche tra chi possiede il potere economico[192] e chi no, livellando le posizioni degli utenti, possibili generatori di ricchezza[193].

Come i *Big Data*, nella loro accezione più generale, stanno cambiando il modo di generare profitto, progresso, informazione per gli imprenditori, le imprese, gli scienziati, i giornalisti e le società in generale, così gli *open data* stanno determinando la consapevolezza che al fine di avvantaggiare l'intera comunità anche in termini di uguaglianza - e nella prospettiva mercantilistica di rendere il mercato più prospero e la regola della concorrenza più forte - i dati debbano essere resi disponibili al momento della loro genesi, per un uso pubblico in linea di principio[194].

Lasciare che siano i privati e le loro logiche del profitto a spingere verso questa inversione di rotta dal *Foia* all'*Open Data* non è un buon segno per la democraticità del sistema, sarebbe invece preferibile che il decisore politico non delegasse al privato il

---

191 J. GURIN, *op. cit.*, p. 703.

192 Se l'apertura dei dati diventa ancella del mercato, lo stesso potrebbe diventare più prospero ma le porzioni dei profitti potrebbero dipendere dalla quantità e qualità dei dati liberati, nonché dalle posizioni di potere economico assunte sul mercato dai colossi della Rete, che non sarebbero disposti a cedere la loro ragione di ricchezza: cfr. con la posizione di Google approfondita nel capitolo I.

193 Cfr. con quanto argomentato sul rapporto tra eguaglianza e mercato, seppure in riferimento a un altro argomento e cioè all'ordine di Trump di vietare l'accesso agli immigrati provenienti da uno dei 7 Paesi, dalla prof.ssa Giovanna De Minico, in G. DE MINICO, *Uguaglianza come sostegno al mercato,* su *Il Sole 24 ore* del 5 marzo 2017.

194 «Big Data is changing the world for entrepreneurs, businesses, scientists, journalists, and society at large. Now Open Data is having a similar impact. Where Big Data is essentially a technological development, driven by the increased ability to collect data and analyze it, Open Data is more of a philosophical movement, driven by the belief that data should be made available for public use on principle». ID., *op. cit.*, *ibidem,* cit..

vantaggio della prima mossa, ma lo sfruttasse in prima persona al fine di orientare il processo di apertura verso il bene comune. Diversamente, al decisore rimarrebbe solo un intervento in seconda battuta per correggere le eventuali deviazioni patologiche dettate dalla logica mercantilistica.

Capitolo II

La *privacy* e la protezione transnazionale dei dati

SOMMARIO: 1. La *privacy*: in cerca di una definizione (1.1. *La fonte normativa della* privacy *e la sua evoluzione giurisprudenziale: dalla proprietà domenicale alla* reasonable expectation of privacy). – 2. L'avvento delle nuove tecnologie e la *reasonable expectation of privacy* sui *Big Data* – 3. La *General Data Protection Regulation* 2016/679/UE tra consenso e profilazione – 4. Il trasferimento dei dati: l'adeguatezza e le diverse garanzie dell'equivalenza – 5. Il trattamento dei dati e il "legittimo interesse" a trattare i dati nella finalità di *marketing* – 6. Una possibile soluzione nella *reasonable expectations of anonymity*?

1. La *privacy*: in cerca di una definizione

Per proteggere efficacemente la *privacy* nell'era dell'*Internet of Things* e della produzione massiva di dati è necessario comprendere le nuove questioni che la sua tutela pone.

In questa sede esamineremo come si è evoluta e come si sta evolvendo la sua definizione nel corso del tempo.

La nozione di *privacy*[195] non può dirsi unificante[196]. Essa ha assunto valenze diverse in passato, in ragione dei contesti storico e sociale.

Più e più volte, negli ultimi tempi, indipendentemente dalla sede in cui si è discusso, la si è tendenzialmente concepita come antiquata e addirittura, nel peggiore dei casi, dannosa, antiprogressista, eccessivamente costosa e ostile al benessere economico, sociale e politico[197].

Le conseguenze di una «cattiva definizione»[198] di *privacy*, però, sono prevedibili e si manifestano quando la *privacy* e i suoi valori, presumibilmente obsoleti, devono essere

---

195 A. BALDASSARRE, Privacy *e Costituzione. L'esperienza statunitense*, Bulzoni, Roma, p. 64 ss.; ID., *Diritto della persona e valori costituzionali*, Giappichelli, Torino, 1997, *passim*; C. M. BIANCA, *Tutela della* privacy. *Note introduttive*, in *Nuove leggi civili commentate*, fascicoli 2-3, 1999; F. BILOTTA, *L'emersione del diritto alla* privacy, in A. CLEMENTE (a cura di), Privacy, Cedam, Padova, 1999, p. 54 ss.; G. BUSIA, voce *Riservatezza* (*diritto alla*), in *Digesto delle discipline pubblicistiche*, quarta edizione, Agg. 2000, p. 476 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997, *passim*; A. CATAUDELLA, *Riservatezza* (*diritto alla*), I) Diritto civile, in *Enciclopedia giuridica*, XXVII, Roma, 1991; A. CERRI, *Riservatezza* (*diritto alla*), III) Diritto costituzionale, in *Enciclopedia giuridica Treccani*, XXVII (aggiornamento), Roma, 1995; A. CLEMENTE, (a cura di), Privacy, Cedam, Padova, 1999, *passim*; N. COLAIANNI, *Tutela della personalità e diritti della coscienza*, Cacucci, Bari, 2000, *passim;*. S. FARO, voce *Trattamento dei dati personali e tutela della persona*, in *Digesto delle discipline pubblicistiche*, quarta edizione, Agg. 2000, p. 543 ss.; S. FOIS, *Questioni sull'andamento costituzionale del diritto alla "identità personale"*, in G. ALPA - M. BESSONE - M. BONESCHI - P. CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Jovene, Napoli, 1983, *passim*; G.B. FERRI, *Persona e* privacy, in AA. VV. (a cura di), *Il riserbo e la notizia. Atti del Convegno di studi Macerata*, 5-6 marzo 1982, Napoli, 1983, p. 67 ss.; V. FRANCESCHELLI, *La tutela della privacy informatica: problemi e prospettive,* Giuffrè, Milano, 1998; V. FROSINI, *Banche dati, telematica e diritti della persona*, Cedam, Padova, 1981, *passim;* G. GIACOBBE, *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in *Iustitia*, 2, 1999, pp.93 ss.; ID., *Riservatezza* (diritto alla), in *Enciclopedia del diritto*, XL, Milano, 1989, pp. 1245 ss.; E. GIANNANTONIO - G. LOSANO - V. ZENO-ZENCOVICH, (a cura di), *La tutela dei dati personali. Commentario alla legge n. 675/96*, seconda edizione, Cedam Padova, 1999, *passim*; R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003, *passim*; S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997, pp. 583 ss.; ID., *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, XXII, 1991, pp. 525 ss.; ID., *Tecnologie e diritti*, Il Mulino, Bologna, 1995, pp. 106 ss.; ID., *Controllo e riservatezza a garanzia della* privacy *ma senza i "lacci" della Burocrazia*, in *Guida al Diritto*, 1997, pp. 10-14.

196 S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, p. XI, cit.

197 J. E. COHEN, *What privacy is for*, in 126 *Harv. L. Rev.*, 2012-13.

198 R. SHIH RAY KU, *Privacy is the problem*, *19 Widener L.J.* 873 2009-2010.

equilibrati con gli imperativi di difesa della sicurezza nazionale, di efficienza economica e di tutela dell'imprenditorialità; in questi casi, il più delle volte la protezione della *privacy* ne esce sconfitta.

L'elenco dei contrappesi alla *privacy* è infatti lungo e costantemente in crescita. Le recenti innovazioni introdotte da *social media*, piattaforme mobili, *cloud computing*, *data mining* e analisi predittiva minacciano di far pendere la bilancia a favore del valore da equilibrare con la riservatezza, schierando la *privacy* in permanente opposizione con il progresso, la conoscenza e la sicurezza.

Eppure, la percezione della *privacy* come antiquata e socialmente retrograda non può assumersi corretta. È il risultato di un'inversione concettuale che si riferisce al modo in cui è stata inizialmente concepita, nonché allo scopo della sua tutela. La teoria politica liberale ha concettualizzato la *privacy* come una forma di protezione del «sé liberale»[199]. Così caratterizzata, essa diventa reattiva e, in definitiva, inessenziale.

Questo equivale a dire che la sua assenza può a volte «raffreddare» l'esercizio delle libertà costituzionalmente protette, ma poiché il sé liberale possiede intrinsecamente la capacità di scelta autonoma e l'autodeterminazione, la perdita della *privacy* non inficerebbe tali capacità.

Diversamente, sarebbe il sé il vero soggetto della tutela della *privacy* e della politica, socialmente costruito perché emergerebbe a poco a poco da un substrato culturale e relazionale. Di conseguenza, la *privacy* svolgerebbe una funzione che non ha nulla a che fare con la stasi, al contrario è in continuo *fieri*.

Ne sia prova l'evoluzione storica del suo significato. Di seguito ripercorreremo molto brevemente i suoi sviluppi.

La *privacy* nasceva in Grecia come «privazione» ossia rifiuto di accettare o perseguire incarichi pubblici. L'attenzione alla cura di uno spazio privato, inteso in senso opposto alla dimensione pubblica, escludeva l'impegno politico che era considerato l'aspetto più importante della vita umana al punto che: «un uomo che vivesse solo una vita privata e

---

[199] *Ibid.*

che, come lo schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano»[200].

La tutela del privato acquistava valore solo in funzione della vita pubblica perché senza una casa, e quindi senza una ricchezza privata, un uomo non poteva partecipare agli affari della città, non avendo in essa uno spazio propriamente suo. Un uomo impegnato a provvedere ai suoi mezzi di sostentamento non sarebbe stato libero per l'attività pubblica.

In questo senso, «una vita spesa fuori dal mondo comune acquisiva una connotazione quasi antisociale»[201], tanto che si riteneva che in una società ideale non vi fosse alcun bisogno di una sfera privata in cui rifugiarsi perché questo bisogno era considerato un pretesto per sottrarsi agli obblighi etici e sociali[202]. La *privacy* "privava"[203] i singoli dal vivere un rapporto oggettivo con gli altri, dalla condivisione di interessi e dall'efficacia delle proprie azioni.

Col passare del tempo e con l'evoluzione della *societas* il concetto di *privacy* si è ribaltato: la *privacy* è divenuta, in netta opposizione rispetto al passato, essenziale alla piena espressione delle facoltà umane, strumento di protezione della dignità umana nella misura in cui consente al singolo di non essere discriminato, di agire autonomamente, di sviluppare liberamente la propria personalità e di partecipare in modo autonomo alla vita politica e sociale del Paese[204].

---

200 Chi sceglieva il privato sceglieva di mancare (non partecipare) all'ordine sociale costituito, cioè alla vita pubblica. Un uomo che vivesse solo una vita privata era come lo schiavo, che non poteva accedere alla sfera pubblica, o come il barbaro che sceglieva di non istituire un tale dominio, pertanto non era umano: H. ARENDT, *Vita activa. La condizione umana*, trad. it. di A. Dal Lago, Milano, 2001, p.19 ss.

201 F. FABRIS, *Il diritto alla* privacy *tra presente, passato e futuro*, in *Tigor - A.I* (2009) n.1 (luglio-dicembre), p. 95.

202 S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, p. 3 ss.

203 La *privacy* significava «essere privati della realtà che ci deriva dall'essere visti e sentiti dagli altri, essere privati da un rapporto oggettivo con gli altri, quello che nasce dall'essere al tempo stesso in relazione con loro e separati da loro grazie alla mediazione di un mondo comune di cose, privati della possibilità di acquistare qualcosa di più duraturo della vita stessa. La privazione implicita nella *privacy* consiste nell'assenza degli altri; in questo caso, ai loro occhi, l'uomo privato non appare e quindi è come se non esistesse. Qualunque cosa faccia rimane senza significato e senza conseguenze per le altre persone, e ciò che a lui importa è privo di interesse per loro»: H. ARENDT, *Vita activa,* p. 44, cit..

204 Cfr. art. 1 del *Grundgesetz;* art. 1 della Carta Europea dei diritti dell'Uomo; art. 1 della Dichiarazione universale dei diritti dell'uomo; art. 16 del Codice Civile francese o l'art. 2 del Codice italiano sulla protezione dei dati; la Convenzione del Consiglio d'Europa sui diritti dell'uomo e la biomedicina; la Dichiarazione universale sul genoma umano dell'Unesco.

Ne è derivato un luogo di intimità inalienabile e inviolabile in cui ciascuno deve poter abbandonare la propria maschera in tranquillità e sicurezza, mettendosi in pantofole[205], senza il timore di essere visto o spiato.

Con la società dell'informazione questo *ius solitudinis*[206] ha subito dei profondi cambiamenti, trasformandosi quasi in una pretesa ossimorica di partecipazione, di conoscenza, di controllo su tutte le informazioni che possono identificare una persona. La *privacy*, in altre parole, oggi assumerebbe un ulteriore significato che si diramerebbe dallo stesso e intimo bisogno di libertà. Da un lato le esigenze di difesa e di sicurezza nazionale, messe in luce dai recenti episodi di terrorismo, dall'altro le nuove strategie di mercato hanno trasformato la società in una rete di sorveglianza quotidiana[207], che investe la generalità dei consociati. Nel primo caso, il monitoraggio non più limitato per periodi eccezionali, espone l'universalità delle persone e non solo quelle pericolose a una visibilità prima inimmaginabili[208]; nel secondo la logica mercantilistica del prodotto personalizzato aumenta il rischio che il consumatore possa essere discriminato per le sue opinioni, credenze religiose, condizioni di salute e indirizzato intenzionalmente a determinati contenuti o merci.

Alla luce di quanto finora espresso, la domanda «può considerarsi libero e adeguatamente protetto il soggetto il cui passato e presente[209] sono registrati nei minimi dettagli ed è totalmente alla mercé di altri soggetti, pubblici o privati, anche sconosciuti, da cui il monitorato dovrà rassegnarsi ad essere espropriato dei suoi dati?» ha una palese risposta negativa.

Le tecniche di ingerenza nella vita dei singoli hanno sviluppato una lenta e continua opera di erosione delle prerogative della persona, non più «integra» fisicamente e psichicamente. Si rischia di trasformare una persona in mero oggetto da manipolare, annullandone ogni frammento di dignità.

---

[205] S. NIGER, *op. cit.*., p. 3.

[206] Si parla di un *right to be let alone.*

[207] G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016, *passim*.

[208] *Ibid.*

[209] Gli algoritmi sono in grado di predire determinati comportamenti e accadimenti, mediante tecniche di analisi predittiva.

E allora la riservatezza elasticizzando il suo significato si trasformerebbe in «tutela delle scelte esistenziali contro il controllo pubblico e la stigmatizzazione sociale»[210] o «come la richiesta di strumenti sociali che ci mettano al riparo dal rischio d'essere semplificati, oggettivati e giudicati fuori contesto»[211]. Si tratterebbe non più della vecchia pretesa passiva di *let to be alone*, ma di una pretesa attiva finalizzata al controllo dei propri dati, la quale può ben tradursi nella richiesta di non essere visto da terzi e incontrarsi così con la matrice solitaria della *privacy*, ma attraverso strumenti di tutela nuovi che consentano a ciascuno di controllare i propri dati in Rete.

Questa domanda «nuova» di *privacy* conserverebbe un bisogno di protezione della propria interiorità - maturata nel tempo e dettata dai cambiamenti sociali - da sguardi indiscreti e da invasioni esterne, seppure non più collegate al carattere della materialità[212] dello spazio entro cui l'individuo si muove.

In questo panorama tecnologico la tutela della *privacy* diventa tanto più necessaria quanto più forte è il rischio che dall'invasione possa derivare un condizionamento o una discriminazione, che impedirebbe al singolo di esercitare le sue libertà.

E se le tecnologie moderne sono così sofisticate da penetrare la quotidianità di ogni singolo, la domanda di *privacy* incrementa parallelamente all'invasività di quelle tecnologie.

Conseguentemente si affermerebbe nel concetto di *privacy* un'inversione di rotta rispetto alle sue origini greche: la sua tutela rappresenterebbe non più la privazione da una vita sociale bensì condizione di inclusione nella società della partecipazione[213], nel senso che solo la protezione dai condizionamenti che possono derivare dall'uso-abuso delle nuove tecnologie renderà libera la partecipazione dell'individuo alla società.

---

[210] S. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, 26th International Conference on Privacy and Personal Data Protection, Poland, Wroclaw, 14-16 September 2004, in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293*, p. 2, cit.

[211] ID., *ibidem*.

[212] Sulla nozione di *privacy* intesa come sviluppo della proprietà provata si legga il § che segue.

[213] S. RODOTÀ, *op. cit.*, secondo l'autore «la *privacy* diventa lo strumento necessario per difendere la società delle libertà e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale».

In altre parole, dacché era considerata una qualità tipica del soggetto attento al suo "particolare"[214] è divenuta lo strumento imprescindibile per l'esatto contrario: la partecipazione consapevole e autonoma alla vita pubblica.

Non solo, la *privacy* è anche un freno che diventa tanto più vigoroso quanto più raffinate diventano le tecniche di ingerenza. Serve cioè a bloccare le invasioni del proprio campo privato, le interferenze pubbliche e a impedire il condizionamento nel modo che il controllore, sia privato che pubblico[215], ritiene più utile alle sue affermazioni di potere economico o autoritario. Il *right to privacy* assume le sembianze di un "contenitore concettuale[216], all'interno del quale confluiscono

tutte le modalità di tutela della libertà personale garantite al singolo dallo Stato. La *privacy* avrebbe *in re ipsa* una elasticità direttamente proporzionale alle forme di intromissione, per cui oggi acquisterebbe una portata molto più ampia ed esigerebbe, per questo, una tutela variabile, sicuramente più forte rispetto al passato.

Si registra così uno stretto collegamento tra *privacy* e dignità, nella misura in cui la dignità assume la forma della libertà di autodeterminazione; tale collegamento si erge a fondamentale fattore di contrasto contro forme di controllo di massa, e richiede di rispondere e arginare il fenomeno crescente e convulso del *data mining*[217].

Il fine ultimo è quello di proteggere la soggettività dinamica ed emergente degli individui dagli abusi di attori commerciali e governativi i quali hanno interesse a rendere gli individui e le comunità fissi e prevedibili.

Così descritta, la *privacy* sarebbe tutt'altro che antiquata: essa sotto forma di libertà dalla sorveglianza, pubblica o privata, diviene fondamentale per l'affermazione della cittadinanza consapevole, una caratteristica strutturale[218] indispensabile dei sistemi politici democratici. Una simile costruzione è altresì fondamentale per la capacità di innovazione, dunque anche la percezione della *privacy* come «anti-innovazione» sarebbe un *non sequitur*.

---

214 Chi sceglie di spendere la sua vita nel privato, "di ciò che è proprio" è etimologicamente idiota (*idios*).

215 «Liberty against government» in W. M. BEANEY*, The constitutional right to privacy in the Supreme Court*, Sup. Ct. Rev. 212, 1962.

216 A. MANTELERO, *Il costo della* privacy *tra valore della persona ragione d'impresa*, Giuffré, Milano, 2007, p.1.

217 Con l'espressione si intende la raccolta dei dati quali, per esempio, la digitalizzazione delle immagini, le tecniche di riconoscimento facciale che consentono di schedare le persone monitorate.

218 J. CAMPBELL *et alii*, *Privacy Regulation and Market Structure*, Journal of Economics & Management Strategy, Volume 24, Number 1, Spring 2015, 47–73.

L'innovazione che si manifesta in contesti commerciali e sociali, infatti, è il risultato del libero interagire di particolari valori commerciali e sociali. Una cultura commerciale che vede la *privacy* come una minaccia per le proprie pratiche di produzione della conoscenza incentiva forme di competizione scorretta[219]. Ma una società che valorizza l'innovazione rispetta la *privacy* e i processi di gioco e incoraggia la sperimentazione da cui deriva, come si vedrà nel prosieguo, l'innovazione. In breve, sono le incursioni sulla *privacy* a danneggiare gli individui, il progresso e l'innovazione.

Una comprensione dei fenomeni sociali che dia la giusta rilevanza a una protezione efficace della *privacy* richiede un approccio strutturale della normativa.

Le strategie legislative tese al raggiungimento di questi obiettivi dovrebbero rendere i sistemi di controllo dei dati trasparenti e responsabili. Esse devono, inoltre, rispettare lo spazio privato (non necessariamente fisico)[220] di ciascun soggetto perché è una soggettività dinamica quella su cui la democrazia liberale e l'innovazione fanno affidamento dal momento che è negli spazi interstiziali - all'interno di quadri di *information processing* - che essa prospera e allora la normativa sulla *privacy* europea o sovranazionale dovrebbe concentrarsi sul mantenimento di quegli spazi[221].

1.1. La fonte normativa della privacy *e la sua evoluzione giurisprudenziale: dalla proprietà domenicale alla* reasonable expectation of privacy

Per completezza espositiva si premette che in Italia il dibattito intorno al diritto alla *privacy*[222] si è sviluppato in ritardo rispetto alle esperienze statunitensi ed europee, in

---

[219] Cfr. con capitolo III, in part. sulla protezione della *privacy* come variabile qualitativa di un prodotto cfr. con § 3 della presente tesi.

[220] *Infra* § che segue.

[221] J. E. COHEN, *op. cit.*, *ibidem*.

[222] Il professore Auletta parla di «interesse che in base ad una certa valutazione legislativa e sociale risulta fondamentale per l'individuo. Questi ha bisogno per poter condurre la propria vita di vedersi riconosciuto un certo ambito privato dal quale poter escludere l'altrui ingerenza; è la stessa natura umana che rifiuta l'indiscriminata pubblicizzazione di ciò che riguarda nell'intimo. Il rifiuto di tale riconoscimento finirebbe col menomare gravemente l'individuo e col pregiudicare lo stesso valore della persona, quindi la sua dignità; di qui la tutela implicita, anche sotto questo aspetto, del diritto alla riservatezza» T. A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978, p. 36. Cfr. anche con A. RAVÀ, *Istituzioni di diritto privato*, Padova 1938, p. 197. L'autore

particolare francese[223]. Il diritto alla riservatezza, desumibile da una lettura sistematica delle disposizioni costituzionali[224], ha inizialmente trovato riconoscimento e tutela nel nostro ordinamento in via interpretativa[225], grazie all'apporto di dottrina e giurisprudenza, cui sono seguiti timidi interventi legislativi - per lo più inadeguati, determinati da logiche settoriali[226] e non incentrati opportunamente sulla protezione di tale diritto - fino a che si è giunti alla legge n. 675/96[227], che ha subito numerose modifiche nel corso del tempo, per essere poi abrogata dall'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali[228].

Ci concentreremo qui, oltre che sulla fonte costituzionale, sull'evoluzione del concetto di *privacy* nella giurisprudenza anglosassone, più matura per accogliere i nuovi sviluppi di un diritto alla *privacy* oramai scollegato dalla materialità dell'oggetto e dei luoghi di tutela. Passeremo rapidamente in rassegna le pronunce della Corte Suprema sul punto.

Per la prima volta, nella sentenza *Griswold v. Connecticut*[229] la Corte riconobbe come costituzionalmente protetta la scelta di due coniugi di usare contraccettivi nella loro relazione matrimoniale[230] e dichiarò incostituzionale la legge del Connecticut del 1965 che ne vietava l'uso: «Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the

---

individua un «generale diritto alla riservatezza» e A. DE CUPIS, *I diritti della personalità*, in *Trattato di diritto civile Cicu – Messineo*, Milano 1942, I, p. 148.

223 PERREAU, *Les droits de la personnalitè*, in *Rev. Trim. dr. Civ.* 1909, e NERSON, *Les droits extrapatrimoniaux*, these, Lyon, 1939.

224 Il fondamento della tutela alla *privacy* è stato rinvenuto negli articoli 2 (diritto inviolabile), 3 (diritto alla dignità) 13 (inviolabilità della persona), 15 (libertà e segretezza della corrispondenza) della Costituzione.

225 Trib. Roma, sentenza del 14 settembre 1953, in *Foro it.*, 1954, I, c. 115 riconobbe un «diritto alla riservatezza che si concreta nel divieto di qualsiasi ingerenza e indiscrezione da parte di terzi nella sfera della vita privata della persona»; invece App. Roma 17 maggio 1956, *in «Foro it.»*, 1956, I, c. 796, non si pronuncia sul problema dell'esistenza o meno del diritto alla riservatezza. Inizialmente la Corte di Cassazione afferma che «il semplice desiderio di riserbo non è stato ritenuto dal legislatore un interesse tutelabile» e quindi che nell'ordinamento italiano non esiste «un generale diritto alla "riservatezza", o "privatezza"» in Cass., 22 dicembre 1956, n. 4487, in *Giust. Civ.*, 1957, I, p.5.

226 Il legislatore interviene solo nel 1970 emanando la legge 20 maggio 1970 n. 300, il c.d. Statuto dei lavoratori, che contiene alcune previsioni a tutela della privacy dei lavoratori e pertanto applicabili solo nell'ambito del rapporto di lavoro.

227 Legge 31 dicembre 1996, n. 675 - *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* - pubblicata nella Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - Supplemento Ordinario n. 3.

228 Decreto Legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali - pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

229 381 U.S. 479 (1965), *Griswold v. Connecticut*, in https://supreme.justia.com/cases/federal/us/381/479/#501.

230 Nel 1972 tale diritto fu esteso anche alle persone non sposate con la sentenza *Eisenstadt v. Baird*, 405 U.S. 438.

notions of privacy surrounding the marriage relationship. We deal with a right of privacy older than the Bill of Rights older than our political parties, older than our school system»[231].

Il giudice estensore avanzò la «*penunbra theory*»[232]*,* secondo la quale nei primi otto emendamenti della Costituzione americana ci sarebbero *peripheral rights,* zone di penombra create dalle garanzie testuali della Costituzione che produrrebbero situazioni costituzionalmente protette. Il diritto alla *privacy* diverrebbe strumentale alla tutela dei diritti ivi enucleati. Secondo questa impostazione la *privacy* si sviluppa come penombra di diritti e altre libertà e da lì vedrebbe crescere a dismisura[233] un ambito tutelato, ma anche inevitabilmente la minaccia di abusi[234].

Tuttavia le posizioni dei giudici sul punto furono discordanti: il giudice Harlan[235] la ricavò dal principio del *due process* del XIV Emendamento, fonte di tutti i diritti fondamentali non scritti; il giudice Goldberg diede rilievo al IX Emendamento, contenente una clausola aperta la quale avrebbe esteso la copertura costituzionale oltre i *certain rights.*

Orbene, la parte maggioritaria della dottrina ha ritenuto che la tutela della *privacy* sia radicata nel IV emendamento della Costituzione che protegge «the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause,

---

231 *Supra* nota 229, p. 381 U. S. 486.

232 Il giudice Douglas dichiarò che «[t]he foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance». Egli individuò un diritto alla *privacy* nelle "zones of privacy" protette dal Primo, Terzo, Quarto, Quinto e Nono Emendamento: «Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people».

233 Attraverso l'innovazione tecnologica.

234 Si pensi che oggi si può intervenire sul DNA con tecnologie «copia e incolla» (cd bioterrorismo). Così Massimo Villone in occasione della presentazione del volume della prof.ssa Giovanna De Minico "Costituzione. Emergenza e terrorismo", tenutasi presso la Biblioteca del Senato il 27 febbraio 2017.

235 381 U.S. 479, 501 (1965), Harlan, J., concurring in the judgment: « I fully agree with the judgment of reversal, but find myself unable to join the Court's opinion. The reason is that it seems to me to evince an approach to this case very much like that taken by my Brothers Black and Stewart in dissent, namely: the Due Process Clause of the Fourteenth Amendment does not touch this Connecticut statute unless the enactment is found to violate some right assured by the letter or penumbra of the Bill of Rights».

supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized»[236].

Tale disposizione configurerebbe la *privacy* come protezione informazionale[237] concentrata sulla segretezza delle proprie informazioni[238].

È stata l'evoluzione giurisprudenziale a non arrestare l'estensione del concetto di *privacy*, che trova «esplicazione in situazioni profondamente differenti che vanno dal diritto del singolo a impedire comportamenti intrusivi nella propria vita privata ad opera dei media, al diritto di aborto, alla libertà sessuale». Si è parlato di *informational privacy* e di *decisional privacy*. Il loro fulcro risiede nel «riconoscimento e nella garanzia del potere di autocontrollo in capo al singolo, che nel primo caso si manifesta in una sorta di signoria sulle informazioni inerenti la propria persona, traducendosi in un limite non solo alla diffusione di indiscrezioni sulla vita privata, ma anche, più in generale, alla raccolta e all'impiego arbitrario dei dati personali; mentre nella seconda declinazione la *privacy* diviene la libertà di autodeterminarsi rispetto alle scelte personali, siano esse pertinenti alla procreazione, alla libertà sessuale o alla libertà di organizzazione»[239].

In riferimento al carattere proprietario della *informational privacy* occorre precisare che la nozione americana di *privacy,* come «*right to be let alone*» promana proprio dal diritto di proprietà. Essa nasce alla fine del diciannovesimo secolo con la pubblicazione dell'articolo di Warren e Brandies[240], pubblicato nel volume 1890-91 dell'*Harvard Law Review*[241], in cui gli autori sostenevano che l'individuo deve avere la possibilità di scegliere «to what extend his thoughts, sentiments and emotions shall be communicated to others» e che la *privacy* configura la difesa di una sorta di cittadella privata «my house, my castle». Warren e Brandeis avviarono nel loro ragionamento un parallelismo con la disciplina delle leggi dello

---

[236] «Non potrà essere violato il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, di fronte a perquisizioni e sequestri ingiustificati; e non si rilasceranno mandati di perquisizione se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare».

[237] BARSOTTI V., *Privacy e orientamento sessuale. Una storia americana*, Torino, Giappichelli, 2005, p.16.

[238] e non ancora sul controllo dei propri dati.

[239] A. MANTELERO, *Il costo della* privacy *tra valore della persona e ragione d'impresa*, p.1.

[240] Proprio alcuni «pettegolezzi» sulla propria moglie, apparsi sul Saturday Evening Gazette, si dice abbiano spinto Louis D. Brandeis a scrivere, insieme con Samuel D. Warren, quel breve saggio intitolato «The Right to Privacy».

[241] S. D. WARREN - L. D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, 4, p. 193, ora in «Landmarks of Law», 1960, p. 261.

«slander» e del «libel», nonché con la disciplina della proprietà artistica e intellettuale. La tutela della *privacy* si sarebbe ottenuta tramite un'azione di responsabilità civile, ossia un «tort for damages»[242] oppure, in casi limitati, tramite una «injuction». La responsabilità civile si sarebbe così configurata in qualunque caso di «injury to feelings»[243].

Qui si può cogliere una chiara corrispondenza tra la proprietà privata e la *privacy* intesa nella sua concezione domenicale, come il diritto di ciascuno di tutelare la propria intimità, esattamente come ciascuno ha il diritto di tutelare la proprietà privata.

«When it comes to the Fourth Amendment, the home is first among equals[244] [...] The amendment's very core stands the right of a man to retreat into his own home and there be free from unreasonable government intrusion»[245]. Questo diritto protegge la casa e i luoghi fisici vicini, come il *curtilage*[246]: «This right would be of little practical value if the state's agents could stand in a home's porch or side garden and trawl for evidence with impunity»[247]. Dunque, la ragionevole attesa del soggetto di mantenere riservate certe informazioni coprirebbe non solo la propria casa, ma anche il perimetro di terreno immediatamente circostante la casa, che comprende gli edifici e le strutture strettamente adiacenti, entro le quali si può ritenere che il proprietario detenga una legittima

---

242 *Contra* H. KALVEN JR, *Privacy in tort law – Where Warren and Brandeis wrong?,* 31 *L. Contemp. Probs.* 327, 1966; R.C. POST, *Rereading Warren and Brandeis: Privacy, property and appropriation*, 41 *Case Western Reserve L.R.* 647, 1991.

243 ID., *op. cit.*, p. 275.

244In *Florida v. Jardines* la Corte Suprema degli Stati Uniti ha stabilito il 26 marzo 2013, che la polizia ha violato il Quarto Emendamento dei diritti del proprietario di una casa quando ha portato un cane antidroga sul portico di fronte alla casa sospetta di essere utilizzata per la coltivazione di marijuana. La Corte ha detto che la polizia ha condotto una perquisizione dopo essere entrata nella proprietà (estesa al *curtilage*) del soggetto interessato. Dal momento che gli ufficiali non hanno ottenuto il mandato in anticipo, la loro perquisizione era incostituzionale. La Corte ha stabilito che gli agenti di polizia hanno violato una regola fondamentale del Quarto Emendamento che tutela la riservatezza delle persone dalle intrusioni fisiche nella zona circostante la propria casa privata per fini investigativi, senza ottenere un mandato. Così il giudice Scalia nella sentenza *Florida v. Jardines*.

245 Così il giudice Scalia nella sentenza *Florida v. Jardines*: «Nel cuore dell'Emendamento si erge il diritto di un uomo a ritirarsi nella sua casa e a essere libero dalla irragionevole intrusione del governo».

246 «An area immediately surrounding a house or dwelling is curtilage if it harbors the intimate activity associated with the sanctity of a man's home and the privacies of life». *Oliver v. United States*, 466 U.S. 170, 180 (1984) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Per la determinazione del *curtilage* occorre guardare alla distanza dall'abitazione, alla recinzione, alla natura d'uso del perimetro, alla protezione dall'osservazione (*plain view doctrine*), tutti elementi che ne fanno una parte integrante della casa. Nel caso *California v. Ciraolo, 476 U.S. 207 (1986)* in relazione al test «enhanced view» si utilizza il parametro dell'occhio nudo e si ritiene che laddove non sia stata utilizzata la dovuta protezione da occhi indiscreti pur essendo le rilevazioni effettuate da un drone ma visibili ad occhio nudo, non sono da ritenersi coperte da protezione.

247 Così il giudice Scalia nella sentenza *Florida v. Jardines*: «sarebbe di scarso valore pratico se gli agenti dello Stato potessero stare in veranda o a lato del giardino di una casa e rovistare in cerca di prove impunemente».

aspettativa[248] di non essere spiato, tenuto anche conto del rapido progresso della tecnologia, che ha sviluppato droni sempre più sofisticati[249].

In riferimento all'oggetto coperto dalla protezione della *privacy*, già nel 1967 la Corte Suprema degli Stati Uniti pronunciava una storica sentenza: nel caso *Katz vs United States*[250], in cui offriva una nuova declinazione del diritto alla riservatezza con riferimento alle interferenze esterne introdotte dalle nuove tecnologie.

Con essa si allontanava dalla concezione proprietaria della *privacy* e dunque dalla materialità degli oggetti personali protetti.

La Suprema Corte introduceva il principio della «reasonable expectation of privacy» affermando che una conversazione, per quanto fatta da una cabina telefonica e dunque in un luogo pubblico, meritava comunque tutela ai sensi del Quarto Emendamento.

Il soggetto, che, nel caso sottoposto alla Corte, aveva utilizzato il telefono pubblico per una scommessa illegale si aspettava di non essere intercettato. Nonostante l'intercettazione non avesse determinato una «physical entrance into the area occupied by Charles Kats» la Corte riconobbe una violazione del IV emendamento: «Fourth Amendment protects people, not places [and what] a person knowingly exposes to the public, is not a subject of Fourth Amendment protection [while] what he seeks to preserve as private, may be constitutionally protected»[251].

Due le questioni fondamentali che la Corte Suprema degli Stati Uniti volle affrontare:

---

248 *Ex multis* COHEN J. E., *op. cit., ibidem;* R. SHIH RAY KU, *Privacy is the problem,* in *19 Widener L.J. 873,* 2009-10.

249 In *Florida v. Jardines* la Corte Suprema degli Stati Uniti ha stabilito il 26 marzo 2013, che la polizia ha violato il Quarto Emendamento dei diritti del proprietario di una casa quando ha portato un cane antidroga sul portico di fronte alla casa sospetta di essere utilizzata per la coltivazione di marijuana. La corte ha detto che la polizia ha condotto una perquisizione dopo essere entrata nella proprietà (estesa al *curtilage*) del soggetto interessato. Dal momento che gli ufficiali non hanno ottenuto il mandato in anticipo, la loro perquisizione era incostituzionale. La Corte ha stabilito che gli agenti di polizia hanno violato una regola fondamentale del Quarto Emendamento che tutela la riservatezza delle persone dalle intrusioni fisiche nella zona circostante la propria casa privata per fini investigativi, senza ottenere un mandato.

250 *Katz v. United States, 389 U.S. 347 (1967).* Il fatto: Charles Katz aveva utilizzato una cabina telefonica per la trasmissione di scommesse di gioco illegali da Los Angeles a Miami e Boston. All'insaputa di Katz, l'FBI aveva registrato le sue conversazioni tramite un dispositivo di intercettazioni elettroniche collegato all'esterno della cabina telefonica. Katz veniva condannato sulla base di queste registrazioni. Egli sosteneva che le registrazioni erano state ottenute in violazione del Quarto Emendamento. La Corte d'Appello aveva dato ragione all'FBI ritenendo che non vi fosse una violazione del IV emendamento perché "no physical entrance into the area occupied by Charles Kats".

251 *Ibidem.*

1) se il diritto alla *privacy* si estendeva alle cabine telefoniche e agli altri luoghi pubblici[252];

2) se fosse necessaria l'intrusione fisica per integrare una violazione del IV Emendamento.

La Corte, per rispondere ai due interrogativi, individuò due tipi di aspettativa: a) una aspettativa di *privacy* soggettiva nella previsione di un certo individuo che una certa posizione o situazione rimanga privata, questa percezione in quanto relativa si assume variabile; b) una aspettativa di *privacy* oggettiva, legittima e ragionevole generalmente riconosciuta dalla società.

In generale, si ritenne che non si può avere una ragionevole aspettativa di *privacy* nelle cose offerte al pubblico[253]. La valutazione di quello che ciascuno si aspetta è risultata dunque fondamentale per distinguere una perquisizione legittima da una illegittima. In questa pronuncia il giudice Harlan elaborò un test diviso in due parti, in seguito adottato dalla Corte Suprema degli Stati Uniti come strumento per determinare se una perquisizione della polizia o del governo è compatibile con quanto stabilisce il Quarto Emendamento:

1. L'azione governativa deve contravvenire l'aspettativa soggettiva e concreta dell'individuo;

2. L'aspettativa deve essere ragionevole, nel senso che la società deve riconoscerla come tale, pertanto essa dovrà essere una «objectively reasonable expectation of privacy».

Per soddisfare la prima parte del test, la persona di cui sono state ottenute le informazioni deve dimostrare che, in realtà, aveva un'effettiva aspettativa personale che

---

[252] Esempi di luoghi in cui una persona ha una ragionevole aspettativa di *privacy* sono la residenza o la stanza di albergo di una persona; luoghi pubblici che sono stati appositamente previsti dalle imprese o dal settore pubblico, al fine di tutelare la *privacy*, come ad esempio bagni pubblici, porzioni private di penitenziari, o proprio una cabina telefonica. *Contra Smith v. Maryland, 442 US 735 (1979)*, la Corte Suprema ha ritenuto che gli individui non hanno "legittima aspettativa di *privacy*" per quanto riguarda i numeri di telefono che compongono perché consapevolmente danno quelle informazioni alle compagnie telefoniche quando compongono un numero.

[253] Un esempio ben noto è che non ci sono diritti di *privacy* nella spazzatura lasciata per la raccolta in un luogo pubblico. Non vi è generalmente nessuna perquisizione quando gli agenti di polizia guardano attraverso la spazzatura perché una persona ragionevole non si aspetterebbe che oggetti posti nella spazzatura rimangano privati, di conseguenza, un individuo non ha alcuna legittima aspettativa di privacy nelle informazioni finite nelle mani di terze parti.

l'informazione ottenuta, divenuta prova dell'illecito, non sarebbe stata disponibile al pubblico. La prima parte del test è correlata, quindi alla nozione «in plain view». Se una persona non ha effettuato ogni ragionevole sforzo per nascondere qualcosa da un osservatore casuale, allora nessuna aspettativa personale di *privacy* si deve presumere.

La seconda parte del test analizza oggettivamente l'aspettativa: occorre chiedersi se la società ritiene l'aspettativa ragionevole. Se è chiaro che una persona non abbia mantenuto le informazioni in questione in un luogo privato, allora nessuna perquisizione è necessaria per scoprirle, dunque l'aspettativa non si ritiene ragionevole.

Successivamente la Corte Suprema ha riconosciuto l'elasticità dell'aspettativa di *privacy*, in ragione dell'evoluzione storico-sociale, essa ha dichiarato che l'installazione di un sistema di posizionamento globale (GPS)[254], su un veicolo per esempio, per monitorarne i movimenti in assenza di un mandato costituisce una violazione del Quarto Emendamento: «you know, I don't know what society expects and I think it's changing. Technology is changing people's expectations of *privacy*. Suppose we look forward 10 years, and maybe 10 years from now 90 percent of the population will be using social networking sites and they will have on average 500 friends and they will have allowed their friends to monitor their location 24 hours a day, 365 days a year, through the use of their cell phones. Then - what would the expectation of *privacy* be then?»[255]. E qui è agevole il collegamento con il costante uso delle geolocalizzazioni[256] degli utilizzatori di *smartphone* da parte degli *OTT*, per scopi commerciali non resi noti ai proprietari dei dati, ma nascosti dietro il motivo di implementare i servizi erogati.

Un importante passo in avanti ha compiuto la Corte Suprema nella sentenza *Riley v. California,* 573 U.S. (2014)[257], dove la stessa ha chiaramente statuito all'unanimità che la

---

254 Sentenza *United States v. Jones 132 S. Ct. 945, 565 U.S. (2012).*

255 *United States v. Jones* (Oral Argument Transcript) p. 44.

256 S. NOUWT, *Reasonable Expectations of Geo-Privacy?*, Volume 5, Issue 2, August 2008, p. 377 ss..

257 La Corte si era già pronunciata su un caso analago: in *Chimel v. California (1969)*, aveva stabilito che se la polizia arresta qualcuno, la stessa potrà perquisire il corpo della persona senza un mandato e «l'area che potrebbe raggiungere» (the area into which he might reach) al fine di distruggere le prove o attentare alla sicurezza degli ufficiali, impugnando un'arma, per esempio. I Tribunali di grado inferiore ritenevano, diversamente che il Quarto Emendamento non permettesse alla polizia di perquisire i contenuti digitali di un telefono cellulare, senza prima ottenere un mandato, in quanto in virtù del IV emendamento le persone hanno il diritto di essere libere da perquisizioni e sequestri ingiustificati. I due casi in cui la Corte ha avuto modo di rivedere la sua posizione hanno riguardato due diverse versioni di cellulari: il tradizionale «*flip-phone*», che è più vecchio del moderno «*smartphone*», che detiene potenzialmente molti più dati sull'utente, tuttavia sono stati risolti analogamente. Nel primo caso,

perquisizione senza mandato e il sequestro di contenuti digitali di un telefono cellulare durante un arresto è incostituzionale perché «modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple- get a warrant»[258]. Allo stesso modo, il fatto che nell'utilizzo dello *smarthphone* il soggetto accetta che le informazioni in esso inserite vengano salvate su *server* ubicati in uno spazio esterno allo *smartphone* non può significare che il soggetto abbia voluto rinunciare alla propria riservatezza.

Nella sentenza *Riley v. California* la Corte Suprema, applicando il test *Chimel*[259], ha ritenuto che i dati digitali memorizzati su un telefono cellulare non possono essere

David Leon Riley era stato fermato il 22 agosto 2009, perché aveva le targhe scadute. Durante la sosta, l'Agente di polizia ha anche scoperto che Riley stava guidando con una patente di guida sospesa. La politica del Dipartimento di Polizia di San Diego vuole che il veicolo venga sequestrato e che gli agenti siano tenuti a eseguire una ricerca di inventario del veicolo, che in questo caso ha portato alla scoperta di due pistole dentro il cofano del veicolo. Test balistici successivi hanno confermato che le pistole erano state le armi utilizzate in un omicidio di malavita il 2 agosto del 2009, per il quale Riley era sospettato. A causa della scoperta delle pistole nascoste e cariche - insieme con l'armamentario della banda - durante la perquisizione del veicolo, la polizia ha arrestato Riley e perquisito il suo telefono cellulare senza un mandato. La ricerca del telefono cellulare ha prodotto informazioni da cui è emerso che Riley era un membro della banda Lincoln Park; le prove comprendevano immagini, contatti del telefono cellulare, i testi dei messaggi, e video clip. Inclusa nelle foto c'era una foto del veicolo coinvolto nella sparatoria. Sulla base delle immagini e dei video recuperati dal telefono cellulare, la polizia ha accusato Riley di aver partecipato alla sparatoria. Il giudice ha permesso l'utilizzo processuale della prova. Riley è stato condannato e la Corte d'Appello della California ha confermato la condanna. Nel secondo caso, Brima Wurie era stato arrestato dopo che la polizia lo aveva visto partecipare ad una vendita di droga. Alla stazione di polizia, gli agenti hanno sequestrato due telefoni cellulari di Wurie, tra cui il «telefono cellulare a conchiglia», oggetto di questo caso. Poco dopo il suo arrivo alla stazione, la polizia ha notato che il telefono stava ricevendo una serie di chiamate da una fonte identificata come «casa mia» sul *display* esterno del telefono. Gli agenti hanno aperto il telefono, effettuato l'accesso al suo registro delle chiamate, identificando il numero salvato come "casa mia", e sono risaliti all'appartamento di Wurie. Hanno ottenuto un mandato di perquisizione per la posizione e, durante la ricerca hanno trovato 215 grammi di cocaina, crack, marijuana, armamentario di droga, armi da fuoco, munizioni e denaro contante. Wurie è stato successivamente accusato per spaccio di droga e traffico di armi da fuoco e condannato. Il giudice ha ritenuto che i telefoni cellulari, in generale, sono distinti da altri possedimenti fisici che possono essere perquisiti senza mandato a causa della quantità di dati personali che possono contenere e rispetto ai quali la minaccia che rappresentano per gli interessi delle forze dell'ordine è trascurabile.

[258] «I telefoni cellulari moderni non sono solo un altro vantaggio tecnologico. Con tutto quello che contengono e tutto quello che possono rivelare sono titolari dell'intimità di molti americani. Il fatto che la tecnologia ora permette a un individuo di portare queste informazioni in mano non rende le informazioni meno degne di essere tutelate. La nostra risposta alla domanda su quello che la polizia deve fare prima di perquisire un telefono cellulare sequestrato durante un arresto è quindi semplice: ottenere un mandato».

[259] *Supra* nota 257.

utilizzati come arma per colpire un ufficiale o per fuggire. Gli agenti, dunque, possono esaminare le caratteristiche materiali di un telefono cellulare per assicurarsi che non possa essere utilizzato come arma[260], ma una volta verificata l'inoffensività dell'oggetto o eliminate eventuali minacce fisiche, non possono analizzare i dati che il telefono contiene[261].

L'intervento dell'ufficiale non eliminerebbe il rischio di una possibile pulitura a distanza, perché un ufficiale che afferra un telefono potrebbe non essere in grado di iniziare la sua ricerca nel breve tempo che rimane prima che il telefono si blocchi e che i dati vengano crittografati. Da queste valutazioni deriva che i telefoni non possono essere perquisiti senza mandato, perché la capacità di archiviazione dei moderni cellulari, porta con sé conseguenze importanti sulla *privacy*: attraverso una combinazione di foto, video, messaggi di testo, registri delle chiamate, cronologie di navigazione e simili, la polizia, attraverso la loro analisi, può ricostruire tutta la vita privata dell'individuo, creando una sorta di *avatar* a pieno titolo o una *IPerson*.

Una perquisizione del cellulare sfrenata - ha concluso la Corte - può essere ancora più invadente del saccheggiamento della casa di un sospettato. Come la tecnologia continua a espandere i suoi confini, l'aspettativa di *privacy* delle informazioni memorizzate all'interno dei propri telefoni cellulari aumenta proporzionalmente.

Dunque, uno *smartphone* produce un'aspettativa maggiore di *privacy* perché va ben oltre le semplici attività di fare e ricevere telefonate[262].

---

[260] per verificare, per esempio, se sia nascosta una lametta nel telefono. Questa ipotesi pare fosse plausibile con i telefoni a conchiglia.

[261] Anche se è possibile che una prova memorizzata su un telefono venga distrutta con la pulitura a distanza o con la crittografia dei dati è «il normale funzionamento delle caratteristiche di sicurezza di un telefono, a prescindere da qualsiasi tentativo dell'imputato o dei suoi complici, che consente di nascondere o distruggere le prove al momento dell'arresto»: Così il giudice Roberts.

[262] I telefoni cellulari comprendono una vasta gamma di attività, tra cui le rubriche, calendari, messaggi di testo, scambi di posta elettronica, immagini, applicazioni di *social network*, *browser* internet, cronologia di navigazione, carte di credito e informazioni bancarie, e *file* di *word*. Non è stato agevole determinare se un telefono cellulare si inserisce nella categoria di un contenitore rispetto alla definizione che i tribunali hanno fornito. In *Belton*, un contenitore è stato definito come «qualsiasi oggetto in grado di contenere un altro oggetto» Questa definizione comprende gli oggetti che contengono fisicamente un altro oggetto. Questa classificazione, tuttavia, è stata difficile, perché i telefoni cellulari non rientrano esattamente in questa categoria. Il tribunale nel caso *Smith v. Maryland, 442 US 735 (1979),* aveva dichiarato che un telefono cellulare non è un contenitore chiuso. La Corte Suprema ha seguito Smith e ha stabilito che un cellulare non è un contenitore chiuso; a differenza di un pacchetto di sigarette o di un portafogli, non contiene fisicamente un altro elemento fisico. Allora la Corte si è chiesta cosa sia un telefono

L'equilibrio tra l'interesse dello Stato in materia di sicurezza, la conservazione delle prove e l'aspettativa di un individuo di essere al sicuro da occhi indiscreti dovrebbe riflettere la portata delle informazioni contenute in un telefono cellulare e spostarsi nella direzione opposta[263] a quella intrapresa nel senso che sicuramente l'aspettativa di tutela della *privacy* nel proprio telefono cellulare può, oggi, prevalere sugli interessi di polizia, di sicurezza o di conservazione delle prove.

Dunque, mentre inizialmente la Corte confermava la scelta di ancorare la copertura della tutela del IV emendamento alle intrusioni materiali nella proprietà dei cittadini[264], con la sentenza *Katz v. United States* riconosce che la protezione della *privacy* si estende al di là degli angusti confini della proprietà privata, ad ogni caso in cui il singolo può vantare una ragionevole aspettativa di *privacy* «the fourth emendament protects people, not places». Nello stesso senso la sentenza *Whalen v. Roe, 429 U.S. 589 1977*, in cui la Corte pur rigettando il *claim* dell'appellante, riconobbe che il diritto alla *privacy* includeva l'interesse a non rivelare i propri dati personali: «he cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in indipendence in making certain kinds of important decision»[265].

È evidente, come anticipato, che la *privacy* si sdoppia e diventa *privacy of disclosure* o *informational privacy* e *privacy of autonomy,* la prima si riferisce alla raccolta e alla circolazione di informazioni personali e alla seconda la sfera decisionale che interessa la persona nei suoi ambiti privati.

La nozione informazionale di *privacy* consente di recuperare la distinzione tra *privacy* e *liberty*. Si può concepire una violazione della *privacy* senza che si verifichi una compressione della *liberty*. Questa nozione di *privacy* è comunque correlata alla *liberty*, nella

---

cellulare ed è pervenuta alla risposta che è un telefono cellulare non equiparabile minimamene a un pacchetto di sigarette o a una borsa, per cui ha abbandonato il ricorso alla categoria del «contenitore».

263 B. C. NEWELL, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, *XVII Rich. J.L. & Tech.* 12 (2011), *http://jolt.richmond.edu/vi 7i4/article 12.pdf.*

264 227 U.S., 439 (1928), *Olmated v. United States.* Con tale pronuncia la Corte ha esaminato l'uso di intercettazioni di conversazioni telefoniche private, ottenuto dagli agenti federali senza l'approvazione giudiziaria e successivamente utilizzate come prova, in violazione del Quarto e Quinto Emendamento. La Corte ha dichiarato che né il Quarto Emendamento né il Quinto Emendamento erano stati violati. Questa decisione è stata poi rovesciata dalla sentenza *Katz v. United States* 389 U.S. 347 (1967).

265 L. R. BEVIER , *What privacy is not*, in *12 Harv. J. L. & Pub. Pol'y* 99 1989, p. 100 ss.

misura in cui la protezione della *privacy* è spesso strumentale alla garanzia della *liberty* soprattutto quella che si manifesta nella non interferenza esterna nella sfera personale di ciascuno. Dunque, libertà, autonomia e *privacy* sono valori strettamente collegati in quanto non si può essere completamente liberi o pienamente autonomi, senza poter godere della propria *privacy*.

La Corte in *Katz v. United States* ha stabilito che gli interessi di *privacy* dell'individuo superano le preoccupazioni del governo per la sicurezza.

Vi è ancora una questione che ha affrontato la Corte, ovvero se i tribunali siano i più adatti a pronunciarsi sulle questioni legate alla *privacy*. Il giudice Alito ha osservato che nei prossimi anni «la natura dei dispositivi elettronici che gli americani comuni utilizzeranno continuerà a cambiare». Con i cambiamenti repentini, forse è necessario che il Congresso, meglio equipaggiato per un simile intervento, adotti una legislazione più dettagliata sulle perquisizioni dei telefoni cellulari e dei sequestri, alla luce di tutte le considerazioni sulla *privacy* e le esigenze delle forze dell'ordine fin qui svolte. La Corte ha ristabilito l'equilibrio tra *privacy* e sicurezza, riconoscendo che i diritti di *privacy* sui dati contenuti in un telefono cellulare non sono diminuiti, ma piuttosto aumentati.

Argomentazioni analoghe riguardano le informazioni di geolocalizzazione. La questione presentata in *State v. Earls*[266] era se il governo potesse costituzionalmente ottenere e utilizzare le informazioni di geo-localizzazione dal *provider* di telefonia cellulare di un imputato per rintracciare la posizione di un sospettato senza un mandato, in conformità al Quarto Emendamento. Il governo si impegnava in questa tecnica di indagine spesso, anche se la sua costituzionalità era ancora in discussione in molti tribunali. Il giudice d'appello[267], nel confermare la condanna, aveva stabilito che il tracciamento della localizzazione era costituzionale, perché il monitoraggio della polizia aveva avuto luogo su strade pubbliche[268]. Tuttavia, successivamente, la Corte Suprema degli Stati Uniti decise

---

[266] Thomas Earls, era sospettato in una serie di furti residenziali con scasso. Al fine di localizzare Earls, la polizia ha contattato il suo operatore di telefonia cellulare. L'operatore ha così notificato alla polizia la posizione Earls; la polizia ha trovato l'auto Earls in un parcheggio di un motel nella zona di destinazione e all'interno della sua camera d'albergo un televisore a schermo piatto e altri beni rubati. Earls ha contestato l'illegittimità della prova, negata dalla Corte.

[267] Il Circuito DC non aveva esplicitamente analizzato se Jones avesse avuto una aspettativa personale di *privacy*, ma ha presunto che lo avesse fatto.

[268] richiamando le pronunce *United States v. Knotts* e *United States v. Karo.*

su *United States v. Jones*[269] in senso contrario. In questa decisione, la maggioranza della Corte affermò che alcuni tipi di monitoraggio della localizzazione, anche se fatti interamente su strade pubbliche, sono in grado di violare la ragionevole aspettativa di *privacy* di un soggetto.

Per determinare se un'azione di governo costituisce una perquisizione legittima bisogna chiedersi se la persona indagata ha avuto un'aspettativa di *privacy* e se la società ritiene questa aspettativa ragionevole.

Quando si analizza questo fattore, come già si è scritto, la Corte Suprema ritiene che se una persona ha preso le precauzioni verso l'esterno per proteggere la sua attività dal pubblico, allora presumeva che fosse coperta dalla riservatezza.

Nel caso Jones la probabilità che un estraneo potesse osservare tutti quei movimenti non era solo remota, ma essenzialmente prossima allo zero[270]. Inoltre, anche se il singolo spostamento si era svolto in pubblico, era la totalità dei movimenti letti cronologicamente a dare informazioni dettagliate.

Da quanto argomentato risulta evidente che l'aspettativa di *privacy* copre si estende alle informazioni che fuoriescono dalla sfera di entro cui il soggetto può esercitare una signorie sulle cose. L'utilizzo quotidiano di *device* elettronici, mette a rischio la privacy di chi li utilizza e minaccia la *liberty* costantemente, per cui solo un aumento della tutela della *privacy*, nel ventaglio di strumenti per proteggerla per esempio, comporterebbe un'adeguata protezione della *liberty* degli individui e della collettività, in generale.

---

[269]L'FBI ha installato un dispositivo di tracciamento GPS sulla macchina di Antoine Jones mentre era parcheggiata in un parcheggio pubblico. L'FBI poi usato il dispositivo per monitorare i movimenti del suo veicolo ininterrottamente per un mese. Sulla base dei dati relativi all'ubicazione generati dal dispositivo GPS Jones è stato condannato per spaccio di cocaina. La Corte d'Appello del Circuito DC ha invertito la convinzione di Jones consolidata in *United States v. Maynard,* 615 F.3d 544 (DC Cir. 2010). Gli investigatori della polizia avevano chiesto e ricevuto un mandato per collegare un dispositivo di tracking GPS alla parte inferiore della macchina del convenuto, ma poi avevano superato la portata del mandato sia in senso geografico che temporale. D.C. Circuit Court non ha ammesso le prove perché ottenute in violazione del Quarto Emendamento. La Corte ha ritenuto che installando fisicamente il dispositivo GPS sulla vettura dell'imputato, la polizia aveva commesso una violazione della *privacy* Jones.

[270] «The likelihood a stranger would observe all those movements is not just remote, it is essentially nil.».

2. L'avvento delle nuove tecnologie e la *reasonable expectation of privacy* sui *Big Data*

Come ampiamente argomentato sopra, la protezione della sfera personale intesa come libertà di non subire interferenze nelle scelte adottate nell'ambito privato[271], precondizione della libertà di autodeterminazione, veniva riconosciuta solo nel 1965 al singolo, in quanto parte del rapporto di coniugio, limitatamente all'ambito familiare[272]. Questa nozione si è gradualmente estesa, ma solo con l'affermarsi delle nuove tecnologie la *privacy* si è spinta più in là fino a travolgere la collettività intera[273] al punto che oggi si tradurrebbe nel diritto di ciascuno di mantenere il controllo dei propri dati personali[274], ovvero i dati raccolti dagli apparecchi elettronici che usiamo quotidianamente, i quali, se incrociati, sono in grado di rivelare i dettagli più intimi della nostra esistenza.

Non può negarsi che l'innovazione tecnologica ha fatto espandere insieme agli algoritmi predittivi il senso della tutela di una sfera della persona che si sottrae all'esercizio arbitrario del potere.

Dalla rassegna della giurisprudenza americana, che ha preceduto questo paragrafo, è risultato che la *privacy* copre tutto ciò che il titolare presume essere privato, anche se fisicamente fuoriuscito dalla sua materiale disponibilità.

Si aggiunga che tale protezione, come più volte ribadito dalla Corte Suprema, deve essere assicurata all'indagato, anche in occasione di un arresto. Questa precisazione vuole evidenziare come sia più forte la tutela del soggetto nei confronti del quale nessuna indagine è stata avviata, ma che giornalmente viene monitorato dai gestori delle *app* del suo *smartphone* per motivi di lucro o dai governi per motivi di sicurezza.

Coloro che utilizzano le applicazioni dello *smartphone* per servizi di *social networking* o *e-commerce* cedono i loro dati personali agli OTT "consentendo" l'accesso alle proprie

---

271 *Griswold v. Connecticut*, 381, U.S. (479) 1965. La Corte dichiara incostituzionale una legge del Connecticut che vietava la prescrizione e l'uso di contraccettivi.

272 Cfr. con *Eisenstadt v. Baird,* 405 U.S., 438 (1972), sempre in materia di libertà di utilizzo di contraccettivi. Cfr. anche con *Stanley v. Georgia,* 394 U.S., 557 (1969) sul diritto di detenere in casa propria materiale pornografico e *Roe v. Wade,* 410 U.S., 113 (1973), in materia di aborto.

273 M.F. DE TULLIO, *La* privacy *e i* big data *verso una dimensione costituzionale collettiva*, in *Pol. Dir.,* 4/2016, p. 642 ss..

274 J. E. COHEN, *op. cit.*, *ibidem*.

informazioni di geolocalizzazione, ai dati della fotocamera, della galleria, della cronologia delle ricerche, dei contatti, dell'agenda personale etc., questi dati vengono trasferiti e conservati nei *server* di turno.

Ora, ci chiediamo se un dato non è più nella stretta disponibilità del suo titolare perché fa parte di una banca dati pubblica o privata, cioè tenuta e gestita, anche temporaneamente dal soggetto che offre lo specifico servizio richiesto, diremo che il titolare di quei dati intende rinunciare alla sua *privacy* e quindi nel momento in cui acconsente ad essere monitorato, perde completamente il controllo delle informazioni che lo identificano?

Ancora una volta chiamiamo a fare luce sul punto una risalente pronuncia della Corte Suprema degli Stati Uniti, *Whalen v. Roe*[275]. In questo caso rileverà l'argomentazione e non la decisione[276] della Corte che si trovava a sindacare su una questione diversa.

---

[275] *Whalen v. Roe* 429 US 589 (1977).

[276] La Corte dichiara infatti la legittimità costituzionale della legge in esame. La Corte giungeva ad una analoga conclusione in *Sorrell v. IMS Health Inc* (2011) in cui la Corte riconosceva nell'estrazione dei dati dalle ricette mediche per finalità di *marketing* una libertà protetta dal IV emendamento, nonché una «commercial speech» definita come «no more than propose a commercial transaction». In questa occasione la Corte ha sottolineato che la libertà commerciale ha un valore sociale e che il governo non può sopprimere tale libertà per il solo fatto che esistono preoccupazioni sull'uso improprio delle informazioni personali. Già nella decisione del 1980 in *Central Hudson Gas v. Public Service Commission of New York*, la Corte aveva istituito un test di quattro parti per misurare la legittimità della normativa sulla libertà commerciale. La Corte avrebbe dovuto stabilire 1) se la libertà riguardava un'attività lecita; 2) se il governo avesse un interesse sostanziale nel regolare la libertà in questione; 3) se la regolazione in questione perseguisse direttamente ed efficacemente l'interesse affermato dal governo; 4) se la normativa non fosse più restrittiva di quanto necessario per raggiungere l'obiettivo desiderato («narrowly tailored to achieve the desired objective»). Il *Central Hudson test* è utilizzato dagli studiosi di diritto costituzionale per stabilire un livello intermedio di controllo per la regolazione della libertà commerciale ed è stato lo *standard* in vigore al momento in cui il caso *Sorrell* è sorto. Quest'ultimo caso aveva ad oggetto una legge del Vermont del 2007 che vietava alle farmacie e a entità simili di vendere o rivelare informazioni di identificazione-prescrittorie per scopi di m*arketing* in assenza del consenso del medico prescrittore. La legge inoltre vietava alle case farmaceutiche e di m*arketing* di utilizzare le informazioni prescrittorie identificabili per le vendite di *marketing* o promozionali. La legge non vietava tutte le comunicazioni, ma la divulgazione a fini di *marketing* senza il consenso del medico mentre consentiva la distribuzione e l'uso delle informazioni-prescrittorie di identificazione per altri scopi, come la ricerca.

Era prima consentito alle farmacie di raccogliere informazioni-prescrittorie di identificazione. Le farmacie potevano anche vendere queste informazioni ai «data miners» che a loro volta potevano redigere relazioni sui comportamenti prescrittori (che de-identificassero i pazienti, ma che identificassero il medico curante) e vendere tali relazioni alle case farmaceutiche. Le case farmaceutiche, poi avrebbero potuto impiegare «detailers» (comunemente noti come rappresentanti farmaceutici), i quali utilizzano le relazioni in modo strategico nel mercato per promuovere i loro farmaci ai medici. Lo scopo della legge del Vermont, che si opponeva a questa prassi, era quello di perseguire l'interesse dello Stato volto a tutelare la salute pubblica degli abitanti del Vermont, proteggere la *privacy* dei medici e le informazioni di prescrizione, e garantire che i costi del sistema sanitario fossero contenuti. I *Data miner*, così come le aziende farmaceutiche, sollevarono l'incostituzionalità della legge per violazione della libertà di parola. Il primo circuito aveva concluso che la legge regolava pratiche di *marketing* non la libertà commerciale. Per contro, la Corte d'Appello del Secondo Circuito capovolse la sentenza del tribunale. Il secondo Circuito aveva concluso che la legge violava la libertà commerciale e che l'interesse della *privacy* affermata dal medico era troppo astratta. Pertanto, il giudice ritenne che la legge che limitava la libertà economica era incostituzionale.

La Corte, difatti si pronunciava sulla legittimità costituzionale di una legge dello Stato di New York che aveva istituito un archivio informatico centralizzato, contenente i nomi e gli indirizzi di tutte le persone cui erano state prescritte sostanze stupefacenti. Tale sistema informatico, però seppure creato per evitare perdite di dati, rendeva facilmente divulgabili le identità dei pazienti, destando preoccupazione nei titolari, i quali temevano che le loro informazioni potessero essere rivelate, con il rischio che pazienti tossicodipendenti fossero marchiati come tali, in violazione dei loro diritti fondamentali, in particolare di quello alla *privacy*.

La Corte, in questo caso ha ritenuto che la raccolta di informazioni incide su "*two privacy interests*": 1) un «*individual interest in avoiding disclosure of personal matters*». Nel valutare l'interesse di non divulgazione, la Corte ha constatato che nel caso specifico le misure di sicurezza impiegate dalla legge in questione per proteggere le identità dei destinatari delle prescrizioni erano sufficienti a garantire che i dati personali sarebbero stati protetti dal pubblico dominio. La Corte aveva, inoltre rilevato che le garanzie di legge proteggevano adeguatamente l'interesse a non divulgare informazioni personali. 2) un «*interest in independence in making certain kinds of important decisions*». In proposito, ha dichiarato che la decisione in questione era se la medicina necessaria sarebbe stata acquisita e utilizzata, cioè quanto condizionamento sarebbe derivato al soggetto che avrebbe dovuto assumerla, in altre parole avrebbe rinunciato alla medicina per non essere schedato? La Corte ha rilevato che anche se «alcuni pazienti [erano] riluttanti a usare, e alcuni medici erano riluttanti a prescrivere questi farmaci necessari, a causa della paura che tale informazione sarebbe diventata "di pubblico dominio" e avrebbe "influenzato negativamente" la loro reputazione», l'indipendenza nel prendere certi tipi di decisioni importanti era stata mantenuta, perché la decisione di prescrivere, o di utilizzare il farmaco «è rimasta tra medico e paziente».

Con una decisione 6-3, la Corte Suprema confermò la decisione del secondo circuito ritenendo che la legge del Vermont violava il Primo Emendamento. Schierandosi con *IMS Health*, la Corte concluse che lo statuto imponeva una limitazione alla libertà di parola, che la libertà dei soggetti economici. La Corte ha respinto l'affermazione dello Stato secondo cui le restrizioni della legge erano necessarie per tutelare un «interesse sostanziale del governo» a tutela della *privacy* del medico e per ridurre i costi di assistenza sanitaria. La maggioranza dei giudici concluse che le informazioni non erano infatti completamente private, potendo essere utilizzate per scopi "non di *marketing*" da una varietà di pubblico (ad esempio, ricercatori).

Inoltre, il giudice Stevens, profeticamente, in quella sentenza ha lasciato aperta la possibilità che alcuni *database* in futuro potrebbero non essere «costituzionalmente accettabili» qualora non fossero adeguatamente protetti contro usi impropri: «A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure [429 U.S. 589, 606] of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions».[277]

Rileva qui che la Corte, pur rigettando *il claim* dell'appellante, ha riconosciuto a chiare lettere che il diritto alla *privacy* include da un lato l'interesse a controllare i propri dati personali. Si distinguono nella individuazione dei due interessi sopramenzionati una *informational privacy* e una *privacy of autonomy* interdipendenti. La prima fa riferimento al controllo sui propri dati e la seconda alla possibile interferenza di soggetti terzi nelle scelte personali di un individuo che si avvale di servizi[278]. Secondo consolidato orientamento dottrinale, occorre distinguere la dimensione fisica dalla dimensione proprietaria. L'una investirebbe i profili dell'invasione non autorizzata degli spazi in cui una persona detiene una ragionevole aspettativa di riservatezza. L'altra che includerebbe le questioni relative allo sfruttamento commerciale non consentito dei dati. Ne deriva che la *privacy* così come

[277] *Whalen v. Roe*, (1977) No. 75-839, 34, US.

[278] In questo caso i dati sono medici.

finora descritta, declinata in chiave moderna e non nella sua versione eremitica, coprirà anche quei dati che sono usciti dalla stretta disponibilità materiale del soggetto a cui appartengono e chiederà di sapere ce fine fanno i dati di cui si consente il monitoraggio e per quali motivi e per quanto tempo vengono trattenuti, in quali server e con quali tecniche di sicurezza.

Se vogliamo fare nostro il ragionamento della Corte andremo a verificare 1) il presumibile mantenimento dei dati nella sfera privata da parte del suo titolare; 2) l'interesse a non divulgare i propri dati e 3) l'interesse a prendere decisioni autonome e indipendenti dalla cessione dei dati. Queste tre verifiche si risolvono nella domanda: quel soggetto che consente l'accesso ai suoi dati per utilizzare il servizio e che apparentemente continua a "mantenere il controllo materiale" dei dati che produce – conservati sul suo telefonino - si aspetterà ragionevolmente che il custode pubblico o privato conservi attentamente i suoi dati e che non li usi a proprio piacimento, senza – tra l'altro- specificarne le finalità.

Per rispondere a questa domanda gli utenti dovrebbero conoscere le condizioni del servizio e cioè a quali utilizzi saranno destinati i loro dati, a quale genere di catalogazione saranno sottoposti e quali misure di sicurezza saranno adottate per proteggerli.

Molte persone, infatti, oggi forniscono i loro dati personali sul *web* e sui *social network*, senza allentare le proprie aspettative di *privacy* perché non conoscono i termini del servizio, gli scopi per i quali quei dati vengono raccolti o comunque sono disposti a negoziarli pur di avere un servizio di posta elettronica efficiente o per beneficiare degli effetti di rete di *messenger* o *whatsapp* e comunicare con parenti e amici vicini e lontani. Spesso gli utenti accettano solo per eliminare le schermate temporanee del consenso (*cookies*) che bloccano la pagina su cui si sta navigando, cliccano senza leggere, o accettano, dopo aver letto frettolosamente condizioni generali del contratto troppo vaghe o troppo tecniche per l'utente medio della Rete, in cui la sproporzione tra costo del servizio e remunerativitá dei dati, estrapolati dagli utilizzi – considerata la posizione economica di partenza del fornitore e del consumatore - è evidente.

L'accettazione, apparentemente libera degli utenti, senza la quale gli stessi sarebbero costretti a rinunciare al servizio, consente alle aziende di sfruttare per qualsiasi scopo le informazioni personali, le *e-mail*, le credenze religiose e politiche, le fotografie e i video di

scene altamente personali, in cui possono essere impiegati gli algoritmi di riconoscimento facciale e di determinazione dell'ambiante circostante per profilare i comportamenti e le abitudini, l'età, il sesso, gli amici, il tipo di luoghi frequentati e le tipologie di prodotti acquistati.

I dati possono rivelare se una persona avrà un attacco di cuore e possono pertanto determinare il prezzo del premio assicurativo, costringendo quella persona a pagare quello più alto o possono prevedere che una determinata persona non riuscirà a rimborsare un mutuo ipotecario, inducendo la banca a negarle il finanziamento, o che ancora un'altra persona commetterà un crimine facendola arrestare preventivamente. La previsione svilirebbe l'autodeterminazione e potrebbe rivelarsi sbagliata se i dati, sulla base dei quali viene fatta non sono corretti[279], con gravi conseguenze sulla libertà fondamentali degli individui.

Il nuovo panorama tecnologico impone regole nuove a tutela dell'autodeterminazione contro il determinismo dei dati[280].

Se un soggetto visita siti filo-jihadisti non commetterà necessariamente un crimine, ma, se l'algoritmo prevede che possa farlo, le Autorità potrebbero intervenire con un arresto preventivo o limitarne le libertà. Nel caso proposto si rischierebbe di sovvertire il contenuto del principio di offensività[281], o si amplierebbe a dismisura la nozione di «nocumento potenziale» nella definizione dell'esposizione al pericolo, snaturandone il radicamento costituzionale[282]. Se è vero che il principio di legalità, in senso formale, vuole che in astratto qualunque fatto possa diventare reato, essendo sufficiente che sia pubblicata una legge che lo consideri tale, è altrettanto vero che la gerarchia delle fonti privilegia le disposizioni costituzionali. Allora, il libero agire dei singoli rischierebbe di essere minacciato da una sorta di «dittatura dei dati»[283], la quale se oggi può apparire inverosimile,

---

279 Si pensi al caso del soggetto che per errore o per dimenticanza non ha disposto un bonifico per pagare il canone di locazione, una banca potrebbe leggere il suo nominativo nella *black list* degli insolventi.

280 V. MAYER- SCHÖNBERGER - K. N. CUKIER, *Big Data. Una rivoluzione che trasformerà il modo di vivere e già minaccia la nostra libertà,* Garzanti, 2013, p. 30 l'era dei *Big Data* imporrà nuove regole a tutela della "sacralità" (inviolabilità) dell'individuo.

281 G. FIANDACA - E. MUSCO, *Diritto penale Parte generale*, Bologna, Zanichelli, 2014, pp. 213-220; ID., *Diritto penale Parte speciale*, vol. 1, Bologna, Zanichelli, 2012, pp. 505-509; F. MANTOVANI, *Diritto penale Parte generale*, Padova, Cedam, 2013, pp. 209-215 e D. PULITANÒ, *Diritto penale*, Torino, Giappichelli editore, 2013, pp. 208-220.

282 In violazione degli articoli 13, 21, 25, 27, Cost.

283 V. MAYER-SCHÖNBERGER - K. N. CUKIER, *op. cit.*, p. 237.

ben si potrebbe adattare alla deriva autoritaria di uno stato democratico. I dati potrebbero, infatti, fare previsioni errate o fare previsioni corrette, ma rivelarle a coloro che i produttori dei dati non volevano sapessero e che non erano e non sono tenuti a sapere. Se questo modello è positivo, da un lato, per combattere l'evasione fiscale, per esempio, dall'altro è negativo per il cliente delle compagnie assicurative, le quali possono imporgli un prezzo più alto, sostituendo alle analisi delle urine, certamente più costose, una valutazione delle abitudini, degli interessi, degli *hobby* e delle patologie dell'assicurando.

Per nascondersi l'individuo, in *extrema ratio*, potrebbe rinunciare alla libertà di scegliere i contenuti a cui accedere e i siti da visitare in Rete, auto-limitando la propria libertà di espressione per paura di essere spiato. Proprio in un simile scenario l'«*interest in independence in making certain kinds of important decisions*» e quindi la *privacy of autonomy* verrebbero minate alla radice.

La previsione si sostituirebbe all'autodeterminazione e dunque, la «scatola nera» del singolo, che oggi raccoglie tutti i suoi dati, diverrebbe il nuovo cuore pulsante della riservatezza dell'individuo, che trova fondamento nei principi del costituzionalismo moderno, per cui difenderla significherebbe difendere la dignità[284] del singolo, rileggendo in chiave evolutiva le carte fondamentali dei diritti nazionali ed europee[285]. Esiste, infatti un margine insuperabile finanche dal legislatore, dato dal rispetto della dignità della persona umana[286].

[284] Il rispetto della dignità umana appare il primo tra i valori fondativi dell'Unione Europea racchiusi nell'art. 2 tue, esso precede «la libertà, la democrazia, l'uguaglianza, lo Stato di diritto e il rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze».

[285] In particolare gli artt. 2 e 13 della nostra Carta Costituzionale e gli artt. 1-5 della Carta di Nizza.

[286] Cfr. sentenza della Corte Costituzionale del 22 ottobre 1990, n. 471 che riconosce di «valore costituzionale della inviolabilità della persona costruito, nel precetto di cui all'art. 13, primo comma, della Costituzione, come "libertà", nella quale è postulata la sfera di esplicazione del potere della persona di disporre del proprio corpo».

3. La *General Data Protection Regulation* 2016/679/UE tra consenso e profilazione

Il 4 maggio 2016, dopo un travagliato *iter* legislativo, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il testo del Regolamento UE in materia di protezione dei dati personali 2016/679/UE[287]. Dopo 20 giorni è entrato ufficialmente in vigore e diventerà definitivamente applicabile in via diretta in tutti i Paesi Membri a partire dal 25 maggio 2018.

Il nuovo Regolamento dà sicuramente un notevole apporto[288] alla disciplina dei nuovi fenomeni[289] che hanno preso piede in Rete, come si può evincere dalla nomenclatura giuridica utilizzata: è stato ampliato l'elenco delle definizioni in materia di protezione dei dati personali dell'art. 2 della previgente dir. 95/46/CE, oggi divenuto l'articolo 4 del

[287] 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), in *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA&toc=OJ:L:2016:119:TOC*.

[288] Tra le principali novità il nuovo pacchetto di protezione dei dati introduce il principio di «responsabilizzazione»: il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità, ma è compito dello stesso titolare. Cfr. con l'articolo 4, paragrafo 1, n. 8) e con l'intero Capo IV del Regolamento.

[289] G. ARNÒ, *La tutela della* privacy *nella rete Internet*, Giappichelli, Torino, 2002, *ibidem*; P. CAREY, *E-privacy and online data protection*, Butterworths, London, 2002, *passim*; L. LESSING, *Code and other laws of cyberspace*, Basic Books, New York, 1999, *passim*; A. LISI, *La privacy in internet*, Esselibri Simone, Napoli, 2003, *passim.*

Regolamento UE. Risultano aggiunte descrizioni più calzanti al contesto tecnologico[290], quali quella di profilazione, dati genetici, dati biometrici e così via[291].

È cambiata altresì la definizione di «consenso dell'interessato»[292] che l'articolo 6 configura come caposaldo di liceità di un trattamento dei dati personali. Secondo quest'ultima disposizione il trattamento deve trovare radicamento in un'idonea base giuridica e in una serie di fondamenti che, in linea di massima coincidono con quelli previsti dal Codice *Privacy*[293], ossia oltre al consenso, l'adempimento degli obblighi contrattuali, gli interessi vitali[294] della persona interessata o di terzi, gli obblighi di legge cui è soggetto il titolare, l'interesse pubblico o l'esercizio di pubblici poteri e l'interesse legittimo prevalente del titolare o dei terzi cui i dati vengono comunicati.

L'articolo 4, al n. 11) definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che

---

290 Tra le principali novità introdotte vi è il diritto a richiedere la cancellazione dei dati: il cosiddetto *Right to be forgotten* (articolo 17 del nuovo Regolamento), nonché il diritto alla portabilità dei dati disciplinato dall'articolo 20 del Regolamento. Tale diritto non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati «forniti» dall'interessato al titolare (si veda il considerando 68 per maggiori dettagli). Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile. Il Gruppo Articolo 29 ha pubblicato recentemente linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità in *http://ec.europa.eu/newsroom/document.cfm?doc_id=44099*; per la versione italiana *http://www.garanteprivacy.it/garante/document?ID=6058842*. Al riguardo, si ricordano i numerosi provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice. Si vedano, fra molti, *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3251012* e, con riguardo all'attività bancaria in generale, *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247*.

Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un formato interoperabile secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

291 Cfr. con articolo 4 del Regolamento 2016/679/UE, rispettivamente ai numeri 4, 13 e 14.

292 Cfr. con articolo 4, n. 11.

293 Decreto legislativo 30 giugno 2003, n. 196, in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248*.

294 Alla luce del considerando 46, con riferimento all'interesse vitale di un terzo si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione.

i dati personali che lo riguardano siano oggetto di trattamento»[295]. Il chiarimento è teso a cancellare ogni dubbio relativo all'*opt in*[296] che richiederebbe sempre un consenso espresso preventivo al trattamento da parte dell'interessato.

Resta da definire il significato di ciascuno dei 4 requisiti richiesti per il rilascio di un consenso valido:

1) il primo requisito attiene alla libertà: il consenso può essere valido soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso. Se le conseguenze del consenso minano la libertà di scelta dell'individuo, esso non può essere considerato libero. Nel parere WP 131, seppure reso sulle cartelle cliniche elettroniche[297], quindi su dati sensibili, il Gruppo di lavoro ha rammentato che il «consenso "libero" significa una decisione volontaria, presa da una persona in pieno possesso di tutte le sue facoltà e senza alcuna forma di coercizione, sociale, finanziaria, psicologica o d'altro tipo. Un consenso dato in una situazione medica sotto la minaccia di non essere curati o di ricevere cure peggiori non può essere considerato "libero". […] qualora la situazione medica imponga in modo necessario e inevitabile all'operatore sanitario di trattare i dati personali in un sistema di CEE [cartelle cliniche elettroniche], è fuorviante che questi cerchi di legittimare tale operazione attraverso il consenso dell'interessato. Il fatto di basarsi sul consenso dovrebbe essere limitato ai casi in cui la persona interessata è veramente libera di scegliere e può in seguito ritirare tale consenso senza venire danneggiata». Un consenso può dirsi effettivamente libero quando non costituisce il prezzo del servizio.
2) Il secondo riguarda la specificità del consenso, il Gruppo di lavoro Articolo 29 nello stesso parere sopra citato aveva già chiarito il significato di specificità del consenso: «il consenso "specifico" deve riferirsi a una situazione ben

[295] Quanto al consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (art. 8 del Reg. 679/EU).

[296] E. R. ALO, *Eu privacy protection: a step towards global privacy, 22 Mich. St. Int'l L. Rev.* 1095 2013-2014, p. 1112 ss.

[297] WP 131 del 15 febbraio 2007, in http://194.242.234.211/documents/10160/10704/1411979, p. 9.

definita e concreta in cui si prevede un trattamento dei dati […]. Pertanto un "consenso generale" dell'interessato – (ad esempio) alla raccolta dei suoi dati medici per una CCE e ai trasferimenti successivi di tali dati, passati e futuri, a operatori sanitari coinvolti nella cura – non costituisce un consenso conformemente all'articolo 2, lettera h) della direttiva»[298], divenuto l'articolo 4 del Regolamento.

3) Il terzo requisito riguarda la necessaria informazione, se la dichiarazione richiesta per il rilascio del consenso prevede più materie, la richiesta di consenso deve essere presentata in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro[299] per ciascuna materia. In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di una modulistica[300].
4) Il consenso dovrebbe, inoltre, applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere dato per l'insieme delle finalità del trattamento. Non sarebbe dunque conforme al Regolamento una richiesta che accorpi finalità disomogenee o che disturbi o impedisca la fruizione del servizio offerto sul *web*. Un consenso può dirsi effettivamente informato quando le informazioni destinate agli interessati non sono lunghe, ma concise, facilmente accessibili e di facile comprensione e quando è utilizzato un linguaggio semplice e chiaro, che renda l'utente consapevole dei termini di servizio che va a sottoscrivere, soprattutto quando si rivolge ai minori, tanto più se si considera che «la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato

---

298 P. 9 del WP 131/2007.

299 Cfr. con l'articolo 7, paragrafo 2.

300 «Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente Regolamento è vincolante».

comprendere se, da chi e per quali finalità sono raccolti i dati personali che lo riguardano».

5) Infine, il requisito dell'inequivocabilità del consenso: per «inequivocabile» sembra volersi intendere un consenso «non ambiguo». Secondo il parere WP 187 del Gruppo Articolo 29[301] il consenso inequivocabile deve essere «fondato su dichiarazioni o azioni intese a esprimere un consenso valido» e sembrerebbe implicare la necessità di un'azione positiva. Dunque, un comportamento inerte non dovrebbe rientrare nella nozione di manifestazione, ma il comportamento dell'interessato non dovrebbe lasciare adito a dubbi in merito alla sua intenzione di manifestare il suo consenso. In altre parole, la manifestazione con la quale l'interessato accetta il trattamento dei suoi dati personali non deve lasciare spazio ad ambiguità per quanto concerne la sua intenzione. Se sussiste anche un ragionevole dubbio circa l'intenzione dell'interessato, l'ambiguità non può essere esclusa. Il Considerando 32 del nuovo Regolamento specifica le modalità di espressione di un consenso: potrebbe essere reso «mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito *web*, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Inoltre, il titolare, ai sensi del paragrafo 1 dell'articolo 7, deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Alla luce di quanto esposto, un sistema di *opt-in*[302] sembrerebbe più chiaro nel Regolamento Europeo, che presuppone che il consenso non costituisca mai la scelta di *default*, ma debba essere sempre espresso. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle».

---

301 WP 187, parere 15/2011, in http://www.privacy.it/archivio/grupripareri201115.html.

302 Nell'ambiente *online* è il consenso esplicito manifestato con la firma elettronica o digitale o con un *click* di conferma su un'icona.

Definiti i requisiti normativi del consenso e considerato il quadro fenomenico di riferimento si ritiene di evidenziare per ciascuno dei punti sopra esaminati delle criticità nella prassi consolidata in Rete:

In riferimento al requisito della libertà di cui al punto *1)* un consenso richiesto come corrispettivo di un servizio pone dei grandi interrogativi sulla effettiva libertà di scelta del fruitore, perché il soggetto che decidesse di non prestare consenso non potrebbe accedere a servizi di messaggistica per esempio, e dovrebbe rinunciarvi. Questi dubbi si intensificano soprattutto se si considera che questi servizi sono divenuti indispensabili per le comunicazioni interpersonali, il soggetto potrebbe operare una «scelta coartata». Quando un soggetto presta il consenso per il trattamento dei suoi dati al fine di fruire di un servizio, senza il quale quel servizio non sarebbe disponibile non può dirsi effettivamente libero, così come stabilito dal Regolamento e chiarito dal Parere del Gruppo Articolo 29, nonché dal considerando 42. Il punto centrale sul quale il regolamento tace è che i dati non possono essere richiesti come prezzo di un servizio perché un simile scambio del baratto non può considerarsi libero, soprattutto se di fronte alla libertà economica ci sono i diritti fondamentali delle persone[303]. Il legislatore europeo avrebbe potuto porre un chiaro divieto in capo agli OTT di offrire servizi chiedendo come corrispettivo i dati, ma imporre una politica di trattamento trasparente e informata.

---

303 G. VETTORI, *Diritti fondamentali e diritti sociali. Una riflessione fra due crisi*, in *www.europeanrights.eu*; sulla persona come entità sociale, sulla quale si era fondata la stessa democrazia pluralista voluta dai costituenti cfr. con A. BALDASSARRE, voce *Diritti inviolabili*, in *Enc. Giur.*, IX, Roma, 1989, 1 ss.; ID., voce *Diritto sociali*, *ivi;* A. PACE, *Problematica delle libertà costituzionali*, Padova, 1985. Vettori rimanda a «un concetto depurato da elementi naturali (di origine religiosa) o funzionali (di origine laica) e perciò capace di porsi al di sopra di ogni potere pubblico compreso quello legislativo al punto di instaurare un rapporto di dipendenza con il principio democratico. Una entità dotata di alcune situazioni immodificabili che si identificano con la forma stessa dello Stato ed altre da salvaguardare, non in modo assoluto, ma tramite il confronto con altri valori, salvo il rispetto di un contenuto essenziale». L. MENGONI, *Persona e iniziativa economica privata nella Costituzione*, in. G. VETTORI (a cura di), *Persona e Mercato*, Lezioni, Padova, 1996, p. 34 ss.; N. IRTI, *Intervento*, in G. VETTORI (a cura di), *Persona e mercato*, *op. cit.*, p. 93; e in *Riv. dir. priv.*, I, 1995, p. 289 ss.; M. LUCIANI, *Diritti sociali e integrazione europea*, in *Politica dir.*, 2000, p. 367 ss.; M. PANEBIANCO, *Bundesverfassungsgericht, dignità umana e diritti fondamentali*, in *Diritto e società*, 2002, p. 151; A. RUGGERI E A. SPADAIO, *Dignità dell'uomo e giurisprudenza costituzionale*, in *Politica dir.*,1991, p. 343 ss. il tema del bilanciamento è affrontato anche dalla prof.ssa De Minico secondo cui il preciso ordine esistente tra diritti fondamentali e libertà economiche richiede che i primi meritino protezione anche in danno delle seconde: G. DE MINICO, *Libertà e* copyright *nel diritto dell'Unione*, in G. DE MINICO, *Antiche libertà e nuove frontiera digitale*, Giappichelli, Torino, 2016, p. 145 ss.

Quanto al requisito della specificità di cui al punto *2)* notevoli perplessità pongono richieste del consenso vaghe e generiche come quelle che seguono l'installazione di un'applicazione sullo *smartphone*.

Con riferimento al carattere informato di cui al punto *3)* La richiesta del consenso e la relativa informativa devono essere chiare, concise e non devono interferire immotivatamente con il servizio per cui il consenso è espresso. Quest'ultima previsione contrasterebbe con la legge sui *cookies*, per esempio perché non interferire in un servizio *web* significa non interrompere la navigazione per richiedere il consenso al trattamento dei dati, impedendo all'internauta di fruire di un contenuto, cosa che invece attualmente accade.

Con riguardo al requisito della inequivocabilità di cui al punto *4)* Con riguardo alla forma del consenso, occorre sottolineare che non deve essere necessariamente «documentato per iscritto», né è richiesta la «forma scritta», anche se questa sembrerebbe la modalità più idonea a configurare l'inequivocabilità del consenso e il suo essere «esplicito» nei casi in cui è prescritto[304]; se il consenso dell'interessato è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso[305]. Sulla definizione di azione positiva inequivocabile, atta a determinare l'*opt in*: sul *web* l'atto positivo richiesto per consentire il trattamento dei dati potrebbe tradursi semplicemente nel selezionare una casella su un sito internet, o nel cliccare su una determinata icona. Con riferimento al concetto di «azione positiva» o «atto positivo»: c'è da chiedersi se un semplice *click* sulla pagina *web* o uno *scroll on* del sito potrebbero significare inequivocabilmente che l'interessato accetta il trattamento dei propri dati. Il punto starebbe nella definizione delle finalità di trattamento per cui è richiesto il consenso, qualora le finalità fossero conformi al servizio offerto, tali comportamenti potrebbero essere ritenuti idonei ad esprimere un consenso pieno; se al contrario le finalità riguardano ulteriori aspetti, non meglio precisati, o genericamente mascherati dietro lo scopo di implementare e migliorare i servizi offerti, allora, dovrebbe

---

[304] Cfr. con l'articolo 9 e Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, in *http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*.

[305] Cfr. con il considerando 32.

essere necessario un consenso apposito e specifico, chiaro e distinto per tali ulteriori scopi, che dovrebbero essere resi noti, senza il quale nessun dato dovrebbe essere trattato.

Il consenso[306] rilasciato per il trattamento dei dati personali[307] differisce da quello rilasciato per il trattamento dei dati sensibili[308].

Rimane fermo, come già specificato, rispetto alla disciplina precedente, che il consenso deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto; deve, inoltre, essere egualmente manifestato attraverso «dichiarazione o azione positiva inequivocabile». Per i dati sensibili, però, l'articolo 9 pone un divieto generale[309] di trattamento[310], mentre il paragrafo 2 alla lett. a) dello stesso articolo elenca una lunga serie di deroghe, tra cui il rilascio di un consenso «esplicito» per una o più finalità specifiche.

---

306 Le condizioni per il consenso sono disciplinate dall'articolo 7 del Regolamento. Il consenso raccolto precedentemente alla data del 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra indicate. Diversamente, è opportuno adoperarsi per raccogliere nuovamente il consenso degli interessati in conformità al Regolamento. È, inoltre, prevista la possibilità di revocare il consenso in qualsiasi momento.

307 Ai sensi dell'art. 4, n. 1 del Reg. 679/EU per «dato personale» si intende «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».

308 Come stabilito dal Considerando 51 «Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente Regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente Regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente Regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente Regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali».

309 Il considerando 42 prevede che il consenso espresso dall'interessato non è sufficiente nemmeno per derogare al divieto relativo al trattamento di talune categorie specifiche di dati personali.

310 Secondo quanto stabilito dal paragrafo 1 dell'articolo 9.

Occorre ora fare chiarezza sul carattere dell'esplicitezza che si aggiunge agli altri requisiti del consenso, come deroga al divieto generale di trattare dati sensibili per una o più finalità specifiche: il parere del Gruppo di lavoro Articolo 29 sulle cartelle cliniche elettroniche aveva già precisato che «nel caso di dati personali sensibili, e quindi delle CCE, il consenso deve essere esplicito. Non soddisfa il criterio del carattere "esplicito" la soluzione del silenzio-assenso (*opt-out*)». Il caso di un paziente che viene informato da una clinica sul fatto che il suo fascicolo medico sarà trasmesso a un ricercatore, a meno che il paziente non sollevi obiezioni in tal senso (chiamando un numero) non soddisfa il requisito del consenso esplicito. Quindi sui dati sensibili il consenso richiesto sembrerebbe più forte, perché al consenso dell'interessato si aggiunge l'attributo «esplicito». Secondo il parere del Gruppo Articolo 29 già citato «nel linguaggio giuridico, l'espressione "consenso esplicito" (*explicit*) equivale all'espressione "consenso manifesto" (*express*). Essa cioè comprende tutte le situazioni in cui agli interessati è proposto di accettare o rifiutare un particolare utilizzo oppure l'oscuramento di informazioni personali che li riguardano ed essi rispondono attivamente a tale proposta, verbalmente o per iscritto. Ma la scelta legislativa di voler aggiungere un ulteriore requisito non può solo voler dare rilievo al sistema dell'*opt in*, che regola anche il rilascio del consenso per il trattamento dei dati personali, ma vuole anche significare che il consenso dovrà essere esplicitamente riferito al trattamento di dati sensibili, in modo che sia distinguibile da quello eventualmente reso per il trattamento dei dati personali. In più dovranno essere esplicitate le finalità specifiche per le quali i dati sensibili saranno trattati.

Non solo in Rete sembrano si siano diffusi sistemi di trattamento incompatibili con la nuova disciplina introdotta a livello europeo cui le imprese dovranno adeguarsi, ma lo stesso Regolamento non contiene una disciplina forte in grado di correggere le storture della prassi, ma sembra carente sotto diversi aspetti. In riferimento alla definizione di dati sensibili nella società digitale, nel Regolamento 679/UE non viene mai utilizzata l'espressione *Big Data*, tantomeno viene evidenziato che un'aggregazione di dati personali è in grado di restituire, come si è già scritto, informazioni «più che sensibili» sugli utenti. Basti pensare ai dati di geolocalizzazione che sono in grado di rivelare se una persona frequenta luoghi di culto, quindi il suo credo religioso. Questa lacuna è sintomatica di un

apparato normativo carente. Un mancato riconoscimento di un fenomeno che prende solo le mosse dalla profilazione, che trova un accenno nel nuovo Regolamento, non può prevedere alcuna tutela giuridica per i soggetti ai quali quei *Big Data* appartengono.

Dunque, quelle informative veloci che chiedono i dati personali come corrispettivo del servizio che offrono per finalità generiche e disomogenee, ma soprattutto che non fanno luce sul fatto che l'aggregazione dei dati mette in chiaro i dati «più che sensibili»[311] della persona, sembrerebbero contrastare nettamente con le previsioni regolamentari sopra descritte. Inoltre, in riferimento al requisito ulteriore dell'esplicitezza che è quello richiesto per il trattamento dei dati sensibili, quindi più robusto rispetto all'altro tipo di consenso, solo generalmente, tale consenso «esplicito» o manifesto è concesso per iscritto o elettronicamente ed è accompagnato da una firma scritta a mano o digitale, a certe condizioni esso si può desumere in base al comportamento attivo dell'interessato. In questo modo, seppure entro certi limiti, si aprono spazi per forme di consenso desunto da comportamenti concludenti, espressi mediante azioni positive da parte dell'interessato, di non semplice individuazione o comunque forieri di discrezionalità.

Il «consenso esplicito» è richiesto anche[312] per il consenso a decisioni basate su trattamenti automatizzati come il *profiling*[313]. La profilazione[314] intesa come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» richiederebbe sì un consenso esplicito, ma un artificio giuridico ne allenterebbe l'efficacia. Secondo la definizione che ne dà il Regolamento l'analisi dei dati presenti nei propri archivi con strumenti informatici,

---

311 L'aggregazione dei dati non solo può rivelare dati sensibili, ma addirittura predire il comportamento di una persona. La previsione si sostituirebbe all'autodeterminazione e dunque, la «scatola nera» del singolo, che oggi raccoglie tutti i suoi dati, diverrebbe il nuovo cuore pulsante della riservatezza dell'individuo, che trova fondamento nei principi del costituzionalismo moderno, per cui difenderla significherebbe difendere la dignità del singolo, rileggendo in chiave evolutiva le carte fondamentali dei diritti nazionali ed europee.

312 Ai sensi del paragrafo 2, lett. c) dell'articolo 22.

313 Il consenso «esplicito» è richiesto oltre che per il trattamento dei dati sensibili, anche per il *profiling*. Si coglie un parallelismo quasi a voler rimarcare l'invasività della profilazione.

314 Essa analizza i dati cui fa seguito un'azione automatica senza l'intervento dell'uomo. Cfr. articolo 4, parag. 1, n. 4.

la cui elaborazione viene sottoposta alla valutazione preventiva di una persona - eventualmente prima dell'utilizzo dei dati stessi, per esempio al fine di adattare e verificare i dati stessi - non costituisce profilazione. Quindi non occorrerebbe un consenso rafforzato per svolgere tale attività di analisi.

Tra le deroghe al rilascio del consenso se ne aggiunge un'altra: il considerando 43[315] e l'articolo 9 precisano che i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali. Il Regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti[316].

Ulteriori limitazioni sono contenute nell'art. 23, il quale stabilisce che il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34[317], in materia di trasparenza, informazione e accesso ai dati personali, rettifica e cancellazione, opposizione e processo decisionale automatizzato relativo alle persone fisiche, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare: a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o

---

315 «Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.»

316 Il Considerando 47 offre alcuni criteri per il bilanciamento in questione. Appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217 Con riferimento ai requisiti indicati dall'Autorità in materia di bilanciamento di interessi si veda, per esempio, *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992* con riguardo ad alcune tipologie di trattamento di dati biometrici; *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680* con riguardo all'utilizzo della videosorveglianza; *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256* in merito all'utilizzo di sistemi di rilevazione informatica anti-frode; ecc.] con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, con eccezione ovviamente delle disposizioni che il Regolamento ha espressamente abrogato (per es.: obbligo di notifica dei trattamenti). I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

317 Nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22.

l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g)le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g); i) la tutela dell'interessato o dei diritti e delle libertà altrui; j) l'esecuzione delle azioni civili.

Le eccezioni contenute nell'articolo 23 che derogano, per esempio, al diritto alla portabilità per i motivi già elencati rischiano di essere eccessivamente vaghe da inglobare significati discrezionali anche contrastanti da parte degli Stati Membri. Al contrario deroghe uniformi e ben delimitate cancellano gli spazi entro i quali possono annidarsi abusi.

La tutela effettiva esigerebbe che al consumatore venisse garantita congrua protezione, tenuto conto delle peculiarità della Rete[318] ma la sua consistenza è molle nel nuovo Regolamento.

Un consenso che diventa una «cessione di dati» e quindi trasferimento di informazioni riservate, le più intime degli utenti, non può dirsi valido tantomeno compatibile con le disposizioni del Regolamento UE, che comunque non riesce a stare al passo con le tecnologie, perché omette di regolare fattispecie ormai consolidate sulla Rete. I *Big Data*: quelle informazioni che quotidianamente sono raccolte e incrociate diventano nella società dell'informazione dati ipersensibili che incidono sull'esplicarsi delle libertà degli utenti al punto che esse stesse costituiscono il nucleo di quelle libertà fondamentali indisponibili[319].

---

318 V. MAYER-SCHÖNBERGER- Y. PADOVA, *Regime change? enabling big data through Europe's new Data Protection Regulation*, in *The Columbia Science & Technology Law Review*, vol. XVII, 2016.

319 Cfr. sentenza della Corte Costituzionale del 22 ottobre 1990, n. 471 che riconosce di «valore costituzionale della inviolabilità della persona costruito, nel precetto di cui all'art. 13, primo comma, della Costituzione, come "libertà", nella quale è postulatala sfera di esplicazione del potere della persona di disporre del proprio corpo».

4. Il trasferimento dei dati: l'adeguatezza e le diverse garanzie dell'equivalenza

Per motivi di organicità sia consentito procedere con un rapido accenno al panorama normativo internazionale al fine di delineare le principali problematicità connesse all'accordo di trasferimento dei dati EU-USA, che per ragioni di spazio non potrà essere approfondito in questa sede.

Il profilo del trattamento dei dati personali e della tutela della *privacy* ha assunto, difatti, una rilevanza tale che diversi sono stati negli ultimi tempi gli interventi legislativi a riguardo, anche a livello internazionale. Il 2 febbraio 2016, infatti, la Commissione Europea e il governo degli Stati Uniti d'America hanno raggiunto un accordo politico su un nuovo regime giuridico per gli scambi transatlantici di dati personali, per fini commerciali[320]. A seguito del parere WP 238 del Gruppo di Lavoro Articolo 29 *Data Protection Working Party* del 13 aprile[321], della Risoluzione del Parlamento europeo del 26 maggio 2016 sui flussi transatlantici[322] e delle osservazioni formulate dal Gruppo art. 29,

---

320 2016/4176 UE-U.S. Cfr. con V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/1/1; G. RESTA, *La protezione transnazionale dei dati personali dai "safe harbour principles" al "privacy shield"*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/2/2; C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor della Corte di giustizia dell'Unione Europea*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/4; O. POLLICINO – M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/5/5; G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/6; S. SICA - V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/7/7; P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems nel nuovo regolamento generale sulla protezione dei dati*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/8/8; G. GIANNONE CODIGLIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in file:///C:/Users/maat2/Downloads/11-21-1-SM.pdf, p. 271 ss.

321 16/EN WP 238, *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 13 april 2016, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

322 *Risoluzione del Parlamento europeo del 26 maggio 2016 sui flussi di dati transatlantici (2016/2727(RSP)*, in http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0233+0+DOC+XML+V0//IT.

nello *Statement of the Article 29 Working Party* del 29 luglio 2016[323] la Commissione ha completato la procedura di adozione del *Privacy Schield*[324].

Il cosiddetto scudo UE-USA per la protezione della *privacy* avrebbe recepito le indicazioni della sentenza del 6 ottobre 2015 con cui la Corte di Giustizia dell'Unione Europea[325] ha invalidato il vecchio regime dell'accordo *Safe Harbor*.

La Corte di Giustizia dell'Unione Europea annullava questo accordo perché i "*Safe Harbour Privacy Principles*"[326] emessi dal Dipartimento Usa del Commercio non offrivano un sufficiente livello di protezione dei dati come richiesto dal diritto europeo[327]; più in particolare, la Corte sottolineava come una normativa che consentisse alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche dovesse essere considerata lesiva del contenuto essenziale[328] del diritto fondamentale al

---

323 *Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield*, in http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf.

324 Il testo è reperibile al *link https://www.privacyshield.gov/EU-US-Framework*.

325 Nota come Sentenza *Schrems*, Corte di Giustizia dell'Unione Europea, c-362/14, 6 ottobre 2015. Schrems aveva sollevato una questione interpretativa preliminare per accertare se la decisione *Safe Harbour* determinasse l'effetto di impedire che una Authority nazionale potesse decidere su un ricorso che contestava l'adeguatezza del livello di protezione dei dati di un paese terzo.

326 Per approfondimento si rinvia a G. RESTA – V. ZENO-ZENCOVICH, *La protezione transnazionale dei dati personali*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/3/3.

327 La Corte di Giustizia richiama il diritto alla protezione dei dati personali garantito dalla Carta e i compiti di tutela demandati sempre dalla Carta alle Autorità nazionali di garanzia..

328 Sulla definizione di «contenuto essenziale» si riportano alcuni stralci delle sentenze della Corte di Giustizia che si è pronunciata sul punto in diverse occasioni. Corte di Giustizia, causa C-283/11, 22 gennaio 2013: « qualsiasi limitazione all'esercizio dei diritti e delle libertà riconosciuti dalla Carta deve essere prevista per legge, deve rispettarne il contenuto essenziale e deve, nel rispetto del principio di proporzionalità, essere necessaria e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. A tal riguardo, si deve rilevare che l'articolo 15, paragrafo 6, della direttiva 2010/13 non incide sul contenuto essenziale della libertà d'impresa. Infatti, tale disposizione non impedisce l'esercizio dell'attività imprenditoriale stessa da parte del titolare di diritti esclusivi di trasmissione televisiva. Inoltre, essa non esclude che il titolare medesimo possa sfruttare i propri diritti effettuando egli stesso, a titolo oneroso, la ritrasmissione dell'evento di cui trattasi o, ancora, cedendo contrattualmente tale diritto, a titolo oneroso, ad un'altra emittente televisiva o a qualsivoglia altro operatore economico; C-400/10 PPU, 5 ottobre 2010: «Ne consegue che, ai fini dell'applicazione del regolamento n. 2201/2003, per accertare la liceità del trasferimento di un minore, il quale sia stato condotto in un altro Stato membro dalla madre, il padre naturale deve avere il diritto di rivolgersi al giudice nazionale competente, prima del trasferimento, per chiedere che gli venga conferito un diritto di affidamento del figlio, il che costituisce l'essenza medesima del diritto di un padre naturale ad una vita privata e familiare in un tale contesto»; causa C-157/14, 17 dicembre 2015: « Sebbene tali libertà possano essere limitate, qualsiasi limitazione del loro esercizio dev'essere, ai sensi dell'articolo 52, paragrafo 1, della Carta, prevista dalla legge e rispettare il contenuto essenziale di dette libertà. Inoltre, come emerge da tale disposizione, nel rispetto del principio di proporzionalità possono essere apportate limitazioni solo qualora siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. A tale riguardo, occorre rilevare che, da un lato, l'ingerenza di cui al punto 67 della presente sentenza è prevista dalla normativa, ossia dall'articolo 8, paragrafo 1, del regolamento n. 1924/2006, in combinato disposto

rispetto della vita privata. L'accordo, infatti, risultava applicabile soltanto alle imprese americane che vi avevano aderito, non anche alle autorità pubbliche degli Stati Uniti, con un evidente pericolo di ingerenza da parte loro nei diritti fondamentali delle persone. Inoltre, esigenze di sicurezza nazionale, di pubblico interesse e la stessa applicazione di principi normativi dell'ordinamento degli Stati Uniti d'America sarebbero prevalsi sullo Schema *Safe Harbor*; di conseguenza le organizzazioni con sede negli USA sarebbero state obbligate, senza limitazione alcuna, a disapplicare i principi di tale schema cui pure avevano aderito, in caso di conflitto con le superiori esigenze pubbliche appena descritte.

Si aggiunga che non consentire al singolo di esperire rimedi giuridici diretti ad accedere ai dati personali che lo riguardassero o a ottenerne la rettifica o la cancellazione violava apertamente il contenuto essenziale del diritto fondamentale a una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta, facoltà, questa, che è connaturata all'esistenza di uno Stato di diritto[329]. La stessa Corte ha evidenziato che «l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà, garantiti dal diritto dell'Unione, siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo,

---

con l'allegato a tale regolamento, e dall'articolo 9, paragrafo 2, della direttiva 2009/54, in combinato disposto con l'allegato III a tale direttiva. Dall'altro lato, il contenuto essenziale della libertà di espressione e d'informazione dell'imprenditore non è pregiudicato da dette disposizioni, qualora queste ultime si limitino a sottoporre l'informazione che può essere comunicata al consumatore circa il contenuto di sodio o di sale delle acque minerali naturali a talune condizioni, quali precisate ai punti da 44 a 56 della presente sentenza; c-112/00, 12 giugno 2003: «Così, neppure i diritti alla libertà d'espressione e alla libertà di riunione pacifica garantiti dalla CEDU — contrariamente ad altri diritti fondamentali sanciti dalla medesima convenzione, quali il diritto di ciascuno alla vita ovvero il divieto della tortura, nonché delle pene o di trattamenti inumani o degradanti, che non tollerano alcuna restrizione — appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale. Ne consegue che possono essere apportate restrizioni all'esercizio di tali diritti, a condizione che tali restrizioni rispondano effettivamente ad obiettivi di interesse generale e non costituiscano, rispetto allo scopo perseguito da tali restrizioni, un intervento sproporzionato e inaccettabile tale da ledere la sostanza stessa dei diritti tutelati»; c-129/14 PPU, 27 maggio 2014: « Ai sensi dell'articolo 52, paragrafo 1, prima frase, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta devono essere previste dalla legge e

rispettare il contenuto essenziale di detti diritti e libertà. Secondo la seconda frase del suddetto paragrafo, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui». Sul nocciolo duro dei diritti fondamentali si rinvia a p. 95 ss..

[329] In tal senso, cfr. sentenze CGUE, *Les Verts/Parlamento*, 294/83, EU:C:1986:166, punto 23; *Johnston*, 222/84, EU:C:1986:206, punti 18 e 19; *Heylens e a.*, 222/86, EU:C:1987:442, punto 14, nonché, *UGT-Rioja e a.*, da C-428/06 a C-434/06, EU:C:2008:488, punto 80.

l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto»[330].

Questa decisione ha condotto i Garanti delle diverse giurisdizioni europee, Italia inclusa, a sospendere i trasferimenti alle società negli Stati Uniti, perché non fornivano adeguate protezioni nei confronti dei dati degli utenti. L'invalidazione del programma *Safe Harbor* ha spinto le società americane a ricercare e adottare velocemente altre soluzioni consentite dalla normativa *privacy* europea per disciplinare il trasferimento dei dati personali, ricorrendo alle *standard contractual clauses* e ai *binding corporate rules*[331], individuate nella Direttiva 95/46/CE e riprese anche nel testo del nuovo Regolamento europeo 2016/679 (GDPR), anche dette «clausole contrattuali tipo»[332].

I punti più significativi del nuovo accordo si possono sintetizzare in tre punti: il primo è relativo agli obblighi sul trattamento dei dati e vuole che le aziende statunitensi che desiderano importare i dati personali dall'Europa dovranno impegnarsi nel mantenimento di solidi obblighi sul trattamento dei dati e sulla garanzia dei diritti individuali. Il Dipartimento del Commercio controllerà che le aziende pubblichino i loro impegni, rendendoli applicabili nella giurisdizione del Paese di destinazione.

Il secondo riguarda la sorveglianza di massa e richiede che l'accesso delle autorità pubbliche per questioni di ordine e sicurezza nazionale sia sottoposto a chiare limitazioni, garanzie e meccanismi di controllo. Queste eccezioni dovranno essere utilizzate solo nella misura necessaria e in maniera proporzionata, evitare ogni tipo di sorveglianza di massa dei dati personali trasferiti negli Stati Uniti[333]. Per monitorare regolarmente il funzionamento del nuovo regime ci sarà una revisione congiunta annuale, che comprenderà anche la questione dell'accesso sicurezza nazionale.

Il terzo attiene al diritto di ricorso e alla previsione del difensore civico[334]. Viene riconosciuto ai cittadini Ue la possibilità di denunciare gli abusi, qualora dovessero ritenere

---

330 CGUE, causa C-362/14, 6 ottobre 2015, punto 95, cit.

331 Una serie di clausole che stabiliscono principi vincolanti al cui rispetto sono tenute tutte le società appartenenti allo stesso gruppo d'impresa.

332 G. M. RICCIO, *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/9/9.

333 G. DE MINICO, Costituzione. Emergenza e terrorismo, Jovene, Napoli, 2016, p. 85 ss..

334 Il cosiddetto «Ombudsperson», a cui i cittadini europei si possono rivolgere nel caso sospettino un abuso sui propri dati personali da parte delle autorità di intelligence statunitensi.

che la riservatezza dei loro dati sia stata violata e le aziende avranno precise scadenze per rispondere alle accuse.

Accanto a ciascun punto si individua una serie di problematicità che di seguito espliciteremo.

Come rilevato dal Parlamento Europeo e dal Gruppo di Lavoro Articolo 29 *Data Protection Working Party*, già prima che l'accordo *Privacy Shield* venisse firmato, permanevano forti dubbi relativi al *gap* tra il trattamento dei dati personali raccolti nell'Unione europea e quella che sarebbe stata la loro sorte, una volta trasferiti negli Stati Uniti.

La prima che indicheremo con *a)* riguardava l'incertezza delle decisioni da parte delle società americane di dismettere l'attuale soluzione di *compliance privacy* per adeguarsi al *Privacy Shield*; la seconda che indicheremo con *b)* attiene alla probabilità che la scelta di non adottare i dettami del *Privacy Shield* possa essere dovuta anche a motivi di carattere pratico, visto che gli obblighi che impone sono più complessi e onerosi di quelle imposti dalle «clausole contrattuali tipo». Tuttavia, la scelta di adottare tali clausole non può considerarsi sufficiente nell'ottica di una tutela adeguata dei cittadini dell'Unione Europea in materia di trattamento dei dati personali da parte delle aziende degli Stati Uniti. L'inserimento di simili clausole contrattuali all'interno di un contratto consente di eludere la richiesta di consenso specifico degli interessati da parte dei titolati del trattamento, ottenendo un'autorizzazione dall'Autorità competente per il trasferimento verso un paese terzo che non offre tutela adeguata. Si tratta, insomma, di una facilitazione per le aziende che debbano procedere al trasferimento dei dati all'estero. Secondo questo tipo di clausole tanto l'importatore, quanto l'esportatore dei dati sono tenuti a rispettare le regole generali: il primo, secondo le leggi del paese d'origine; il secondo, in particolare, dovrà adempiere a delle regole «minime», chiarendo i fini del trattamento, garantendo proporzionalità, correttezza, esattezza e pertinenza dei dati, fornendo un'informativa, adottando opportune misure di sicurezza.

Infine la terza, *c)* la scelta di alcune società americane di spostare i *server* utilizzati per ragioni di *business* in Europa potrebbe apparire molto costosa per le piccole e medie

imprese[335], incluse soprattutto le *start up*. I cittadini europei, pertanto, stante una normativa europea in materia di *privacy* maggiormente onerosa, correrebbero il rischio di non godere di servizi innovativi o di riceverli con notevole ritardo.

Sul piano europeo, il Capo V del Regolamento 2016/679/UE è intervenuto a fare chiarezza, esso disciplina i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. Specificamente, l'articolo 44 enuncia un principio generale per il trasferimento: qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere tali dopo il trasferimento verso un paese terzo o un'organizzazione internazionale[336], ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni stabilite dal Regolamento. Il fine ultimo è quello di assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato. Tuttavia, ai sensi il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato[337]. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

In conformità alla previgente direttiva questo capo del Regolamento ha confermato l'approccio già vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il Regolamento elenca in ordine gerarchico:

i. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea[338];

---

335 A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbour e Privacy Shield,* in http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/10/10, 239 ss.

336 Compresi i trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale.

337 Articolo 45 del Regolamento 2016/679/UE.

338 Cfr. art. 44, comma 1, lettera b), del Codice.

ii. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti[339];

iii. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni[340].

Le decisioni di adeguatezza sinora adottate dalla Commissione, si pensi al livello di protezione dati in Paesi terzi, a partire dal *Privacy Shield*, e alle clausole contrattuali tipo per titolari e responsabili e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica[341]. Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente alle decisioni di adeguatezza della Commissione[342]. Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi[343], sino a loro eventuale modifica.

L'adeguatezza viene valutata sulla base di una serie di parametri tra i quali lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale; l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale; gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni[344]. Per la valutazione di adeguatezza vengono presi in considerazione la natura dei dati, le finalità del trattamento previsto, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

---

339 fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello. Si veda Art. 44, comma 1, lettera a) del Codice.

340 corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice.

341 si vedano art. 45, paragrafo 9, e art. 96.

342 Cfr. *http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1.*

343 si veda art. 46, paragrafo 5.

344 Elencati al paragrafo 2 dell'articolo 45.

In mancanza di una decisione[345], il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate[346] e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Tra le garanzie adeguate sono comprese «clausole tipo di protezione dei dati» adottate dalla Commissione oppure adottate da un'autorità di controllo e approvate dalla Commissione e un codice di condotta. Particolari garanzie adeguate possono essere offerte da clausole contrattuali e accordi amministrativi tra autorità pubbliche o organismi pubblici[347].

Questo vuol dire che «in mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate da un'autorità di controllo o clausole contrattuali autorizzate da un'autorità di controllo. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato

345 Ai sensi dell'articolo 45, paragrafo 3.

346 Secondo quanto previsto dall'articolo 46, parag. 2 del Regolamento 679/UE «possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; b) le norme vincolanti d'impresa in conformità dell'articolo 47; c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati». Il paragrafo 3 aggiunge che «fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1: a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati». Il parag. 4 che «l'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo. 5.Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo».

347 Cfr. con articolo 46, parag. 3.

ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default. I trasferimenti possono essere effettuati anche da autorità pubbliche o organismi pubblici ad autorità pubbliche o organismi pubblici di paesi terzi, o organizzazioni internazionali con analoghi compiti o funzioni, anche sulla base di disposizioni da inserire in accordi amministrativi, quali un memorandum d'intesa, che prevedano per gli interessati diritti effettivi e azionabili. L'autorizzazione dell'autorità di controllo competente dovrebbe essere ottenuta quando le garanzie sono offerte nell'ambito di accordi amministrativi giuridicamente non vincolanti»[348].

L'art. 49 elenca una serie di deroghe, quindi il trasferimento verso un paese terzo che non garantisce una tutela adeguata può avvenire se: a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento sia necessario per importanti motivi di interesse pubblico; e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a

[348] Cons. 108.

condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Con riferimento al trasferimento da un titolare a un altro, non esiste una specifica disposizione per il trasferimento dei dati da un titolare a un altro, ma essa si riscostruisce sulla base delle altre disposizioni che definiscono il consenso e l'obbligo di informativa. Il trasferimento presso un altro titolare è ammesso se il trattamento ha finalità compatibili con quelli per le quali è stato rilasciato e quindi senza consenso. Se non è compatibile e se non è stato reso il consenso quando il responsabile del trattamento ha adempiuto l'obbligo di informativa, anticipando all'interessato che i suoi dati sarebbero stati trasferiti presso un altro destinatario, è richiesto specifico consenso sulla base della definizione stessa del consenso.

Tirando le linee del ragionamento, viene meno il requisito dell'autorizzazione nazionale[349]. Ciò significa che il trasferimento verso un Paese terzo «adeguato» ai sensi della decisione che assumerà la Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto previsto dall'art. 44 del Codice *Privacy*[350].

Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali *ad-hoc*[351] oppure accordi amministrativi stipulati tra autorità pubbliche[352].

Come anticipato, il Regolamento permette di ricorrere anche a codici di condotta ovvero a schemi di certificazione per dimostrare le «garanzie adeguate» previste dall'art.

---

[349] Cfr. art. 45, paragrafo 1, e art. 46, paragrafo 2.

[350] Secondo l'art. 44 «1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime; (1) b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti».

[351] Cioè non riconosciute come adeguate tramite decisione della Commissione europea.

[352] Una delle novità introdotte dal Regolamento.

46. Ciò significa che i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia[353], tali titolari dovranno assumere, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente vincolante e azionabile dagli interessati.

Il Regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati[354]. Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve evidenziare che il Regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato «per importanti motivi di interesse pubblico», in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto dell'Ue[355] e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

La nuova normativa fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del Regolamento – ossia, è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati[356].

Si badi bene, la principale problematicità che emerge dall'esame della disciplina del trasferimento dei dati riguarda proprio la valutazione dell'adeguatezza. L'adeguatezza rispetto all'equivalenza può prevedere garanzie inferiori ma sufficienti. Inoltre, «le clausole

---

353 Cfr. art. 40, paragrafo 3 e art. 42, paragrafo 2.

354 Cfr. art. 48.

355 Cfr. art. 49, paragrafo 4.

356 Cfr. art. 65, paragrafo 1, lettera d).

contrattuali modello» rischiano di minimizzare la tutela dei dati per ridurla a un livello meno che sufficiente. Questi modelli sarebbero destinati a diventare lo strumento che traghetterà i *Big Data* al di fuori dell'Europa con un livello di garanzia più basso rispetto a quello del Paese di provenienza. Ci chiediamo se sia compatibile una informativa che rimandi genericamente a un «modello di clausole contrattuali approvato dalla Commissione europea».

In conclusione, le deroghe rischiano di trasformare l'adeguatezza in approssimazione. Se è vero che il Regolamento risulta più dettagliato e disciplina fenomeni nuovi, con la molteplicità di deroghe rischia di "annacquare" la tutela, perché già una tutela adeguata dà garanzie inferiori rispetto a una equivalente, accettare una garanzia meno che sufficiente rischia di compromettere l'efficacia della tutela, anche se l'adeguatezza viene fissata in modelli di.

Il regime di trasferibilità dei dati richiesto agli Stati dell'Unione dopo la sentenza *Schrems* del 6 ottobre 2015 C-362/14, con la quale la Corte di Giustizia si è pronunciata sulla inadeguatezza del *Safe Harbor* statunitense in materia di tutela dei dati personali, invalidando la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE, non si accontenta di una misura di adeguatezza. La sentenza, infatti, ha aperto una nuova *issue*: quale livello di protezione dovrà essere previsto per il trasferimento dei dati verso un paese terzo o un'organizzazione internazionale dal Regolamento 2016/679/UE. Ci chiediamo, in altre parole, se ammettere un trasferimento dei dati a un paese terzo, se esso assicura garanzie adeguate significa proteggere efficacemente la riservatezza dei cittadini europei[357].

Facciamo un esempio solo per rendere concreto il problema che ci siamo da ultimo posti: se lo Stato d'origine richiedesse per il trattamento dei dati una tutela molto alta, che per ragioni di semplificazione indicheremo con il numero 10, per trasferire i dati a un Paese terzo potrà dirsi sufficiente un livello di protezione 5, perché semplicemente adeguato - seppure non equivalente - oppure la piena tutela della riservatezza dei cittadini di quello Stato membro, garante di una copertura 10, potrebbe realizzarsi solo mediante la garanzia

[357] *Supra* nota 320.

di un livello di protezione equivalente, cioè se e solo quello Stato membro, a cui i dati vengono trasferiti, garantisce una tutela 10?

5. Il trattamento dei dati e il "legittimo interesse" a trattare i dati nella finalità di *marketing*

Una delle principali innovazioni della normativa europea si rinviene nel principio di responsabilizzazione. Si esamineranno di seguito le disposizioni che lo prevedono.

L'articolo 26 del Regolamento disciplina la contitolarità del trattamento e impone ai titolari di definire specificamente[358] il rispettivo ambito di responsabilità[359] e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

Rispetto all'art. 29 del Codice *Privacy*, il Nuovo Regolamento fissa più dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento, attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto o comunque di un altro atto giuridico conforme al diritto nazionale e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce «garanzie sufficienti» – quali, in particolare, la natura, la durata e le finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel Regolamento.

L'articolo 28, paragrafo 4 consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi

---

[358] con un atto giuridicamente valido ai sensi del diritto nazionale.

[359] G. KELLY, *A Public Policy Analysis of the European Union's Data Protection Regulation Principles and the U.S Consumer Privacy Bill of Rights*, May 1, 2013, in http://dx.doi.org/10.2139/ssrn.2295659, p. 23.

obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso «non gli è in alcun modo imputabile»[360] .

L'articolo 37 del Regolamento prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti[361]; l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti[362]; la designazione di un RPD-DPO, nei casi previsti dal Regolamento o dal diritto nazionale.

Rispetto alla previgente direttiva il Regolamento definisce caratteristiche soggettive e la responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE. Pur non prevedendo espressamente la figura dell' «incaricato» del trattamento[363], il Regolamento non ne esclude la presenza in quanto fa riferimento a «persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile»[364].

Deve aggiungersi alle disposizioni sopra richiamate una precisazione: il *Considerandum* 47 del Nuovo Regolamento Europeo GDPR n. 679/2016 individua nella finalità del *marketing* un «legittimo interesse» che giustifica il trattamento dei dati personali. A prescindere dall'inadeguatezza del *nomen iuris* prescelto - l'interesse legittimo è una situazione giuridica soggettiva della quale è titolare un soggetto, nei confronti della pubblica amministrazione, che esercita un potere autoritativo attribuitole dalla legge e consiste nella pretesa che tale potere sia esercitato in conformità alla legge - le eccezioni aggirano e diluiscono l'efficacia della tutela della *privacy* che ha ispirato la normativa di revisione della direttiva 95/46/CE. Può essere considerato legittimo interesse trattare dati personali per finalità di *marketing* diretto. Lo stesso considerando prevede che il legittimo interesse possa costituire una base giuridica del trattamento, a condizione che non

360 si veda art. 82, paragrafo 1 e paragrafo 3.

361 ex art. 30, paragrafo 2.

362 *ex* art. 32 Regolamento.

363 *ex* art. 30 Codice.

364 si veda, in particolare, art. 4, n. 10, del Regolamento.

prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

A questo punto, sembrerebbe, a dispetto di quanto osservato nei paragrafi precedenti che il sistema normativo sovranazionale ponga la regola dell'*opt-out* come strumento di tutela della *privacy* del *data subject*[365], in caso di finalità di *marketing*.

Tale scelta non è coerente con lo scopo di assicurare un elevato livello di protezione delle persone fisiche con riguardo al trattamento dei dati[366]. Mediante tale opzione di rinuncia il soggetto interessato potrà manifestare il diritto di opposizione a un trattamento dei dati per le finalità sopra descritte, solo dopo che il trattamento è già iniziato, e cioè dopo la ricezione della comunicazione invasiva, contenente il *disclaimer*.

6. Una possibile soluzione nella *reasonable expectations of anonymity*?

Nel tentativo di individuare una soluzione condivisa per una penetrazione di garanzie a tutti i livelli si propongono una serie di possibili soluzioni alla tutela della ragionevole aspettativa di *privacy* del consumatore sui dati che immette in Rete ogni giorno, mediante l'utilizzo dello *smartphone* sul mercato digitale.

Un primo modo sarebbe quello di tutelare la *privacy* delle persone in sede di progettazione senza svilire la potenza dei dati[367], mediante la *privacy by design*[368]. In questa

---

365 Cioè del soggetto interessato.

366 Cfr. in particolare Cons. 10 del Regolamento UE 2016/679.

367 Silver Nate in "Il segnale e il rumore" scrive che quello che cerchiamo è la conoscenza e non le informazioni. Silver è l'autore di un *software* che utilizzando i dati gli ha consentito di prevedere correttamente l'elezione di Obama in 49 Stati su 50, analizzando i dati numerici di affluenza al voto. Si ritiene sia superata l'era degli exit poll per il fatto che *Facebook, Google* e *twitter* sono in grado di dire molto di più delle tradizionali previsioni. L'autore sostiene che come l'era del computer ha richiesto una decina di anni prima di produrre ricchezza e innovazione, allo stesso modo, l'era dei *B.D.* richiede tempo per tradurre le informazioni in conoscenza utili, potremmo nel frattempo fare dei passi indietro.

368 G. D'ACQUISTO, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, in www.enisa.europa.eu, dicembre 2015.

direzione sembra si sia mosso il Regolamento 679 con la previsione dell'articolo 25, il quale stabilisce che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione[369], e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e a tutelare i diritti degli interessati.

Il paragrafo 2 stabilisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per «impostazione predefinita», solo i dati personali necessari per ogni specifica finalità del trattamento.

Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

La vera sfida è, dunque quella di riuscire ad anonimizzare[370] gli utenti senza cancellare l'interesse dei dati raccolti. Una proposta potrebbe essere quella dei *Topic Data* di *Facebook*.

Si tratta di dati anonimi raccolti in forma aggregata che riguardano attività specifiche, marche, prodotti, eventi etc. che le persone seguono. Tuttavia, si tratta di sistemi complessi perché la raccolta, la conservazione e l'elaborazione dei dati si scontrano con le operazioni per rendere i dati anonimi. Si potrebbe utilizzare la crittografia «omomorfica», che consente di eseguire calcoli su dati cifrati senza prima decrittarli. Dati e anonimato sono un ossimoro perché il dato è tanto più interessante quanto più dettagli mi dà sulla persona osservata, al punto da consentirmi di identificarla.

Si sta comunque radicando un interesse sempre maggiore non solo verso i *topic data* ma anche verso delle vere e proprie nicchie del settore, gli *small data.*

---

369 Cfr. Con l'articolo 25, paragrafo 1 del Regolamento 679: «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

370 J. M. SKOPEK, *Reasonable expectations of anonymity*, in 101 Va. L. Rev. 691 2015, p. 692 ss.

Con riguardo ai primi, l'interesse verso l'anonimato, quel processo che rende i dati in origine o a seguito di trattamento non associabile a un individuo identificato o identificabile, seppure sembra stia diventando sempre più evanescente (sono gli stessi utenti a rinunciare alla tutela della *privacy* condividendo sui *social* i momenti più intimi della propria vita), potrebbe essere soddisfatto da appositi sistemi. Il dato trattato con il cd. processo di *Big Data Anonymization* diventerebbe di origine ignota, esso si avvale di crittografia, *hashing* e generalizzazione, e serve a consentire il trattamento dei dati nel rispetto della *privacy*.

Per dare un taglio pratico al discorso seguiranno alcuni esempi di *software* che hanno fatto fortuna nel settore.

SimilarWeb è una *startup* israeliana, con sede a Londra che ha raccolto 400 milioni di dollari di investimenti per finanziare un servizio basato sull'analisi dei dati anonimi, provenienti da cento milioni di dispositivi e migliaia di siti in tutto il mondo. Esso traccia una sorta di *"traffic ranking*" cui sono interessati migliaia di clienti che pagano[371] per avere accesso a *benchmark* e rapporti dettagliati per lo studio della concorrenza al fine di individuare rapidamente *trend* e strategie migliori sul *web*.

Con *DataSift* vengono analizzati gli *status* degli utenti e i *post* delle pagine, compresi quelli privati, commenti e "mi piace", da queste analisi è possibile sapere quante persone parlano di un determinato argomento, il loro sesso, la loro età, la loro residenza, la loro istruzione, il loro grado di soddisfazione su un evento o marca, i *link* più condivisi, la materia che sta loro più a cuore al momento. Il sistema *DataSift* anonimizza i dati prima di processarli sulla piattaforma *Facebook*, inoltre analizza una soglia minima di cento unità di utenti maggiorenni per evitare analisi individuali. I risultati che il sistema restituisce sono dati aggregati e anonimi, che dopo trenta giorni vengono cancellati.

Ne traggono giovamento le strategie di *marketing* perché si può analizzare la fedeltà a una marca, l'intenzione di acquistare o meno il prodotto, la soddisfazione del consumatore. Si tratta però di dati anonimi che non devono essere messi in sicurezza da appositi istituti ma possono essere analizzati dettagliatamente senza entrare in contatto con l'identità dell'utente.

[371] La versione Pro costa 200 sterline al mese.

Per quanto riguarda gli *small data* e il *data driven management* occorre precisare che l'interesse per i *Big Data* è soprattutto dei grandi colossi che hanno gli strumenti non solo per raccoglierli ma anche per elaborarli e utilizzarli, spesso la parte di dati utilizzabile è minima perché dipende dalla strutturazione; allora pochi dati strutturati possono essere molto più utili per piccole e medie imprese. In questo modo vengono estratti i dati più interessanti e ci si concentra sui dettagli.

Tim Berners Lee ha suggerito nel suo progetto Solid[372] sui cd. *Data pods* un insieme di proposte di convenzioni e strumenti per la creazione di applicazioni sociali decentrate, basate sui principi *linked data*. Solid è modulare ed estensibile e si basa il più possibile su *standard* e *protocolli W3C* esistenti.

Il progetto si muoverebbe lungo tre direttrici:

1) *True data ownership*: gli utenti dovrebbero avere la libertà di scegliere dove i loro dati devono risiedere e chi è autorizzato ad accedervi scollegando i contenuti che non intende condividere o cedere dall'applicazione stessa.
2) *Modular design*: poiché le applicazioni sono scollegate dai dati che producono, gli utenti saranno in grado di evitare il *vendor lock-in* - il blocco da fornitore, cioè il rapporto di dipendenza che si instaura tra un cliente e un fornitore di beni o servizi, tale che il cliente si trova nella condizione di non poter acquistare analoghi beni o servizi da un fornitore differente senza dover sostenere rilevanti costi e rischi per effettuare questo passaggio - cambiando *app* senza difficoltà e *server* di archiviazione dei dati personali, senza alcuna perdita di dati o di connessioni sociali.
3) *Reusing existing data*: Gli sviluppatori saranno in grado di innovare facilmente con la creazione di nuove applicazioni o migliorare le applicazioni attuali, il tutto riutilizzando dati esistenti creati da altre applicazioni.

Da quanto finora argomentato, si evince che oggi diventa più complesso, da un lato, capire fin dove si spinge la ragionevole aspettativa di *privacy*, dall'altro frenare il

[372] Acronimo che deriva da *SOcial LInked Data* in *pods*: *https://solid.mit.edu/*.

trasferimento indiscriminato dei dati, oggi divenuti, come anticipato, nocciolo duro di diritti fondamentali inalienabili.

Per adattarsi a questo rapido mutamento sociale e tecnologico è necessario che la garanzia dei diritti non venga rimessa al singolo consumatore, confidando nella sua prudenza, ma, al contrario, che sia il legislatore a imporre agli *OTT* condizioni contrattuali chiare e *privacy designed* nonché fermi divieti. Un consenso rilasciato nelle forme attualmente previste dagli *OTT* sarebbe aggirabile, alla luce della disciplina europea.

Va ribadito in questa sede che i dati non dovrebbero essere negoziabili e rinunziabili o cedibili analogamente agli organi vitali[373]. I dati che si raccolgono consentono non solo l'identificazione del soggetto, ma potrebbero rivelare dettagli della sua vita di cui egli stesso potrebbe essere all'oscuro[374] o che comunque non vorrebbe divulgare.

Non può passare in secondo piano, l 'evoluzione costante del concetto di *privacy:* i nostri nonni non avrebbero forse mai voluto rivelare a terzi le proprie malattie e le medicine che assumevano, forse i loro pronipoti vorranno cedere i loro dati per sostenere la ricerca di una cura o supportare uno studio scientifico[375]. Si pensi alla genomica di consumo e alle aziende che consentono a chiunque di interagire con i dati ed esplorare direttamente i propri dati genomici, in cerca di antenati o di diagnosi e cure.

Sempre più pazienti condividono i loro dati con gli altri, per consentire alla comunità scientifica di risolvere problemi relativi alla loro condizione, senza essere inutilmente ostacolati da regole restrittive che impediscono, in nome della *privacy*, a un paziente di beneficiare dei vantaggi connessi all'uso dei dati.

Piuttosto, le nuove forme di consenso dovrebbero mirare a educare i soggetti della ricerca su ciò che i dati raccolti su di loro possono dire e il grado con cui possono o non possono essere protetti.

---

373 M.G. RADIN, *Market-inalienability*, in *Harv. Law. Rev.*, 100, 1987, p. 174; M. MADDEN - M. GILMAN - K. LEVY – A. MARWICK, *Privacy, poverty and big data: a matrix of vulnerabilities for poor americans*

374 L'esempio è quello di una coppia di coniugi che separatamente acquista profilattici nella stessa farmacia a breve distanza, il farmacista potrebbe conoscere dettagli di cui gli stessi sarebbero all'oscuro.

375 L'esempio è di John D. Halamka «If you asked my mother her attitude toward privacy, she would say, 'Oh, I never want anyone in the community to know my medicines or my diseases.' What you see in the 20-year-olds is, 'What's the big deal?' Over time the medical privacy preferences of individuals will change.» in *Mit Technology Review*, *Data-Driven Health Care*, vol. 117, n. 5, p. 13.

Quanto al modello europeo, esso si presta a un'applicazione meramente formalistica che facilmente si riduce ad un modulo di informativa e alla prestazione di un consenso vuoto e ineffettivo[376].

L'interessato cui viene richiesto di esprimere un consenso è la parte più debole del rapporto contrattuale sotto ogni profilo: culturale, economico, tecnologico e conoscitivo.

Occorrerebbe avviare un'analisi di tipo economico sul modello che si adotta, considerato anche il mercato su cui si interviene.

Il Regolamento lascia vuoti nella disciplina del bilanciamento del diritto alla protezione dei dati personali con altri diritti di pari rilievo costituzionale.

L'Europa con il Regolamento erge un muro protettivo per difendersi ma si isola dal resto del mondo. Questi temi richiederebbero un tavolo di discussione più ampio[377].

[376] G. FINOCCHIARO, *op. cit.,* p. 134.
[377] *Ibid.*

Capitolo III

I *Big Data* tra sfruttamento economico e vocazione democratica

SOMMARIO: 1. I *Big data* da mezzo di sviluppo economico a strumento di democrazia (1.1. *Opportunità e rischi nell'utilizzo dei* Big Data). - 2. Il radicamento costituzionale dei *Big Data*: nocciolo duro dei diritti fondamentali – 3. *Big Data*, privacy e *competition policy*. (3.1. L'*asset* dei dati sul mercato e le sue declinazioni egoistiche). - 4. La catena di valore dei dati e la posizione di *Google* (4.1. *I servizi di Google e l'estrazione dei dati* – 4.2. *Le pratiche anticoncorrenziali nello sfruttamento abusivo della dominanza* – 4.3. *Il mercato rilevante e la quota di mercato* – 4.4. *Altri fattori strutturali indicativi dello sfruttamento abusivo della dominanza* – 4.5. *Le indagini della Commissione Europea e la decisione sul caso* Google Shopping – 4.6. *Il mercato individuato dalla Commissione Europea* - 4.7. *L'opportunità di un nuovo mercato di riferimento nello sfruttamento dei dati*). - 5. L'accesso ai diritti di esclusiva sui dati e la protezione della *privacy* come benefici per la concorrenza e l'innovazione.

1. I *Big Data* da mezzo di sviluppo economico a strumento di democrazia

L'utilizzo delle tecnologie informatiche ha rivoluzionato la vita quotidiana[378] dei consumatori e gli interi processi produttivi: da un lato, sul piano microeconomico, la convergenza tecnologica[379] ha offerto al singolo, raggiungendolo fino a casa, *carnet* di prodotti sempre più diversificati; dall'altro, sul piano macro, ha sviluppato nuovi modelli di *business* intorno alle inedite unità produttive di ricchezza: i dati.

La tecnologia dunque è entrata nei meccanismi di produzione, modificando i modi di progettare, realizzare e distribuire i prodotti, incidendo sulle aspettative lucrative e sulle condotte del *fair play* competitivo.

Ne è risultato un mercato dei servizi e dei contenuti digitali profondamente ristrutturato in cui sono mutati il «tipo» di operatore economico, il terreno di gioco e la fonte del profitto, nonché le logiche di mercato e i paradigmi della disciplina *antitrust*.

I vecchi apparati normativi analogici si sono rivelati carenti, inadatti a coprire il raggio d'azione dei nuovi attori privati che si muovono su una «prateria dai confini senza limiti»[380]: la Rete.

Su questo spazio, avulso dalle regole, si sono affermati pochi *big Player*.

L'aggregazione di informazioni e l'accessibilità ai *Big Data* da parte di pochi, ottenuti attraverso forme non negoziate di profilazione degli utenti, impattano inevitabilmente sull'ecosistema digitale, modificandone assetti ed equilibri. Chi possiede i dati possiede conoscenza e quindi denaro: è in grado persino di spostare gli equilibri geopolitici[381].

---

[378] Si pensi alle transazioni bancarie, alle conversazioni con gli amici su *whatsapp* o *skype*, agli spostamenti registrati dallo *smartphone*. Secondo Martin Hilbert, ricercatore dell'Università della California, nel 2000 il 25% di tutta l'informazione prodotta nel mondo era registrata su supporto digitale, nel 2013 il 98%. Si badi bene nulla o poco è cambiato nella riduzione della carta e della plastica.

[379] La convergenza tecnologica è in grado di offrire una vasta gamma di servizi accessibili ovunque il cittadino digitale risieda, purché abbia un dispositivo e un collegamento veloce a Internet. Per quanto attiene al superamento del concetto di «convergenza dei mezzi» a favore di una «convergenza dei contenuti», si veda G. DE MINICO, *Una guida alla lettura*, in *Ead.* (a cura di), *Nuovi media e minori*, Roma, Aracne, 2012, *passim*.

[380] L'espressione è stata utilizzata nella forma negativa nella sentenza del Tribunale di Milano del 24 febbraio 2010, n. 1972/2010, caso *Google-Vividown*, nella quale il Giudice Oscar Magi, nel condannare i manager *Google* per violazione degli art. 23, 17, 26 e 167 del d.lgs. 196/2003 scriveva che «non esiste la sconfinata prateria di Internet dove tutto è permesso e niente può essere vietato, esistono invece leggi che codificano comportamenti che creano degli obblighi che ove non rispettati conducono al riconoscimento di una penale responsabilità».

[381] Si prevede che la Cina nel 2020 sarà in possesso di un quinto delle informazioni mondiali disponibili. I *big* cinesi in tale settore si stanno velocemente muovendo verso i dati, si pensi che il leader di *e-commerce Alibaba*, uno dei 20

La raccolta delle informazioni e la loro gestione giocano un ruolo decisivo per le imprese, al punto che i dati personali sono divenuti *asset* strategico[382], secondo la logica dei mercati multiversante[383], e attraverso forme di profilazione e definizione di algoritmi che possono incidere sia sul mantenimento della *net neutrality*[384] tra operatori di rete e fornitori di contenuti, sia sulla pluralità della rappresentazione di fatti e opinioni presso gli utenti, i quali accedono alle notizie sempre di più tramite intermediari[385], ovvero per mezzo delle piattaforme sociali[386].

«The way this type of market works is in conflict with fundamental principles that should apply in democratic societies. Citizens should not be lied to, and markets for ideas in democratic societies should help citizens make better-informed decisions. It is reliable information that democratic societies need to expect from functioning markets for ideas,

---

siti più visitati al mondo con più di un miliardo di prodotti e vendite per 170 miliardi di dollari nel 2012, si sta orientando verso il *cloud* e il *data computing*. *Aliyun,* divisione dei servizi in cloud, si propone di superare *Amazon* nel giro di 3 o 4 anni. Accanto alla Cina stanno emergendo Brasile, India, Russia, Messico che secondo l'*Emc Digital Universe* capovolgeranno le fette di mercato impadronendosi della quota maggiore.

382 La *Boston Consulting Group* ha valutato le nostre vite digitali per mille miliardi di euro entro il 2020, l'8% del PIL dell'Ue, solo in Europa.

383 Occorre precisare che la dottrina sul punto è contrastante. Un mercato multilaterale è formato da una piattaforma, che è comune ai lati e che coordina gli scambi tra di essi, internalizzando gli effetti indiretti di rete che si generano. Ogni lato riceve un beneficio positivo crescente in relazione al numero dei componenti dell'altro, riducendo sostanzialmente il costo di transazione degli scambi. Una condizione fondamentale è che senza la piattaforma i soggetti non riescano ad effettuare fra loro scambi efficienti. Il modello dei mercati multiversanti è stato applicato, fra gli altri, anche al *search advertising*, i lati sarebbero gli inserzionisti e i navigatori. Così V. V. COMANDINI, *Google e i mercati dei servizi di ricerca su Inernet*, in *Mercato concorrenza e regole*, a. XV, n.3, pp. 541-569. Si parla di mercati multiversanti anche nell'indagine Conoscitiva congiunta Agcom – Antitrust. Secondo parte della dottrina i *multisided market*, inoltre, possono essere a transazione unica o a più transazioni, come nel *search advertising* dove gli inserzionisti acquistano spazi che le piattaforme offrono agli utenti della Rete, offrendo loro dei contenuti, qui gli scambi sarebbero almeno due, così: L. FILISTRUCCHI, *A SSNIP test for two-sided markets: the case of Media*, in *Social Science Research Network*, 2008, in *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287442*. *Contra* LUCHETTA, il quale ritiene che il mercato del *search advertising* non possa essere considerato un mercato bilaterale perché mancherebbe la reciprocità delle esternalità positive per i due lati: sarebbero chiare, infatti, quelle generate dal crescente numero di utenti, non quelle generate dal crescente numero di inserzionisti.

384 Per un approfondimento sul tema, che non è oggetto del nostro studio, si rinvia a G. DE MINICO, Net neutrality *come diritto fondamentale di chi verrà*, in *www.costituzionalismo.it*, 20 aprile 2016; F. DELL'AVERSANA, *Le libertà economiche in Internet:* competition*,* net neutrality *e* copyright, Aracne, Roma, giugno 2014, p. 296 ss..

385 O. TENE – J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Nw. J. Tech. & Intell. Prop.*, vol 11, n. 5, 2013 a p. 252: «increased personalization based on opaque corporate profiling algorithms poses a risk to open society and democratic speech».

386 «Can and should democratic societies accept the way in which modern digital markets provide news? The answer is a clear no» così Drexl in J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in *Max Planck Institute for Innovation and Competition Research*, Paper No. 16-16, p. 11, cit..Cfr. anche con Indagine conoscitiva Antitrust-Agcom-Garante Privacy del 1 giugno 2017 su *Big Data*, in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6441412*. Per evidenti ragioni di spazio queste ultime problematiche non saranno oggetto del nostro studio. Si è tuttavia, ritenuto doveroso, per completezza espositiva, farvi un rapido cenno.

and not purely that they respond at best to the emotions of citizens. This conclusion derives from constitutional considerations beyond economic efficiency. Such constitutional considerations are key to the regulation of the economic activity of private actors in markets for ideas»[387].

In un simile scenario la *privacy* risulta minacciata dal traffico indiscriminato dei dati; il pluralismo informativo[388] dal potere economico dei *Big*[389] della Rete, che hanno accesso esclusivo[390] al patrimonio delle informazioni condensate nei dati; le libertà degli utenti limitate da profilazioni sempre più puntuali e analitiche, fonti di nuove forme di discriminazione[391] per le persone; infine il processo democratico è messo in discussione dalla personalizzazione discriminatoria e quindi dalla distribuzione selettiva di contenuti politicamente rilevanti[392] senza che siano chiari i termini di regolazione di questa attività[393].

Tali discriminazioni[394] sono suscettibili di intaccare le libertà di scelta e il diritto all'autodeterminazione[395] informativa degli individui, nonché le fondamenta della democrazia[396]: «safeguarding the democratic process in the context of markets is one of

---

387 J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in *Max Planck Institute for Innovation and Competition Research*, Paper No. 16-16, p. 11, cit.

388 Infatti, la fruizione delle notizie in rete avviene sempre più spesso attraverso intermediari digitali quali *social network* e motori di ricerca che utilizzano i dati personali e possono veicolare informazioni parziali o addirittura *fake news* personalizzate

389 Ci si riferisce ai cd. *Over the top* quali *Facebook*, *Google*, *Apple, Amazon* etc. La Presidente della Camera Laura Boldrini, in occasione della presentazione della Relazione Annuale del Garante Privacy, tenutasi in data 6 giugno 2017, ha affermato che *Google*, *Apple*, *Facebook* e *Microsoft* hanno una capitalizzazione di borsa equivalente al Pil della Francia.

390 I *Big Data* possono tradursi in barriere all'entrata nei mercati o favorire comportamenti restrittivi della concorrenza tali da ostacolare lo sviluppo e il progresso tecnologico. Sia consentito rinviare al *paper* dell'autrice, quantomeno alla parte in cui la titolarità dei dati viene assimilata a una *essential facility*, di carattere immateriale, indispensabile per competere sul mercato: in M. OREFICE, *Big Data: Regole e concorrenza*, in *Politica del diritto,* 4/2016, p. 730 ss.

391 L'articolo 5, comma 7 della Dichiarazione dei Diritti in Internet, approvata dalla Commissione per i diritti e i doveri relativi a Internet e pubblicata il 28 luglio 2015, in *http://www.camera.it/leg17/1179*, vieta espressamente di trattare i dati per finalità anche indirettamente discriminatorie.

392 M. NIJHUIS, *How to call b.s. on big data: a practical guide*, in *http://www.newyorker.com/tech/elements/how-to-call-bullshit-on-big-data-a-practical-guide*, June 3, 2017.

393 O. TENE – J. POLONETSKY, *op. cit.*,p. 270: «we propose that organizations reveal not only the existence of their databases but also the criteria used in their decisionmaking processes, subject to protection of trade secrets and other intellectual property laws».

394 *Ibid.*

395 Si rinvia all'articolo 6 della Dichiarazione dei Diritti in Internet, la prof.ssa De Minico ha sostenuto a più riprese l'importanza del riconoscimento del diritto all'autodeterminazione informativa che ha guidato la stesura dell'articolo. Si leggano, a tal fine, i relativi Resoconti in part. n. 5, pp. 14-15, e n. 9. pp. 37-38.

396 *The Guardian view on big data: the danger is less democracy*, in *The Guardian*, February 26, 2017.

the objectives of the regulation at the interface of competition law and media law in democratic jurisdictions»[397].

Di conseguenza, si rende necessaria una regolazione mirata non solo, da una parte, alla tutela del «consumatore» e, dall'altra, alla tutela della concorrenza, ma anche alla garanzia dei diritti fondamentali, dimensione sostanziale della democrazia[398].

I dati si fanno allora strumento democratico perché i diritti fondamentali e le libertà costituzionali che essi consentono di esercitare in forma più piena, rispetto al passato[399], hanno un radicamento popolare: «si riferiscono al "popolo" nella totalità dei suoi componenti ed esprimono perciò, in capo a ciascuno, un frammento di sovranità. E in questo senso è democratica una costituzione: perché i suoi contenuti, cioè i diritti in essa stabiliti, garantiscono tutti»[400].

Il potere economico rende gli *Over the Top* più forti dei governi, ma in una democrazia non possono esistere zone grigie, tutti i poteri devono rispondere alle istituzioni e alle regole[401].

---

397 J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, p. 11, cit.

398 L. FERRAJOLI, *La democrazia costituzionale*, in *https://revus.revues.org/2291*, p. 16, cit.

399 *Ex multis*: VILLONE M., *La Costituzione e il diritto alla tecnologia*, in DE MINICO G. (a cura di), *Dalla tecnologia ai diritti. Banda larga e servizi a rete*, pp. 257-267; MODUGNO F., *I diritti del consumatore: una nuova «generazione» di diritti?,* in *Scritti in onore di Michele Scudiero*, Napoli 2008, p. 1380 ss, in cui l'autore sostiene che sia per i nuovi diritti sia per i vecchi la volontà del legislatore si precisa nell'attività ermeneutica; CARETTI P., *I diritti fondamentali, Libertà e diritti sociali,* Giappichelli, Torino, 2011, 176; SCAGLIARINI S., *Diritti sociali nuovi e diritti sociali in fieri nella giurisprudenza costituzionale*, relazione al Convegno annuale dell'Associazione "Gruppo di Pisa", *I diritti sociali: dal riconoscimento alla garanzia. Il ruolo della giurisprudenza*, Trapani, 8-9 giugno 2012, in *www.gruppodipisa.it/wp-content/.../ScagliariniDEF.pdf*; MAZZIOTTI M., *Diritti sociali*, in *Enc. dir.,* vol. XII, Milano 1964, p. 804, egli definisce il diritto sociale «l'insieme delle norme attraverso cui lo Stato attua la funzione equilibratrice e moderatrice delle disparità sociali, allo scopo di "assicurare l'eguaglianza delle situazioni malgrado la differenza delle fortune"». Sul legame tra diritti sociali e art. 3, co. II cfr. SCAGLIARINI S. (p. 3, nt. 7 e nt. 9); Cfr. PEZZINI B., *La decisione sui diritti sociali*, Giuffré, Milano, 2001, 122 ss., egli definisce l'art. 3, co. II, Cost., una sorta di clausola generale dello stato sociale (p. 125).

400 L. FERRAJOLI, *Diritti fondamentali e democrazia costituzionale*, Testo rivisto della relazione presentata alle "Primeras Jornadas Internacionales de Derechos Fundamentales y Derecho Penal", Asociación de Magistrados y Funcionarios Judiciales de la Provincia de Córdoba – I.N.E.C.I.P., Córdoba, 10-12 aprile 2002, p. 342, cit.

401 È quanto è stato osservato dalla Presidente della Camera dei Deputati, Laura Boldrini, nel suo discorso, in occasione della presentazione Annuale del Garante *Privacy*. Cfr. con *Relazione Garante Privacy, il discorso di Laura Boldrini 'No allo strapotere degli OTT'*, in *Key4biz*, 6 giugno 2017, reperibile al *link* *https://www.key4biz.it/relazione-garante-privacy-discorso-integrale-laura-boldrini-no-allo-strapotere-google-co/192009/*.

1.1. *Opportunità e rischi nell'utilizzo dei* Big Data

Allo scopo di identificare le nuove categorie giuridiche[402] con cui dovremo operare, i nuovi paradigmi della disciplina *antitrust*, utili a incasellare i nuovi fenomeni e infine i nuovi strumenti regolativi che facciano da argine alle violazioni, sopra accennate, occorre in partenza descrivere brevemente cosa sono i grandi archivi di dati, come funzionano e quali sono i benefici legati al loro uso nonché i rischi connessi al loro possibile abuso.

Nell'era dell'*Internet of Things*[403] le informazioni sono generate in forma di dati (tradotte in numeri) dai dispositivi elettronici connessi a Internet - fissi, mobili o indossabili[404], sensori e *smart machine* – registrate e memorizzate e infine elaborate[405] per una serie indefinita di finalità.

La digitalizzazione delle relazioni e la diffusione capillare di dispositivi intelligenti rendono possibile la registrazione di ogni transazione tra persone e di ogni scambio di merci. Per mezzo di Internet[406] gli esseri umani sono diventati misurabili: non solo lo *smartphone* e il pc, ma persino il frigorifero e la racchetta[407], sono in grado di raccogliere una enorme mole di dati.

---

[402] La professoressa De Minico sostiene che «under pressure from the big data revolution the old categories of the fundamental rights are falling to pieces», in G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?*, in *Blog of the IACL*, AIDC, August, 27, 2017.

[403] Per *IoT* si intende lo spazio virtuale all'interno del quale avviene lo scambio dei dati tra oggetti e l'accesso a informazioni ricevute da banche dati, grazie alla rete Internet. A p. 15 del volume di M. E. STUCKE – A. P. GRUNES, *Big Data and Competition Policy*, New York: Oxford University Press, 2016, *l'Iot* si riferirebbe a come i computer, i sensori e gli oggetti tecnologici interagiscono tra loro e come processano dati, con particolare attenzione ai dispositivi comprati e utilizzati dagli utenti, compresi quelli realizzati per scopi commerciali interni, di monitoraggio, uso elettrico, macchina ad alte prestazioni. *Sullo* stato e sulle implicazioni collegate alla crescente connessione dei dispositivi elettronici si legga il *Report Internet of Things Status and implications of an increasingly connected world*, United States Government Accountability Office Center for Science, Technology, and Engineering Report to Congressional Requesters, may 2017.

[404] Si pensi all'accessorio *Fitbit*, un *fitness tracker* che è in grado di misurare i battiti del cuore e il numero di passi compiuti dalla persona che lo indossa nell'arco della giornata.

[405] Tecnicamente dopo la raccolta e l'elaborazione i dati vanno resi "visualizzabili". La fase di visualizzazione può risultare complessa, per questo servono appositi *software* come *Tableau software*.

[406] Vi accedono 2,5 miliardi di persone ogni giorno, tali accessi a Internet producono un corrispettivo di 2,5 quintilioni di byte di dati.

[407] Come riportato da De Biase in L. DE BIASE, *La miniera dei big data,* in *Nòva lezioni di futuro* de *Il sole 24 ore,* 3 dicembre 2015, p. 30 ss., nel tennis, Rafa Nadel utilizza una racchetta iper-connessa attraverso dei sensori che registrano ogni colpo per valutare quanto sia buona la sua performance e calcolare come migliorarla, e addirittura se e quanto sia gestibile il suo "colpo a effetto" (*top spin*).

Per *Big Data*[408] si intendono dati quantificabili[409] in almeno 100 *petabyte*[410], le informazioni che essi racchiudono descrivono semplici fatti registrati nello svolgimento delle attività quotidiane[411].

Secondo la definizione dell'OCSE[412], i *Big Data* includerebbero tutti quei contenuti che permettono l'identificazione di un individuo (*data subject*): i contenuti generati dagli utenti, inclusi *blog*, foto, video; dati comportamentali, incluso quello che le persone cercano in rete, e guardano su Internet, cosa comprano *online*, quanto spendono e come pagano; i dati sociali, inclusi i contatti degli amici sui *social network*; dati di geolocalizzazione, inclusi l'indirizzo di residenza, il segnale gps, l'indirizzo ip; i dati demografici, inclusi l'età, il genere sessuale, l'orientamento sessuale, le affiliazioni politiche; i dati identificativi ufficiali quali nome, informazioni finanziarie, numero di conto, informazioni sulla salute e così via.

La peculiarità di questi dati sta nel fatto che, rispetto al passato, non sono estrapolati statisticamente da campioni rappresentativi della popolazione, attraverso sistemi complessi, costosi e fallibili, ma da «tutta» la popolazione osservata[413]. La loro quantità prevale sulla loro esattezza, nel senso che non si cerca più la causalità, ma si sfrutta la correlazione senza che desti alcuna preoccupazione il fatto che i dati siano confusi[414]

---

408 La genomica e l'astronomia hanno coniato per prime il termine nel 2000, avendo per prime sperimentato l'esplosione dei dati. L'espressione *big* faceva riferimento al fatto che il volume delle informazioni era divenuto così alto da risultare incompatibile con la memoria dei computer, utilizzata per la processazione. Nascevano così strumenti di analisi come *MapReduce* di *Google* e *Hadoop* di *Yahoo*.

409 Vengono scambiate 2,9 milioni di *e-mail* ogni secondo, 375 *megabytes* di dati consumati da una famiglia ogni giorno, 72,9 oggetti ordinati su *Amazon* ogni secondo, 20 ore di video caricati ogni minuto su *youtube*, 24 *petabytes* di dati processati da *Google* ogni giorno, 50 milioni di *tweet* ogni giorno, 1,3 *exabytes* di dati inviati e ricevuti da dispositivi mobili, 700 miliardi di minuti spesi su *Facebook* ogni mese. I numeri sono destinati a salire se consideriamo che il 60% della popolazione mondiale non ha Internet. Vedi p. 10, infografica di Giorgio Donghi.

410 1 petabyte è un milione di Gigabyte.

411 L'anno di nascita dei *big data* è convenzionalmente il 2010, esattamente quando viene pubblicato un *paper* scientifico di *Google* noto come *Dremel*, in http://tinyurl.com/c8wdacz, il quale spiega come compiere ricerche su milioni di *Gigabytes* di informazioni in frazioni di secondo. Già nel 2004 *Google* testò *MapReduce*, un *framework* per gestire la potenza di calcolo distribuita su grandi moli di dati.

412 OCSE, *Exploring the economics of personal data: a Survey of Methodologies for Mesauring Monetary Value*, in http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en, p. 7.

413 «Che ruolo rimane all'intuito, alla fede, all'incertezza, all'agire in contraddizione con il dato empirico e all'apprendimento dall'esperienza. Con il passaggio progressivo dalla causalità alla correlazione, come possiamo avanzare pragmaticamente senza intaccare le basi stesse della società, dei rapporti umani e del progresso fondato sulla ragione?». V. MAYER-SCONBERGER - K. N.CUKIER, *Big Data. Una rivoluzione che trasformerà il modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013, cit., p. 31.

414 *Dataset* più numerosi offrono un valore così alto che compensa abbondantemente la confusione. La confusione può derivare da un errore nella misurazione da parte di uno dei sensori utilizzati, per esempio, per misurare la

perché l'esattezza, che si perde in termini micro, viene recuperata in termini di comprensione a livello macro[415].

Tali informazioni sono composte da una serie di coordinate: dimensione, complessità e tempo[416], se ciascuna di queste variabili viene collegata al tipo di informazioni che si vogliono approfondire e alla logica del *business*, la stessa restituisce un grafo di conoscenza (*Knowledge graph*) che, raccogliendo più variabili di un'informazione, è in grado di rilevare correlazioni non evidenti[417].

I dati[418], o meglio le decisioni legate ai dati, non hanno valore senza il calcolo automatizzato, basato su logiche algoritmiche[419], cioè senza *software* in grado di estrapolare, gestire e processare le informazioni ivi racchiuse entro un tempo ragionevole. In effetti, i processi decisionali *Big Data driven* aumentano la produttività delle imprese[420] perché gli

temperatura dei vigneti, oppure può riferirsi all'incongruenza della formattazione per cui il dato deve essere ripulito, o ancora la confusione può derivare dalle combinazioni di informazioni provenienti da varie fonti.

415 Volendo applicare il principio di falsificabilità delle teorie scientifiche di K. Popper ai *Big Data* sosterremmo che la scienza dei *Big Data* ha preso il posto del campionamento, utile in una epoca in cui scarseggiavano i dati. Cfr. K. POPPER, in AA.VV., *Filosofia e pedagogia dalle origini a oggi*, vol. 3, p. 615, La Scuola, Brescia,1986 «L'inconfutabilità di una teoria non è (come spesso si crede) un pregio, bensì un difetto. Ogni controllo genuino di una teoria è un tentativo di falsificarla, o di confutarla. La controllabilità coincide con la falsificabilità; alcune teorie sono controllabili, o esposte alla confutazione, più di altre; esse per così dire, corrono rischi maggiori.».

416 Parlano di 4 V (Volume, Varietà, Velocità, Valore) dei *Big Data* Stucke e Grunes a p. 16 del volume citato.

417 L. DE BIASE, *La miniera dei big data*, p. 12.

418 La mera esistenza dei computer non basta a rendere i dati disponibili. È necessaria la "datizzazione", prendere le informazioni su tutto ciò che esiste anche apparentemente inutile, per esempio, sulle vibrazioni di un motore perché serve alla predizione. I *Big Data* modificano la natura del *business,* non più case, terreni, fabbricati e nemmeno *brand* e proprietà intellettuale, ma dati. Le norme a tutela della *privacy*, secondo Viktor Mayer-Schönberger e Kenneth Cukier, nel volume citato, si rivelano inutili, le persone condividono in prima persona le loro informazioni di carattere personale su *facebook, twitter etc* e la condivisione è una forza, non una vulnerabilità. È la fonte dei servizi.

419 Meglio nota come *algorithmic economy. Per questo si dovrebbe considerare il rapporto tra investire tempo e denaro nello sviluppo* degli algoritmi, e investire le stesse risorse nell'ampliamento della raccolta di testo (studio su correttore ortografico di *Banko* e *Brill,* che ha utilizzato 3 algoritmi utilizzando un milione di parole, ha funzionato meglio l'algoritmo peggiore ma con un n. maggiore di dati piuttosto che quello più sofisticato ma con un numero minore di dati, cfr. MAYER-SCHÖNBERGER - KENNETH CUKIER, *op. cit.*, p. 56).

420 R. FELDMANN, M. HAMMER- K. SOMERS, *Pushing manufacturing productivity to the max*, in *http://www.mckinsey.com/business-functions/operations/our-insights/pushing-manufacturing-productivity-to-the-max,* May 2017.

strumenti di *advanced analytics* - come i sistemi di *machine learning* e di *text mining*, analisi semantica e reti neurali[421], nonché ricercatori specializzati[422] - producono profitto.

Alcune imprese stanno addirittura eliminando le posizioni di gestione per sostituirle con i dati[423].

Le informazioni vengono utilizzate principalmente per scopi commerciali: il *data mining*[424] consente di perfezionare il commercio virtuale, ridurre a zero gli errori e le spese inutili, fidelizzare i clienti, personalizzando i singoli prodotti e tenendo traccia del loro comportamento.

Il Rapporto Mc Kinsey[425] ha esaminato i vantaggi economici[426] derivanti dall'impiego dei dati[427], gli analisti hanno studiato una serie di esempi in cui essi si sono mostrati in grado di «creare valore nelle organizzazioni pubbliche e private, nei mercati e nei prodotti e servizi in sette settori dell'economia mondiale: istruzione, trasporti, prodotti di consumo, energia elettrica, gas e petrolio, assistenza sanitaria, credito al consumo»[428].

---

421 Servono altresì investimenti, oggi le aziende italiane catturano solo il 17% della spesa per i *Big Data*. Si aggiunga che servono figure manageriali (come il *Chief Data Officier* , che è il responsabile dei dati all'interno delle aziende, è un membro del *team* manageriale che si occupa della gestione delle funzioni aziendali collegate alla valorizzazione dei dati e il *Data Scientist* che è la nuova figura professionale, oggi molto ricercata - 40.000 negli USA, 825.000 nell'UE entro il 2020 - richiede competenze di statistica, sociologia, matematica e ingegneria) appropriate che sappiano massimizzare il valore dei dati per evitare il propagarsi dei cosiddetti *dark data* cioè dati duplicati inutili e obsoleti.

422 Figure specializzate trasformano le informazioni in azioni di mercato, attraverso la *Big Data analytics*. Secondo il Rapporto *Mc Kinsey* le posizioni ricercate negli Stati Uniti saliranno entro il 2018 a 190.000.

423 I numeri ordinati e intelligenti potrebbero domani sovvertire le gerarchie aziendali. Si pensi che una *startup* americana *Chubbies* che si occupa di abbigliamento affida i poteri manageriali ai suoi dipendenti che hanno accesso ai dati in tempo reale (non hanno un AD), grazie a sistemi di *cloud computing* integrati. Parla di lavoro in «state of flux» Manyika in J. MANYIKA *Technology, jobs, and the future of work*, in *http://www.mckinsey.com/global-themes/employment-and-growth/technology-jobs-and-the-future-of-work*, May 2017. *Contra* si legga B. D'AMICO, *Jobless Society/Non è vero che i robot ci ruberanno il lavoro,* in *il Corriere della Sera*, 29 maggio 2017.

424 M. HILDEBRANDT, *Profiling and the rule of law*, in *Identity in the Information Society*, 1, 1, 2008, pp. 55-70 e T.Z. ZARSKY, *Transparent predictions*, in *U. Ill. L. Rev.*, 2013, 4, pp. 1503-1570.

425 In *http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation*.

426 I benefici sono stati misurati dal Rapporto Mc Kinsey già citato e vanno dai quaranta miliardi ai mille miliardi di dollari l'anno. Gli Stati Uniti potrebbero guadagnare un potenziale di mille miliardi di dollari e l'Europa novecentomila milioni di dollari e il resto dei paesi millesettecento miliardi di dollari. L'impiego dei dati consente di migliorare l'istruzione scolastica, innalzando le competenze dei lavoratori e la produttività, quindi aumentando anche i salari e innescando un circolo virtuoso.

427 Le transazioni es. *Xoom* ha scoperto transazioni illegali analizzandone l'andamento di tutti i dati p. 44; es. scoperti incontri truccati nel sumo, V. MAYER-SCHÖNBERGER - KENNETH CUKIER, *op. cit.*, p. 45. Cfr anche con l'esempio degli scacchi a p. 55.

428 L. DE BIASE, *La miniera dei big data,* p. 14., cit.

L'impiego di modelli predittivi[429] basati su dati statistici e *opinion* della gente semplifica ulteriormente le scelte di mercato[430].

Per comprendere il flusso di benefici, non solo economici, innescato dall'utilizzo dei dati, basti pensare che se conosciamo le preferenze delle persone, attraverso quello che loro dichiarano sui *social network,* per esempio, siamo in grado di comprendere meglio i loro bisogni e possiamo progettare servizi migliori, più efficienti, o migliorare le politiche di governo a beneficio dell'intera comunità. Grazie ai dati si possono conoscere agevolmente le strade più pericolose, i voli più economici, i sindaci più spreconi, le città meno inquinate e di conseguenza si possono prendere decisioni consapevoli e pianificare soluzioni alternative[431].

L'utilizzo di queste informazioni[432], oltre a implementare lo sviluppo economico nel settore pubblico e privato, può migliorare sia la vita di tutti i giorni[433], in termini di qualità, sia facilitare il godimento e l'esercizio dei diritti fondamentali.

Si pensi alla salute pubblica: nel campo della sanità l'impiego dei dati produce esternalità positive perché migliora le diagnosi e le cure. I dati salvati sul *cloud* possono diventare pozzi da cui il medico potrà estrarre dati[434] per fare analogie, diagnosticare una

---

[429]Il *Machine learning* è un apprendimento automatico che consente in tempo reale di estrarre numerosi dettagli (infortuni, squalifiche, propensione offensiva o difensiva di una squadra etc.).

[430] L'agire umano resta sempre imprevedibile, si pensi all'errore commesso dalla predizione errata di *Microsoft* di vittoria in *Champions League* del Real sulla Juventus: L. DE BIASE, *La miniera dei big data,* p. 29. *Bing* aveva predetto correttamente 3 risultati su 4 e per i mondiali del Brasile aveva predetto correttamente 15 risultati su 16.

[431] N. BOBBIO, *L'età dei diritti*, Einaudi, Torino, 1990, p. XV.

[432] Secondo l'*Open Data Index* di *Open Knowledge* (in *https://index.okfn.org/place/*) solo il l'10% delle informazioni mondiali sono disponibili in formato aperto e accessibile a tutti. Il dato fa riferimento alla disponibilità e accessibilità dei dati in dieci aree tra cui finanza pubblica, trasporti pubblici e livelli di inquinamento ed evidenzia la scarsa sensibilità di governi e istituzioni alla trasparenza. Solo due paesi su 97 e cioè Gran Bretagna e Grecia forniscono accesso ai dettagli delle spese di governo. Nel *ranking* 2016 l'Italia occupa il 17° posto.

[433] Nello sport le applicazioni dei dati possono servire a migliorare le *performance* degli atleti o a realizzare modelli predittivi sempre più efficaci, da applicare anche al mercato delle scommesse. Nel calcio precisamente, la Germania di Joachim Löw è stata la prima a utilizzare un sistema costruito sui grandi dati in fase di allenamento e di conseguenza preparare le partite per vincere i mondiali. Ogni *match* produce 60 milioni di dati che analizzati dall'allenatore forniscono particolari dettagliati su ogni calciatore (km percorsi, accelerazioni, passaggi sbagliati, aree più e meno coperte). Così lo "sport agonistico perderebbe il suo *appeal*", così L. DE BIASE, *La miniera dei big data,* cit. p. 30. Cfr. ANDERSON C.-SALLY D., *The numbers Game – why everithing you know about football is wrong,* in cui però gli autori sostengono che il risultato di ogni singola partita è dettato per il 50% dalla fortuna. *Ea sports* è stata l'unica a prevedere la vittoria della Germania mediante simulazione da computer su videogioco (Fifa14). Sono le agenzie di scommessa a ottenere dai *Big Data* il maggiore profitto. Es. l'inglese *Paddy Power.*

[434] Un individuo produce fino a 150.000 miliardi di *Gigabyte* di informazioni.

patologia e individuare la terapia curativa[435]. Tale sistema è in grado di produrre anche un risparmio di spesa di 450 miliardi di dollari l'anno[436].

Tutte queste informazioni possono salvare delle vite umane. In Canada il monitoraggio dei dati[437] ha permesso ai medici di salvare i bambini nati prematuri, è stato osservato, infatti, che, in apparenti condizioni vitali stabili, essi avevano alte probabilità di sviluppare una febbre grave e mortale, nel giorno successivo al parto, così si è potuti intervenire prima. Sempre nel settore sanitario, i dati e cioè le informazioni su frequenza cardiaca, flusso sanguigno e pressione, consentono di simulare la normale funzione cardiaca e migliorare i dispositivi che devono essere impiantati[438]. Per di più, cuori artificiali esterni collegati al cuore con delle cannule hanno salvato numerose vite di pazienti in lista d'attesa per il trapianto, grazie ai dati raccolti. Senza informazioni tutto ciò non sarebbe stato possibile.

Nel campo delle assicurazioni, grazie alla «scatola nera», posta nelle auto, che raccoglie dati, rilevando spostamenti, è possibile profilare gli autisti, che potranno sottoscrivere polizze personalizzate, ma a patto di essere costantemente monitorati.

Nel turismo, la preferenza degli utenti (raccolte da *Trivago* o *Booking*, per esempio) può guidare le offerte e le strategie commerciali[439].

Nell'edilizia i dati possono servire per progettare un'abitazione ecologica: negli Emirati Arabi questi dati sono serviti a progettare edifici «a energia positiva» in grado di autoalimentarsi energicamente.

---

[435] Un programma sviluppato dall'italiano Gianmauro Calafiore, *Loop AI lab solutions*, consente di inserire migliaia di CCE relative a una stessa patologia con lo scopo di ottenere con il *deep learning* la cura da prescrivere sulla base di un confronto per analogia. Steve Jobs si è fatto sequenziare per intero il DNA, i medici così per curare il suo tumore hanno potuto selezionare le terapie in base all'efficacia che avrebbero avuto per la composizione specifica del suo codice genetico. Così quando una cura non era efficace perché il tumore la eludeva potevano impiegare un altro farmaco.

[436] La ricerca è stata condotta da *NetApp*. Uno studio IBM rivela che saranno 4,9 milioni le persone controllate in ambito sanitario entro il 2016.

[437] Ne vengono prodotti mille al secondo.

[438] La dimostrazione è stata fatta dagli Stati Uniti durante l'evento internazionale organizzato da Austin della *National Instruments*. Tutti gli esempi sono presi in prestito a L. De Biase sopra citato.

[439] Cfr. con lo studio condotto da *Skyscanner* e riguardante e viaggi.

Nell'agricoltura, i dati relativi al meteo e le informazioni agronomiche dei singoli vigneti d'interesse, raccolti attraverso appositi sensori (posti su dei droni, per esempio), possono alimentare un sistema di supporto alle decisioni in ambito vinicolo.

Nel settore dei trasporti, a Stoccolma i taxi sono disseminati per tutte le strade della città, qui, sui veicoli sono stati posizionati più di 1.600 gps per raccogliere notizie sul traffico, gestite da appositi *software* al fine di decongestionare la viabilità[440].

L'Università del Michigan ha realizzato una città simulata, con veicoli intelligenti su cui sono stati installati sensori allo scopo di sperimentare l'efficienza comunicativa tra le auto per ridurre incidenti e traffico[441].

Negli aeroporti, l'impiego intelligente dei *Big Data* può ridurre le code ai *check in* oppure migliorare la gestione delle coincidenze e degli scali, implementare la Rete di connessioni a Internet e ridurre i casi di smarrimento bagagli[442].

Ancora, i dati possono essere impiegati per migliorare l'istruzione e le competenze degli insegnanti con forme di apprendimento adattivo, e quindi per creare modelli personalizzati. In Kenya, *Bridge* ha sperimentato approcci all'insegnamento di concetti *standard*, mediante lo svolgimento di due versioni di una stessa lezione (impartita secondo un programma prestabilito e standardizzato) contemporaneamente in un ampio numero di classi. Questo metodo ha consentito di determinare la lezione più efficace. Inoltre, sempre nel settore dell'istruzione, l'osservazione dei progressi degli studenti mediante l'elaborazione dei dati consente di adattare l'insegnamento al singolo, in base al livello di apprendimento degli studenti.

Le informazioni raccolte con le modalità sopra descritte possono addirittura essere utilizzate in politica: nel 2012, Barack Obama ha vinto per la seconda volta le elezioni a Presidente degli Stati Uniti anche grazie ai dati[443]. Gli *spin doctor*[444] di Obama hanno raccolto

---

[440] Il traffico è sceso del 20%, i tempi per gli spostamenti si sono ridotti del 50% e le emissioni diminuite del 10%.

[441] *Mobility Transformation Center.*

[442] A Catania, dove è stato elaborato un *software* (*View* elaborato dalla *Bizmate*) che raccoglie ed elabora dati su voli, passeggeri ed operatività dei *gate* e li incrocia*;* esso ha consentito, grazie a un sistema di allarme integrato, di allertare il personale di servizio per anomalie relative alla sicurezza quale quella verificatasi concretamente e riguardante un passeggero che aveva superato i controlli e stava per salire su un aereo diverso, usando una seconda carta d'imbarco.

[443] Il dipartimento di Analisi matematica della Casa Bianca è diventato 5 volte più grande. Jim Messina, responsabile della campagna elettorale di Obama aveva affidato la responsabilità del dipartimento analisi *big data* a Rayid Ghani, ricercatore della *Silicon Valley*, presso gli *Accenture Labs* prima di dirigere il *Center of Data Science*.

[444] I suoi consulenti di immagine.

dati sugli elettori, tracciando la strategia politica giusta, volta soprattutto a convincere gli indecisi. Le informazioni hanno guidato, in forma meno ortodossa[445], la campagna elettorale di Trump, direzionando al pubblico messaggi elettorali anche microscopicamente diversi (*microtargeting*), ma personalizzati per il singolo elettore[446]. Questi strumenti di analisi sono in grado di capovolgere i risultati elettorali, in danno della sana competizione democratica[447], alterando gli strumenti propri della sovranità popolare[448].

Alexander Nix[449], responsabile della campagna di Trump, ha spiegato che «se vogliamo fare breccia su un'elettrice coscienziosa e nevrotica, converrà mostrargli l'immagine di una rapina in casa, con tanto di mano minacciosa che spacca il vetro e lo slogan "oltre che un diritto, una pistola è un'assicurazione sulla vita" […]; se invece il bersaglio è un tipo tradizionalista, ma ben disposto verso il prossimo, funzionerà meglio la foto di nonno e nipote a caccia, con un *claim* tipo "dal padre al figlio, sin dalla nascita della nostra nazione"»[450]. Similarmente: «a un pubblico di madri, sia casalinghe che in carriera, di età inferiore ai 55 anni, parlavamo di misure di supporto alle famiglie (maternità pagata, agevolazioni fiscali) sostenuto da Donald e Ivanka Trump. A un pubblico di maschi disoccupati provenienti da zone con alto tasso di crisi e fenomeni di decentramento industriale, tipo Wisconsin e Michigan, il messaggio sarebbe ruotato intorno a misure di creazione di nuovi lavori e tassazione sulle società americane che esportano lavori all'estero»[451].

---

445 Cfr. con l'articolo *Se Facebook e i Big Data minacciano la democrazia*, in *www.left.it*, 22 febbraio 2017 e con l'articolo *Nix, il cervello della campagna elettorale di Trump: "Grazie ai big data sappiamo cosa vogliono i cittadini"*, in *La Stampa*, 8 settembre 2016; P. WOOD, *The British data-crunchers who say they helped Donald Trump to win Are Cambridge Analytica brilliant scientists or snake-oil salesmen?*, in *www.thespectator.co.uk*, December 3, 2016.

446 Cfr. con l'articolo *«Così, con i social network, abbiamo fatto vincere Donald Trump»*, in *il Venerdì di Repubblica,* 7 febbraio 2017. Cfr. Anche con l'articolo di R. BOOTH, *Inquiry launched into targeting of UK voters through social media*, in *the Guardian,* May 17, 2017.

447 J. DREXL, *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in *Max Planck Institute for Innovation and Competition Research*, Paper No. 16-16, p. 11 ss.

448 La condotta abusiva del dominante può avere un impatto negativo sulle elezioni, attraverso la manipolazione dei risultati elettorali, dei *search rankings* e quindi coartando le preferenze degli indecisi per i candidati, così Stucke e Grunes nel volume citato a p. 253.

449 Nix è l'amministratore delegato della *Cambridge Analytica*, la succursale americana dell'inglese *Strategic Communication Laboratories*, un'azienda che opera nel settore delle "operazioni psicologiche" e che vanta contratti con il Ministero della Difesa di Sua Maestà, con la NATO e con il Dipartimento di Stato USA.

450 *«Così, con i social network, abbiamo fatto vincere Donald Trump»*, cit..

451 *Ibid.*

La stessa politica governa i *dark post*, annunci *Facebook* visibili solo a destinatari con caratteristiche specifiche, come quella utilizzata per ricordare la *gaffe* della Clinton sui neri «super predatori», indirizzata esclusivamente a un pubblico nero.

Ne risulta un panorama digitale profondamente modificato al punto che il messaggio politico e il candidato alle elezioni diventano un prodotto, il voto è facilmente coartabile perché «è la tua visione del mondo che decide come ti comporterai, non tanto il fatto che tu sia donna o abbia un certo reddito»[452].

Dunque tanti i vantaggi economici e sociali, altrettanti i rischi, collegati al traffico dei dati, per la *privacy*, per i diritti di libertà[453] e per il futuro della democrazia.

Le imprese che possiedono i dati sono in grado di controllare e conoscere anche la vita *offline* degli utenti osservati[454]. *Google* ha spudoratamente dichiarato di avere concluso con alcune aziende esterne per avere accesso ai dati degli acquisti *offline* effettuati dal 70% delle carte di credito statunitensi. Lo scopo perseguito quello di «controllare le transazioni per dimostrare che la pubblicità in rete ha effetti anche sulla vita nella realtà fisica, cosa che le attribuisce un valore ben maggiore di quanto si immagini»[455].

La raccolta indiscriminata di informazioni personali, geolocalizzazioni e preferenze ha sollevato numerose perplessità e preoccupazioni[456], in primo luogo – come precedentemente rilevato – esse sono collegate alle possibili violazioni della *privacy* delle persone, che inconsapevoli dei futuri utilizzi dei loro dati, senza espresso consenso[457], per finalità non meglio specificate, negoziano la loro riservatezza e cedono il flusso informativo che producono ogni giorno, in cambio di servizi su *smartphone* e *tablet*. I *cloud*

---

[452] *Ibid.*

[453] Nella nostra Costituzione, la disciplina dei diritti di libertà, oltre che nei principi fondamentali (art. 1-12) è collocata nella prima parte della Costituzione, che è intitolata Diritti e doveri dei cittadini (art.13-54) e si sviluppa nei titoli dedicati ai "rapporti civili", ai "rapporti etico-sociali", ai "rapporti economici" e ai "rapporti politici".

[454] F.G. SANTORI, *Google spia anche le nostre carte di credito*, 3 giugno 2017, in *http://www.pagina99.it/2017/06/02/Google-carte-di-credito-sorveglianza-controllo-privacy/*.

[455] *Ibid.*

[456] Il 30 maggio 2017, l'Autorità Antitrust, l'Autorità per le Garanzie e nelle Comunicazioni e l'Autorità Garante per la protezione dei dati personali hanno avviato un'indagine conoscitiva congiunta riguardante l'individuazione di eventuali criticità connesse all'uso dei *big data* e la definizione di un quadro di regole in grado di promuovere e tutelare la protezione dei dati personali, la concorrenza dei mercati dell'economia digitale, la tutela del consumatore, nonché i profili di promozione del pluralismo nell'ecosistema digitale.

[457] Cfr. con il primo capitolo della tesi.

provider, che conservano buste paga, *mail*, foto personali controllano dati, anche sensibili[458]. Quando utilizziamo i servizi di *Google* e *Facebook* «accettiamo» di essere monitorati, in questo modo i grandi colossi di Internet utilizzano i nostri profili per fare *business*, e non solo.

Il rischio maggiore è che siano solo i grandi "latifondisti della conoscenza"[459] a trarre benefici economici dai dati e non solo *Google*, *Facebook* e *Microsoft* ma anche le agenzie di sicurezza dei governi in missione antiterroristica[460], o i governi stessi con vocazione autoritaria. Uno scambio inconsapevole e non trasparente non può dirsi equo perché nasconde i fini sottesi alle discriminazioni e agevola tacitamente la deriva autoritaria delle politiche di governo.

In compenso chi decide di farsi osservare, la maggioranza, se non la totalità dei fruitori[461] di Internet, riceve messaggi pubblicitari e contenuti informazionali mirati e parziali, che minacciano la democrazia perché incidono inevitabilmente sul libero agire dei singoli. Se una persona riceve un certo tipo di informazioni, quelle informazioni formeranno la sua personalità e radicheranno i suoi convincimenti, coartando, indirettamente, il suo voto.

Eppure i diritti fondamentali contenuti nei patti sociali rappresentati da costituzioni rigide, come la nostra, e dalle convenzioni internazionali del Novecento, nonché dalle Carte Europee[462] costituiscono «non solo limiti e vincoli giuridici, ma anche programmi politici»[463] e perciò si impongono alla politica quale fonte della sua legittimità democratica.

---

458 Per tali dati il Nuovo Regolamento Privacy 2016/679/UE (cfr. Conss. 10-51-91) richiede un elevato livello di tutela, e per i quali già il d. lgs. 30 giugno 2003, n. 196 richiedeva un maggiore livello di garanzia. Trattasi di categorie particolari di dati, raccolte da sempre più invasive wearable technologies, che già solo in potenza possono generare disparità di trattamento, in L. CALIFANO – C. COLAPIETRO (a cura di), *op. cit.*, *passim*.

459 D. PEDRESCHI, *Il compromesso tra dati e libertà*, in *Nòva - Il sole 24 ore*, 1 marzo 2015, cit..

460 Per un approfondimento sull'appropriato punto di equilibrio tra il pericolo del terrorismo e i valori costituzionali si rinvia al volume di G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016; ID., *Le libertà fondamentali in tempo di ordinario terrorismo*, in www.federalismi.it, n. 10, 20 maggio 2015; ID., *Internet and fundamental rights in time of terrorism*, in *Rivista AIC*, 4/2015, 6 novembre 2015.

461 L'espressione è ricercata perché vuole evidenziare che l'utilità dell'utilizzo di Internet sta proprio nella fruizione di servizi che chiedono in cambio dati. È evidente che colui che naviga è principalmente interessato ai servizi su Internet.

462 Carta dei diritti fondamentali dell'Unione Europea, firmata a Nizza, 2000, in http://www.europarl.europa.eu/charter/pdf/text_it.pdf.

463 L. FERRAJOLI, *Diritti fondamentali e democrazia costituzionale*, p. 342, cit.

Il legislatore dovrebbe intervenire nel rispetto dei vincoli garantisti propri del costituzionalismo democratico per regolare i nuovi fenomeni orientando la tecnica[464], a favore di tutti.

Questo tipo di intervento eteronomo dovrà tenere conto di chi è già in posizione di dominanza e intende rafforzarla, o lo sta già facendo, sui nuovi scenari tecnologici per moltiplicare il suo iniziale vantaggio politico-economico.

Proprio per questo, la regolazione si fa necessaria: quando «l'aumento del potere dell'uomo sull'uomo, che segue inevitabilmente al progresso tecnico crea nuove minacce alla libertà dell'individuo oppure consente nuovi rimedi alla sua indigenza»[465]. Essa dovrà declinare i cambiamenti a favore dell'eguaglianza, della regola della concorrenza[466] e piegarli ai bisogni dei più deboli, offrendo loro un'occasione di effettiva inclusione politica per compierne la dimensione costituzionale di individui come annunciata negli artt. 2 e 3, comma 2, Cost..

Il metodo del *policy maker* in una democrazia costituzionale, impone un dialogo incessante tra le libertà e il potere costituito, e questo scambio dialettico dovrà essere una delle chiavi di lettura dei nuovi fenomeni, «utile per vivere la tecnica, non nella dimensione minimale di consumatori-utenti distratti dai benefici economici della Rete, ma da cittadini consapevoli nell'esercizio dei diritti fondamentali»[467].

Da ciò deriva che i valori costituzionali, come anticipato, dovranno essere il limite all'agire di ogni maggioranza e le precondizioni per un effettivo e autentico esercizio di essa, vincolo per lo stesso potere sovrano del popolo[468].

---

464 E. CHELI, *Scienza, tecnica e diritto: dal modello costituzionale agli indirizzi della giurisprudenza costituzionale*, in *Rivista AIC*, 1/2017.

465 N. BOBBIO, *L'età dei diritti*, Einaudi, Torino, 1990, p. XV.

466 G. GHIDINI - E. AREZZO, *La prospettiva costituzionale della tutela della concorrenza*, in *Giur. comm.*, I, 2012, pp. 464 ss.

467 G. DE MINICO, *Antiche libertà e nuova frontiera digitale*, Giappichelli, Torino, 2016, p. 2.

468 In altre parole il singolo per definizione non può rinunciare ai diritti inviolabili in quanto tali, perché essi non sono trasferibili. Aggiungi dottrina su diritti inviolabili.

Dunque, la regolazione del "fenomeno dei *Big Data*" non può sottrarsi a questo tipo di valutazioni in uno «Stato di diritto»[469], strumento essenziale, insieme al riconoscimento della democrazia pluralista, per la garanzia dei diritti fondamentali[470].

2. Il radicamento costituzionale dei *Big Data*: nocciolo duro dei diritti fondamentali

Se nei diritti costituzionali possiamo rinvenire il basamento della democrazia costituzionale perché essi rappresentano lo strumento di «permanente e costante salvaguardia della sovranità popolare»[471], allora i *Big Data*, in quanto facilitatori dei diritti fondamentali, ma anche inevitabilmente delle loro possibili violazioni, sono strumentali al quotidiano esplicarsi della sovranità.

«Internet ha generato nuove declinazioni di diritti acquisiti e forse nuovi diritti, e dunque, per converso, ha generato aree di non libertà». Una ridefinizione potrebbe essere richiesta dall'avvento di Internet nei diritti[472], ma la stessa non dovrebbe essere isolata dai diritti fondamentali «analogici» perché rischierebbe, da un lato, di essere superflua e ridondante, dall'altro, di non cogliere le aree di non libertà generate dal nuovo mezzo.

I diritti al tempo di Internet[473], alcuni dei quali enucleati[474] nella Dichiarazione dei diritti in Internet italiana, sono sì premessa indispensabile per un'efficace tutela dei diritti fondamentali nell'era tecnologica, ma non necessitano di una puntuale descrizione delle

---

469 J. CHEVALLIER, *L'État de droit*, Paris, 2010, p. 112 ss.

470 R. BIN, *Stato di diritto*, in www.robertobin.it, p. 16.

471 L. FERRAJOLI, *La democrazia costituzionale*, Il Mulino, Bologna, 2016, p. 50, cit.

472 C. BLENGINO, *Non i diritti in Internet ma Internet nei diritti*, in O. POLLICINO – M. BASSINI (a cura di), *Verso un Internet Bill of Right,* p. 43 ss.

473 Sono gli stessi diritti fondamentali ad essere tutelati, benché al tempo di Internet.

474 Una puntuale enucleazione di diritti già scritti seppure ridimensionati per via del mezzo che li incorpora rischia di essere impossibile perché un simile tentativo finirà per tralasciare il possibile sviluppo della libertà. Sarebbe inutile reiterare principi e valori già scritti da testi costituzionali e fonti di diritto internazionale, a meno che sia previsto il conferimento di carattere internazionale – o "sovranazionale" a questi diritti, nei termini di una Dichiarazione che possa integrare la Dichiarazione Universale dei Diritti dell'Uomo del 1948 e dai Patti internazionali del 1966.

nuove modalità di godimento e dei nuovi sviluppi delle vecchie libertà, perché essi sono desumibili da una lettura evolutiva della nostra Costituzione.

Si vuole dire che una qualsivoglia Dichiarazione dei diritti su Internet, il cui valore è elevato a servizio pubblico dal Consiglio d'Europa[475], non deve considerarsi esaustiva perché in essa non possono consumarsi tutte le possibili forme di esercizio delle libertà, in continua evoluzione e le cui radici sono piantate nella Costituzione. Inoltre, essa appare destinata a essere documento programmatico e quindi regolata tra le fonti di *soft law*, con una mera funzione di *moral suasion*[476].

Si pensi, invece, che la tutela cogente della libertà di manifestazione del pensiero scritta nell'articolo 21, Cost. copre non solo la creazione, la diffusione e la fruizione delle informazioni e delle idee, a parità di condizioni, ma riconosce oltre che un diritto di accesso a Internet[477], quindi già esistente sotto forma di *hard law*[478], un diritto di accesso ai *Big Data*[479].

Il primo diritto si inserisce nelle pieghe del primo comma, nella parte in cui l'art. 21, superando lo strumento della stampa tipografica[480], stabilisce che «tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione», qui, l'espressione «ogni altro mezzo di diffusione» prescrive la garanzia dell'accesso al nuovo mezzo e ai servizi che esso offre, di modo che ciascuno possa veicolare il proprio pensiero, rivolgendosi a un pubblico più ampio di quello raggiungibile dallo stampato; il secondo, nella previsione di una manifestazione «libera» del pensiero,

---

475 Raccomandazione CM/Rec(2007)16 del COMITATO DEI Ministri agli Stati Membri relativa alle misure volte a promuovere il valore di servizio pubblico di Internet.

476 M. BASSINI, *Le tecnologie avanzano, le norme passano ma le costituzioni rimangono*, in O. POLLICINO – M. BASSINI (a cura di), *op. cit.,* p. 21, cit.

477 Per un approfondimento sul tema, si legga: F. BORGIA, *Riflessioni sull'accesso ad Internet come diritto umano*, in *La Com. Intern*., 2012; P. COSTANZO, *Miti e realtà dell'accesso ad Internet (una prospettiva costituzionalistica)*, in P. CARETTI (a cura di), *L'informazione. Il percorso di una libertà*, vol. II, Passigli, 2012; G. DE MINICO, *Uguaglianze e accesso a Internet*, in *Forum di Quaderni costituzionali*, 6 marzo 2013; T. E. FROSINI, *Il diritto costituzionale di accesso a Internet,* in *AIC*, n. 1/2011; P. PASSAGLIA*, L'accesso ad internet è un diritto,* (Nota a Conseil Constitutionnel de France 10 giugno 2009, n. 580), in *Il Foro italiano*, 2009; R. PISA, *L'accesso a Internet: un nuovo diritto fondamentale?*, in Treccani.it, 07/01/2010; J. RIFKIN, *L' era dell'accesso. La rivoluzione della* new economy, Mondadori, 2001; P. TANZARELLA, *Accesso a Internet: verso un nuovo diritto sociale?*, Relazione al Convegno annuale dell'Associazione "Gruppo di Pisa", "I diritti sociali: dal riconoscimento alla garanzia: Il ruolo della giurisprudenza", Trapani, 8-9 Giugno 2012;

478 P. COSTANZO, *Miti e realtà dell'accesso ad Internet*, in *Giur. Cost.*, 2012, p. 4 ss.

479 C. BLENGINO, *op. cit.,* p. 43 ss.

480 Seppure difesa minuziosamente.

che presuppone ed esige una conoscenza completa e funzionale alla piena informazione e alla partecipazione consapevole alla società, oggi condensata nei *Big Data*.

Una lettura restrittiva dell'articolo svilirebbe tutto il suo potenziale e moltiplicherebbe le discriminazioni tra chi ha accesso al patrimonio informativo dei dati - che diviene anche materia prima per il soggetto che decide di perseguire un fine economico *ex* art. 41, Cost. - e chi no.

Il diritto scritto nell'articolo 21 è diventato il diritto di ciascuno di partecipare alla società dell'informazione, di informare, di informarsi e di formarsi liberamente e consapevolmente con contenuti neutrali che circolano sulla Rete. Questo diritto, che è scritto anche nelle Carte internazionali dei diritti[481], e che include secondo una lettura estensiva, quello di accesso ai dati, intesi come patrimonio informativo comune[482], si interseca con il principio di uguaglianza, che è il filo conduttore delle libertà in Rete.

L'eguaglianza giuridica è l'uguale sottoposizione alla legge, ma anche l'eguale garanzia dei diritti e rappresenta la direzione, il fine ultimo cui tendono le libertà[483].

Di conseguenza, la libertà di espressione diventa anche tutela della neutralità della Rete, «da intendersi come il diritto di ogni persona che i dati che trasmette e riceve in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale legittime scelte delle persone»[484] ed esige un pluralismo informativo, la tutela della concorrenza e, come a più riprese anticipato, della libertà d'impresa, *ex* art. 41[485].

---

481 Dichiarazione universale dei diritti dell'uomo (1948), art. 19; Patto sui diritti civili e politici (1966), art. 19; CEDU (1950), articolo 10; TUE, art. 6,§§ 1-2 TUE; Carta dei diritti fondamentali dell'Unione Europea (2000), artt. 11 § 2, 42.

482 E. OSTROM, *Governare i beni collettivi*, Venezia, Marsilio, 2006, *passim*; P. BARNES, *Capitalismo 3.0*, Egea Università Bocconi editore, Milano, 2006, *passim*; C. HESS - E. OSTROM - P. FERRI - I. KATERINOV (a cura di), *La conoscenza come bene comune. Dalla teoria alla pratica*, Mondadori, Milano, 2009, *passim* e J. STIGLITZ, *Knowledge as a Global Public Good, New York*, Oxford University Press, 1999, *passim*.

483 P. CARETTI, *L'eguaglianza da segno distintivo dello Stato costituzionale a principio generale dell'ordinamento comunitario*, in P. CARETTI – M.C. GRISOLIA, *Lo Stato costituzionale. Scritti in onore di Enzo Cheli*, il Mulino, Bologna, 2011, p. 513 ss.

484 L. NANNIPIERI, *Sulla bozza della Dichiarazione dei diritti in Internet*, in O. POLLICINO – M. BASSINI (a cura di), *Verso un Internet Bill of Right,* p. 61, cit.

485 La lettura congiunta dei due articoli è suggerita dal Tar del Lazio nell'ordinanza 25 giugno 2014 sul Regolamento A.G.Com..

La Corte Costituzionale già nel 1972, nella sentenza n. 105, metteva in evidenza la «coessenzialità»[486] della libertà di espressione del pensiero con la libertà d'impresa e con la forma di stato democratico[487], al punto che l'articolo 21 sarà poi definito dalla stessa Corte «pietra angolare della democrazia»[488].

La forma di stato democratico implica «una pluralità di fonti di informazione, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei alla circolazione delle notizie e delle idee»[489]. Queste esigenze rimangano invariate nella finalità, ma non nei mezzi, tant'è che esse richiedono oggi, l'accesso non solo a Internet ma anche ai dati. Le utilità offerte dal mezzo sono interdipendenti dalle informazioni contenute nei dati.

Il profilo passivo della libertà contenuta nell'articolo 21 si pone a tutela del singolo, fruitore di contenuti, il profilo attivo a tutela dei *players*, che operano sulla Rete per assicurare che le informazioni immesse sul mercato contribuiscano alla crescita dello stesso continuando a «stimolare la corretta competizione e crescita in un contesto democratico»[490], senza distorsioni al gioco della concorrenza.

Dunque, i dati sono informazioni e la loro conoscenza diviene non solo la precondizione dell'esercizio della libertà di espressione per fini informativi, ma anche il carburante dell'economia dell'informazione[491] perché essi generano conoscenze nuove, più analitiche rispetto al passato, profitti maggiori perché mirati al conseguimento di specifici obiettivi, anche punto di avvio di attività di utilità e interesse sociale[492] nonché fonte di servizi propedeutici al godimento di altri diritti fondamentali[493], per citarne solo uno si pensi alle applicazioni dei dati nei servizi sanitari e conseguentemente nel soddisfacimento del diritto alla salute[494].

---

[486] C. BLENGINO, *op. cit.,* p. 47, cit.

[487] ID., *ibid.*

[488] Corte Costituzionale, sentenza del 30 maggio 1977, n. 94.

[489] Corte Costituzionale, sentenza del 15 giugno 1972, n. 105.

[490] L. BELLI, *Non i diritti in Internet ma Internet nei diritti*, in O. POLLICINO – M. BASSINI (a cura di), *op. cit.,* p. 37 cit.

[491] Se si può misurare un fenomeno lo si può conoscere. Sono i dati a rendere gli algoritmi più efficaci Il carburante per l'avvio di attività economiche.

[492] Cfr. articolo 41 e articolo 118.4, Cost.

[493] Cfr. con P. CARETTI – G. T. BARBIERI, *I diritti fondamentali. Libertà e diritti sociali*, Giappichelli, Torino, 2017, p. 537 ss.

[494] Cfr. con le possibili applicazioni dei *Big Data* alla telemedicina, ampiamente descritte nel *sub* § 1.1.

Allora, queste enormi quantità di dati veicolano il più generale diritto alla dignità della persona umana, cuore pulsante dell'articolo 2, Cost., che anima l'intero ordinamento e di cui la libertà di espressione del pensiero è «diretta emanazione»[495].

L'impegno contenuto nell'art. 3, comma 2 si applicherebbe all'accesso ai *Big Data* sopra descritti nel senso che la Repubblica dovrà intervenire per eliminare quegli ostacoli, quali le asimmetrie informative[496] e quindi l'accesso esclusivo ai dati[497] che limitando di fatto la libertà e l'eguaglianza dei cittadini - perché i contenuti forniti sono discriminatori - impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti all'organizzazione politica, economica e sociale del Paese.

Parallelamente, l'articolo 15[498] esigerà l'oscuramento e la cd. «data minimization»[499] di tutti i dati personali, soprattutto sensibili, i quali già solo in potenza possono generare

---

[495] C. BLENGINO, *op. cit.,* p. 47, cit.

[496] European Commission, "*Online* Platforms and the Digital Single Market Opportunities and Challenges for Europe" (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, May 25, 2016 COM(2016) 288), 13, *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0288*. Cfr. Anche con UK Competition and Markets Authority (CMA), "*Online* Platforms and the EU Digital Single Market" (written evidence, (OPL0055), CMA, London, October 23, 2015), *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-internal-market-subcommittee/online -platforms-and-the-eu-digital-single-market/written/23391.html*. «To the extent that such data is of central importance to the offering but inaccessible to competitors, it may confer a form of 'unmatchable advantage,' making it hard for those competitors to compete»; Organization for Economic Co-operation and Development (OECD), Committee for Information, Computer and Communications Policy, "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by 'Big Data,"' (Paris: OECD, Directorate for Science, Technology and Industry, June 18, 2013), *http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2012)9/FINAL&docLanguage=E*n. «Data are a core asset that can create significant competitive advantage and drive innovation, sustainable growth, and development.»; O. TENE – J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Nw. J. Tech. & Intell. Prop.*, vol 11, n. 5, 2013, p. 255, cit.: Yet those transactions appear to take place in an inefficient market hampered by steep information asymmetries, which are further aggravated by big data. Transacting with a big data platform is like a game of poker where one of the players has his hand open and the other keeps his cards close. The online company knows the preferences of the transacting individual inside and out, perhaps better than the individual knows him or herself. It can therefore usurp the entire value surplus available in the transaction by pricing goods or services as close as possible to the individual's reservation price.

[497] Blengino suggerisce tale soluzione per l'accesso a Internet, ma a differenza dell'autore citato non si ritiene che sia necessaria una riscrittura dei diritti costituzionali nelle società dell'informazione del XXI secolo, cfr. ID., *op. cit.,* p. 47 ss.

[498] Cfr. con artt. 4 e 5 della Dichiarazione dei diritti in Internet. Si precisa che il problema non è nuovo: già la letteratura degli anni 70 parlava di rischio di profilazione in S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973, p. 16, cit.

[499] Ne parlano O. TENE – J. POLONETSKY, *op. cit.,* p. 259: «Organizations are required to limit the collection of personal data to the minimum extent necessary to obtain their legitimate goals. Moreover, they are required to delete data that is no longer used for the purposes for which they were collected and to implement restrictive policies with respect to the retention of personal data in identifiable form». E a p. 260: « in a big data world, the principle of data minimization should be interpreted differently, requiring organizations to de-identify data when

disparità di trattamento. La forza precettiva di questi articoli ramificati e comunicanti, per mezzo dell'articolo 3, non può essere affidata alla buona volontà dell'interprete o di una carta programmatica perché la Costituzione detta i nuovi diritti e disegna oltre alle caratteristiche del mezzo, la titolarità dei *Big Data* in capo a tutti, nel *set* di garanzie già scritte, è proprio la sua elasticità e cogenza a richiedere l'intervento positivo del legislatore sovranazionale, stante l'a-territorialità della Rete, affinché i nuovi fenomeni si spieghino nella piena attuazione dei diritti.

In questo senso i *Big Data* diventano il nuovo nocciolo duro delle libertà fondamentali, ma si tratta di un nucleo bifronte: da un lato la loro conoscenza è precondizione per l'esercizio delle libertà fondamentali, in questo senso l'accesso ai *Big data* deve dare all'internauta «tutto quello e proprio quello che egli avrebbe diritto di conseguire»[500] perché l'accesso ai dati è strumentale all'esercizio delle libertà come sopra definite; dall'altro i *Big Data* rappresentano l'intimità più profonda della persona, in grado di rivelare informazioni sull'individuo riservate, che in quanto tali devono essere protette, anonimizzate e minimizzate in modo che la persona cui si riferiscono non sia identificabile.

La garanzia dell'accesso ai dati, come quella della neutralità è strumentale a un fine: quello di permettere il pieno godimento dei diritti fondamentali degli utenti di Internet.

E se un diritto per essere effettivo deve essere suscettibile di azione in giudizio, esso deve essere esercitabile, con la fornitura dei mezzi adatti al fine[501]. Qui il mezzo ha un'entità immateriale: è rappresentato dai *Big Data*.

---

possible, implement reasonable security measures, and limit uses of data to those that are acceptable from not only an individual but also a societal perspective».

[500]Si prendono in prestito al Chiovenda le parole riferite al processo, secondo l'autore esso per quanto possibile «*deve dare al titolare del diritto tutto quello e proprio quello che egli avrebbe diritto di conseguire*», sulla base del diritto sostanziale ai fini dell'effettività dell'art. 24, in virtù del quale il processo è strumentale al diritto sostanziale. Cfr. CHIOVENDA G., *Principi di diritto processuale civile*, Jovene, Napoli, 1912 (ristampa inalterata, Napoli, 1965), p. 81, cit..

[501] La nostra Corte Costituzionale (CORTE COSTITUZIONALE sentt. nn. 48/1964 e 225/1974 e 112/1993. In dottrina, in senso adesivo: BARILE P., *Libertà di manifestazione del pensiero*, in *Enc. Dir.*, XXIV, 1974, p. 424 ss., nonché ESPOSITO C., *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Giuffrè, Milano, 1958, p. 26) aveva *illo tempore*, seppure con riferimento alla pretesa di accesso al mezzo radiotelevisivo, riconosciuto, nella protezione della libertà di espressione, l'"indispensabile strumentalità" tra il diritto e l'accesso allo strumento essa aveva ritenuto l'accesso al mezzo fase antecedente necessaria alla realizzazione della libertà. Similmente il *Conseil Constitutionnel* (CONSEIL CONSTITUTIONNEL, *Décision n. 2009-580 DC*, del 10 Giugno 2009, in *AJDA*, 2009, p. 1132 o in *http://www.conseilconstitutionnel.fr/conseilconstitutnel/francais/lesdecisions/accespardate/decisionsdepuis1959/2009/2009580dc/decisionn2009580dcdu10juin2009.42666.html*), *Cons.a* n. 11-16) ha riconosciuto il nesso di strumentalità, soprattutto quando l'accesso al mezzo sia prodromico al risultato perché «*soprattutto con i diritti emergenti è evidente che la struttura*

È chiaro che una Rete ubiqua si presta da un lato a potenziali violazioni della riservatezza delle comunicazioni e dall'altra alla concentrazione del potere in capo a pochi operatori privati.

Allo stesso tempo, la subordinazione a intermediari privati al fine di accedere ai contenuti di Internet e di utilizzare qualsivoglia tipo di servizio fa sì che la regolazione contrattuale definita da tali intermediari attraverso le condizioni generali del contratto non negoziabili – incida direttamente sui diritti dell'utente. Il comportamento del privato, tenderà alla massimizzazione del profitto e alla stesura di regole generali orientate in tal senso, piuttosto che verso la massimizzazione dei diritti fondamentali dell'utente[502].

«If you're not paying for it, you're not the customer; you're the product. The exclusion of individuals from the benefits of the use of their data manifests in two main ways. First, *online* interactions are barter-like transactions where individuals exchange personal data for free services. Yet those transactions appear to take place in an inefficient market hampered by steep information asymmetries, which are further aggravated by big data. Transacting with a big data platform is like a game of poker where one of the players has his hand open and the other keeps his cards close. Second, organizations are seldom prepared to share the wealth created by individuals' personal data with those individuals»[503].

In questo mosaico di norme costituzionali la tutela della concorrenza, di cui all'art. 117, secondo comma, lettera e), Cost., ne rappresenta il *fil rouge*.

Essa «non ha solo un ambito oggettivamente individuabile che attiene alle misure legislative di tutela in senso proprio, quali ad esempio quelle che hanno ad oggetto gli atti e i comportamenti delle imprese (che incidono negativamente sull'assetto concorrenziale dei mercati e ne disciplinano le modalità di controllo), ma, dato il suo carattere "finalistico", ha anche una portata più generale e trasversale, non preventivamente

---

del diritto si intreccia con la tecnologia». (VILLONE M., *La Costituzione e il "diritto alla tecnologia"*, cit., a p. 261; ma anche RODOTÀ S., *Una Costituzione per Internet?*, in *Pol. Dir.*, 3, 2010, in part. a p. 348).

502 L. BELLI, *op. cit.,*. 38.

503 O. TENE – J. POLONETSKY, *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Nw. J. Tech. & Intell. Prop.*, vol 11, n. 5, 2013, p. 255, cit..

delimitabile, che deve essere valutata in concreto al momento dell'esercizio della potestà legislativa sia dello Stato che delle Regioni nelle materie di loro rispettiva competenza»[504].

Per una tutela efficace - proprio perché i vecchi rimedi si sono rivelati carenti perché riferiti a un mezzo i cui effetti erano limitati nello spazio - è necessario, si ribadisce, che intervenga il legislatore sovranazionale, con norme speciali, che partendo dai diritti fondamentali universalmente riconosciuti[505], rivedano il diritto *antitrust* e la tutela dell'utente in Rete, alla luce dei cambiamenti tecnologici per definire i nuovi mercati rilevanti, su cui operano gli *Over the Top*; le responsabilità e rimedi più opportuni al ripristino della situazione *quo ante*.

3. *Big Data*, *privacy* e *Competition policy*

«Big Data is neither inherently good, evil, nor neutral. Its social value depends, among other things, on the industry and the purpose and effect of the data-driven strategy. Ultimately competition policy can play a key role in ensuring that citizens get the benefits of a data-driven economy, and in minimizing its risks»[506].

La crescita della *data driven economy* e il fatto che le imprese investano grandi somme di denaro per sviluppare applicazioni sempre più utili per gli utenti, senza chiederne agli utilizzatori il prezzo, evidenzia il fatto che i dati sono remunerativi e danno un enorme vantaggio competitivo[507] a chi li possiede mediante il *targeted online advertising*, l'*online search*, il *social networking* e i *software products*[508]. Se così non fosse i *players* della Rete non

[504] Corte Costituzionale, sentenza del 21 aprile 2011, n. 150.

[505] Dichiarazione universale dei diritti dell'uomo (1948), art. 19; Patto sui diritti civili e politici (1966), art. 19; CEDU (1950), articolo 10; TUE, art. 6,§§ 1-2 TUE; Carta dei diritti fondamentali dell'Unione Europea (2000), artt. 11 § 2, 42.

[506] M. E. STUCKE – A. P. GRUNES, *Big Data and Competition Policy*, p. 2, cit..

[507] ID., *ivi*, p. 36 ss.; p. 155; 201; 324 ss.

[508] ID., *ivi*, p. 37.

spenderebbero denaro per raccogliere, conservare, indicizzare e analizzare il crescente volume dei dati[509], donando generosamente servizi costosi.

I *Big Data,* che altro non sono che i dati personali degli utenti, costituiscono un *critical key input*[510] per le imprese, che consente loro di guidare innovazione e crescita, non certo per merito, ma solo perché il dato fa da carburante al costante sviluppo dei servizi offerti e rappresenta la fonte remunerativa degli investimenti, finalizzati a perfezionare i servizi, offerti alla collettività gratis, e a finanziare altri progetti remunerativi come quelli sull'Intelligenza Artificiale[511].

Le fusioni[512] giocano un ruolo fondamentale nell'utilizzo dei dati perché consentono la loro concentrazione: si pensi alle fusioni *Google-Waze*; *Tom Tom-Tele Atlas, Facebook* e *Whatsapp*. I dati si sommano velocemente, il loro volume aumenta, la loro varietà e il loro valore si moltiplicano[513] perché dalla loro combinazione vengono fuori nuove comprensioni, reimpiegate nel circuito economico per fini lucrativi.

Per questo, le imprese hanno interesse economico a non aprire i dati ai concorrenti e sono contrari a politiche di portabilità dei dati[514], le quali favorirebbero un benessere teso alla promozione dell'innovazione e incentiverebbero la concorrenza tra imprese che intendono offrire ai consumatori il controllo e la visibilità dei propri dati. La possibilità di migrare i dati aumenterebbe la domanda dei *data agents* e aiuterebbe gli individui a comprendere e apprezzare il valore dei loro dati e quindi a chiedere maggiori garanzie ai collezionatori. Le imprese competerebbero anche lungo la dimensione *privacy*, a vantaggio

---

509 ID., *ivi*, p. 35 ss.

510 OCSE, *Data-Driven Innovation for Growth and Well-Being: Interim Synthesis Report*, October 2014, p. 11. Cfr. anche M. E. STUCKE – A. P. GRUNES, *op. cit.*, p. 277. Gli autori parlano di *data-opoly*.

511 «Alphabet has leveraged all the data harvested from its users to build advanced services, many of them based on artificial intelligence, that can be sold to governments and corporations. Here, it is Alphabet's scale that makes the difference. Given how much data it already possesses and the services it has built with it, it will be far ahead of the competition in the race to identify malicious cyberattacks, find a cure for cancer or slow down ageing. Armed with advanced data-intensive products and services, Alphabet can sell them like any normal company – the "new economy", with its promise of free stuff, be damned». Così E. MOROZOV, *To tackle Google's power, regulators have to go after its ownership of data*, in *The Guardian*, July 2, 2017.

512 Per un'attenta analisi *antitrust* delle fusion si rimanda al volume citato di M. E. STUCKE – A. P. GRUNES a p. 69 ss.

513 Si parla di 4 V dei dati (volume, velocità, varietà e valore) in M. E. STUCKE – A. P. GRUNES., *Op. cit.*, p. 16 ss.

514 M. E. STUCKE – A. P. GRUNES, *op. cit.*, p. 38.

del gioco della concorrenza: sul mercato sarebbero disponibili prodotti di qualità crescente rispetto a un unico prodotto con una politica *privacy* invasiva.

L'obiettivo delle imprese è invece proprio quello di mantenere il vantaggio competitivo delle strategie *data driven* mediante *tying contracts*[515] e altre pratiche escludenti che impediscono alle altre imprese il raggiungimento di un *minimum efficient scale*, pratiche con le quali le imprese mantengono o conseguono potere di mercato, creano barriere all'ingresso e riducono la qualità del prodotto e il conseguente benessere del consumatore. Così esse possono avviare pratiche scorrette come ingannare le persone sulla loro *privacy policy* abbassandone la garanzia.

L'inganno di per sé non è una violazione *antitrust* ma lo diventa quando è ragionevolmente capace di contribuire significativamente a mantenere o creare potere di monopolio.

Alcune aziende tecnologiche, per mantenere il loro dominio, avranno forti incentivi per sviluppare strategie anticoncorrenziali e per impedire ai rivali di accedere ai dati (ad esempio attraverso accordi di esclusività con i fornitori di terze parti)[516] falsando il gioco della concorrenza; per esempio precludendo le opportunità ai rivali di procurarsi dati simili, ovvero rendendo più difficile per i consumatori l'adozione di altre tecnologie o piattaforme. In questo senso i dati diventano *core economic asset*[517].

La risorsa critica nei mercati multiversante[518] è rappresentata dai dati: essi non consentono solo di «targetizzare» gli utenti per fini pubblicitari, ma anche di ottimizzare prodotti e servizi, monetizzando i dati. Le imprese che hanno un vantaggio competitivo nelle cosiddette 4 V dei *Big Data* (Volume, Velocità, Varietà e Valore) non sono solo nella condizione di dominare i loro stessi settori, ma anche di estendere la dominanza ad altri e abusarne[519].

---

515 *Infra* nota 624.

516 *Infra* § 5.

517 Si citano i documenti OCSE, *Supporting Investement in Knowledge Capital, Growth and Innovation,* 10 ottobre 2013, p. 319; OCSE, *Data Driven Innovation,* p. 10; OCSE, *Exploring the economics of personal data*, p. 4. Parla di *key competitive asset* l'UK Competition and Market Authority, *The Commercial Use of Consumer Data: report on the CMA's Call for Information*, CMA 38, Giugno 2015.

518 Non può essere considerate solo il versante dei prodotti gratis ma anche quelli remunerativi della pubblicità e dei dati. ID., *ivi*, p. 116.

519 ID., *ivi*, pp. 123-124.

Ma vi è di più, perché questo «reality mining»[520] permette ai dominanti di raccogliere finanche informazioni politiche sugli elettori[521].

Basti pensare che il 20 giugno scorso Christ Vickery, un analista di *ciyber security* di *Upguard*, ha scoperto quella che, secondo la *Bbc*, sarebbe la più grande violazione di dati elettorali negli Stati Uniti. La *Deep Root Analytics* avrebbe pubblicato accidentalmente i dati sensibili (data di nascita, indirizzo, numero di telefono, idee religiose, opinioni personali sulla legge sulle armi e sull'aborto, pregiudizi etnici e politici) di quasi duecento milioni di americani, raccolti per influenti organizzazioni politiche repubblicane, con lo scopo di profilare gli elettori[522].

Tali informazioni sono state estrapolate, a insaputa degli utenti, da diverse fonti: dai *social network* ai comitati di raccolta fondi per il partito repubblicano e sarebbero tuttora disponibili a chiunque abbia accesso al *server* di *Amazon cloud*. Una *data breach* di queste dimensioni «raises significant questions about the privacy and security Americans can expect for their most privileged information»[523].

«When company become so dominant that they can violate their users' privacy without worrying about market pressure, all that's left is the incentive to get more and more information about you. That's big problem if you acre about privacy, and it's a problem that the Antitrust community should be talking about»[524].

Le autorità *Antitrust* dovrebbero valutare le implicazioni delle fusioni *data driven,* dando alle questioni che involvono la *privacy* il necessario rilievo, considerando gli effetti di rete e il comportamento abusivo sulla *competition policy*.

In generale, gli effetti di rete diretti si verificano quando l'utilità del consumatore a utilizzare quel prodotto cresce se lo utilizzano anche gli altri[525]: nella fattispecie è chiaro che se tutti i miei amici sono su *Facebook* sarà per me inutile scegliere un *social network*

---

[520] ID., *op. cit.,* p. 336, cit.

[521] *ibid.*

[522] «This is deeply troubling. This is not just sensitive, it's intimate information, predictions about people's behaviour, opinions and beliefs that people have never decided to disclose to anyone» (in *http://www.independent.co.uk/news/world/americas/us-politics/us-leak-data-americans-personal-information-deep-root-analytics-republican-national-committee-a7798251.html*).

[523] in *http://www.dw.com/en/deep-root-analytics-behind-data-breach-on-198-million-us-voters-security-firm/a-39318788*

[524] Cosi il senatore US Al Franken, American Bar Association's antitust bar.

[525] L'esempio classico è quello del telefono.

diverso. Effetti indiretti si hanno quando la popolarità della piattaforma cresce quanto più crescono i prodotti compatibili con quella piattaforma o tecnologia: se per utilizzare un telefonino con il sistema operativo *Android* ho necessariamente bisogno di un *account Gmail*, sarò costretto a utilizzare quel servizio a meno che non voglia utilizzare lo *smartphone* come una suppellettile.

Ora, riepilogando, lo scopo delle *app* gratuite è quello di raggiungere un bacino di utenti, *a critical mass of users* tale che una volta superato il punto critico gli effetti di rete renderanno quella *app* la più attrattiva sul mercato, impedendo ai consumatori di andare altrove e rendendola «l'unica utilizzabile»[526] a causa degli effetti di *lock in*[527] e degli *switching costs*[528].

Il fatto che un'impresa calamiti tutti gli utenti perché offre i «migliori» prodotti, per di più gratuitamente, impedisce al nuovo entrante, privo delle conoscenze necessarie per mettere a punto applicazioni appetibili, di attirare nuovi utenti, pur sostenendo ingenti costi di sviluppo.

Questo accade non perché i concorrenti siano meno bravi, ma perché più persone utilizzano un servizio, più quel servizio migliorerà la *user experience*, tramite l'esperienza *trial and error* o tramite il *learning by doing*. Gli algoritmi imparano dagli errori degli utenti: più sono gli utenti, più gli *input*, migliore saranno il sistema di *feedback* e la conseguente e costante auto-correzione dell'algoritmo. Questo apparato, che perfeziona strumenti di *data analitycs* ancora una volta rende chi già è forte più forte e chi invece è debole più debole[529], e il debole oltre al concorrente sarà il consumatore finale.

Un esempio chiarirà il concetto: le *query* inserite in un motore di ricerca migliorano i risultati, il loro aumento, collegato all'aumento del numero di coloro che «googlano», li rende sempre più rilevanti[530] e quindi sempre più utili per gli utenti che cercano risposte

---

526 Si ripropone quanto argomentato dagli autori Stucke e Grunes a p. 157 ss del volume citato.

527 Se i consumatori sono bloccati (*locked in*) su *Facebook* per esempio, alimenteranno il monopolio con i dati.

528 Sono costi economici e di apprendimento: si pensi a *Facebook*, se volessi cambiare *social network* per utilizzarne uno con una politica di protezione della *privacy* più forte rischierei di non trovare i miei amici e la mia famiglia e quindi sarei costretto in via di fatto a rimanere su *Facebook*.

529 M. E. STUCKE – A. P. GRUNES, *op. cit.,* p. 170.

530 ID., *ivi,* p. 173.

pertinenti alle loro domande e che certamente non si rivolgeranno al servizio più scadente offerto dal concorrente.

La rilevanza e pertinenza della risposta che dà per esempio Google alle *queries* degli utenti è strettamente connessa al numero di utenti perché è il valore dei dati raccolti a remunerare i servizi offerti.

Inoltre, quando un utente clicca sulla pubblicità i dati di quell'utente aiutano a migliorare la qualità del prodotto che a sua volta aumenta, da un lato la possibilità di attrarre nuovi utenti perché avrà migliorato il servizio, dall'altro il numero degli inserzionisti, che avranno interesse a rivolgere la pubblicità a chi molto probabilmente acquisterà. Se tutti vanno da *Google* perché è in grado di profilare meglio, il merito non è di *Google* e dei suoi algoritmi, ma dei dati che estrapola dagli utilizzi degli utenti, e seppure i suoi algoritmi fossero migliori saranno stati i dati che non gli appartengono a renderli tali. Di conseguenza, i concorrenti perderanno i guadagni derivanti dalla pubblicità degli inserzionisti cui converrà rivolgersi a chi riesce a profilare meglio in base ai dati comportamentali.

A ciò si aggiunga, solo per fare un esempio, che *Google* e il suo *Google maps* sono preinstallati sugli *smarthphone* con sistema *Android* ed *Apple* mediante dei *licensing agreements*.

Dunque, i concorrenti si imbattono in costi di sviluppo e investimento per offrire prodotti e servizi parimenti gratis, ma senza che la loro attività sia remunerata dalla pubblicità o dai dati degli utenti. Questa attività diventa ancora più costosa quando i concorrenti devono competere con applicazioni preinstallate sui dispositivi elettronici. Che interesse ha l'utente a cercare un'*app* se questa è già disponibile sul suo *smartphone*? Così *Google* è *ictu couli* nelle condizioni di abusare della dominanza: con la sua super-piattaforma può finanziare progetti di autoguida e collezionare nuovi e ulteriori dati per le finalità remunerative che più lo aggradano, a spese della *privacy* degli utenti e della libertà d'impresa dei concorrenti, nonché del corretto esplicarsi del gioco della concorrenza.

Questo sistema impedisce ai nuovi di entrare sul mercato perché gli effetti di rete aiutano Google a diventare primo motore di ricerca, prima piattaforma video, primo servizio di mappatura, primo in tutto.

A questo punto il dominante può degradare la qualità con la riduzione della protezione della *privacy* e potrà usare il suo potere di mercato e gli effetti di *lock in* per estrarre sempre più dati; offrirà termini di servizio *take it or leave*, per sé vantaggiosi, soffocando la libertà dei consumatori di scegliere altre piattaforme con altre politiche *privacy* più convenienti o comunque più protettive della loro riservatezza.

«The economics of data favour market concentration and dominance»[531].

Gli individui continueranno a combattere con uno squilibrio di potere che li costringerà a scegliere tra *privacy* e servizi ormai indispensabili perché la loro rinuncia li escluderebbe dai circuiti sociali e culturali. Sarebbe paradossale, se per proteggere la propria *privacy* il soggetto dovesse rinunciare all'esercizio dei diritti fondamentali, o accontentarsi del peggiore servizio di posta elettronica offerto dal mercato perché nessuno offrirebbe impostazioni *privacy* sicure.

Tutto ciò si traduce, si ribadisce, in barriere all'ingresso per i nuovi entranti. Con meno utenti e meno esperienze *trial and error*, i servizi offerti dai concorrenti saranno meno efficaci, non avranno *chances* per competere con i colossi della Rete. Se aumentano i dati, aumenta la variabile della varietà, la quale incrementa il loro valore e perfeziona la profilazione, rendendo il *targeting* più succulento per gli inserzionisti e parallelamente per i venditori. Ne derivano ampi effetti *spill over*[532].

La crescita degli utenti da un lato del mercato multi-versante attrae più inserzionisti e venditori dall'altro lato della piattaforma. Quindi più utenti, più inserzionisti, più venditori in un circolo vizioso che avvantaggia solo il dominante. Si pensi a *coupon.com*[533]: se più venditori usano la piattaforma ci saranno varietà di sconti per i consumatori, perché più informazioni hanno i venditori sui consumatori e sulla loro sensibilità al prezzo, migliori offerte diversificate faranno: il consumatore non ne beneficerà se lo sconto sarà compensato da una politica discriminatoria dei prezzi e delle notizie e da una violazione generalizzata della sua *privacy*. Gli effetti di rete guidati dai dati sul lato gratuito del mercato

---

[531] M. E. STUCKE – A. P. GRUNES, p. 336, cit.

[532] M. E. STUCKE – A. P. GRUNES, p. 190.

[533] ID., p. 191.

hanno ripercussioni sul lato a pagamento del mercato; ognuno di questi versanti rinforza l'altro.

Allora questi effetti di rete: barriere, effetti *trial and error*, volume e varietà dei dati ed effetti *spill over* rendono Google una piattaforma *killer* per i concorrenti[534].

Se il potere di mercato diventa incontrollato, i danni alla *privacy* nuoceranno principalmente ai nostri ideali democratici di autonomia e libertà perché si rafforzeranno le disuguaglianze e le strategie anti-competitive intensificheranno le ineguaglianze sociali, rendendo i poveri ancora più poveri.

Questo perché le autorità sono inclini a esaminare le questioni *antitrust* sotto la lente dell'incremento dei prezzi e non sono abituate a considerare aspetti *non-price* come la qualità in generale e la tutela della *privacy* in particolare. Quando il prodotto è gratuito la qualità diventa un'importante componente della concorrenza[535]: per esempio se un motore di ricerca intenzionalmente degrada i risultati di ricerca più rilevanti in favore di quelli meno rilevanti, ma sponsorizzati, la garanzia della qualità diventa *key parameter of competition.*

La qualità guiderebbe l'innovazione e la crescita economica, e, una diminuzione di qualità potrebbe essere dannosa per i consumatori al pari della crescita del prezzo. Allora il mantenimento e l'aumento della qualità sono obiettivi importanti di *competition*.

La violazione *antitrust* potrebbe consumarsi anche in una diminuzione della varietà dei prodotti o in una diminuzione di innovazione, ben potendo la tutela della *privacy* rappresentare la variabile lungo la quale sono chiamate a concorrere le imprese per migliorare i loro prodotti e servizi. Le concentrazioni *data driven*, si ribadisce, mettono in discussione le regole convenzionali[536] con le quali le autorità *Antitrust* erano solite operare e che ovviamente non sono adatte a tutti i tipi di concentrazione[537] e richiedono nuovi strumenti che tengano conto della natura dinamica di questi fattori «incorporating the intangible, non economic injury from invasions of privacy interests into their competition

---

534 ID., *ivi*, p. 213.

535 ID., *ivi*, p. 116.

536 ID., *ivi*. Le convenzioni che andrebbero a scardinare le nuove valutazioni sono le seguenti: la categorizzazione delle concentrazioni (p. 127 ss.); l'idea che prodotti/servizi simili competano più ferocemente di prodotti/servizi diversi (p. 129 ss.); l'attenzione alla sostituibilità dei prodotti (p. 134 ss.).

537 «Data is not like any other commodity and data markets are not like any other markets». Così E. MOROZOV, *To tackle Google's power, regulators have to go after its ownership of data*, in *The Guardian*, July 2, 2017.

analisys»[538]. Occorrerebbe guardare all'impatto sull'innovazione, ai potenziali benefici e ai danni concreti ai consumatori e ai concorrenti, in termini di competitività e stabilità della rete finanziaria complessiva.

Allora i *Big Data* sollevano preoccupazioni per la concorrenza e chiedono un coordinamento con la tutela del consumatore e la protezione della *privacy*.

Nell'ottobre 2014 Margaret Vestager, Commissario Europeo per la concorrenza, ha definito i dati la nuova moneta di Internet[539] e ha posto l'attenzione su come la raccolta su larga scala di dati consolidi la forza delle imprese *big tech*. A tal proposito la Vestager rivolgendosi al Parlamento Europeo ha argomentato che Google «was a business with a huge, huge and huge market share»[540].

Tuttavia, alla premessa non sembra essere seguita la conseguente valutazione. Diversamente da quanto sostenuto dalla commissaria Vestager[541], le autorità garanti della concorrenza dovrebbero prendere in considerazione le politiche sulla *privacy* ogni volta che queste politiche possono influenzare la concorrenza, in particolare nelle indagini sull'abuso di posizioni di dominanza di quelle imprese per le quali i dati costituiscono la principale remunerazione dei loro prodotti o servizi. I dati servono a prevedere le nostre necessità di informazioni che ci impediscono anche solo di cercare[542]. Proprio queste considerazioni avrebbero dovuto guidare la Commissione anche nella determinazione del mercato rilevante nel recente caso Google[543], su cui si esporrà nel paragrafo 4.5.

Eppure sarebbe bastato seguire le indicazioni del Trattato di Lisbona e della Corte di Giustizia.

---

[538] ID., *ivi,* p. 106, cit..

[539] In originale: «new currency of the Internet».

[540] Ne parla J. Kanter in un articolo pubblicato su *The New York Times, Antitrust nominee in Europe promises scrutiny of big tech companies*, 3 ottobre 2014.

[541] «She does not think the Commission needs to look to competition enforcement to fix privacy problems.» Discorso DLD 16, Munich, 17 January 2016, in *https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big-data-world_en*. La commissaria ha comunque sottolineato che ciò non significa che la Commissione europea ignorerà le vere e proprie questioni relative alla concorrenza solo perché hanno un legame con i dati.

[542] «That data trove allows Alphabet to predict our information needs in a way that does not always require us to type in a search query». Così E. MOROZOV, *To tackle Google's power, regulators have to go after its ownership of data*, in *The Guardian*, July 2, 2017.

[543] «Alphabet's future revolves around information-intensive services, not around running matchmaking platforms for advertising». Così E. MOROZOV, *To tackle Google's power, regulators have to go after its ownership of data*, in *The Guardian*, July 2, 2017.

In un primo momento la Corte di Giustizia Europea ha ritenuto che qualsiasi preoccupazione relativa alla vita privata dovuta alla maggiore concentrazione dei dati, diretta conseguenza di una fusione, non rientrava nel campo di applicazione del diritto comunitario in materia di concorrenza, bensì nell'ambito della normativa di tutela della *privacy*[544]. Successivamente, la Corte ha avuto modo di precisare che ciò non significa che la legge sulla concorrenza sia completamente estranea alla protezione dei dati personali. Al contrario, requisiti di legge derivanti da altri apparati normativi possono sempre essere presi in considerazione quando si esegue un'analisi legale nel quadro della regolamentazione della concorrenza, anche se solo come elemento contestuale[545].

Sebbene la legge sulla protezione dei dati e la legge sulla concorrenza abbiano obiettivi diversi, le questioni relative alla protezione dei dati non devono essere escluse da un'analisi del diritto di concorrenza semplicemente sulla base della loro natura. Le azioni delle imprese relative alla raccolta e all'uso di dati personali possono avere implicazioni sulla concorrenza.

Inoltre, l'articolo 167, n. 4 del Trattato sul funzionamento dell'Unione europea (TFUE) afferma che «l'Unione tiene conto degli aspetti culturali nelle sue azioni secondo altre disposizioni dei trattati, in particolare per rispettare e promuovere la diversità delle sue culture». La Commissione europea ha espressamente considerato[546] la diversità culturale. L'articolo 16 TFUE, una disposizione che ha applicazione generale, afferma che «ogni persona ha il diritto alla protezione dei dati personali». Tale articolo, in combinato disposto con l'articolo 7 TFUE, che impone alla Commissione (e ad altre istituzioni dell'Unione europea) di garantire la coerenza tra le politiche, obbliga la Commissione europea a tener conto delle preoccupazioni in materia di protezione dei dati.

Pertanto, vi è la possibilità di argomentare che la legge sulla concorrenza dovrebbe essere applicata in aggiunta alla legge sulla protezione dei dati per migliorare l'efficacia

---

544 European Court of Justice, Case C-238/05, *Asnef-Equifax*. Questo orientamento è stato poi confermato dalla European Commission in Case M.4731, *Google/DoubleClick* e Case M .7217, *Facebook/Whatsapp*.

545 European Court of Justice, Case C-32/11, *Allianz Hungária*. Qui la Corte di Giustizia ha ritenuto che la violazione di un altro insieme di regole nazionali potrebbe essere presa in considerazione per valutare se vi sia una restrizione della concorrenza. A livello nazionale, la Corte federale di giustizia tedesca ha dichiarato, nella causa KZR 61/11, *VBL-Gegenwert*, che i termini contrattuali incompatibili con il diritto generale contrattuale potrebbero costituire un abuso di posizione dominante.

546 Causa M.6458, Universal Music Group/ EMI Music.

delle norme comunitarie in materia di protezione dei dati. Inoltre, le istituzioni dell'UE sono tenute a rispettare i diritti stabiliti nella Carta dei diritti fondamentali dell'UE e promuovere la loro applicazione. L'articolo 8 dell'ECFR include il diritto alla protezione dei dati. Quindi, la Commissione europea è obbligata a rispettare e promuovere il diritto alla protezione dei dati. Nel 2014, il Garante europeo della protezione dei dati ha sostenuto un cambiamento di politica e un approccio più olistico all'applicazione. Il garante europeo della protezione dei dati ha inoltre invocato un maggiore dialogo tra autorità competenti, autorità di tutela dei consumatori e dei dati nei casi in cui emergono problemi di tutela dei consumatori e di protezione dei dati. Inoltre, il supervisore della protezione ha invocato un maggiore dialogo tra le autorità competenti per la concorrenza, i consumatori e la protezione dei dati nei casi in cui sorgano problemi di tutela dei consumatori e / o di protezione dei dati[547].

Dunque, la Corte Suprema degli Stati Uniti ha definito le leggi sulla concorrenza come «*Magna Carta* della libertà d'impresa» e le ha qualificate come «important to the preservation of economic freedom and our free-enterprise system as the Bill of Rights is to the protection of our fundamental personal freedoms». Resta inteso che nonostante questo ampio mandato non possiamo assumere la concorrenza come panacea di tutte le questioni concernenti la *privacy* e la tutela del consumatore[548]. Tuttavia, la *privacy* può servire un obiettivo *antitrust* nel momento in cui essa, rappresentando una variabile della qualità di un prodotto diventa *non-price parameter of competition*[549]. In parole più semplici, se gli utenti della Rete non fossero bloccati dagli effetti di Rete, e se potessero agevolmente portare tutti i propri contenuti verso una piattaforma con una *privacy policy* più forte, si migliorerebbe la concorrenza sulla qualità del prodotto offerto.

In conformità all'articolo 102 TFUE, il deterioramento della protezione dei dati potrebbe diventare una questione *antitrust* problematica, in particolare se un potente operatore di mercato viole intenzionalmente le leggi sulla protezione dei dati per imporsi

---

547 B. BÄR-BOUYSSIÈRE - D. COLGAN, *European Union, France, Germany*, in *DLA Piper LLP*, July 18, 2016.

548 Si traduce quanto affermato da M. E. STUCKE – A. P. GRUNES a p. 335 del volume citato.

549 M. E. STUCKE – A. P. GRUNES, *op. cit.*, p. 259. Cit.

sul mercato e se esiste un forte legame tra la posizione di mercato di tale impresa e la raccolta di dati.

L'«*Amassing data*» è il fattore che intensifica il potere delle imprese digitali come *Google* e domanda la valutazione della *privacy competition,* tralasciando i comuni meccanismi *price centric*. Le questioni relative all'applicazione delle regole sulla gestione dei dati non si fermano ai confini nazionali. E se le autorità indipendenti non sono in grado di dare una risposta, dovrà darla il legislatore[550].

3.1. *L'asset dei dati sul mercato e le sue declinazioni egoistiche*

Il nuovo terreno di gioco delle libertà economiche in Internet è la piattaforma digitale: il profitto è collegato, in misura di proporzionalità diretta, alle risorse economiche dei dati e quindi al numero di utenti che li producono, proprio utilizzando quella piattaforma.

Dunque, ne deriva che chi si è assicurato la posizione migliore sul mercato tecnologico tenderà a concentrare su di sé il maggior numero di utenti e i conseguenti profitti.

Da qui, per esempio, la posizione di predominio di *Facebook*[551], che gli ha consentito, da privato, di determinare i prezzi delle inserzioni e indirettamente dei prodotti[552], potendoli far incrementare in modo che tutti paghino di più, mentre i profitti finiscono

---

[550] M. E. STUCKE – A. P. GRUNES, *op. cit.*, p. 338.

[551] Sulla condotta di concorrenza sleale di Facebook con riferimento si rinvia alla sentenza n. 9549 del 1° Agosto 2016, la Sezione Specializzata in materia di Impresa del Tribunale di Milano ha accertato la responsabilità delle società *Facebook S.r.l.*, *Facebook Inc. e Facebook Ireland LTD* per atti di concorrenza sleale nei confronti di *Business Competence*, una società da 2 milioni e mezzo di fatturato annui, e violazione del diritto d'autore nella creazione di una applicazione per ottenere informazioni su bar e ristoranti individuati attraverso la geolocalizzazione del cellulare. Sul tema M. D'OSTUNI - R. TREMOLADA *Facebook v. Business Competence S.r.l.*, in *Company Law Division of the Court of Milan,* Ruling No. 9549, 1 August 2016, in *https://www.clearygottlieb.com/~/media/cgsh/files/2017/publications/leading-internet-case-law-facebook-v-business-competence-srl-05-30-17.pdf*.

[552] Con una pubblicità mirata *Facebook* permette di raggiungere i clienti imponendo prezzi diversi per uno stesso prodotto.

nelle sue mani[553], in spregio alla libertà di impresa, alla leale concorrenza e alla eguale distribuzione di valore da parte di consumatori e contribuenti.

Questo accade perché laddove i modelli di *business* di interi ecosistemi di Piccole e Medie Imprese dipendono dall'accesso a un piccolo numero di piattaforme *online* e laddove solo tali piattaforme hanno accesso a *set* di dati di dimensioni senza precedenti, a monte si creano forti asimmetrie e barriere all'ingresso per i *new entrants*.

Inoltre, in tali situazioni, a valle, i consumatori che si muovono sulle piattaforme vengono esposti in modo sproporzionato a pratiche di negoziazione scorretta[554].

In realtà tutte le aziende che possiedono dati possono estrarre valore da questi grandi *set* e ottenere un vantaggio competitivo rispetto ai loro concorrenti, in quanto sono in grado di utilizzare queste informazioni per prendere decisioni migliori[555]. Ad esempio, *GE* e *Siemens*[556] stanno lavorando attivamente sui servizi che raccolgono e analizzano i dati delle macchine che vendono. *IBM* sta integrando i dati provenienti dalle cartelle cliniche elettroniche[557] con le immagini mediche e i dati genetici per migliorare il suo servizio di analisi *Watson Health*[558]. Le aziende automobilistiche, come *Audi*, sperano di utilizzare i dati

---

[553] *Joseph Stiglitz: «Questi cinque monopolisti minacciano la democrazia»*, in http://www.pagina99.it/2017/05/21/nobel-joseph-stiglitz-apple-Google-microsoft-amazon-e-facebook-monopolio-privacy/, 22 maggio 2017.

[554] Secondo J. Kennedy la raccolta di grandi quantità di dati non rappresenta di per sé una minaccia alla concorrenza. Sebbene l'utilizzo di dati in circostanze specifiche giustifichi l'intervento normativo, nella maggior parte dei casi l'acquisizione e l'utilizzo dei dati non riducono la concorrenza e il quadro giuridico esistente conferisce alla regolamentazione della concorrenza e della protezione dei dati personali tutta la flessibilità necessaria. Proprio queste grandi quantità di dati, incluse le informazioni personali, sono sempre più un elemento fondamentale per alcune delle più importanti innovazioni dell'economia, tra cui piattaforme *online* , diagnosi mediche, assistenti digitali, traduzione linguistica, urbanistica e sicurezza pubblica. Cfr. J. KENNEDY, *The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown*, in *Information technology & innovation foundation*, march 2017, pp. 2 e 3.

[555] *Contra* J. Kennedy a p. 7 dell'articolo citato: «the possession of large amounts of data, by itself, does not usually create a large barrier to entry. Even if it did, competition policy should not seek to create a level playing field for all companies at all times, especially when companies benefit from advantages that they created with their own resources and which others are free to emulate».

[556] *Siemens and General Electric Gear Up for the Internet of Things*, in *The Economist*, December 3, 2016, *http://www.economist.com/news/business/21711079-american-industrial-giant-sprinting-towards-its-goal-german-firm-taking-more*.

[557] S. LOHR, *IBM Buys Truven for $2.6 Billion, Adding to Trove of Patient Data*, in *The New York Times*, February 18, 2016, in *https://www.nytimes.com/2016/02/19/technology/ibm-buys-truven-adding-to-growing-trove-of-patient-data-at-watson-health.html*.

[558] Il 15 maggio 2017 è stato rilanciato da Paul-Olivier Dehaye, cofondatore di PersonalDataIO, sul suo canale *Twitter* il programma *Watson Health* di IBM. Il messaggio twittato era il seguente: "Italy trades the whole country's health dataset with IBM in exchange for local investments. IBM trains Watson", in https://twitter.com/podehaye/status/864198814873378817. Il programma *Watson Health* verrebbe avviato a Milano, dove *IBM* intende aprire il primo Centro di Eccellenza europeo, con il cofinanziamento del Governo Italiano che si sarebbe impegnato a cedere i nostri dati sanitari (non è ancora noto in quali modalità). Trattandosi di *collective data protection*, decisioni ad impatto così esteso sui cittadini dovrebbero seguire *iter* trasparenti e partecipativi. Cfr.

prodotti dai veicoli per ottimizzare le loro auto. Per diversi anni, le catene di supermercati come *Tesco* e *Sainsbury* hanno utilizzato dati estratti da tabelle di fedeltà per offrire sconti personalizzati[559] e ora vogliono utilizzare dati aggiuntivi, provenienti da terze parti, per migliorare la tempistica di quelle promozioni e competere con marchi come *Lidl*.

Le industrie intere stanno rapidamente adottando sistemi di raccolta di dati sui loro clienti e prodotti[560]. Tuttavia, le maggiori preoccupazioni in materia *antitrust* sono rivolte principalmente alle grandi piattaforme radicate sulla Rete, come *Google*, *Apple*, *Facebook* e *Amazon*[561]. Queste società occupano un posto centrale su Internet, grazie alla posizione che per primi hanno assunto su uno spazio anarchico[562]. Tali *players* oggi sono in grado di raccogliere un volume e una varietà di informazioni enormi in tempo reale, più velocemente di chiunque altro.

Il principale timore è che, grazie alla loro posizione di vantaggio, queste piattaforme, piuttosto che aziende come *Audi* o *Tesco*, siano in grado di raccogliere un'ampia fetta di

---

con http://www.ilfattoquotidiano.it/premium/articoli/i-nostri-dati-sanitari-allibm-il-garante-apre-uninchiesta/; http://www.giannibarbacetto.it/2017/03/19/a-ibm-tutti-i-nostri-dati-sanitari-in-cambio-della-nuova-sede-sullarea-expo-2/; http://www.mind-spa.it/2017/04/24/the-mother-of-all-data-grabs/.

559 R. WILLCOX, *Big Data, Empty Bellies: How Supermarkets Tweak Prices Just for the Sake of YOUR LOVE*, in *The Register*, February 5, 2015, *http://www.theregister.co.uk/2015/02/05/big_data_tech_weapons_in_supermarket_price_wars/*.

560 *Will Artificial Intelligence Help to Crack Biology?*, in *The Economist*, January 7, 2017, *http://www.economist.com/news/science-and-technology/21713828-silicon-valley-has-squidgy-worlds-biology-and-disease-its-sights-will*; S. LOHR, *Medicaid's Data Gets an Internet-Era Makeover*, in *The New York Times*, January 9, 2017, *https://www.nytimes.com/2017/01/09/technology/medicaids-data-gets-an-internet-era-makeover.html*; V. ESTES, *How Big Data is Disrupting Agriculture from Biological Discovery to Farming Practices*, in *Agfunder News*, June 9, 2016, *https://agfundernews.com/how-big-data-is-disrupting-agriculture-from-biological-discovery-to-farming-practices5973.html*; *A New Industry Has Sprung Up Selling 'Indoor-Location' Services to Retailers*, in *The Economist*, December 24, 2016, *http://www.economist.com/news/business/21712163-there-money-be-made-tracking-shoppers-paths-inside-stores-new-industry-has-sprung-up*.

561 *Google Dominates Search. But the Real Problem Is Its Monopoly on Data*, in *The Guardian*, April 19, 2015. «[*Google*'s] overwhelming strength comes from its ownership of vast datasets—and that data has often been acquired under exclusive deals or with ill-informed consent»; A. BERNASEK - D.T. MONGAN, *Our Massive New Monopolies: Amazon, Google and Facebook Have the Power to Move Entire Economies,* in *Salon*, June 7, 2015, *http://www.salon.com/2015/06/07/our_massive_new_monopolies_amazon_Google_and_facebook_have_the_power_to_move_entire_economies/*. «The data giants are fundamentally different. Companies like Amazon or Facebook know (or infer) not just who you are but what you are like. They know not only where you are but they can guess where you are going. They don't just know what you are doing right now—they have a pretty good idea why you are doing it. And they make excellent guesses about what you will do next, guesses that grow more accurate every day as you go about the business of daily life while being carefully observed by the data giants».

562 G. DE MINICO, *Internet. Regola e anarchia*, Jovene, Napoli, 2012*, passim*.

potere di mercato che i dati conferiscono loro[563], per falsare il gioco della concorrenza[564], estendendo la loro dominanza anche in altri settori.

Questi colossi oggi sono anche i maggiori intermediari di notizie e informazioni, quindi di conoscenza, al punto che possono decidere cosa diffondere e cosa no, in quale forma e con quanta viralità. Una delle principali pratiche da loro adottate è quella del *clickbaiting*[565], la tecnica utilizzata consiste nella elaborazione e diffusione di articoli con «titoli esca», appositamente realizzati per attirare *click* e quindi visualizzazioni di pagine pubblicitarie, con la conseguente distorsione del contenuto ed eventualmente del «*sentiment* politico per fini geopolitici»[566].

Da ciò derivano una serie di conseguenze.

In primo luogo, il semplice possesso di grandi quantità di dati conferisce all'azienda che li possiede un notevole vantaggio competitivo, al punto che i suoi rivali non potranno sfidarla perché non possono competere con una raccolta di dati. E ciò risulta *ictu oculi* dal fatto che quei dati sono stati raccolti quando ancora non esisteva una regolazione e dei *competitors* sulla Rete, soprattutto se si aggiunge che la registrazione dei primi dati è avvenuta in forma occulta tramite connessioni *Wi-Fi* non protette, che hanno permesso di scaricare i dati illegittimamente e in forma non criptata, per scopi molteplici e non noti agli utenti[567].

Il possesso dei dati si traduce in limitazione degli accessi o degli sbocchi ai mercati, degli investimenti, dello sviluppo tecnico o del progresso tecnologico.

---

563 Si traduce quanto affermato da Kennedy nell'articolo citato, a p. 3; tuttavia l'autrice qui utilizza le stesse considerazioni per una tesi contraria a quella dell'autore.

564 G. GHIDINI - E. AREZZO, *La prospettiva costituzionale della tutela della concorrenza*, in *Giur. comm.*, I, 2012, pp. 464 ss.

565 La tecnica adoperata è comune anche ai siti che diffondono *fake new*s, ma non solo.

566 Il prof. Giuseppe Attardi nella *newsletter* dell'8 giugno 2017 del Centro *Nexa* di Torino su *Report: "Information Operations and Facebook" (Stefano Quintarelli)* propone il seguente esempio: «La settimana scorsa, molti i giornali hanno titolato: L'ISTAT rivede al rialzo la crescita del PIL al 1.2% *http://www.corriere.it/economia/17_giugno_01/istat-rivede-rialzo-crescita-piu-12percento-primo-trimestre-2017-7ecc7af4-46a2-11e7-b9f8-52348dc803b5.shtml* (NB. nel titolo presente nella prima pagina di corriere.it <http://corriere.it/> mancava il riferimento al trimestre). Il titolo accattivante riporta un'inesattezza: il 1,2% si riferisce alla crescita del PIL del I trimestre 2017 rispetto a quello del I trimestre 2016, e quindi include l'aumento di 0,8% annuo avvenuto nel corso del 2016. Tanto è vero che il sito ISTAT riporta che la sua previsione di crescita per il 2017 è dell'1% (Prospettive per l'economia italiana <http://www.istat.it/it/archivio/200170>). Il sottotitolo insiste: *l'Istat aveva ipotizzato un Pil al +0,8% su base annua.?*, anche questo fuorviante, perché su base trimestrale, non su base annua. Mala fede, ignoranza, o intenzione di "distorcere il sentiment politico per fini geopolitici??».

567 In riferimento alla posizione di vantaggio assunta da *Google* sul mercato dei dati (con particolare riguardo al servizio *Google Maps*) si rinvia al *paper* dell'autrice, *op. cit.*, p. 704 e al corrispondente apparato bibliografico.

In secondo luogo, la politica della concorrenza come attualmente è strutturata, non è in grado di rispondere alle minacce competitive derivanti dalle grandi quantità di dati, perché i rimedi previsti per l'analogico non sono adatti alle dimensioni del nuovo fenomeno. Si pensi all'azione risarcitoria, alle sanzioni pecuniarie, ai provvedimenti a contenuto prevalentemente inibitorio o di *reductio in pristinum*, come previsti dalla l. 247/1990[568]. Il divieto di immediata desistenza dalla condotta abusiva non sarebbe in grado di modificare la situazione di fatto affermatasi sul mercato e, tale atto inibitorio sarebbe agevolmente eludibile, date le peculiarità della Rete, terreno di ricaduta del provvedimento inibitorio.

In terzo luogo, l'acquisizione di grandi quantità di dati sugli utenti costituisce una grave minaccia per la *privacy* che le autorità di tutela dei consumatori non sono in grado di gestire[569].

In diversi modi le aziende possono utilizzare i dati per ostacolare la concorrenza: 1) possono imporre prezzi o altre condizioni contrattuali ingiustificatamente gravose[570], per esempio decidendo di aumentare i prezzi di mercato senza che i consumatori possano rivolgere altrove la loro domanda perché il prodotto offerto dai «collezionatori di dati» è molto più appetibile, 2) le aziende potrebbero procedere con vendite sottocosto (cd. *predatory pricing*), prolungate e motivate dal solo intento di escludere dal mercato concorrenti attuali o potenziali; 3) le imprese che detengono le principali quote di mercato possono fondersi e unire le loro informazioni per avere conoscenza sempre più invasive; 4) possono utilizzare il potere di mercato in un settore per impedire ingiustamente la concorrenza in un altro; 5) un'azienda dominante può cercare di estendere la sua posizione acquistando un *partner* a monte o a valle. In ognuno di questi casi, la legge *antitrust* esistente non consente ai regolatori di adottare misure efficaci.

---

568 Per un approfondimento su danno *antitrust* e sistema rimediale, si legga L. PROSPERETTI - M. SIRAGUSA - M. BERETTA - M. MERINI, *Economia e diritto Antitrust*, Roma, Carocci, 2006, p. 229 ss.

569 M. E. STUCKE – A. P. GRUNES, *op cit.,* pp. 1-11.

570 L'orientamento dell'Antitrust è di considerare ingiustificatamente gravoso il prezzo che risulti fissato con criteri palesemente irrazionali o arbitrari (ad es. tariffe forfettarie che prescindano dalla quantità di servizi resi effettivamente o dal valore dei beni ceduti).

Alcune di queste condotte tipizzate dalla legge[571] tenderebbero allo sfruttamento abusivo della dominanza.

Questo strapotere, come ampiamente descritto nei paragrafi che precedono, rappresenta non solo un pericolo per le democrazie e al tempo stesso strumento di ineguaglianza, perché discrimina l'accesso alle conoscenze e alla cultura, che dovrebbero essere liberi e garantiti a tutti[572], ma diventano minaccia al corretto esplicarsi del gioco della concorrenza e alla efficace tutela del consumatore. «This harm from anticompetitive data-driven strategies can be significant. The harm can go beyond higher advertising rates; it can include the loss of innovation, consumer choice, privacy, individual autonomy and freedom, and the citizens' trust in a market economy. Such harm, the OECD recognized, can strike "the core values of democratic market economies and the well-being of all citizens"»[573].

4. La catena di valore dei dati e la posizione di *Google*

Al fine di comprendere come il possesso dei dati si sia concentrato nelle mani di pochi *players*, occorre descrivere la catena di produzione e del conseguente valore dei dati.

I dati appena generati dai *prosumer*[574], nel circuito dell'*Internet of Things*, sfuggono dalle mani dei loro legittimi proprietari per approdare in quelle degli *over the top* quali *Amazon*, *Microsoft* o *Google*. Si aggiunga che spesso gli utenti della Rete decidono di conservare i loro dati nelle nuvole[575] degli *OTT*. I dati così raccolti e conservati sono utilizzati dai grandi collezionatori per diversi scopi lucrativi, non meglio specificati.

---

571 art. 3 l. 287/90 di contenuto conforme all'art. 102 ex 82 TFUE.

572 A. AFFATICATI, *Joseph Stiglitz: «Questi cinque monopolisti minacciano la democrazia»*, in http://www.pagina99.it/2017/05/21/nobel-joseph-stiglitz-apple-Google-microsoft-amazon-e-facebook-monopolio-privacy/.

573 M. E. STUCKE & A. P. GRUNES, *Debunking the Myths over Big Data and Antitrust*, in *CPI Antitrust Chronicle*, May 2015, p. 9, cit.

574 K. NORDSTRÖM - J. RIDDERSTRALE, *Funky business forever. E adesso godetevi il capitalismo!*, Franco e Angeli editore, Milano,16 dic 2011, *passim.*

575 Questi operatori partendo da altri servizi, come per esempio *Google* dal *Search,* hanno sviluppato con i profitti inizialmente ottenuti, una piattaforma *cloud* aperta a tutti in cui conservare i dati, e a cui si rivolgono la maggior

Nei segmenti sopra descritti si inserisce *Google*[576] che opererebbe in tutti gli anelli della catena e cioè raccoglierebbe i dati e li userebbe per integrarli nei suoi servizi e, con molte altre delle sue attività, trarrebbe vantaggio dalla sua posizione di operatore verticalmente e orizzontalmente integrato per abusare della dominanza, secondo la parte maggioritaria della dottrina, nel mercato pubblicitario, imponendo prezzi agli inserzionisti[577] e calamitando presso di sé tutte le domande di spazi pubblicitari.

La pubblicità offerta da *Google*, che sarebbe il suo modello di *business*, aprirebbe e chiuderebbe la catena di produzione dei dati. Il gigante della Rete oltre a offrire più servizi differenziati e autonomi partendo dalla pubblicità, svilupperebbe sistemi integrati che includono: contenuti digitali, il sistema operativo *Android*, piattaforme *cloud* e crea «sistemi chiusi verticalmente integrati dal terminale ai sistemi operativi, alle infrastrutture *Information technology*, ai servizi partendo dal proprio specifico business»[578] allo scopo di creare una egemonia nel mercato in cui opera.

Nella catena di valore dei *Big Data*, *Google* occuperebbe tutte e tre le posizioni: raccoglierebbe i dati, metterebbe a disposizione degli altri soggetti le interfacce di programmazione di un'applicazione, c.d. API[579], in modo da raccogliere altri dati perché queste interfacce consentono di sviluppare applicazioni che richiedono un *account Google*, e quindi una registrazione a *Google*, senza la quale non risulterebbe possibile fruire dell'*app*, e infine trae valore dai dati.

In una simile catena di produzione titolare del trattamento titolare del trattamento colui che controlla i dati e ne trae utilità economica. Costui, una volta raccolte le informazioni, può utilizzarle direttamente, oppure darle in licenza a terzi affinché ne

parte degli utenti della Rete. Tali piattaforme offrirebbero nuovi dati ai loro gestori, diversi da quelli estrapolati autonomamente.

576 Si precisa che *Google* fa capo ad Alphabet Inc., che è un'azienda statunitense, fondata nel 2015 come *holding* insieme ad altre società controllate. Nel prosieguo, per semplicità espositiva ci riferiremo all'impresa come *Google*.

577 J. FARREL, P.J. WEISER, *Modularity, vertical integration and open access policies: towards a convergence of antitrust and regulation in the Internet age*, in *Harvard Journal of Law & Technology*, 17, 1, 2003, pp. 86 ss.

578 F. BERNABÈ, *Libertà vigilata*, Roma-Bari, Laterza, 2012, p. 20 ss.

579 L'acronimo sta per *Application programming interface*, in informatica, si fa riferimento alle procedure offerte al programmatore, necessarie per l'espletamento di un determinato compito all'interno di un certo programma.

estraggano il valore, in questi casi colui che li cede si assicura una percentuale del valore estratto, anziché una somma fissa mediante formule contrattuali *ad hoc*, simili a *royalties*[580].

Se è vero che mediante le API i terzi possono sviluppare applicazioni proprie e monetizzarle, è altrettanto vero che questo sviluppo da parte di altri soggetti creerà comunque valore aggiunto nell'anello finale della catena, a *Google*, fornendogli nuovi proseliti, le sue fonti di profitto.

Specificamente, la nicchia redditizia di *Google* sarebbe, ad avviso della dottrina, ma anche della Commissione Europea, come si vedrà nei paragrafi che seguono, la pubblicità: essa costituisce il 96% dei suoi ricavi[581], nel mercato USA della pubblicità *online* il colosso della Rete occuperebbe una quota del 40,7% delle *revenue*[582], il 60% insieme a *Facebook*, con il quale condividerebbe un duopolio.

Insieme occuperebbero, infatti, il 20% del mercato pubblicitario mondiale, in crescita rispetto all'11% del 2012, e insieme le due aziende reppresenterebbero il 64% della crescita globale del mercato tra il 2012 e il 2016[583].

In Italia la quota occupata da *Google* e *Facebook* sarebbe pari ai due terzi[584] del mercato[585].

Il primo, che possiede anche *YouTube*, dominerebbe la pubblicità legata alle ricerche sui suoi motori di ricerca. Ad alimentare la raccolta di *Google* sarebbe dunque il *search advertising*[586].

Il secondo, che controlla anche *Instagram*, dominerebbe invece il mercato *display*, cioè quello della «banneristica», con il video che occuperebbe una fetta crescente del tempo

---

580 V. MAYER-SCÖNBERGER, K. CUKIER, o*p. cit.*, p. 165.

581 L. KEELEY - R. PIKKEL - B. QUINN - H. WALTERS*, I 10 tipi di innovazione. L'arte di costruire svolte decisive*, Milano, Edizioni lswr, 2014, p. 70 ss.

582 M. GIANNI, *Google e* Facebook *dilagano nel mercato della pubblicità online* , in *https://www.digital4.biz/marketing/advertising/Google-e-facebook-dilagano-nel-mercato-della-pubblicita-online_436721510101.htm*, 27 marzo 2017.

583 Cfr. con l'articolo *Google e* Facebook *controllano il 20% del mercato pubblicitario mondiale.* Zenith*: nella top30 delle concessionarie, 7 sono legate al* digital. *Gli Stati Uniti il paese più presente*, in http://www.primaonline.it/2017/05/03/256536/dati-zenith-su-top30-concessionarie/, 3 maggio 2017.

584 66%. La quota sale a 68 se si considerano anche gli altri *Over The Top* internazionali (quindi anche *Linkedin, Twitter*, *Microsoft* e *Bing*).

585 Cfr. con Osservatorio Internet Media del Politecnico di Milano, in http://www.osservatori.net/it_it, 2016.

586 una discreta quota deriva dal *display* e da *YouTube*.

passato dagli utenti, sia per le trasmissioni in diretta che per i contenuti registrati, attirando crescenti investimenti.

Un cospicuo numero di imprese investe una grossa fetta del suo *budget* in pubblicità su *Google* o *Facebook* per il fatto che essi sono capaci «di attrarre grandi bacini di utenza, la semplicità di pianificazione consentita dalle loro soluzioni tecnologiche, il lancio frequente di nuovi formati pubblicitari, soprattutto sui *social network*, e i costi bassi sono i principali punti di forza»[587].

Proprio perché i dati costituirebbero l'*asset* strategico di *Google*, il suo interesse sarà quello di tenerseli stretti o di far pagare a terzi un prezzo elevatissimo per accedervi.

«While it is true that data can be used in anticompetitive ways, competition policy is capable of dealing with such abuses»[588], tuttavia i legislatori o i regolatori sovranazionali dovrebbero adottare leggi vincolanti per proteggere la *privacy* e le libertà in Rete, a prescindere da ciò che dicono i termini di utilizzo[589].

A questo punto, occorre descrivere quali siano i servizi erogati da *Google*, in che modo le sue pratiche commerciali possano definirsi anticoncorrenziali e quale sia la specifica condotta abusiva tenuta dal *Big Player*.

Per fare ciò sarà necessario individuare lo specifico mercato di riferimento[590].

Ci domanderemo se la dominanza, e la conseguente condotta abusiva dello sfruttamento della stessa, debbano essere individuati guardando al fatturato economico della pubblicità nell'attività del *Search*, così come ha fatto la Commissione, oppure al numero di utenti che utilizzano i servizi *Google* e quindi con riguardo all'*asset* dei dati; quindi se rilevi il carattere merceologico o finalistico del mercato.

Infine ci interrogheremo sulla eventuale estensione della dominanza sui mercati collegati.

---

587 Così MARTA VALSECCHI, direttore dell'Osservatorio Internet Media del Politecnico di Milano nell'articolo di M. Gianni citato.

588 ID., *op.cit*, *ivi,* p. 2, cit.

589 J. KENNEDY, *op. cit.,* p 17, cit.: «Perhaps most important, the terms of use do not prevent legislators or privacy regulators from enacting binding laws on how companies protect and use data, irrespective of what the terms of use say».

590 mercato del prodotto e mercato geografico.

4.1. *I servizi di* Google *e l'estrazione dei dati*

Procediamo con la descrizione dei servizi «offerti» da *Google* e dell'apporto fornito dai dati nell'erogazione di questi servizi.

Da quanto finora esposto si evince chiaramente che *Google*, grazie ai dati che estrae e analizza, può migliorare il *search advertising* e con i suoi servizi integrati ricavare sempre nuovi dati, in un circolo vizioso che vede come destinatario degli introiti un solo grande ingordo: *Google* stesso.

Specificamente la piattaforma pubblicitaria di *Big G.* consta di due servizi *AdSense* e *AdWords*. Il primo offre *banner* pubblicitari dietro pagamento agli utenti che vogliano pubblicare annunci pubblicitari sul proprio sito *web*, consentendo loro di guadagnare in base al numero di *impression* o *click* sugli annunci pubblicati sul proprio sito. I contenuti pubblicitari sono di soggetti terzi rispetto al *publisher* che li ospita sulle proprie pagine.

Il secondo permette di inserire spazi pubblicitari all'interno delle pagine di ricerca di *Google*. Questi annunci sono visualizzati, fino a quattro, sopra i risultati di ricerca non a pagamento e vengono selezionati da un algoritmo che, tra le tante variabili, tiene conto delle parole chiave ricercate dall'utente. A*dWords* nel 2013 ha permesso a *Google* di guadagnare più di 50 miliardi di dollari. L'algoritmo, impiegato per questo servizio, utilizza la chiave di ricerca e il profilo dell'utente per relazionarlo al potenziale inserzionista[591].

Il primo servizio è collegato con il secondo che è in grado di gestire gli annunci degli inserzionisti adattandoli al contenuto della pagina *web* in base alla pertinenza.

Il prodotto di punta di *Google* sarebbe proprio la ricerca generale che oltre ai risultati fornisce ai consumatori annunci pubblicitari in linea con le ricerche, orientandole. Una quota significativa delle entrate di *Google* deriva proprio dalla pubblicità collegata alle ricerche. *Google* ha quindi interesse a massimizzare il numero di utenti che visualizzano i messaggi pubblicitari inseriti sui suoi siti o su quelli di terzi e può farlo a discapito di quei siti che per le pubblicità si sono rivolti ai suoi concorrenti, ma che vengono penalizzati nella restituzione dei risultati da parte di *Google*, che li metterà agli ultimi posti.

---

[591] F. BERNABÈ, *op. cit.*, pp. 32 ss.

Quello che accade *online* sfugge alla regolazione perché il terreno di gioco è «friabile», nonostante le operazioni economiche che ivi prendono piede siano identiche a quelle attuate un tempo *offline*: gli operatori di comunicazione elettronica, nella dimensione analogica, erano vincolati per legge a utilizzare le informazioni derivanti dall'identità associata alla *sim* o a un doppino telefonico, al solo fine di erogare i servizi, garantirne la qualità e addebitarne i costi. Gli operatori dell'*offline* erano sottoposti dalla legge a procedure rigide di conservazione e gestione dei dati raccolti. *Google*, invece non ha vincoli normativi, è autolegittimato a estrarre i dati che vuole e a utilizzarli per gli scopi che preferisce.

In altre parole se volessimo paragonare il servizio di *e-mail* di *Google* al postino[592] dell'analogico, dovremmo immaginare e accettare come legittimo che lo stesso apra la nostra corrispondenza, la legga e selezioni i suoi contenuti più rilevanti per inviarci pubblicità mirata. Allo stesso modo dovremmo ritenere non lesivo della nostra riservatezza il comportamento dell'operatore telefonico che si mettesse ad ascoltare le nostre conversazioni a costo zero perché è esattamente questo quello che accade *online.*

Google tratterebbe i nostri dati in cambio di servizi gratuiti. Tuttavia, se l'insieme dei dati personali è soggetto alla normativa *privacy* quando è assoggettato al trattamento, vale a dire quando i dati personali sono oggetto di operazioni quali «la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati»[593], *Google* sarebbe titolare del trattamento dei dati[594], e in

---

[592] ID., *ivi*, p. 31.

[593] Si riproduce il contenuto dell'art. 4, comma 1, lett. a), del d.l. 196/2003.

[594] La Corte di Giustizia dell'Unione Europea, nella sentenza del 13 maggio 2014, in relazione al caso *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (causa C-131/12)* ha riconosciuto in *Google* il titolare dei dati personali, statuendo che esso tratta sui suoi *server* i dati che raccoglie sul web e li tratta per un fine che gli è proprio, l'attività commerciale da cui lucra, offrendo un servizio che è diverso da quello svolto dai siti da cui estrae i dati. Il caso in esame si riferiva a una questione specifica: *Google* indicizzando i contenuti di terzi presenti sul web diventava titolare del trattamento di quei dati e quindi responsabile o co-responsabile di quei dati, nel caso specifico il suo trattamento si differenziava da quello del sito che aveva riportato la notizia di cui l'attore chiedeva la cancellazione, ma che solo *Google* era obbligato a cancellare dall'indicizzazione perché la notizia pubblicata dall'editore rispondeva al diritto di cronaca e al dovere di informazione della testata. Dunque le finalità del trattamento dei dati del motore di ricerca sono specifiche e differenziate. In dottrina cfr. K. KOWALIK-BANCZYK- O. POLLICINO, *Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information*, in *German Law Journal*, 17, 3, 2016.

capo a lui dovrebbero riconoscersi se non più stringenti, quantomeno gli stessi obblighi del titolare del trattamento sul versante analogico.

Google rispetto agli operatori dell'analogico possiede strumenti e tecniche più penetranti e invasive. La sua fitta rete di *software* e servizi interconnessi che raccolgono informazioni su ricerche, preferenze, ubicazione territoriale fa di lui il principale «collezionatore» *Over The Top* di dati personali, al punto che viene considerato uno dei principali fornitori di identità digitali.

Servizi quali *Google Search*, *Gmail*, *YouTube*, *Google Maps*, *Google Shopping*, *Google Books* raccolgono dati sull'oggetto delle nostre ricerche, sui contenuti della nostra posta personale, sui video che ci piace guardare, sui posti in cui ci troviamo e sui libri che leggiamo. Utilizzando questi dati potrebbe proporci una notizia «faziosa», sulla quale molto probabilmente cliccheremo perché *Google* conosce anche le nostre debolezze e sa utilizzare il titolo giusto per adescare ciascuno di noi, può suggerirci un itinerario alternativo, più lungo solo per portarci fisicamente dinanzi a un negozio o a un ristorante in cui probabilmente ci fermeremo, il quale ha ovviamente pagato *Google* per ottenere questo genere di servizio pubblicitario.

L'interesse dell'investitore a rivolgersi a *Google* e solo a *Google* sta nel fatto che se maggiore e ben profilata è la platea di *Google,* il messaggio pubblicitario raggiungerà più efficacemente il suo scopo.

Ciascuno di noi paga con i propri dati e accetta possibili restrizioni alla sua libertà: se *Google* non ci avesse proposto quello specifico itinerario, non ci saremmo mai fermati in quel ristorante, se *Google* non ci avesse proposto quelle notizie non avremmo radicato quel particolare convincimento

Google inoltre raccoglie altri dati estrapolandoli dall'utilizzo di telefoni che utilizzano il sistema operativo *Android* di *Google* e le rispettive *app* con esso compatibili.

Allora i suoi servizi, più che servizi per clienti o sistemi per offrire annunci pubblicitari, sono strumenti utili a estrarre quante più informazioni possibili sull'utente.

Tali informazioni, utilizzate nel *search advertising*, remunerano le ulteriori attività di *Google*, che offrirebbe i più disparati servizi allo scopo di alimentare lo stesso mercato dominato del *search advertising*.

Conseguentemente, sulla Rete vivono forti asimmetrie che distorcono la concorrenza. I profili integrati precisi di utenti, offerti solo da *Google* agli inserzionisti, i quali cercano di indirizzare i propri tiri, danno a *Google* un vantaggio competitivo enorme, forse inattaccabile.

4.2. *Le pratiche anticoncorrenziali nello sfruttamento abusivo della dominanza*

Intendiamo qui definire la condotta di «abuso di posizione dominante»[595], come elaborata dalle pronunce della Corte di Giustizia Europea e dalle Comunicazioni della Commissione Europea, per inquadrare la posizione di *Google* in riferimento alle indagini, in corso, per presunta condotta anticoncorrenziale.

Partiremo dalle categorie generali del diritto *antitrust*[596], cui non è sufficiente affidarsi, per indicare una serie di considerazioni utili a correggere la direzione in cui la Commissione Europea si sta muovendo, in particolare riguardo all'individuazione del mercato rilevante.

Come ha osservato il *Chief Economist* di *DG Competition* Tommaso Valletti, «niente di sbagliato se *Google* è il primo motore di ricerca in Europa, nessuno nega che siano bravissimi. Ma vogliamo essere sicuri che *Google* non usi il suo potere di mercato per soffocare la concorrenza e l'innovazione»[597].

In particolare, in riferimento alla configurazione della condotta abusiva non abbiamo una descrizione legislativa della dominanza, tuttavia la giurisprudenza comunitaria[598] la

---

[595] In part., all'art. 102 TFUE e art. 3, l. n. 287/1990.

[596] Per un approfondimento sul tema si rimanda a F. DELL'AVERSANA, *Le libertà economiche in Internet: competition, net neutrality e copyright*, Roma, Aracne, 2014, pp. 49 ss. e a M.F. DE TULLIO, *Iniziativa economica e libertà di informazione nel «mercato integrato» dei motori di ricerca*, in *Astrid*, 14, 2015.

[597] P. LICATA, *Tommaso Valletti: "Concorrenza & innovazione, così l'Europa affronta la sfida"*, in http://www.corrierecomunicazioni.it/l-europa-che-verra/43247_tommaso-valletti-concorrenza--innovazione-cosi-l-europa-affronta-la-sfida.htm, 8 settembre 2016, cit..

[598] La prima definizione della nozione si può trovare nella decisione della Commissione del 9 dicembre 1971 relativa ad una procedura contro la *Continental Can Company*, laddove si legge: «un'impresa si trova in posizione dominante quando può disporre di un'ampia libertà di comportamento che le permette di agire prevalentemente senza tener conto dei concorrenti, degli acquirenti o dei fornitori; che questa situazione si presenta quando tale impresa, in virtù della sua parte di mercato o della sua parte di mercato unita in particolare al possesso di conoscenze tecniche e alla disponibilità di materie prime o di capitali, ha la possibilità di determinare i prezzi o di controllare la produzione o la distribuzione di una parte cospicua dei prodotti considerati; che questa possibilità non deve necessariamente scaturire da un dominio assoluto che consenta all'impresa in questione di eliminare ogni iniziativa

definisce come «una posizione di potenza economica, grazie alla quale l'impresa che la detiene è in grado di ostacolare la persistenza di una concorrenza effettiva sul mercato in questione, e ha la possibilità di tenere comportamenti alquanto indipendenti nei confronti dei concorrenti, dei clienti e, in ultima analisi, dei consumatori»[599].

Se da un lato la presenza sul mercato di un'impresa in grado di tenere comportamenti «alquanto indipendenti» da quelli dei concorrenti sarebbe di per sé legittima, se non presupposta dalla stessa qualifica di «abuso di posizione dominante»[600]; dall'altro, l'ordinamento comunitario si è dotato di una normativa *ad hoc* per controllare le concentrazioni. Tale disciplina ha come obiettivo quello di impedire creazioni e rafforzamenti di posizioni dominanti, mediante un giudizio pronostico, in grado di ridurre o eliminare in modo durevole la concorrenza sui mercati interessati.

L'impresa dominante ha, infatti, una doppia responsabilità[601] che le impedisce di tenere comportamenti che in regime di libero mercato le sarebbero consentiti e le impone di compiere scelte che favoriscano lo sviluppo della concorrenza.

Se la concorrenza è già compromessa, l'impresa egemone nel mercato non dovrebbe comportarsi in un modo, che seppure legittimo nel mercato concorrenziale, ostacolerebbe ulteriormente la concorrenza.

Alla luce di ciò, come indicato a più riprese dalla Commissione, sarebbe opportuno guardare alla condotta[602] più che al divieto in sé, quest'ultimo ha lo scopo di limitare la rendita di posizione di cui gode il monopolista e di invocare la tutela della concorrenza laddove non c'è più.

---

da parte dei suoi partner economici, ma è sufficiente che sia complessivamente talmente forte da assicurare a questa impresa un'indipendenza globale di comportamento, anche se esistono delle differenze di intensità della sua influenza sui vari mercati parziali». Cfr. Cfr. causa *Continetal Can Company/Commissione*, in *Racc.*1972, L7/35, punto 3.

599 Corte di Giustizia Europea, causa C-85/76, *Hoffmann La Roche/Commissione*, sentenza del 13 febbraio 1979.

600 Altrettanto legittima sarebbe la possibilità da parte dell'impresa di trarre dalla dominanza il giusto profitto: F. GHEZZI - G. OLIVIERI, *Diritto Antitrust*, Giappichelli, Torino, 2014, p. 200 ss.

601 Corte di Giustizia, 9 novembre 1983, causa C-322/81, *Nederlandsche Banden Industrie Michelin c. Commissione delle Comunità europee*, in *Racc.*, 1983, I-3461, par. 57: «La constatazione dell'esistenza della posizione dominante non comporta di per sé alcun addebito nei confronti dell'impresa interessata, ma significa solo che questa indipendentemente dalle cause di tale posizione è tenuta in modo particolare a non compromettere con il suo comportamento lo svolgimento di una concorrenza effettiva e non falsata nel mercato comune» e par. 70.

602 L. F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, Jovene, Napoli, 2013, pp. 95 ss.; S. BASTIANON, *L'abuso di posizione dominante*, Giuffrè, Milano, 2001, pp. 34 ss.

Nella Comunicazione della Commissione[603] relativa alle linee direttrici sulla nozione di pregiudizio al commercio tra Stati membri di cui agli articoli 101 e 102[604] del TFUE sono indicate alcune modalità attraverso le quali può verificarsi il pregiudizio al commercio in relazione alle diverse tipologie di condotta abusiva dell'impresa in posizione dominante.

Secondo l'articolo 102, testé menzionato, «è incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo.

Tali pratiche abusive possono consistere in particolare:

a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque;
b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori;
c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza;
d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi».

L'elenco dei comportamenti abusivi non ha carattere esaustivo perché le pratiche sono descritte a mero titolo esemplificativo.

---

603 in G.U.U.E. C-101, 27 aprile 2004, p. 81.

604 L'Articolo 102 del TFUE recita: «È incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo.
Tali pratiche abusive possono consistere in particolare:
a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita od altre condizioni di transazione non eque;
b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori;
c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza;
d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi».

Anche se la condotta di *Google* esclude inizialmente parte della concorrenza, non significa automaticamente che gli sia imputabile qualche forma di illiceità[605], tuttavia il comportamento di un'impresa che goda di una forza economica, come quella di *Google*, potrà qualificarsi come abusivo quando l'impresa ostacola lo sviluppo della concorrenza utilizzando mezzi diversi da quelli su cui si fonda la normale concorrenza[606].

La effettività della concorrenza non è un fine in sé, ma la condizione per realizzare un mercato interno libero e dinamico; strumento di sviluppo di un benessere economico comune. Non si può trascurare l'inadeguatezza della disciplina *antitrust* rispetto la *new economy* e ai nuovi modelli di *business.*

Per tale ragione, partiremo da una lettura in chiave nuova dei fattori che concorrono a determinare la posizione dominante quali quota di mercato, quote di mercato concorrenti, la stabilità nel tempo della quota di mercato, caratteristiche dell'impresa e barriere[607] all'entrata dei nuovi entranti[608].

4.3. *Il mercato rilevante e la quota di mercato*

Primo elemento costitutivo per la qualificazione della dominanza[609] di *Google*, e in via logicamente consequenziale del concreto atteggiarsi dello sfruttamento abusivo della stessa, è la quota di mercato. Per determinarla sarà necessario guardare al mercato

---

605 G. A. MANNE - J. D WRIGHT , *Google and the Limits of Antitrust: The Case Against the Case against Google,* in "*Harvard journal of Law & Public Policy*", volume 34, pp. 178- 189.

606 N. NEWMAN, *The Cost of Lost Privacy: Search, Antitrust and the Economics of the Control of User Data*, in *Yale J. On Reg.*, 31, 401, 2014.

607 Commissione europea (2008), 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, Gazzetta Ufficiale dell'Unione Europea.

608 Cfr. caso COMP/34.780, *Virgin/British Airways*, (1999), punto 87; Cause riunite T-24/93, T-25/93, T-26/93 e T- 28/93 *Compagnie Maritime Belge Transports e altri/Commissione*, *Racc.* 1996, pag. II-1439, punto 76.

609 Corte di giustizia, 14 febbraio 1978, causa C-27/76, *United Brands Company e United Brands Continentaal BV c. Commissione delle Comunità europee*, in *Racc.*, 1978, 207; 13 febbraio 1979, causa C-85/76, *Hoffmann – La Roche c. Commissione delle Comunità europee*, in *Racc.*, 1979, 461, par. 21.

rilevante[610] secondo le due variabili: mercato del prodotto e mercato geografico che sono così definiti:

a) «Un 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 prezzi e dell'uso al quale sono destinati».
b) «Un mercato geografico rilevante comprende l'area nella quale le imprese in causa forniscono prodotti o servizi rilevanti, nella quale le condizioni di concorrenza sono sufficientemente omogenee e che può essere tenuta distinta dalle zone geografiche contigue perché, in particolare, in queste ultime le condizioni di concorrenza sono sensibilmente diverse».

Il primo è, come si leggerà, a giudizio della Commissione Europea, quello del *search advertising*, la Commissione sembrerebbe focalizzare la sua attenzione sul carattere merceologico del mercato; il secondo deve essere parcellizzato in più segmenti relativi all'area geografica di insistenza.

L'ampiezza del mercato rilevante dipende quindi dalle proprietà del prodotto, dalla presenza e dall'atteggiamento dei consumatori nonché dalla loro disponibilità a passare a un prodotto alternativo.

Con riferimento ad a) per determinare tali circostanze bisogna verificare la sostituibilità dal lato della domanda attraverso lo studio dell'elasticità incrociata[611], ossia si verifica se «i clienti delle parti passerebbero a prodotti sostitutivi prontamente disponibili, o si rivolgerebbero a fornitori siti in un'altra zona, in risposta ad un ipotetico piccolo incremento (dell'ordine del 5-10%) di carattere permanente del prezzo dei prodotti stessi nell'area considerata. Se il tasso di sostituzione è sufficiente a rendere non redditizio l'incremento del prezzo a causa del calo di vendite che ne conseguirebbe, si aggiungono al mercato considerato altri prodotti ed altre aree finché non viene individuato un insieme di prodotti e di aree tale che un lieve incremento permanente dei prezzi sarebbe redditizio».

---

610 F. CINTIOLI (a cura di), *Concorrenza, istituzioni e servizio pubblico*, Milano, Giuffré, 2010, pp. 41 ss.

611 Gazzetta Ufficiale (1997), C 372 Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto comunitario in materia di concorrenza, pag. 7, punto 17.

La funzionalità d'uso è il parametro principale per verificare la sostituibilità della domanda[612], ma è altrettanto importante il prezzo che è rappresentativo del grado di omogeneità dei mercati in merito alle condizioni contrattuali[613].

Successivamente si esamina la sostituibilità dal lato dell'offerta vale a dire se i «fornitori siano in grado di modificare il loro processo produttivo in modo da fabbricare i prodotti in causa ed immetterli sul mercato in breve tempo, senza dover sostenere significativi costi aggiuntivi o affrontare rischi eccessivi, in risposta a piccole variazioni permanenti dei prezzi relativi».

Va ora precisato che il prodotto offerto da *Google* e cioè l'inserzione mirata non sarebbe sostituibile con gli altri prodotti presenti sul mercato.

I difensori di *Google* hanno cercato di minimizzare la dominanza di *Google* nel settore, sostenendo che il *search advertising* è un sostituto della pubblicità tradizionale, ma già la Corte Suprema[614] ha considerato la pubblicità personalizzata come un mercato rilevante ai fini *antitrust*[615].

In *Times-Picayune Pub. Co. v. Stati Uniti*, la Corte ha distinto la pubblicità su giornale dalla «pubblicità inserita su altri mezzi di comunicazione» sulla base di una «propria caratterizzazione del commercio dei prodotti coinvolti» e sul modo in cui l'industria della pubblicità distingue «tra pubblicità sui giornali e su altri mezzi di comunicazione»[616].

Dunque, nel *search advertising*, nelle parole dell'economista David Evans, «sarà necessario considerare il prodotto gratuito insieme al suo prodotto-compagno che produce ricchezza»[617].

---

612 Cfr. causa COMP/M.3354 *Sanofi/Aventis* (2004), pag. 3-4, punto 14 e seguenti.

613 Cfr. causa COMP/M.3770 *Lufthansa/Swiss Air* (2005), pag. 4.

614 Corte Suprema degli Stati Uniti, 25 maggio 1953, *Times-Picayune Pub. Co. v. Stati Uniti*, 345 us 594, 1953, 610 - 614.

615 Commissione Europea, 27 Maggio 1998, caso IV/JV.1, *Telia/Telenor/Schibstedt,* para 5.142; caso IV/M.1439, 3 ottobre 1999 *Telia/Telenor,* para 3.27; caso IV/M.0048, 20 luglio 2000, *Vodafone/Vivendi/Canal Plus* para 6.65; caso COMP/M.4731, 11.
marzo 2008, *Google/DoubleClick*; caso COMP/M.5727, 18 febbraio 2010, *Microsoft/ Yahoo!Search business*.

616 *iab Internet Advertising Revenue Report: An Industry Survey Conducted by PwC and Sponsored by the Interactive Advertising Bureau (iab)*, in *www.iab.net*, 2012, p. 20-27.

617 D.S. EVANS, *The Antitrust Economics of Free*, in *Competition Policy International*, 2011, p. 17, cit. Il passaggio in lingua originale è il seguente «will need to consider the free product together with its companion moneymaking product».

Posto che i servizi di *Google* non sono gratuiti se chi li usa diventa il prodotto venduto ai clienti reali di *Google*, e cioè ai suoi inserzionisti, il prodotto che vende *Google* è un *click* su un annuncio pubblicitario. Ebbene, data la sua posizione dominante, *Google* ottiene molti più *click* di qualsiasi altro concorrente e quindi maggiori entrate. In un contesto competitivo ci aspetteremmo che il *click* sul sito di un concorrente abbia lo stesso valore di un *click* su *Google*[618]; invece, il Prezzo per *click* (*Pay per click*) che gli inserzionisti pagano a *Google* sembrerebbe più alto rispetto a quello imposto dagli altri concorrenti agli inserzionisti, e allo stesso tempo più vantaggioso per gli inserzionisti perché *Google* consente di rivolgere una determinata pubblicità a chi molto probabilmente acquisterà e lo farà anche a un prezzo discriminato per *bundles*[619].

I profili cuciti addosso ai consumatori, nelle mani di *Google* sovvertirebbero i tradizionali meccanismi di adeguamento domanda e offerta e aprirebbero le strada a una possibile *price discrimination* da parte dei fornitori, i quali si servirebbero della pubblicità presso gli utilizzatori di *Google* per diversificare i prezzi. Il prezzo sarà tanto più alto quanto maggiore sarà la disponibilità del cliente ad acquistare quel prodotto, con il rischio che vengano sviluppate pratiche predatorie[620], difficilmente individuabili *ex post*.

I dati, allora diventano la nuova discriminante competitiva: chi non li ha non può entrare sul mercato.

Quindi, qualsiasi concorrente di *Google* deve pagare non solo i costi fissi per la creazione di un servizio concorrente che sia all'altezza, per di più con un minor numero di utenti iniziali, ma guadagnerà molto meno di *Google* perché pochi saranno i *click* sugli annunci. E se pochi saranno i *click*, scarse saranno le possibilità di raccogliere dati e impacchettarli per orientare gli annunci pubblicitari futuri da vendere agli inserzionisti. Ai fini della nostra indagine, occorre stabilire, successivamente, se l'impresa sia in grado di esercitare un potere qualificabile in termini di posizione dominante.

---

[618] N. NEWMAN, *op. cit.*, p. 25 ss.

[620] F. GHEZZI - G. OLIVIERI, *op. cit.*, pp. 229 ss.

Con riferimento a b) la posizione dominante viene considerata in relazione al mercato interno, valutato nel suo insieme o in riferimento a una parte sostanziale di esso, prenderemo qui in esame il mercato europeo.

Guarderemo allora, alla quota di mercato[621], la quale viene calcolata in base al fatturato realizzato dall'impresa sul mercato rilevante.

Quando essa è maggiore del 70% la dominanza è presunta, essendo già sufficiente una quota superiore al 50% a dare prova dell'esistenza di una posizione dominante sul mercato, tuttavia la Commissione si è riservata di esaminare il comportamento di quelle imprese con soglie anche inferiori al 40% in casi specifici in cui i concorrenti non riescano a contrastare il potere di mercato dell'impresa e che ben potrebbero essere dominanti, come nel caso in esame.

Occorre guardare, inoltre, ai mercati collegati, interdipendenti benché mercati distinti, su cui *Google* ha una posizione preminente rispetto al mercato dominato, ma che lo influenzano e alimentano, fornendo sempre più dati a *Google*. La verifica delle quote di mercato non va effettuata in termini assoluti, ma nel quadro di una valutazione comparativa - che tenga conto della posizione degli altri concorrenti sul mercato – e temporale[622].

Sebbene non vi siano vere e proprie pratiche leganti (*tying contract*)[623], intese come pratiche attraverso le quali l'impresa dominante impone ai suoi utenti l'acquisto di servizi supplementari a quelli richiesti, e non necessari per la fruizione o il godimento dei primi, avvalendosi del collegamento tecnico, funzionale o commerciale esistente tra i due beni, tuttavia va rilevato, per esempio che la navigazione mediante il *browser Chrome* di *Google* offre migliori prestazioni in termini di funzionalità nell'utilizzo del suo servizio *Cloud*, tali funzionalità aggiuntive inibiscono la libera scelta di utilizzare un altro *browser* quale

621 P. POZZI, *I nuovi padroni della pubblicità, la mappa di chi comanda e investe sui media in Italia*, in *New Tabloid*, 3, 2014.

622 L. C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza,* Cedam, Padova, 2007, p. 2487.

623 Le pratiche leganti sono quelle con le quali l'impresa dominante impone ai suoi contraenti l'acquisto di beni o servizi supplementari rispetto a quelli richiesti ma che non siano strettamente necessari per la fruizione o il godimento dei beni o servizi principali, avvalendosi del collegamento tecnico, funzionale o commerciale esistente tra i due beni (come nel caso *Microsoft* del 1998). Simile è anche la tecnica del *Bundling* che consiste nel praticare politiche di prezzo che rendano conveniente acquistare una intera gamma di prodotti piuttosto che un singolo prodotto di punta (v. i prezzi I-Tun di singole canzoni o di interi cd). Cfr. F. SCAGLIONE, *Il mercato e le regole della concorrenza*, p. 224 ss.

Firefox[624]. Allo stesso modo, se i dispositivi con sistema operativo *Android*, richiedono per il funzionamento delle applicazioni incorporate e incorporabili un *account* di posta elettronica *Gmail*, l'utente è «costretto» a rivolgersi ai servizi offerti da *Google*. Dunque, se si vuole fruire dei servizi e delle applicazioni del proprio *smartphone*, quale quella per raggiungere un posto geografico[625], utilizzare uno spazio *cloud* o ascoltare la radio è essenziale registrarsi su *Google*. E se è vero che *Google* mette a disposizioni le A.P.I., come già si è scritto, per consentire a terzi lo sviluppo delle sue applicazioni *Android*, saranno pur sempre applicazioni che apportano maggiori utilità a *Google*. Non è sufficiente, pertanto, escludere la dominanza di *Google* con l'abusato argomento secondo cui occorre semplicemente considerare se i consumatori possono rivolgersi a un altro fornitore[626].

Seguendo questo ingenuo ragionamento, poiché i servizi offerti sono gratuiti e gli utenti possono andarsene quando vogliono, *Google* non sarebbe in dominanza. Si considera, in questo modo, il mercato dominante da un punto di vista meramente merceologico, e quindi funzionale alla sostituibilità del prodotto, senza cogliere tutto ciò che comporta la dimensione di un operatore orizzontalmente e verticalmente integrato, i cui servizi coartano[627] le libertà dell'utente.

Ulteriore elemento sintomatico della dominanza di *Google* si evincerebbe dalla risposta alla seguente domanda: quanto probabile e agevole sarebbe per gli inserzionisti passare a un'altra piattaforma? Considerato che *Google* non è un fornitore di contenuti che si autofinanzia con la pubblicità, ma una società che vende l'accesso agli inserzionisti, o meglio vende loro il profilo a cui direzionare il prodotto, la conoscenza pervasiva di *Google* degli utenti rende pressoché impossibile per un nuovo entrante corteggiare gli inserzionisti che si rivolgono a *Google*.

---

624 Parla della dittatura dell'assenza di alternative quando ci viene fatto credere che *Gmail* sia il miglior servizio di posta il teorico sociale brasiliano Roberto Unger.

625 Se si cerca un indirizzo geografico sul motore di ricerca di *Google*, utilizzando il *browser* dello *smarthphone*, il servizio offerto da *Google* invita l'internauta a scaricare l'*app Android* sul telefonino, inibendo in caso contrario il calcolo degli itinerari.

626 R. BORK, *Antitrust and Google, in Chicago tribune*, 6 aprile 2012 in cui l'autore afferma: «There is no coherent case for monopolization because a search engine, like *Google*, is free to consumers and they can switch to an alternative search engine with a click.» e D. BALTO, *Google is No Microsoft*, in *Huffington post*, 30 giugno 2011.

627 S.D. HOUCK, *Search, Innovation, and Antitrust*, in *Huffington post*, 10 novembre 2011.

4.4. *Altri fattori strutturali indicativi dello sfruttamento abusivo della dominanza*

Secondo la giurisprudenza comunitaria la quota di mercato è solo uno dei fattori che l'interprete è chiamato ad accertare, pertanto, si considereranno: *a*) la stabilità della quota di mercato; *b*) il numero delle imprese concorrenti e le pressioni concorrenziali da loro esercitabili sulla strategia commerciale del *leader*; *c*) il ruolo della concorrenza potenziale e cioè se il mercato è in grado di estendersi grazie ai concorrenti già operanti o nuovi; *d*) le barriere all'ingresso o all'espansione del mercato; *e*) la forza finanziaria dell'impresa, e cioè se l'impresa è in grado di attingere risorse economiche, anche al di fuori del mercato rilevante per finanziare la propria attività nel settore. Con riferimento ad *a*) il monitoraggio della quota di mercato mette in evidenza che *Google* ha stabilmente mantenuto per alcuni anni una quota significativa del mercato senza che la stessa sia stata erosa dai concorrenti.

Con riguardo a *b*) e *c*) molto è già stato scritto, la pressione esercitabile dai concorrenti, che si ribadisce non hanno i dati che ha *Google*, al punto che i nuovi entranti non riescono nemmeno ad entrare sul mercato, è prossima allo zero, tantomeno il mercato è idoneo a estendersi ai concorrenti già operanti nel mercato. In riferimento a *d*) relativamente alla barriera all'ingresso dei nuovi entranti occorre interrogarsi su come il controllo dei dati personali possa tradursi nel potere di monopolio, in una economia sempre più modellata sul potere dei *Big Data* e come un simile controllo sui dati personali degli utenti, in continua espansione possa creare una barriera all'ingresso insormontabile ai nuovi entranti.

La nozione di barriera si identifica con qualsiasi ostacolo considerevole all'insediamento di un nuovo entrante a prescindere da ogni raffronto con gli eguali costi che l'impresa già insediata ha a suo tempo dovuto affrontare, includendo oltre alle barriere legali (tariffe o quote) e ai vantaggi di cui può godere un'impresa dominante (economie di scala e scopo, accesso privilegiato a materie prime o risorse naturali), anche le tecnologie[628],

[628] Cfr. causa T-30/89, *Hilti/Commissione*, in *Racc.* 1991, pag. II-1455, punto 19.

network distributivi e di vendita[629], costi e altri impedimenti derivanti da effetti di rete[630], nonché investimenti significativi[631].

Gli effetti di rete, naturalmente, non sono sempre cattivi per i consumatori, tuttavia, «network effects, at times, enable big firms to become bigger until they dominate the industry»[632].

Si tratta, innanzi tutto di una barriera economica[633], più che giuridica[634], che impedisce agli altri operatori di competere con l'impresa dominante.

L'accesso ai dati potrebbe essere paragonato a risorse naturali[635] o a diritti di proprietà intellettuale, quale un brevetto sul principio attivo di un farmaco[636].

Ulteriori barriere all'ingresso, in quanto impeditive dell'ingresso dei nuovi operatori sono le economie di scala e la necessità di effettuare ingenti investimenti che seppure, in qualche modo superati non riuscirebbero a traghettare un'impresa senza dati che sarebbe costretta a uscire dal mercato. Con riguardo alla forza finanziaria dell'impresa, di cui alla lettera *e*), rileva la posizione verticalmente integrata di *Google*, la sua scelta strategica è quella di integrare all'interno della propria filiera il maggior numero possibile di servizi produttivi intermedi, orientati alla raccolta dei dati e necessari per ottenere il prodotto finito, l'inserzione mirata, oltre a quella di integrazione orizzontale, che consente all'impresa di offrire più servizi differenziati e autonomi[637].

Seppure non si possa parlare di sussidi incrociati, deve far riflettere che l'impresa utilizzi i ricavi del mercato dominato non per finanziare politiche di prezzo aggressive su altri mercati, dove è esposta a una concorrenza effettiva, ma per mettere a punto servizi

---

629 Cfr. causa 85/76, *Hoffmann-La Roche/Commissione*, in *Racc.* 1979, pag. 524, punto 48.

630 Cfr. causa *COMP/ M.1845 AOL/ Time Warner* (2000), pag. 17, punto 69.

631 Cfr. causa 27/76, *United Brands/Commissione*, in *Racc.* 1978, pag 284, punto 91.

632 M. E. STUCKE - A. P. GRUNES, *Debunking the Myths over Big Data and Antitrust*, p. 6, cit.

633 Si veda agcm, A436 – *Arenaways – Ostacoli all'accesso nel mercato dei servizi di trasporto ferroviario passeggeri*, provv. n. 23770, 25 luglio 2012, in *Boll.*, n. 30, 2012.

634 Si pensi alla concessione demaniale marittima e di accosto necessaria per il servizio di traghettamento attraverso lo stretto di Messina, in agcm, A267 – *Diano/Tourist Ferry Boat – Caronte Shipping,* provv. n. 10650, 17 aprile 2002, in *Boll.*, n. 16, 2002.

635 Come i gessi utilizzati per finalità escludenti in agcm, A383 – *Mercato del cartongesso*, provv. n. 21297, 30 giugno 2010, in *Boll.*, n. 26, 2010.

636 agcm, A431 – *Ratiopharm/Pfizer*, provv. n. 23194, 11 gennaio 2012, in *Boll.*, n. 2, 2012.

637 J. FARREL - P.J.WEISER, *op. cit.*, p.

efficienti, finalizzati a calamitare quanti più utenti, non di certo per uno spirito missionario, ma lucrativo e in qualche modo limitativo della libertà degli utenti della Rete.

Dall'analisi fin qui svolta, la condotta di *Google* sembrerebbe accostarsi alla fattispecie dell'abuso di posizione dominante con natura escludente[638], *ex* art. 102, lett. *b*), tfue e 3 della l. n. 287/1990, la quale sembrerebbe finalizzata a ridurre sensibilmente la concorrenza nel mercato, mediante strategie dirette a ostacolare le attività dei concorrenti, con lo scopo di monopolizzare il mercato[639].

Google, con tale abuso, precluderebbe ai concorrenti di competere sul mercato senza neanche dare loro la possibilità di rimanere attivi sullo stesso, e senza bisogno di incrementare la propria quota e scalfire la posizione dominante. E non perché i concorrenti offrono servizi meno efficienti, ma perché non hanno i dati per farlo. Un rapido accenno alla *efficiency defense* di *Google*: l'argomento secondo cui l'impresa avrebbe guadagnato il vantaggio competitivo attraverso la sua innovazione nella tecnologia dei motori di ricerca e il proprio comportamento sarebbe idoneo a produrre efficienze considerevoli, quali miglioramenti tecnici e riduzione dei costi dei servizi di cui i consumatori beneficiano, dovrà correggersi. *Google* avrebbe, infatti, aggressivamente espanso il proprio controllo attraverso l'allargamento a nuovi settori merceologici per raccogliere i dati aggiuntivi degli utenti, con il chiaro intento di usare la sua presenza in tali altri mercati per rafforzare il suo monopolio nel *search advertising*.

Gli eventuali incrementi di efficienza non possono compensare il pregiudizio per la concorrenza che in ogni caso deriverebbe dall'assenza di competizione tra le imprese. Non può essere, pertanto, giustificato con le efficienze un abuso escludente che rafforza un monopolio.

Lo sfruttamento abusivo di Google della dominanza nel mercato del *search advertising* deriva dalla posizione di vantaggio nella «*data collection*»[640] collegata alla sua posizione

---

638 Sugli effetti di simile condotta si legga la Comunicazione della Commissione Europea 2009/C 45/02, in *http://eur-lex.europa.eu.*

639 A tal riguardo si evidenzia come lo *Sherman Act* statunitense sanziona solo i comportamenti in cui l'impresa «*monopolize*» o «*attempt to monopolize*».

640 Jonathan Rosenberg, vp del Product Management e Marketing di *Google* ha spiegato in una dichiarazione incauta nel 2008: «We get more users because we have more advertisers because we can buy distribution on sites that understand that our search engine monetizes better. So more users more information, more information more

preminente nel mercato dei servizi *online*. A tal proposito va evidenziato che *Google* non ha i migliori algoritmi, ma ha molti più dati di chiunque altro[641].

Dunque, i dati racchiudono le ricchezze future e chi li possiede e li controlla occupa una posizione di vantaggio perché sono i dati a rendere gli algoritmi più efficaci[642] e non i semplici algoritmi a determinare scelte di profitto. Per questo la capacità di sviluppare *software* sofisticati e contribuire così all'innovazione mediante le proprie competenze non è sostituibile con il controllo dei dati, che tra l'altro non gli appartengono.

Chi possiede i secondi potrà sicuramente sviluppare *software* sempre più utili, ma chi possiede solo i primi non potrà generare quei dati che non ha in un ambiente sempre meno concorrenziale.

Il potere di monopolio che danneggia la libera concorrenza si nasconde e si insidia nel controllo dei dati.

4.5. *Le indagini della Commissione Europea e la decisione sul caso* Google Shopping

Secondo il regolamento (CE) n.1/2003 la Commissione Europea ha il potere di indagare, su richiesta o d'ufficio, se ritiene che possa esserci stata un'infrazione delle leggi sulla concorrenza. Se la violazione è accertata essa può ordinarne la cessazione, disporre misure cautelari, chiedere all'azienda incriminata di assumere alcuni impegni o comminare delle ammende.

Le aziende anche se non si ritengono responsabili hanno un effettivo interesse ad accettare l'assunzione di impegni perché questo permette loro di evitare lunghi processi.

---

users, more advertisers more users, it's a beautiful thing, lather, rinse, repeat, that's what I do for a living. So that's (...) the engine that can't be stopped».

641 Peter Norvig, *Google Chief Scientist*, ha apertamente affermato: «We don't have better algorithms than everyone else; we just have more data».

642 Si rimanda all'esempio degli scacchi, in cui gli autori spiegano come suddetto gioco apprenda dalle mosse dei giocatori per migliorarsi, fino a diventare imbattibile da un uomo. Si veda: V. MAYER-SCÖNBERGER, K. CUKIER, *op. cit.*, p. 55 ss. nello stesso volume è riportato l'esempio dello sviluppo del correttore ortografico di *Banko* e *Brill*, che ha utilizzato 3 algoritmi con un milione di parole, e ha messo in luce che a funzionare meglio era l'algoritmo meno elaborato ma con un numero maggiore di dati, piuttosto che quello più sofisticato, ma con un numero minore di dati.

Inoltre, così facendo si mette fine alle contestazioni della Commissione, che se li considera accettabili, li renderà vincolanti per l'azienda e chiuderà il procedimento[643].

Già nel 2010 la Commissione Europea e diverse Autorità nel mondo[644] avevano avviato indagini su un presunto abuso di posizione dominante[645] di *Google*.

Il motore di ricerca nei paesi europei ha una quota di mercato molto più ampia di quella che possiede negli Stati Uniti[646]. La quota di mercato detenuta da *Google* in Europa, come anticipato, nei servizi di ricerca generale su internet è superiore al 90%, nelle inserzioni pubblicitarie sui siti internet di terzi in tutto il SEE è superiore all'80%.

Ictu oculi l'azienda ha un forte potere di mercato[647].

La Commissione ritiene che quote molto alte, comprese tra l'80 e il 100%, «costituiscono di per sé la prova dell'esistenza di una posizione dominante; in effetti, la detenzione di una quota di mercato particolarmente cospicua pone l'impresa che la detiene durante periodi di una certa entità, in una posizione di forza che la rende controparte obbligatoria e che, già per questo fatto, le garantisce, quanto meno per periodi relativamente lunghi, l'indipendenza di comportamento che caratterizza la posizione dominante»[648]; quote intermedie tra il 40% e l'80% invece «sono un valido indizio dell'esistenza di una potenza preponderante»[649], ma bisogna comunque considerare le quote detenute dai concorrenti.

---

643 L. C. UBERTAZZI, *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, Cedam, Padova, 2007, pp. 2517-2585.

644 *Antitrust: Commission Probes Allegations of Antitrust Violations by Google*, Brussels (November 30, 2010); *Google Faces Texas Ag Inquiry, Settles Privacy Suit*, REUTERS (September 3rd, 2010); *Italy Launches Antitrust Probe Of Google News*, LAW 360 (August 27, 2009); *French Mapmaker Takes Google Maps To Court*, RFI, (July 29, 2009); *U.S. v. Google Inc.*, Case No: 1:11-Cv-0,0688; *Tradecomet.Com LLC v. Google Inc.*, Case No.09-Cv-01400; *Google, Inc v. Mytriggers.Com*, Inc. Case No. 09-Cv-1483.

645 Si precisa che la FTC ha chiuso il caso nel 2013 senza rilevare alcun illecito ritenendo che le innovazioni del motore di ricerca, che permettono per esempio di ottenere informazioni e dati direttamente nella pagina dei risultati – si pensi alla ricerca dei voli - senza dovere cliccare sui *link*, sono servite per migliorare l'esperienza d'uso degli utenti e non per penalizzare la concorrenza. Cfr. in *https://www.ftc.gov/news-events/press-releases/2013/01/Google-agrees-change-its-business-practices-resolve-ftc*. *Contra* A. EFRATI E B. KENDALL, *Google Dodges Antitrust Hit FTC Extracts Limited Concessions, Clears Web Giant of 'Search Bias' After Probe*, in *Wall Street Journal*, 3 gennaio 2013, in *http://www.wsj.com/articles/SB10001424127887323874204578219592520327884.*

646 68% secondo i dati elaborati dall' *Adobe Digital Index*.

647 Secondo la Commissione Europea *Google is dominant in the European Economic Area both in web search and search advertising*, cfr. in *MEMO/13/383 Commission seeks feedback on commitments offered by Google to address competition concerns – question and answers*, in *http://europa.eu/rapid/press-release_MEMO-13-383_en.htm* e in *http://europa.eu/rapid/press-release_IP-16-2532_it.htm.*

648 Cfr. causa 85/76*, Hoffmann – La Roche/Commissione*, in *Racc.* 1979, p. 521, punto 41.

649 Cfr. causa 322/81, *Michelin/Commissione*, in *Racc.* 1983, pp. 3509, punto 52.

In riferimento alla procedura europea, la dominanza di *G.* nel mercato dei motori di ricerca[650] veniva denunciata dinanzi alla Commissione Europea, attraverso gli esposti dei motori di ricerca rivali (*Microsoft*, *Expedia* e *Trip Advisor*).

La Commissione Europea il 13 marzo 2013, ha adottato una valutazione preliminare conformemente all'articolo 9, paragrafo 1, del regolamento (CE) n. 1/2003 rivolta a *Google.* Nella sua valutazione preliminare la Commissione ha ritenuto che *Google* ha adottato una serie di pratiche commerciali suscettibili di violare l'articolo 102 del TFUE e l'articolo 54 dell'accordo SEE e ha dato a *G.* l'opportunità di offrire rimedi, da sottoporre al *market test*, per affrontare le preoccupazioni concorrenziali[651].

Tali pratiche anticoncorrenziali sono state individuate in numero di 4:

1. *G.* avrebbe favorito nei risultati orizzontali, i propri servizi a danno di quelli degli altri *competitor*, riservando priorità ai suoi servizi di ricerca verticali in Internet rispetto ai servizi di ricerca verticali della concorrenza[652];
2. *G.* avrebbe utilizzato senza consenso i contenuti di siti terzi inserendoli nei propri servizi di ricerca specializzati[653];
3. *G.* avrebbe utilizzato accordi di esclusiva della pubblicità con i siti partner cioè accordi che obbligano i siti *web* di terzi, cioè gli inserzionisti, a ottenere da *Google* tutti o gran parte dei loro annunci pubblicitari nei motori di ricerca[654];
4. *G.* avrebbe imposto restrizioni contrattuali sulla trasferibilità delle campagne

---

650 in *http://europa.eu/rapid/press-release_IP-10-1624_en.htm.*

651 cfr. con SPEECH/12/372 del Vice Presidente della Commissione Europea e Commissario alla Concorrenza, Joaquín Almunia in *http://europa.eu/rapid/press-release_SPEECH-12-372_en.htm.*

652 «First, in its general search results on the web, *Google* displays links to its own vertical search services. Vertical search services are specialised search engines which focus on specific topics, such as for example restaurants, news or products. Alongside its general search service, *Google* also operates several vertical search services of this kind in competition with other players» – J. Almunia *speech*/12/327.

653 «Our second concern relates to the way *Google* copies content from competing vertical search services and uses it in its own offerings. *Google* may be copying original material from the websites of its competitors such as user reviews and using that material on its own sites without their prior authorisation. In this way they are appropriating the benefits of the investments of competitors. We are worried that this could reduce competitors' incentives to invest in the creation of original content for the benefit of internet users. This practice may impact for instance travel sites or sites providing restaurant guides». – J. Almunia *speech*/12/3272.

654 «Our third concern relates to agreements between *Google* and partners on the websites of which *Google* delivers search advertisements. Search advertisements are advertisements that are displayed alongside search results when a user types a query in a website's search box. The agreements result in de facto exclusivity requiring them to obtain all or most of their requirements of search advertisements from *Google*, thus shutting out competing providers of search advertising intermediation services. This potentially impacts advertising services purchased for example by online stores, online magazines or broadcasters*».* – J. Almunia *speech*/12/3272.

pubblicitarie nei motori di ricerca a piattaforme rivali e sulla gestione di tali campagne in *AdWords* di *Google* nelle piattaforme rivali di inserzioni pubblicitarie nei motori di ricerca[655].

In questo modo si è offerto a *Google* la possibilità di presentare uno schema di rimedi in grado di affrontare le specifiche questioni. Ciò avrebbe consentito[656] di risolvere le preoccupazioni anticoncorrenziali per mezzo di una decisione relativa agli impegni - ai sensi dell'articolo 9 del regolamento Antitrust UE - invece di dover proseguire il procedimento formale con una comunicazione degli addebiti e di adottare una decisione che infligge ammende e rimedi.

Google ha presentato una prima versione degli impegni nell'aprile 2013[657] su tutti e quattro gli addebiti, la quale però, sentito il parere dei concorrenti, è stata ritenuta inadeguata; è seguita una seconda versione nell'ottobre 2013[658], anche questa volta gli impegni[659] sono stati ritenuti insufficienti.

Successivamente il 5 febbraio 2014, il vicepresidente Almunia ha fatto sapere che *Google* si era dichiarata disposta ad assumere degli impegni ai sensi dell'articolo 9 del regolamento (CE) n. 1/2003, proponendo *i)* di etichettare i propri servizi in modo che agli utenti fossero visibili i risultati ottenuti dalle ricerche come annunci sponsorizzati da *Google* stessa e di rendere visibili tra i risultati i *link* ai siti dei concorrenti per le ricerche di attività commerciali[660]; *ii)* la possibilità per gli editori di esercitare l'*opt-out* dei loro contenuti su

---

655 «Our fourth concern relates to restrictions that *Google* puts to the portability of online search advertising campaigns from its platform AdWords to the platforms of competitors. AdWords is *Google*'s auction-based advertising platform on which advertisers can bid for the placement of search ads on search result pages provided by *Google*. We are concerned that *Google* imposes contractual restrictions on software developers which prevent them from offering tools that allow the seamless transfer of search advertising campaigns across AdWords and other platforms for search advertising». – J. Almunia *speech*/12/3272.

656 Almeno secondo il Vicepresidente Almunia.

657 in *http://eurlex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52013XC0426(02)&from=EN.*

658 il Vice Presidente della Commissione Europea e Commissario alla Concorrenza, Joaquín Almunia, ha illustrato il primo ottobre 2013, durante un'audizione al Parlamento europeo lo stato dell'arte del caso *Google*, in *http://europa.eu/rapid/press-release_SPEECH-13-768_en.htm*.

659 *Google* proponeva di etichettare i propri servizi di ricerca verticali per evidenziare la differenza tra questi e quelli organici, in modo che all'utente potesse essere chiaro che quei link erano stati posizionati in alto nella classifica per scopi promozionali dell'azienda. Per rendere ancora più evidente la distinzione, questi risultati sarebbero stati posti in un'area diversa da quella dove apparivano i risultati organici. Infine, si intendeva inserire il rimando a tre link rivali appositamente selezionati da *Google* seguendo determinati criteri e facendoli partecipare ad un'asta. Tra i siti vincitori sarebbero stati selezionati i tre che sarebbero apparsi su *Google*.

660 In contrasto con il principio della *search neutrality*, cfr. G. A. MANNE - J.D. WRIGHT, *If Search Neutrality is the Answer, What's the Question?*, in *Lewis & Clark Law School Legal Research Paper Series*, 2011-14, p. 4-14; A. D. CRANE

Google News; *iii)* a rinunciare a qualsiasi clausola di esclusiva e a favorire la portabilità dei dati verso terzi, senza modificare però il proprio algoritmo di ricerca. Gli impegni di *Google* sono stati bocciati.

Dopo 5 anni di indagini e negoziati infruttuosi, e soprattutto con il cambio dell'esecutivo UE, la commissaria alla concorrenza, Margrethe Vestager insieme al Presidente della Commissione Europea Juncker ha aperto due fronti legali, sulla base di quelle indagini già avviate.

La Commissione Europea ha inviato a *Google* due comunicazioni degli addebiti[661], accuse formali, meglio note come *Statement of Objection*[662] che indicheremo rispettivamente con *a)* e *b)* e una indagine *antitrust*[663] distinta che indicheremo con *c)*.

La prima accusa formale, già indicata con *a)* ha ad oggetto le ricerche *online* del motore sul quale si concentra il 90% delle ricerche degli utenti europei (65% degli USA), essa riprende l'indagine del 2010, secondo cui *G.* mostrerebbe in posizioni più visibili nei risultati di ricerca il suo servizio di comparazione dei prezzi, a prescindere dal merito, quindi non neutri; la seconda *b)* ha ad oggetto il mercato della pubblicità e la terza *c)* il mercato del sistema operativo *Android*.

In riferimento ad *a)* nell'aprile 2015 la Commissione ha formalizzato la conclusione preliminare dell'indagine nel campo della ricerca *online*. Nel settembre 2015 *Google* ha replicato e la Commissione ha proseguito la sua indagine fino al luglio 2016, quando ha presentato una conclusione supplementare. In particolare le denunce sono state mosse da

---

(2012), *Search Neutrality and Referral Dominance*, in *Journal of Competition Law & Economics* 8, n. 3, p. 459-468; M. AMMORI - L. PELICAN, *Proposed Remedies for Search Bias: 'Search Neutrality' and Other Proposals in the Google Inquiry*, 2012, in *http://ssrn.com/abstract=2058159*.

661 Si badi bene, in base al diritto europeo (articolo 101 TFUE e Regolamento 2003/1/CE del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del trattato) se la violazione è accertata la Commissione Europea può ordinarne la cessazione, disporre misure cautelari, chiedere all'azienda di assumere alcuni impegni o comminare delle ammende. Le indagini possono concludersi o con archiviazione o con una conclusione preliminare che in termini tecnici si chiama *Statement of Objections*, con cui la Commissione formalizza le sue preoccupazioni concorrenziali. In tali casi la società potrà replicare, ci sarà anche un'audizione in contraddittorio, tuttavia una volta che si arriva alle conclusioni preliminari in teoria non ci potrebbe essere più spazio per gli impegni, dunque o si accerterebbe che c'è un illecito o che l'illecito non c'è (in *http://ec.europa.eu/competition/antitrust/procedures_101_en.html*).

662 *Antitrust: Commission sends Statement of Objections to Google on comparison shopping service; opens separate formal investigation on Android*, 15 aprile 2015, in *http://europa.eu/rapid/press-release_IP-15-4780_en.htm* e *Antitrust: Commission takes further steps in investigations alleging Google's comparison shopping and advertising-related practices breach EU rules*, 14 luglio 2016, in *http://europa.eu/rapid/press-release_IP-16-2532_en.htm*.

663 La scheda del caso è disponibile qui: *http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099.*

siti di comparazione dei prezzi che hanno accusato *G.* di danneggiarli. «*Google Shopping* è un servizio pubblicitario legato alla ricerca di prodotti. Quando un utente cerca un prodotto attraverso una parola chiave, *Google* offre i cosiddetti "risultati organici": i siti indicati dall'algoritmo. Ci sono, poi i risultati della pubblicità che sono quelli di *Google Shopping*, finestra che appare alla destra della schermata con le ricerche, con la scritta "Sponsorizzati". Servizio a pagamento che negli anni si è evoluto e oggi appare come una striscia che mostra foto, prezzo, valutazioni dei clienti e riporta al *link* dove si può acquistare il prodotto. L'*Antitrust* Ue accusa *Google* di danneggiare la concorrenza perché favorirebbe i propri risultati di *shopping* rispetto a quelli di altri siti di comparazione dei prezzi»[664]. Quindi il consumatore non troverebbe i risultati più pertinenti alla sua ricerca. Nella prima risposta, un anno e mezzo fa, *Google* si difendeva sostenendo che il mercato dell'*online shopping* è un mercato estremamente competitivo, che deve essere considerato accanto alle piattaforme commerciali *Amazon* e *Ebay*[665].

La Commissione sosteneva che, dal momento che siti come *Amazon* a volte pagano siti comparatori di prezzi per reindirizzare traffico al loro sito, questi non possono essere considerati concorrenti. Siti di comparazione di prezzi che, secondo *G.*, invece sarebbero i concorrenti più diretti del motore di ricerca. *Google* sostiene che i rilievi mossi dalla Commissione europea sono errati perché i cambiamenti che vengono apportati al sito seguono sempre la logica di migliorare l'esperienza dell'utente. I consumatori potrebbero cliccare ovunque e navigare su qualunque sito di loro scelta.

L'Ue ha sostenuto invece che i consumatori non vanno su *Amazon* per confrontare prezzi e caratteristiche dei prodotti. La commissione ha evidenziato, inoltre, che seppure si considerassero incluse nel mercato interessato dalle pratiche di *Google* siti come *Amazon,* i servizi di acquisto comparativo di *Google* costituirebbero comunque una fetta importante di quel mercato e che *Google* ha indebolito la concorrenza dei *competitor* più diretti.

Con riferimento a *b) G.* ostacolerebbe la concorrenza limitando la capacità dei concorrenti di inserire pubblicità sui siti internet di terzi. *G.* tutelerebbe la propria

---

664 *Google risponde ai rilievi Ue*, in *Il sole 24 ore, Nòva24Tech*, 3 novembre 2016, cit..

665 la scheda del caso 39740 *Google Search* è disponibile in *http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740*

dominanza nel mercato della pubblicità nei motori di ricerca e piattaforme pubblicitarie.

G. inserisce la pubblicità sul suo motore di ricerca ma lo fa anche con l'intermediazione, cioè su siti terzi attraverso la piattaforma "*adsense for search*", secondo la Commissione *G.* sarebbe dominante anche sul mercato dell'intermediazione pubblicitaria nei motori di ricerca (con una quota di quasi l'80% del mercato). Il sito (di rivenditori, di operatori di telecomunicazioni, di quotidiani) mette a disposizione del navigante la funzionalità *search*, la stringa da cui lancia la ricerca e ottiene pubblicità connesse alla stessa, se poi l'utente clicca sulla pubblicità sia *G.* che il sito percepiscono una commissione (accordi con *partner* diretti). In questo modo *G.* ha l'esclusiva che si esplica nell'obbligo rivolto ai terzi (inserzionisti di pubblicità) di non procacciarsi pubblicità collegate alle ricerche dei suoi concorrenti perché utilizzano quelle di *Google*.

G. obbliga i terzi a un numero minimo di pubblicità collegate alla ricerca (con l'obbligo di dare ai risultati il posto più favorevole) e non collocare pubblicità dei concorrenti accanto alle inserzioni di *G.*, i terzi devono poi chiedere l'autorizzazione a *G.* per modificare la visualizzazione delle pubblicità concorrenti collegate alle ricerche (*Google* avrebbe deciso di modificare le condizioni dei contratti *Adsense*).

La ricerca su *Google* indirizza ai servizi *Google* e dà sempre più spazio agli inserzionisti di *Google*. Una quota significativa del mercato di *Google* deriva dalle pubblicità collegate alle ricerche. *Google* ha interesse a massimizzare il numero di utenti che visualizzano i messaggi pubblicitari inseriti sui suoi siti e su quelli di terzi. La dominanza di per sé non è vietata, ma *G.* cerca di massimizzare il traffico verso i propri siti, dunque verso le proprie pubblicità e limita la capacità dei concorrenti di posizionare pubblicità collegate alle ricerche su siti internet di terzi.

In riferimento a *c)* si precisa che nel 2013 *FairSearch*, un gruppo di organizzazioni supportato da aziende *tech*, ha accusato *Google* di impedire l'utilizzo di sistemi operativi concorrenti basati su *Android*[666].

[666] In *http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_40099.* Si vuole evidenziare che Android è un sistema operativo gratuito, di proprietà di *Google* ma Open source, può essere modificato, sviluppato e immesso sul mercato con le nuove modifiche purché sia anch'esso open source e quindi modificabile e usabile da altri.

L'*antitrust* europea ha aperto un'indagine sull'abuso di posizione dominante relativamente ad *Android*, il sistema operativo di *Google*. Sono state mosse tre accuse contro *G.*:

1. *G.* chiede ai produttori di dispositivi elettronici, *tablet* e *smartphone* che vogliono usare *Android* di pre-installare in esclusiva l'*app* di *Google search* e il *browser* di *Google*, cioè *Chrom*e, (quindi le altre *app* di ricerca non possono essere installate come servizio di *default*), condizione necessaria per avere il *Play store* (cioè il negozio virtuale da cui è possibile scaricare qualsiasi *app* per *Android*);
2. *Google* chiede ai produttori che installano *Android* di firmare un *Anti-fragmentation Agreement* che li obbliga a non vendere prodotti che montano un *fork Android* (cioè una copia dell'originale, ovvero di *Android* sviluppato da altri);
3. *Google* concede incentivi economici ai produttori di telefonini e agli operatori di telefonia per preinstallare *Google search*.

Tra i punti sotto accusa c'è il fatto che *BigG* chieda ai produttori di *smartphone* e *tablet* che vogliono usare *Android* di preinstallare l'*app* di ricerca *Google Search* e il *browser*, sempre di *Google*, *Chrome*. Non solo: nel momento in cui un produttore sceglie sistema operativo e negozio digitale di *Google* gli viene chiesto di firmare un "*Anti-fragmentation Agreement*" che lo obbliga a non vendere prodotti che montano un *fork* di *Android*, ossia una copia dell'originale che gli sviluppatori, essendo *Android open source*, possono creare. Infine, l'*Antitrust* europea contesta anche che *Google* abbia elargito "significativi incentivi finanziari" ad alcuni dei principali produttori di smartphone al mondo e agli operatori mobili alla condizione che preinstallassero *Google Search* e altri servizi[667].

In data 27 giugno 2017 la Commissione Europea ha imposto a Google un'ammenda di 2,42 miliardi di euro[668] per violazione delle norme antitrust dell'UE. «Google ha abusato

[667] *Joseph Stiglitz: «Questi cinque monopolisti minacciano la democrazia»*, in http://www.pagina99.it/2017/05/21/nobel-joseph-stiglitz-apple-Google-microsoft-amazon-e-facebook-monopolio-privacy/, 22 maggio 2017.

[668] European Commission, case n. 39740 Google Search (Shopping), in http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740.

della posizione dominante sul mercato in quanto motore di ricerca accordando un vantaggio illegale a un altro suo prodotto, il servizio di acquisto comparativo»[669].

La Commissione ha quindi abbandonato «la strada delle decisioni patteggiate e delle autorizzazioni condizionate in cui concordano impegni e correttivi per contemperare la spinta all'innovazione con il bene della concorrenza»[670] e ha preferito, non di certo in modo tempestivo, l'accertamento istruttorio e la sanzione[671], tralasciando di ripensare ad alcune delle categorie *antitrust* per modernizzare gli strumenti attraverso i quali rendere efficace ed effettivo l'*enforcement antitrust* nell'«era dell'informazione e della conoscenza»[672].

La sanzione interviene *ex post* per porre rimedio a un abuso già consumato di posizione dominante, diversamente misure asimmetriche come quella che impone nel settore delle telecomunicazioni all'ex monopolista di consentire l'accesso alla propria linea agli OLO affinché tutti gli imprenditori possano iniziare la concorrenza dal medesimo punto di partenza[673], hanno l'obiettivo di evitare l'abuso del potere del mercato e di migliorare il livello di concorrenza esistente[674].

Pertanto, sebbene la Commissione abbia adottato la legge *antitrust* come punto di partenza, ciò che è necessario è la difesa della dignità della persona perché ci sono almeno due valori colpiti: il mercato e il diritto all'autodeterminazione dell'identità virtuale[675]. Nuove forme di sanzioni dovrebbero essere progettate per proteggere questo nuovo aspetto della *privacy*[676], correlato a quelle masse di dati caotiche e in costante crescita che

---

669 Così si legge nel comunicato stampa della Commissione, reperibile al *link http://europa.eu/rapid/press-release_IP-17-1784_it.htm.*

670 V. FALCE, *Google Shopping Da definire i confini del danno al mercato*, in *Il sole 24 ore*, 2 luglio 2017, cit..

671 Secondo la professoressa G. De Minico «The specific sanctions deployed by the Commission are inspired from the remedies provided in the Telecommunications Directive Package 2002, as modified in 2009. This allows the National Regulatory Authorities to mandate that former monopolists – when they are incumbents and are both Internet access and services providers – to share their own fixed network with other communication services providers who do not own a network. The incumbent (in this case Google) will have to provide access to its competitors with the same contractual and technical conditions granted to its own divisions» in G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?*, in Blog of the IACL, AIDC, August, 27, 2017.

672 ID., *ivi.*

673 G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?*, in *Blog of the IACL*, AIDC, August, 27, 2017.

674 Secondo la prof.ssa De Minico «the antitrust law is autonomous from the asymmetrical, and the latter is not applicable here because the European legislator has evaluated the general antitrust rules sufficient to keep the market competitive»: G. DE MINICO, *ibid.*

675 ID., *ibidem.*

676 «Such a concept of privacy is so unprecedented that we could be in doubt whether it is still the 'right to be let alone' or a new fundamental right. It is quite different from the traditional right of privacy, which is satisfied by

generano ulteriori informazioni, sempre nuove e imprevedibili dal momento della raccolta dei dati[677].

4.6. *Il mercato individuato dalla Commissione Europea*

Google è sotto accusa per abuso di posizione dominante nel mercato degli acquisti comparativi e sull'*advertisment*[678]. Il mercato di riferimento individuato dalla Commissione è quello dei servizi di acquisto comparativo[679] nelle pagine dei risultati delle ricerche, che avrebbe limitato artificialmente la possibilità per i siti internet di terzi di visualizzare i messaggi pubblicitari dei concorrenti di *Google*[680].

La Commissione ritiene che *Google* goda di una posizione dominante nei servizi di ricerca generale su internet e nelle inserzioni pubblicitarie sui siti internet di terzi in tutto il SEE, con quote di mercato superiori rispettivamente al 90% e all'80%.

Quote di mercato molto alte, comprese tra l'80 e il 100% «costituiscono di per sé la prova dell'esistenza di una posizione dominante; in effetti, la detenzione di una quota di mercato particolarmente cospicua pone l'impresa che la detiene durante periodi di una

---

some basic rules: informed consent, minimisation of collection – as to its time and object – and specific purposes. Now, the traditional triad is torn apart by the impact with big data. Indeed, how could the consumer consciously consent if she is not aware of the further use of her data? How can she be made aware if such further use is unpredictable, with the consequence that any ex ante consent would be inutiliter datum? Also, the safeguard given by the specificity of the aim vanishes because the biggest profits come exactly from the secondary and collateral uses, which are still undefined when the data are collected. For the same reasons, the gathering of data will not be limited to its duration and object, because the broader is the gathering, and the bigger the data set, the higher the probability of drawing useful behavioral predictions», in ID., *ibidem*, cit..

677 Il nuovo concetto di *privacy* aprirebbe nuove sfide: «it will involve different demands: from informed consent to a juridical liability for those who gather data, or – more precisely – to a demand of preventive policies and risk-assessments. The same rule, from the data producer's point of view, translates at least into a right to know of the search engine's modes of operation; into a right to clear and unambiguous information about the subject collecting our data (such as Google) and the one offering goods on the basis of this data; but also in a right to an impartial third party's oversight on the reliability of the data gathering algorithm and, finally, into a claim to challenge any unreliable behavioral predictions inferred from the big data. This list is not exhaustive and so it doesn't exclude other responsive solutions», in G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?*.

678 Cfr. con la dichiarazione del *chief competition economist* Tommaso Valletti.

679 Cfr. con il Comunicato Stampa della Commissione europea - *Antitrust: nuove iniziative contro Google per pratiche pubblicitarie e di acquisto* comparativo, Bruxelles, 14 luglio 2016 in http://europa.eu/rapid/press-release_IP-16-2532_it.htm.

680 *Google* rischierebbe una multa fino al 10% del suo fatturato. Nel 2016 *Alphabet* (la *holding* di *Google*) ha realizzato un fatturato consolidato di circa 90 miliardi», in *Google, stretta dell'Antitrust Ue. In ballo il 10% del* fatturato, in http://www.corrierecomunicazioni.it, 21 maggio 2017.

certa entità, in una posizione di forza che la rende controparte obbligatoria e che, già per questo fatto, le garantisce, quanto meno per periodi relativamente lunghi, l'indipendenza di comportamento che caratterizza la posizione dominante»[681]; quote intermedie tra il 40% e l'80% invece «sono un valido indizio dell'esistenza di una potenza preponderante»[682] ma bisogna comunque considerare le quote detenute dai concorrenti e valutare se sono in grado di agire alla pari dell'impresa presa in esame.

Sul mercato dei servizi di ricerca generale occupa quote superiori al 90% in Europa, sul mercato dei sistemi di sfruttamento degli *smartphone* oggetto di licenza (il mercato Android in Europa supera il 90%, in USA il 59%), sul mercato delle applicazioni per il sistema *Android*. Qui detiene quote superiori al 90% in ciascun paese UE e non solo[683].

Con una strategia commerciale volta a rafforzare la sua posizione che priva i consumatori di una scelta più ampia di applicazioni e di servizi mobili e frena l'innovazione proveniente da eventuali *competitor*. *Google* guadagna in questo modo terreno in altri mercati adiacenti di servizi e applicazioni (mercati collegati o contigui)[684]. Si frappongono barriere all'entrata per i nuovi *competitors* rafforzate dal *learning by doing*: l'algoritmo di ricerca di *G.* migliora con l'aumentare delle interrogazioni degli utenti che permettono di comprendere quali siano i siti *web* più rilevanti per determinate parole chiave[685].

Volendo tracciare un parallelismo con la posizione di abuso, possiamo menzionare il procedimento sanzionatorio contro *Microsoft*, il cui sistema operativo *Windows* era in posizione di dominanza nel mercato dei computer, *M.* ha abusato della sua posizione preinstallando il *browser* di ricerca *internet explorer* senza consentire la libera scelta all'utente[686].

---

681 Cfr. causa 85/76, *Hoffmann – La Roche/Commissione*, in *Racc.* 1979, pag. 521, punto 41.

682 Cfr. causa 322/81, *Michelin/Commissione*, in *Racc.* 1983, pag. 3509, punto 52.

683 Cfr. con la condanna russa a *Google*: oltre alla sanzione pecuniaria, l'Antritrust russa ha deciso che il sistema operativo *Android* dovrà essere aperto a motori di ricerca diversi da quello di *Google*. Ne parla l'articolo *Abuso di posizione dominante: multa di 7 milioni di dollari per Google in Russia*, in *La Stampa*, 18 aprile 2017.

684 Cfr. F. ETRO, *The dominance of Google*, 2011, in *http://www.voxeu.org/article/understanding-Google-s-antitrustproblems*; S. CLELAND – I. BRODSKY, *Search & Destroy: Why You Can't Trust Google Inc. Hardcover*, Telescope Books, St. Louis, Missouri USA,10 maggio 2011.

685 F. PAVEL, *Competition in the web search market. A report for Microsoft*, in *Diw Economics GmbH*, 2009, in *http://diw-econ.de/en/publications/studies/competition-in-the-web-search-market*; V.V. COMANDINI., *Google e i mercati dei servizi di ricerca su Internet*, in *Mercato concorrenza e regole*, n.3, pp. 541-569, 2013.

686 caso *Comp/C-3/37.792 Microsoft*, decisione della Commissione del 24 Marzo 2004.

Il rimedio dovrebbe quindi consistere, per analogia, nell'obbligo di mostrare sul portale di *Google* tutti i principali motori di ricerca. Se nel caso *Microsoft* però l'obbligo discendeva dalla dominanza del sistema operativo *Windows* che si tentava di estendere ai *browser*, «nel caso *Google* l'utilizzo del suo motore di ricerca è solo una libera scelta del consumatore che, per farne il portale di navigazione, lo deve volontariamente inserire come pagina iniziale del proprio *browser*. Pertanto il consumatore non ha alcuna difficoltà ad avvalersi di altri motori senza subire *switching cost*»[687].

G. ha sempre evidenziato che la scelta di utilizzare il suo motore di ricerca è scelta libera degli utenti (*competition is just one click away*).

«If you do not like the answer that *Google* search provides you can switch to another engine with literally one click, and we have lots of evidence that people do this. If you want to leave other *Google* services, we make it easy for you to do so. You can even take your data with you without any hassle. We want consumers to stay with us because we are innovating and making our products better, not because they are locked in»[688].

Secondo *Google*[689] il sistema *Android* non avrebbe limitato la concorrenza, ma l'avrebbe implementata permettendo l'ampliamento del mercato degli *smarthphone* a più produttori e il calo dei prezzi dei dispositivi. Per i produttori di telefoni avere gratis *Android* significa non dover comprare sistemi operativi costosi. Ci sono 24mila dispositivi, di oltre 13.000 marchi che utilizzano *Android* e gli sviluppatori europei possono distribuire le loro *app* a più di un miliardo di persone in tutto il mondo.

Nonostante ciò, in Russia, l'Autorità Garante della Concorrenza e del Mercato, FAS - *Federal Antimonopoly Service*, ha condannato *G.* al pagamento di una multa di 7,8 milioni di dollari per abuso di posizione dominante sul mercato *Android*. Mosca ha sanzionato Google per aver richiesto ai produttori di telefoni di pre-installare le sue applicazioni su dispositivi mobili *Android*.

---

687 V. VISCO COMANDINI, *Google e i mercati dei servizi di ricerca su Internet*, in *Mercato concorrenza regole*, n. 3, dicembre 2013, p. 562 ss.

688 E. SCHIMDT, *Statement of Eric Schmidt*, executive chairman, *Google* Inc., hearing before the subcommittee on antitrust, competition policy and consumer rights of the committee on the judiciary united states senate, 2011, in *http://www.gpo.gov/fdsys/pkg/CHRG-112shrg71471/pdf/CHRG-112shrg71471.pdf*.

689 così come si legge nella replica alla Commissione di Kent Walker, Senior Vice President & General Counsel di G., in *https://bloG.Google/topics/Google-europe/android-choice-competition-response-europe/*.

La corte federale ha approvato un accordo amichevole tra *Fas*, Russia e *Google*. L'accordo, che è valido per sei anni e nove mesi prevede che *Google* rinuncerà in Russia all'esclusiva dell'installazione delle proprie applicazioni sui dispositivi *Android* e non potrà impedire la preinstallazione di *app* di terze parti, anche in posizione rilevante sullo schermo o come strumento di ricerca di *default*.

Oltre a rispettare questi impegni, per garantire la libertà di scelta nell'ambito del *search*, *Google* metterà a disposizione degli utenti russi di dispositivi *Android* una finestra che nel contesto del *browser Chrome* consentirà di impostare il motore di ricerca di *default*.

Nei prossimi mesi, poi, i nuovi dispositivi in commercio che continueranno a montare il pacchetto *Google Mobile Services*, verranno equipaggiati con un *widget* che al primo avvio consentirà agli utenti di selezionare il motore di ricerca desiderato fra quelli sviluppati dagli attori che ne faranno richiesta.

In ogni caso, gli utenti avranno la possibilità di modificare le impostazioni in qualsiasi momento[690].

Dunque, *Google* sarebbe operatore economico dominante non solo nel settore del *search advertising*, ma anche in quello del sistema operativo *Android*, e proprio per questo con qualche ragione in più, dovrebbe rispettare la legislazione *antitrust* e, oltre a essere sottoposto al rispetto della legge sulla *privacy*, alla fiscalità diretta e indiretta, piegarsi alla regola della concorrenza[691].

4.7. *L'opportunità di un nuovo mercato di riferimento nel mercato dello sfruttamento dei dati*

Ad avviso di chi scrive i mercati oggetto delle indagini della Commissione sono mercati contigui e allo stesso tempo parziali (si pensi che *Google shopping* è solo uno dei servizi privilegiati dal motore di ricerca di *Google*, si pensi a *Google maps* o a *Google books*, l'esito è lo stesso di quello evidenziato) rispetto al mercato che *Google* sovrasta, domina e

690 Cfr. con l'articolo *Antitrust Android, accordo russo*, in *Il punto Informatico,* 19 aprile 2017.
691 L. PROSPERETTI - M. SIRAGUSA - M. BERETTA - M. MERINI, *op. cit.,* p. 21 ss.

sfrutta, su cui sarebbe opportuno che la Commissione concentrasse la sua attenzione, che è quello della raccolta dei dati.

La dominanza nei mercati adiacenti serve a *Google*, operatore orizzontalmente integrato[692], per consolidare la sua posizione di dominanza nel mercato dei dati.

Se *Google* "impone" l'utilizzo di *Android* gratis e dà incentivi economici ai produttori di telefoni che preinstallino *Chrome* e *Google Search*, precondizione per avere il negozio da cui scaricare tutte le altre *app*, utilità del moderno telefonino; se favorisce sul suo motore di ricerca i risultati che collegano ai suoi servizi o ai siti in cui trovano spazio i suoi inserzionisti[693] o di *App Android* e ne incentiva lo sviluppo da parte di terzi - che utilizzerebbero *API Android* che richiedono comunque un *account Gmail etc* - lo fa per un unico scopo che non è quello caritatevole: raccogliere dati, archiviare, catalogare, collegare e vendere i dati che non gli appartengono e che non gli possono essere ceduti in nome di nessuna condizione contrattuale che sia compatibile con i principi fondamentali riconosciuti dalle Carte nazionali, europee e internazionali.

I dati servono sì a *Google* per corteggiare gli inserzionisti che con l'accesso alle informazioni che ha *Google* possono rivolgersi a *target* specifici, a prezzi differenziati per *bundle*, ma servono a *Google* per sviluppare nuovi servizi sempre più invasivi che calamiteranno sempre nuovi utenti che cederanno sempre nuovi dati che *Google* utilizzerà per gli scopi commerciali più disparati e sconosciuti: dalla pubblicità alle macchine che si guidano da sole.

Occorrerebbe guardare allora non alla quota di mercato ma al numero di utenti iscritti ai servizi *Google*.

Si dovrebbe parlare di un mercato di utenti.

Google opera come rivenditore di informazioni degli utenti sulla base di un costante *profiling* e questo dovrebbe essere il criterio rilevante per definire il mercato[694].

---

692 A. VANZETTI – V. DI CATALDO, *Manuale di diritto industriale*, Giuffrè editore, 2012, pp. 627-628.

693 Essi sono felici di pagare di più perché il prezzo della pubblicità su Internet è determinato dal punteggio di qualità, *quality score*.

694 G. LUCHETTA,*op.cit.*, *ivi*, p. 103 ss. *Google* opererebbe come «rivenditore di informazioni degli utenti ad alto livello di *profiling*» ed è questo il criterio rilevante che usa per definire il mercato rilevante. Luchetta sostiene che sia il livello di *profiling* a differenziare i mercati della pubblicità *online* e *offline*, in quanto quello *online* è talmente maggiore, che i due tipi di pubblicità non possono essere considerati sostituti dal punto di vista della domanda degli inserzionisti. Quello che deve essere considerato quindi è se esiste un livello di *profiling* simile da parte di altri siti

Il mercato di riferimento non sarebbe quello della ricerca o della pubblicità, ma quello dei dati e ci sarebbero altri rivenditori di informazioni personali concorrenti su questo mercato, si pensi a *Facebook, Twitter, Instagram* e agli altri fornitori di servizi di posta elettronica.

Tutti questi soggetti inseriscono pubblicità nella pagina dei loro servizi per estrarre dati.

Allora, dal momento che gli operatori a cui si rivolge *Google* sarebbero due, occorrerebbe considerare il mercato a due versanti (*multisided market*). Tuttavia si tratterebbe di un mercato bilaterale *sui generis*.

Un mercato multilaterale[695] è formato da una piattaforma (*Google* o Facebook) che coordina gli scambi tra i due lati (navigatori e inserzionisti), essa dovrebbe produrre esternalità di rete indirette positive per entrambi i versanti, internalizzando gli effetti indiretti di rete che si generano fra essi. La condizione affinché vi sia un tale mercato è che senza piattaforma le parti non sono in grado di comunicare. Uno dei lati (l'inserzionista) riceve un beneficio positivo crescente in relazione al numero dei componenti dell'altro (navigatori), consentendo a entrambi, grazie al coordinamento della piattaforma, di ridurre sostanzialmente il costo di transazione degli scambi (cd. esternalità indiretta di rete)[696]. Tuttavia gli utenti che interrogano *Google* non ricevono alcun beneficio dalla crescita del numero degli inserzionisti.

Gli inserzionisti comprano spazi che le piattaforme offrono agli utenti attraverso la fornitura di contenuti. Il motore di ricerca produce con il medesimo algoritmo due *output* collegati: i risultati generali per gli utenti, e gli *slot* degli inserzionisti, scelti attraverso l'asta e indicati sulle pagine dei risultati.

---

internet attraverso banner e annunci classificati, tanto da poterli considerare come sostituti dal punto di vista della domanda.

695 Cfr. L. FILISTRUCCHI, *A SSNIP test for two-sided markets: the case of Media*, in *Social Science Research Network*, 30/09/2008, in http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287442; A ALEXANDROV. - G. DELTAS - D. SPULBER, *Antitrust and Competition in Two-Sided Markets*, in *Journal of Competition Law & Economics*, vol. 7, n. 4, pp. 775-812; M. ARMSTRONG, *Competition in Two-Sided Markets,* in *Rand Journal of Economics*, vol. 37, n. 3, pp. 668-691; K.L. DEVINE, *Preserving Competition in Multi-Sided Innovative Markets: How Do You Solve a Problem Like Google?*, in *North Carolina Journal of Law and Technology*, vol. 10, n. 1, 2008, pp. 59-118.

696 I risultati organici sono rilevanti anche per i fornitori di contenuti che, grazie alla visibilità generata dall'indicizzazione del motore di ricerca, «incrementano la loro *audience* e dunque l'offerta di inserzioni pubblicitarie sui loro siti. Essi ricevono dalla piattaforma di ricerca un'esternalità positiva indiretta, circolare e simmetrica, che si genera fra essi e gli utenti che ne visitano i siti».

In sintesi *Google* sarebbe un rivenditore di informazioni personali degli utenti. Nel mercato a monte acquisisce le informazioni personali degli utenti dalla rete di distribuzione dei suoi servizi di ricerca o previo pagamento. Poi, utilizza le informazioni personali raccolte per vendere pubblicità mirata agli inserzionisti nel mercato a valle. Sulla base di questa costruzione del mercato, le accuse contro *Google* andrebbero analizzate lungo questa catena verticale come presunte violazioni del diritto della concorrenza.

Si è voluto in questo modo inquadrare il caso *Google* da un'altra prospettiva.

Resta fermo che con la cessione il titolare/proprietario dei dati non può perderne la proprietà, se così fosse non potrebbe esercitare il diritto all'oblio (riconosciuto dal nuovo regolamento europeo 2016/769/UE) tantomeno chiedere l'accesso a quei dati che ha perso e quindi controllarli[697].

La cessione deve avere una finalità temporanea e deve essere specifica e determinata[698].

Partire dal livello di *profiling* delle informazioni personali permette così di capire che il mercato rilevante in cui compete *Google* non si limita ai motori di ricerca. Infatti, ci sono altri rivenditori di informazioni personali ben profilate che dovrebbero essere considerati concorrenti su questo mercato rilevante e che in effetti *Google* considera come concorrenti: i *social network* e i fornitori di servizi di posta elettronica. Entrambi, come i motori di ricerca, possiedono informazioni dettagliate sui propri utenti e le utilizzano per capire quale pubblicità mirata portare alla loro attenzione. Sia i *social network* che gli operatori di posta elettronica, analogamente ai motori di ricerca, includono gli spazi pubblicitari nella stessa pagina *web* in cui forniscono i propri servizi. Alla luce di ciò Facebook andrebbe considerato concorrente di *Google*, piuttosto che altri motori di ricerca, in quanto fornitore di informazioni personali ad alto livello di *profiling*.

Questa analisi consentirebbe di verificare la dominanza di *Google* anche in altri mercati, senza che sia necessario avviare nuove indagini.

---

697 Cfr. con la tutela postmortale della dignità e identità della persona, con il riconoscimento ai prossimi congiunti di una legittimazione *iure proprio* nella sentenza del Tribunale tedesco su accesso ai dati da parte dei genitori in caso di morte di un minore: G. RESTA, *La morte digitale*, in *dir. inf.*, Milano, Giuffrè, 6- 2014, p. 893 ss.

698 C. PERLINGIERI, *Nuovi profili del contratto*, in *Rass. dir. civ.*, 2000, p. 565 ss.

Il nuovo *habitat* delle libertà fondamentali richiede un intervento normativo speciale che, partendo da una interpretazione evolutiva delle Costituzioni nazionali e dalle Carte internazionali, recepisca i nuovi caratteri del mezzo, le nuove logiche di mercato e conseguentemente elabori nuovi paradigmi *antitrust* per consentire l'efficace tutela della concorrenza, delle libertà e della tutela del consumatore. Questo tipo di intervento eteronomo dovrà tenere conto delle caratteristiche del nuovo terreno di gioco delle transazioni economiche e delle libertà, nonché della posizione di chi è già in dominanza e intende rafforzarla, o lo sta già facendo per moltiplicare il suo iniziale vantaggio politico-economico, indisturbato.

5. L'accesso ai diritti di esclusiva sui dati e la protezione della *privacy* come benefici per la concorrenza e l'innovazione

Le pratiche discriminanti o escludenti, includono il rifiuto ingiustificato di contrattare nel caso di *essential facility* (infrastrutture o diritti di privativa non replicabili ed essenziali per l'accesso ad un mercato a valle diverso da quello in cui viene detenuta la posizione dominante). L'*essential facility doctrine* (di origine nordamericana) si è formata e sviluppata in relazione all'accesso ad infrastrutture di pubblica utilità non replicabili o non facilmente replicabili per le quali si poneva l'esigenza di un accesso multiplo da parte di più operatori per garantire la pluralità dell'offerta sul mercato di riferimento.

Successivamente tale teoria è stata adattata per risolvere controversie derivanti dalla chiusura dei mercati delle *information technologies* provocata da abusi del diritto di *copyright* o di proprietà industriale (brevetti, disegni o modelli industriali). Il primo caso in Europa di applicazione in questo settore della *essential facility doctrine* è stato il caso Magill[699] in cui tre emittenti televisive britanniche (BBC, RTE e ITV) si erano rifiutate di comunicare i loro

[699] CGUE, cause riunite C-241/91 e C-242/91 del 6 aprile 1995.

palinsesti alla società irlandese Magill, impedendole in tal modo di realizzare una guida televisiva settimanale generale.

La Corte ha affermato in quella sede che il rifiuto di cedere tali informazioni integrava un abuso di posizione dominante (i.e. un abuso del diritto d'autore sui palinsesti che la legge garantiva loro) in quanto ostacolava l'emergere di un prodotto nuovo che le emittenti non offrivano e quindi la creazione di un nuovo mercato, oltre che apparire il rifiuto di concedere la licenza non giustificato rispetto alla necessaria tutela del diritto di privativa.

Dal 1991 in poi l'illiceità di questi comportamenti è sempre legata all'accertamento dei due requisiti riscontrati nel caso Magill, ossia l'assenza di una causa giustificativa e l'impedimento nella realizzazione di nuovi prodotti per i quali esiste una domanda potenziale su un distinto mercato.

Nessun programma innovativo potrà superare il vantaggio di *Google* nella raccolta dei dati. Il profitto per *Google*, derivante dalla fitta rete di utenti profilati non sta solo nei dati del singolo utente, ma nei dati organizzati e incrociati che consentono di capire come utenti simili si comporterebbero, o di anticipare la definizione dei loro interessi.

I rendimenti in materia di pubblicità si basano non solo sulle azioni precedenti, ma sul comportamento degli altri utenti con un comportamento simile.

In questo modo, *Google* già sa quello che interesserà ai suoi utenti.

Questa impresa, per quanto possa essere stata tra le prime a usare algoritmi di ricerca, non avrebbe ottenuto il controllo dominante dei dati dell'utente, solo attraverso la sua capacità di innovazione. *Google* ha ampliato il suo controllo dei dati degli utenti, non attraverso la libera scelta del cliente di farsi osservare, ma attraverso un'invasione sfrenata della *privacy* degli utenti attraverso l'attività di scansione e raccolta dei dati, iniziata con il progetto *Street View* e con lo «*sniffing*» delle informazioni trasmesse dai *router Wi-Fi* delle strade percorse[700]. Al di là delle presunte violazioni, l'espansione aggressiva di *Google* nei

[700] *Google* registrava le informazioni relative alla posizione di reti *wireless* e intercettava i pacchetti dati in transito sulle *Wi-Fi* aperte. La tesi di *Google* era che le comunicazioni instaurate con *hot spot e router Wi-Fi* sprovviste di protezione erano paragonabili alle trasmissioni radio «in chiaro» per cui chiunque poteva rilevarne la presenza. Nell'aprile del 2012 fu condannata dalla FCC al pagamento di una multa di $ 25.000 perché la raccolta dei dati aveva violato la legge Federale Wiretap. Cfr. con multa della FTC di $ 22,5 milioni per aver inserito di nascosto dei *cookie* nel *browser* Safari, approfittando di una vulnerabilità. Lo scopo era sempre lo stesso: raccogliere dati relativi alla geolocalizzazione.

mercati adiacenti, dove potrebbe raccogliere informazioni sempre più personali sugli utenti, costituirebbe un comportamento di monopolio tanto più se l'obiettivo non era quello di competere in questi mercati, ma solo di guadagnare il controllo di questi mercati sussidiari per rafforzare il proprio monopolio nel *search advertising*.

Partendo dall'ampliamento dell'interpretazione, che si è avuta nel corso degli anni della *essential facility doctrine*[701], al punto da ricomprendere nella nozione di infrastruttura beni immateriali come diritti derivanti da brevetti per invenzione, segni distintivi, diritto d'autore, potremmo riconoscere in capo al monopolista un diritto di accesso ai *Big Data*, al momento diritto esclusivo di *Google*, il cui rifiuto potrebbe costituire un abuso di posizione dominante per i seguenti motivi: *a*) il rifiuto si riferirebbe a un prodotto necessario per poter competere efficacemente nel mercato del *search advertising*; *b*) il rifiuto impedirebbe la realizzazione di nuovi servizi *online* per i quali esiste una domanda potenziale; *c*) non è giustificato; *d*) preclude ogni forma di concorrenza. La crescita dei cosiddetti «*high technologies markets*»[702] renderebbe sempre più incompatibili con l'economia di mercato quei diritti che consentono solo al titolare lo sfruttamento esclusivo di un «prodotto». L'*essential facility doctrine*[703] è stata originariamente applicata alle infrastrutture materiali quali porti, ferrovie, reti energetiche, aeroporti ed è stata applicata nei mercati liberalizzati, dove la gestione delle reti, create in origine con investimenti statali, è stata affidata all'ex monopolista. Il diritto della concorrenza ha così garantito ai *new entrants* l'accesso alla rete, rendendo effettiva la tutela degli interessi dei nuovi operatori verso condotte escludenti da parte dell'*incumbent*[704].

---

701 La teoria è di derivazione statunitense, in part. P. AREEDA, *Essential facilities: An ephitet in need of limiting principles*, in *Antitrust Law Journal*, 58, 1990, pp. 841 ss. Sul tema, G. MOGLIA - A. NICITA - D. DURANTE, *La nozione di essential facility tra regolamentazione e antitrust*, in *Merc. Conc. Reg.*, 2001, pp. 257 ss. e F. GHEZZI - G. OLIVIERI, *Diritto Antitrust*, Giappichelli, Torino, 2014, p. 239 ss.

702 In particolare, con riferimento al diritto d'autore, si rimanda a P.A.E. FRASSI, *Riflessioni sul diritto d'autore. Problemi e prospettive nel mondo digitale*, in *Riv. dir. ind.*, 2002, p. 370 ss.

703 Con riferimento alla regolazione delle ngns si rimanda a G. DE MINICO, *Tecnica e diritti sociali nella regulation della banda larga*, in G. DE MINICO (a cura di), *Dalla tecnologia ai diritti. Banda larga e servizi a rete*, p. 3 ss., in cui l'autrice analizza la possibile regolazione in grado di incentivare gli investimenti degli operatori privati nelle nuove reti e, al tempo stesso, di prevenire la fisiologica attitudine dell'*incumbent* della vecchia rete a spostare la sua dominanza sui nuovi scenari tecnologici. In part., sostiene che «la regola asimmetrica prova a mimare le condizioni che un mercato maturo creerebbe *ex se*, obbligando l'*incumbent* a mettere a disposizione degli altri operatori la sua rete, *essential facility*, alle stesse condizioni praticate alle proprie divisioni commerciali».

704 S. FROVA - E. PONTAROLLO (a cura di), *La liberalizzazione zoppa. Il caso della telefonia fissa*, Milano, Vita e pensiero, 2004, p. 35 ss.

L'essenzialità della rete deve essere considerata oggettivamente. Nel caso di specie l'abuso di posizione dominante potrebbe derivare dal rifiuto di *Google* di dare accesso ai propri diritti di esclusiva sui dati e quindi di concedere una licenza a terzi.

L'obbligo di aprire i dati produrrebbe, invece, benefici per la concorrenza in quanto favorirebbe l'innovazione tecnologica e la sua divulgazione mediante l'apertura a più concorrenti. La stessa giurisprudenza comunitaria[705], pur riconoscendo la legittimità dei diritti di esclusiva, si è riservata di valutare nel merito le singole modalità di esercizio delle restrizioni concorrenziali e ha finito poi per ammettere che, in talune circostanze, il rifiuto di concedere licenza può costituire un abuso di posizione dominante.

In questo caso, la titolarità dei dati verrebbe assimilata a una *essential facility*, di carattere immateriale, indispensabile per competere sul mercato.

Dunque, il fine ultimo sarebbe quello di salvaguardare i mercati competitivi dei *Big Data* per impedire l'ascesa dei *data barons*[706], *Google* seguito da *Facebook*, *Twitter*, *Microsoft*, *Amazon*, che oggi hanno sostituito i *robber barons* che nell'800 dominavano le ferrovie, l'industria dell'acciaio e le reti telegrafiche in America. La regolamentazione *antitrust* dovrebbe prevenire proprio i predomini deleteri, facilitando, in questo caso, le transazioni basate sui dati tramite soluzioni come la concessione in licenza e l'interoperabilità. Un intervento *antitrust* in questo senso, che non favorisce nessuna tecnologia in particolare, si limiterebbe a tutelare la concorrenza senza aggiungere vincoli e aiuterebbe i *Big Data* a penetrare la nostra quotidianità come hanno fatto le ferrovie, a vantaggio della collettività.

Per incoraggiare nuovi operatori o proteggere la posizione dei concorrenti esistenti, le Autorità di concorrenza possono richiedere all'entità risultante dalla fusione di vendere i dati ai rivali a un prezzo di mercato[707].

Ma la concorrenza chiede un contemperamento con le esigenze dettate dalla protezione dei dati personali. Come risultato di questo coordinamento *privacy - competition* avremo:

---

705 Corte di giustizia, 6 aprile 1995, causa C-241/91 P e C-242/91 P, *Radio Telefis Eireann (rte) e Indipendent Television Publications Ltd (itp) c. Commissione delle Comunità europee*, in *Racc.*, 1995, I-743 e 29 aprile 2004, causa C-418/01, *ims Health c. ndc Health,* in *Racc.*, 2004, I-5039.

706 V. MAYER-SCÖNBERGER - K. CUKIER, *op. cit.*, p. 247 ss.

707 J. KENNEDY, *op. cit.,* p. 10, cit.: «traditional antitrust analyses can actually deter incumbents from sharing data. Competition policy only comes into play when a company has power within a specific market».

i. Identificazione e comprensione dei danni potenziali derivanti da una economia *data driven*, compresi quelli causati da una concorrenza insufficiente.
ii. Sviluppo di strumenti per i servizi gratis che aiutino a comprendere come le fusioni e le restrizioni possono causare questi danni.
iii. Capire quali sono gli incentivi per le imprese a competere sulla promozione della privacy e incentivarli.
iv. Elaborazione di un nuovo *framework* per la nuova economia che offra ai consumatori una maggiore scelta tra un modello *business* dipendente dalla pubblicità dove il prodotto è il consumatore e modelli dipendenti dalle sottoscrizioni.
v. Considerazione delle sinergie nel quadro legale privacy, tutela del consumatore e concorrenza per promuovere la concorrenza, gli interessi dei consumatori e il benessere dei cittadini.

A questo punto del discorso possiamo dedurre che l'approccio *antitrust* attuale e la focalizzazione da parte della Commissione sul servizio *Google Shopping* è solo parziale[708] e ha accelerato la transizione «to a perverse form of data feudalism, where the key resource is owned by just one or two corporations»[709].

«If we really want to exploit all the insights that come from putting different data sets together, it's obvious that data should belong to just one entity, but it does not have to be a big tech firm like Alphabet. All of the nation's data, for example, could accrue to a national data fund, co-owned by all citizens (or, in the case of a pan-European fund, by Europeans) Whoever wants to build new services on top of that data would need to do so in a competitive, heavily regulated environment while paying a corresponding share of their profits for using it. Such a prospect would scare big technology firms much more than the prospect of a fine. The current approach – let's have big tech firms swallow as

[708] Secondo la prof.ssa De Minico «the Commission has perceived only a fragment of the problem. Google has built its economic strength upon our data, i.e. the very personal and non-personal information it acquires from us in exchange for its mail or cloud services. These services are, of course, only nominally free: the user pays for them by transferring parts of herself of which she loses track. We have even less rights than a minority shareholder, who is at least entitled to know how things are going in a company governed by others»: G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?*, in *Blog of the IACL*, AIDC, August, 27, 2017.

[709] E. MOROZOV, *To tackle Google's power, regulators have to go after its ownership of data*, in *The Guardian*, July 2, 2017, cit..

much data as they can and apply competition law to how they design their websites – is toothless»[710].

Come «market watchdog», la Commissione è incapace di occuparsi della tutela del diritto fondamentale alla *privacy*. Di conseguenza, sarebbe necessario che la Commissione avviasse un dialogo con le autorità europee in materia di protezione dei dati, siano esse le autorità nazionali per la protezione dei dati degli Stati membri, il Garante europeo della protezione dei dati o il Responsabile della protezione dei dati della Commissione Europea. Infatti, il mercato dei dati influenza sia l'equilibrio concorrenziale che il diritto dell'individuo a sapere cosa sta succedendo sulle sue informazioni. Quest'ultimo interesse è ancora assente nel processo decisionale europeo ed è appena emerso, ma è ancora acerbo, nel Regolamento Europeo sui dati personali. Ma ora il valore rappresentato dal rispetto della persona richiede azioni molto più forti. Il decisore politico europeo deve affrontare una sfida: o ridisegnare i processi decisionali sulla base di nuovi modelli - aperti a più autorità, servendo più valori e porosi al valore dell'integrità personale - o mantenere invariata la struttura giurisdizionale, accettando il sacrificio dei diritti individuali[711].

[710] *Ibid.*

[711] Si traduce il pensiero della prof.ssa De Minico, in G. DE MINICO, *New horizons for the policymaker after the Commission's decision on Google?* Che così conclude «To summarise: the Commission's Google decision opens new horizons to the policymaker. Will she be able and willing to explore them?».

Capitolo IV

Un confronto con l'esperienza francese

SOMMARIO: 1. Una premessa sull'analisi del quadro normativo francese – 2. La trasparenza nell'apertura dei dati al pubblico (2.1. *Le variabili di apertura dei dati: il consolidamento* de les données brutes). – 3. La legge fondamentale sull'accesso: *la loi* CADA - 4. Dall'*essential facility* all'*essential disclosure* - 5. L'apertura dei dati come un *enjeu politique*: quale ruolo per il *policy maker*.

1. Una premessa sull'analisi del quadro normativo francese

L'esame del quadro normativo francese cui è dedicato questo capitolo[712], per ragioni di inerenza al lavoro di tesi svolto, convoglierà al profilo di apertura dei dati al pubblico.

Il fine ultimo è quello di ricomporre i tasselli delineati nel corso dello studio fin qui condotto per congiungere il primo capitolo con l'ultimo, in cerca di una risposta alla domanda che rappresenta *fil rouge* dello scritto: quale regolazione può considerarsi la più adatta a coniugare le esigenze di sfruttamento economico dei dati, di protezione del loro intimo nucleo e del valore pubblico di cui sono portatori, tenuto conto che «la lumière du soleil est le meilleur des désinfectants»[713] sulle azioni di governo e sulla conoscenza, in generale.

Partiremo dalla definizione francese di *Open Data* per avviare una comparazione tra la normativa francofona, che da subito ha avviato una strategia politica – precorritrice di quella europea - di apertura dei dati al pubblico e quella italiana, più resistente e ostile alla *disclosure* delle informazioni ai governati.

Indagheremo quindi, dapprima sulla cogenza del principio di trasparenza, sulle caratteristiche e sull'attribuzione della titolarità del dato, nonché sulla scelta francese del formato più adatto al riutilizzo e allo sfruttamento dello stesso, finalizzato alla estrapolazione della massima utilità dal dato, in ossequio non solo al principio della trasparenza, che dovrebbe guidare l'operato delle pubbliche amministrazioni[714] e della sussidiarietà nella sua accezione orizzontale- che permette ai cittadini di partecipare alla

---

[712] Questo capitolo nasce da un periodo di studio condotto dall'autrice a Parigi presso l'Università Panthéon Assas, sotto l'attenta supervisione dei professori J.G. Guglielmi e C. Santulli, che in questa sede si intende ringraziare per il prezioso contributo.

[713] Nel saggio *Other's People Money and How the Bankers Use It*, 1914, a p. 92 il giurista Louis Brandeis esalta le virtù della trasparenza nel settore privato utilizzando la celebre espressione: «Sunlight is said to be the best of disinfectants; electric light the most efficient policeman. And publicity has already played an important part in the struggle against the Money Trust», il testo è consultabile al *link* http://louisville.edu/law/library/special-collections/the-louis-d.-brandeis-collection/other-peoples-money-by-louis-d.-brandeis. Cfr. Anche P. A. FREUND, *The Supreme Court of the United States: Its Business, Purposes and Performance*. Gloucester, MA: Peter Smith, 1972; D. HEALD, *Pourquoi la transparence des dépenses publiques est-elle si difficile à atteindre?*, in *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78), pp. 33-53.

[714] C.A. DUBREUIL, *La démocratie et la transparence*, in *RFDA*, 2016, pp. 655 ss.

fornitura di servizi di pubblica utilità - ma anche alla libertà di iniziativa economica pubblica e privata.

Questi principi rappresentano, nell'era digitale la più fedele proiezione di ciò che sul piano politico è rappresentato dai principi democratici[715].

L'assunzione dell'iniziativa economica in un'accezione moderna implica, infatti, l'assunzione di una partecipazione, ancorché di minoranza, in una società democratica e in un mercato concorrenziale, quest'ultimo espressione di un interesse pubblico di natura macroeconomica e garanzia di tutela del singolo consumatore.

I dati, inoltre, come si vedrà più avanti, da semplici informazioni, sono divenuti oggi questioni politiche perché strumenti del «valore pubblico» della trasparenza[716]. Il modo - il loro formato, la quantità e la qualità - in cui sono strutturati esercita un ruolo determinante nell'influenzare la politica pubblica in termini di efficienza, equità e responsabilità democratica[717].

2. La trasparenza nell'apertura dei dati al pubblico

Il Manifesto giuridico della trasparenza risiede nell'articolo XV della *Déclaration des Droits de l'Homme et du Citoyen* del 1789: «La Société a le droit de demander compte à tout Agent public de son administration» al punto che «le corps du public compose un tribunal, et un tribunal qui vaut mieux que tous les tribunaux ensemble»[718].

La trasparenza[719], intesa come controllo sociale diffuso e quindi «riequilibrio di conoscenza a favore di coloro che sono soggetti al potere pubblico», diventa un

---

715 E. DIDIER, *En quoi consiste l'Amérique? Les statistiques, le New Deal et la démocratie*, Paris, La Découverte, 2009*, passim*.

716 Cfr. Con il § 5 del presente capitolo.

717 «La façon dont les mécanismes de transparence sont structurés va par conséquent déterminer leur influence sur la politique publique — sur l'efficience, sur l'équité et sur la responsabilité démocratique» D. HEALD, *op. cit.*, *ibid.*

718 J. BENTHAM, *Tactique des assemblées législatives*, J.J. Pascoud, Paris, 1816, pp. 14-48.

719 Cfr. Anche con il Rapporto commissionato nel 1953 dall'*American Society of Newspaper Editors* all'avvocato Harold Cross; il Freedom of Information Act (FOIA) americano del 1966 e il *Memorandum for the Heads of Executive Departments and Agencies* del 21 gennaio 2009, relativo all'applicazione del FOIA. Cfr. É. ZOLLER, *Le principe de*

«contrappeso democratico ai poteri delle PP.AA»[720] nel momento in cui dà sostanza alla forma democratica[721].

Con l'evolversi della società, la trasparenza si è evoluta in *openess*, concretizzando «l'aspirazione a un'azione pubblica visibile e valutabile dai cittadini attraverso il riconoscimento a essi del diritto d'accesso ai documenti amministrativi»[722] e la «tensione verso una democratizzazione della funzione esecutiva grazie al contrappeso costituito dal diritto civico all'informazione pubblica»[723].

Il *quid pluris* del rilascio delle informazioni direttamente conseguibile dai cittadini è divenuto il risultato di un processo di apertura e di rielaborazione dell'informazione che coinvolge le amministrazioni, cittadini e riutilizzatori e rende l'informazione *querable*[724] e *portable*[725].

Così la trasparenza ha assunto una duplice accezione[726], nel senso che può essere spiegata tra PP.AA. o tra P.A. e utenti o altri *stakeholders*, ma in entrambi i sensi richiede

---

transparence et les nouvelles technologies de l'information aux États-Unis. Conférence-débat du CDPC sur la transparence administrative et ses déclinaisons technologiques récentes, Cycle « Les valeurs du droit public», Parigi, 2013, in http://www.u-paris2.fr/CDPC0/0/fiche__pagelibre/ e H.YU – D. ROBINSON, *The New Ambiguity of "Open Government". Ucla Law Review Discourse*, 2012, pp. 184-187.

720 G. MANCOSU, *La transparence publique à l'ère de l'Open Data. Étude comparée Italie-France*, Université Panthéon-Assas (Paris 2), 2016, p. 22, cit..

721 H. VERDIER– P.Y. BAUDOT, *Au-delà de l'ouverture des données, ce qui est en jeu, c'est l'ouverture de la décision*, in *Informations sociales*, 2015/5 (n. 191), pp. 20-25.

722 G. MANCOSU, *op. cit.*, p. 24, cit.

723 *Ibid.*

724 Accessibile.

725 Diffusa.

726 Parlano di trasparenza in senso verticale e in senso orizzontale: J. CHEVALLIER, *Le mythe de la transparence administrative,* in *CURAPP, Information et transparence administratives*. Paris: PUF, 1988 p. 239-275 ; ID., *Le droit administratif entre science administrative et droit constitutionnel*, in J. CHEVALLIER - G. J. GUGLIELMI - D. LOCHAK & CURAPP (a cura di), *Le droit administratif en mutation*, Paris: PUF, 1993, pp. 11-40 ; ID., *La transformation de la relation administrative : mythe ou réalité ? (à propos de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations)*, Recueil Dalloz (38), 2000, pp. 575-584 ; ID., *Les pratiques administratives. Transparence et secret. Colloque pour le XXVe anniversaire de la loi du 17 juillet sur l'accès aux documents administratifs*, Paris: La Documentation française, 2003, pp. 83-98 ; ID., *La gouvernance, un nouveau paradigme étatique? Revue française d'administration publique*, 2003, pp. 203-217 ; ID., *Audition du 9 janvier. In C. Bouchoux, Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique (Rapport)* (Vol. II, p. 7-13), Paris: Sénat, tratto da http://www.senat.fr/rap/r13-589-2/r13-589-21.pdf; R. MARRAMA, *La pubblica amministrazione tra trasparenza e riservatezza nell'organizzazione e nel procedimento amministrativo*, in C. S. COMO, *L'amministrazione pubblica tra riservatezza e trasparenza. Atti del XXXV Convegno di studi di scienza dell'amministrazione, Varenna, 21-23 settembre 1989*, 1991, Milano: Giuffré, pp. 53-88; J. RIDEAU, *La transparence dans l'Union européenne. Mythe ou principe juridique?* Paris: LGDJ, 1999; P. TANDA, voce *Trasparenza* (principio di), in AA.VV., *Digesto delle discipline pubblicistiche*, Torino: UTET, 2008, pp. 884-945; S. BAUME - D. J CARON,. – P.A. COMEAU, *Le principe de transparence en Suisse et dans le monde*, in M. PASQUIER (a cura di) Lausanne: Presses polytechniques et universitaires romandes, 2013; J. MARCHAND, *Réflexions sur le principe de transparence. Revue du droit public et de la science politique en France et à l'Étranger*(3), 2014, pp. 677-703.

che sia riconosciuta l'interoperabilità[727] tra le stesse pubbliche amministrazioni e un formato *standard* per la condivisione delle informazioni.

L'amministrazione è in grado ora di aprire non più un semplice contenuto, ma interi flussi informativi, producendo *set* di dati e rendendo disponibili *online* anche gli applicativi che agevolano la visualizzazione dei dati.

Secondo la definizione accolta dalla parte maggioritaria della dottrina francese «l'open data consiste à mettre à disposition les données utilisées quotidiennement par les acteurs gouvernementaux»[728].

Gli *Open data* (d'ora in poi OD) si sviluppano in Francia parallelamente alla nozione di *Open Government*, che designa in via generale in ambito istituzionale l'accesso all'informazione pubblica. Gli *Open Government Data* (OGD) rappresentano dunque il prodotto e il fine dell'*Open Government*[729], al punto che il dato aperto è divenuto paradigma di declinazione dell'*Open Government* sulla spinta di una domanda civica *bottom-up*[730] e di una politica internazionale *top-down.*

Parallelamente si è trasformata anche la nozione di informazione pubblica, dematerializzandosi sempre più: dacché era considerata un'attività neutra, strumentale o accessoria rispetto a una funzione o prestazione pubblica principale, è divenuta il fine ultimo ovvero essa può rappresentare il servizio richiesto, consistente, non più in casi eccezionali ma di regola, nel rilascio di informazioni *uti singuli* o *uti universi*[731].

Il modello OGD coinvolge sia l'informazione che costituisce il mezzo «données-moyen», sia l'oggetto, «données-objet», dell'azione pubblica[732].

---

[727] Per interoperabilità s'intende «la capacità dei sistemi di tecnologia dell'informazione e della comunicazione e dei processi aziendali che su di essi si basano di scambiare dati e consentire la condivisione di informazioni e conoscenze» (art. 3, lett. f, della Decisione 2004/387/CE del Parlamento Europeo e del Consiglio del 21 aprile 2004 relativa all'erogazione interoperabile di servizi paneuropei di governo elettronico alle amministrazioni pubbliche, alle imprese e ai cittadini (IDABC): *http://ec.europa.eu/idabc/servlets/Doceb76.pdf?id=1895*).

[728] ID., *ibid.*

[729] B. DEBRAS, *Focus - L'engagement de la branche Famille dans la démarche d'open data. S'inscrire dans un mouvement national et européen*, in *Informations sociales*, 2015/5 (n. 191), pp. 92-95.

[730] Tra i *civic hackers* il giurista Lawrence Lessig, fondatore di Creative Commons, e Tim O'Reilly, teorizzatore del Web 2.0..

[731] MERLONI F., *Trasparenza delle istituzioni e principio democratico*, in MERLONI F- ARENA G.(a cura di), *La trasparenza amnministrativa*, Giuffré, Milano, 2008, *passim*.

[732] J.M. BRUGUIERE, *Les données publiques et le droit.* Paris: Litec., 2002, p. 22.

La dottrina francese finisce per qualificare l'OD come un nuovo «service public»[733].

In sintesi, la trasparenza è contemporaneamente un fine dell'attività informativa pubblica e un mezzo, che contribuisce al raggiungimento dell'efficienza, efficacia e imparzialità dell'azione pubblica, migliorando l'accesso ai servizi pubblici, la partecipazione, la sussidiarietà orizzontale, il benessere collettivo e individuale. Per tali motivi il modello OGD apre nuovi scenari evolutivi per la trasparenza pubblica, che ne esaltano sicuramente le potenzialità democratiche, ma accentuano altresì i limiti interni ed esterni connessi alla tutela di valori concorrenti.

Secondo buona parte della dottrina francese la trasparenza sarebbe strumentale a sette valori con cui però potrebbe anche entrare in conflitto, a seconda delle circostanze e del contesto di riferimento: *l'efficacité, la confiance, la responsabilisation, l'autonomie et le contrôle, la confidentialité, le respect de la vie privée et l'anonymat, l'équité et la légitimité*: «la question est essentiellement de savoir si la transparence doit l'emporter sur d'autres valeurs. Cette idée fait apparaître une distinction entre la transparence en tant que valeur intrinsèque et en tant que valeur instrumentale»[734].

Grazie alla liberazione dei dati, le informazioni che essi racchiudono possono essere utilizzate dal cittadino per i più svariati scopi, non da ultimo per controllare l'esercizio del potere pubblico, che risulta ampliato nelle sue modalità di esercizio e nei risultati perseguibili. I confini della conoscenza pubblica si sono allargati: il cittadino non deve unicamente sorvegliare l'amministrazione mentre fornisce decisioni, ma può supportarla nella creazione e nell'analisi dei dati, per partecipare alle decisioni e collaborare nelle attività decisionali. Si afferma una trasparenza più fluida, attraverso la quale i cittadini, in quanto portatori ciascuno di una quota di sovranità popolare, che legittima l'esercizio del potere pubblico, esercitano, in forma più piena rispetto al passato, il diritto non solo a giudicare quello che vedono, ma anche a influire sul funzionamento dell'amministrazione. In questo modo la legittimazione all'esercizio del potere non è

---

733 G. GUGLIELMI, *Open data et service public : les données pubbliques ouvertes sont-elles un service public?,* in D. BOURCIER (a cura di), *Open Data et Big Data, Nouveaux défis pour la vie privée*, Mare et Martin, Parigi, 2016, p. 40 ss.; ID., *Numérisation des données publiques et données publiques numériques*, in B. TEYSSIE, *La communication numérique, un droit, des droits*. Paris: Editions Panthéon-Assas, 2013, pp. 539-556.

734 D. HEALD, *Pourquoi la transparence des dépenses publiques est-elle si difficile à atteindre?*, in *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78), p. 38, cit.

statica e predeterminata ma deve essere «riconquistata ogni volta che l'amministrazione opera»[735].

Un governo trasparente consente al cittadino di conoscere l'attività pubblica, quindi di partecipare, mediante consultazioni, pareri, proposte all'azione amministrativa, per orientarla, eventualmente correggerla e infine per valutarla con la conferma o la disapprovazione del suo operato attraverso il voto[736].

La conoscenza[737] si fa precondizione della libertà e della cittadinanza nel momento in cui fornisce al cittadino gli strumenti per comprendere la realtà. In tal senso la trasparenza non è solo una caratteristica dell'agire pubblico ma anche il banco di prova della democrazia[738].

Come abbiamo visto, anche nel capitolo I, il principio della trasparenza ha una pluralità di fonti giuridiche sovranazionali, che imporrebbero *ipso iure* l'obbligo alle pubbliche amministrazioni di aprire i dati[739], sia che si tratti di valore in sé[740] o di un valore strumentale per il perseguimento di altri interessi, essa esige un intervento regolatorio sistemico tridimensionale che coniughi l'acquisizione mediante un censimento digitale di

---

735 G. ARENA, *Trasparenza amministrativa e democrazia*, in G. BERTI - G. DE MARTIN, *Gli istituti della democrazia amministrativa*, Giuffrè, Milano, 1996, p. 18, cit.

736 A. J. MEIJER *ET AL.*, *La gouvernance ouverte: relier visibilité et moyens d'expression*, in *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78), pp. 13-32; A. MEIJER - M.P. RODRIGUEZ BOLIVAR, *La gouvernance des villes intelligentes. Analyse de la littérature sur la gouvernance urbaine intelligente*, in *Revue Internationale des Sciences Administratives*, 2016/2 (Vol. 82), pp. 417-435 ; A.J. MEIJER *ET AL.*, *La gouvernance ouverte: relier visibilité et moyens d'expression*, *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78), pp. 13-32.

737 Il binomio luce-conoscenza contro le oscurità è un concetto che affonda le sue radici nella filosofia kantiana. «L'illuminismo è l'uscita dell'essere umano dallo stato di minorità di cui egli stesso è colpevole. Minorità è l'incapacità di servirsi della propria intelligenza […] che invece un pubblico [Publikum] si rischiari da sé, è cosa più possibile; e anzi è quasi inevitabile, purché gli si lasci la libertà […] A questo rischiaramento, invece, non occorre altro che la libertà; e precisamente la più inoffensiva di tutte le libertà, quella cioè di fare pubblico uso della propria ragione in tutti i campi [...] il pubblico uso della propria ragione deve sempre essere libero, ed esso solo può realizzare il rischiaramento tra gli uomini», in I. KANT, *Beantwortung der Frage: Was is Aufklarüng?*, in Berlinische Monatsschrift, 1784, pp. 481-494, trad. di Francesca di Donato in M.C. PIEVATELO (a cura di), *Sette scritti politici liberi*, Firenze University Press, 2011.

738 D. HEALD, *Pourquoi la transparence des dépenses publiques est-elle si difficile à atteindre?*, pp. 33-53; DUBREUIL C.A., *La démocratie et la transparence*, in *RFDA*, 2016, pp. 655 ss.

739 articolo XV della Déclaration des Droits de l'Homme et du Citoyen del 1789; articolo 41 della Carta di Nizza del 2000.

740 Birkinshaw parla di *droit humain* in P. J. BIRKINSHAW, *Government and Information: The Law Relating to Access, Disclosure and their Regulation,* 3rd edn. Haywards Heath: Tottel. Birkinshaw, 2005; ID., '*Freedom of Information and Openness: Fundamental Human Rights*', in *Administrative Law Review*, 58(1), 177–218.

dati, la riutilizzabilità[741] e il riutilizzo di informazioni, dei documenti e dei dati con formati adatti a tale scopo. Occorre tenere fermo che l'inflazione informativa e la rumorosità possono tradursi in una forma di opacità perché sono le informazioni veramente significative e non lesive di altri diritti fondamentali quali la protezione della *privacy* e dei dati personali e la riservatezza pubblica[742] a rendere efficace il principio di trasparenza.

Sul piano teorico, la trasparenza, la *privacy* e il segreto pubblico hanno una pari dignità costituzionale, sono valori complementari e non antagonisti, che rispondono a esigenze diverse legate rispettivamente al ruolo di cittadino, individuo o consociato[743].

Sul piano applicativo il bilanciamento tra le diverse aspirazioni deve essere determinato in funzione delle scelte politiche e dello stato evolutivo delle ICT[744].

2.1. Le variabili di apertura dei dati: il consolidamento de les données brutes

La tipologia e la forma dei contenuti informativi che si aprono al pubblico costituiscono gli indicatori principali per valutare il grado di penetrazione della dottrina *Open Government Data* nelle politiche di livello sia nazionale che locale.

Secondo la lettura che ne dà la dottrina francese[745], molto fervida sul punto, affinché il dato si possa definire «aperto» è necessario che possieda una serie di variabili che ne massimizzino il profitto. Le analizzeremo di seguito.

---

741 Essa va intesa come «capacità [dell'informazione] di produrre conoscenza che va al di là della singola dinamica che ha portato alla sua elaborazione» in Carloni, E. (2012a). *Il decreto "crescita". Giornale di diritto amministrativo (11)*, 1041, p. 197.

742 Ossia la salvaguardia di interessi quali la sicurezza e la difesa nazionale, l'ordine pubblico, la politica monetaria, finanziaria e fiscale, le relazioni internazionali.

743 Per esempio la garanzia di imparzialità e integrità degli agenti pubblici richiede la pubblicazione di taluni dati, quali i *curricula,* diversamente in altri casi, questi dati devono essere anonimizzati, con appositi *software* resistenti a eventuali tentativi di de-anonimizzazione.

744 G. MANCOSU, *op. cit.,* p. 50.

745 *Ex multis* M. BERGUIG – F. COUPEZ, *Faut-il réellement craindre l'Open data pour la protection de nos données personnelles?*, in *LEGICOM*, 2016/1 (n. 56), pp. 15-24 ; C. CASTETS-RENARD - N.GANDON, *Open data des données de la recherche publique: entre réformes législatives et retour d'expérience sur un guide pratique à destination des chercheurs*, in *LEGICOM*, 2016/1 (n. 56), pp. 67-75; S. CHIGNARD – J. F. MARCHANDISE, *Open data, comprendre l'ouverture des données publiques*, Fyp éditions, 2012: M. CLEMENT-FONTAINE, *La régulation de l'Open data,* in *LEGICOM,* 2016/1 (N. 56), pp. 113-120 ; L. CLUZEL-METAYER, *Les limites de l'open data*, in *AJDA,* 2016, pp. 102 ss.; K. COLLET THIREAU – J.P. THOMAS J.P., *Big Data et Open Data : quel impact pour les professionnels de l'information?*, in *I2D – Information, données & documents*,

La *fraîcheur des donnée*[746] è la prima qualità attesa dai dati aperti. L'era digitale ha aperto le porte alla «transparence en temps réel», per cui è fondamentale mantenere le utilità legate al dato tempestivo.

La *fraîcheur* può essere intesa in almeno due accezioni diverse: il tempo che intercorre tra un fatto, per esempio la registrazione di una nuova associazione, e il suo inserimento nella banca dati e la frequenza della disponibilità al pubblico del *database*, cioè la data in cui questa associazione appare effettivamente nel registro pubblico.

L'utilizzo di *standard* aperti, facilmente riutilizzabili e leggibili da una macchina rappresenta il secondo criterio necessario. Incluso nell'elenco della qualità dei dati sono le variabili relative all'accuratezza, completezza, attendibilità di dati e metadati.

Similarmente, la trasparenza sugli indicatori di qualità e tracciabilità del processo di produzione dei dati è considerata prerequisito per l'accessibilità ai dati.

La *disclosure*, secondo gli studiosi francesi, come confermato dai Rapporti economici internazionali già esaminati nel capitolo I di questa tesi, sarebbe in grado di incrementare la ricchezza di un Paese o di ridurne la spesa, e pertanto richiederebbe una nuova regolazione, che si adatti all'era tecnologica: «une économie de l'abondance des canaux de diffusion et du faible coût des instruments de rediffusion appelle une rupture du régime juridique des contenus qui y circulent»[747].

La rottura dei vecchi schemi giuridici è determinata dalla consistenza dei nuovi fenomeni: l'evanescenza del dato richiederebbe un regime giuridico che tenga conto della nuova forma, dei rischi e delle potenzialità connesse alla liberazione dei dati.

2015/4 (Volume 53), pp. 9-10; S. GOËTA, *Un air de famille: les trajectoires parallèles de l'open data et du big data*, in *Informations sociales*, 2015/5 (n. 191), pp. 26-34; L. LEYOUDEC, *Reconstruire les conditions d'intelligibilité du document numérique patrimonial : mobilisations documentaire et sémiotique des Linked Open Data*, in *Les Enjeux de l'information et de la* communication, 2015/2 (n. 16/2), pp. 99-112 ; C. MABI, *La plate-forme « data.gouv.fr » ou l'open data à la française*, in *Informations sociales*, 2015/5 (n. 191), pp. 52-59; É. OLLION, *L'abondance et ses revers. Big data, open data et recherches sur les questions sociales*, in *Informations* sociales, 2015/5 (n. 191), pp. 70-79 ; J.C. PLANTIN - J. VALENTIN, *Données ouvertes et cartographie libre. Autour du cas de Montpellier*, in *Les Cahiers du numérique*, 2013/1 (Vol. 9), p. 85-107; A. QUINTARD KAIGRE, *L'Open Data au service du droit à l'information et de la liberté d'expression*, *Documentaliste-Sciences de l'Information,* 2014/4 (Vol. 51), p. 34 ss.; É. ROCHE, *Open data et business models*, in *LEGICOM*, 2016/1 (N. 56), pp. 121-127; K.C. THIREAU - J.P. THOMAS, *Big Data et Open Data: quel impact pour les professionnels de l'information?*, in *I2D – Information, données &* documents, 2015/4 (Volume 53), pp. 9-10 e O.ZAZA, *Vers un Open data visuel: le portail Open Data Paris*, in *I2D – Information, données & documents*, 2015/2 (Volume 52), pp. 53-53.

[746] La tempestività.

[747] G. GUGLIELMI, *Numérisation des données publiques et données publiques numériques*, *ibid.*.

Come si è ampiamente scritto, il grado di apertura di una pubblica amministrazione ha acquisito maggiore flessibilità con l'avvento delle nuove tecnologie, si è ampliato rispetto al passato perché quanto più la tecnica consente di aprire agevolmente e a costi modici i documenti, i dati e le informazioni della P.A. tanto più si espande il diritto del cittadino all'accesso a quei documenti, a quei dati e a quelle informazioni.

Quanto alla tipologia dei dati, oggetto di questo paragrafo, i giuristi francesi si riferiscono ai cd. «données brutes»[748] cioè dati grezzi.

In altre parole «le mouvement de l'open data invite les gouvernements à ouvrir leurs données «brutes» afin que des acteurs externes puissent les utiliser librement, que ce soit pour créer de nouveaux services ou pour renouveler la relation entre les citoyens et leurs administrations»[749].

Dunque, dati non adulterati[750] dalle PP.AA., ma dati collegati secondo il protocollo *http*, e cioè dati con relazioni che siano quindi utili e collegate ad altre informazioni, tali da rendere il dato completo o comunque utile e interessante perché multicontenutistico[751].

I dati, tuttavia, non sono neutri e sono difficilmente utilizzabili nella loro forma originaria: «les données publiques produites sont donc difficilement utilisables en l'état par des acteurs externes pour un usage alternatif à celui pour lequel elles ont été produites. Pour permettre leur insertion dans un autre cadre d'action, il est nécessaire de les consolider, c'est-à-dire d'intercaler une étape supplémentaire dans la chaîne de la donnée pour lui permettre de répondre à un usage non prévu initialement»[752].

Perciò diversamente dall'idea secondo cui i dati devono essere pubblicati nella loro forma nuda e cruda, la dottrina francese ritiene necessario un consolidamento che richiede almeno tre operazioni: *l'enrichissement, la standardisation* e *l'articulation.*

---

748 A. COURMONT, *Open data et recomposition du gouvernement urbain de la donnée comme instrument à la donnée comme enjeu politique*, in *Informations sociales*, 2015/5 (n. 191), pp. 43. *Raw data* secondo Tim Berners Lee, secondo cui «The Semantic Web isn't just about putting data on the Web. It is about making links, so that a person or machine can explore the Web of data. With linked data, when you have some of it, you can find other, related, data».

749 A. COURMONT, pp. 40-50 cit.; *contra* L. GITELMAN, *Raw Data Is an Oxymoron,* Cambridge, MIT Press, 2013.

750 L.D. BENYAYER - S. CHIGNARD, *Focus - Les enjeux économiques de l'ouverture des données : pas de marché, pas de valeur*, in *Informations sociales* 2015/5 (n. 191), pp. 36-39.

751 É. ROCHÉ, *Open data et business models*, in *LEGICOM*, 2016/1 (N. 56), pp. 121-127. Cfr. in particolare con il § 4 del capitol I.

752 A. COURMONT, *ivi*, p. 46, cit.; B. DIDIER - P. PIAZZA, *Les conséquences humaines de l'échange transnational des données individuelles*, in *Cultures & Conflits*, 76, 2009, *passim*.

L'*enrichissement* richiede l'aggiunta di informazioni nel *dataset*, il quale potrà essere utilizzato per nuovi usi. Tale lavoro viene spesso eseguito dai gestori di dati pubblici in modo che rispettino l'evoluzione delle competenze dell'istituzione. Questo arricchimento dei dati richiede di cambiare la sua infrastruttura informativa, la quale può avere un costo finanziario, tecnico e organizzativo.

Soprattutto è richiesto di identificare i nuovi usi per poter modificare i dati.

Sorge, tuttavia un interrogativo: «Comment on va pouvoir l'étoffer afin qu'elle soit réutilisable et intéressante pour le développement d'un service public. Pour l'instant, je pense que personne ne produit de la donnée avec cet oeil-là»[753].

La *standardisation* consente di utilizzare i dati su un più ampio raggio e quindi la interoperabilità tra gli utilizzatori. Il formato è leggibile da qualsiasi macchina e riutilizzabile conservando le utilità che raccoglie.

Infine la terza operazione di *articulation* è quella di inserire «opérateurs d'articulation» nei *set* di dati per facilitare il loro collegamento. Lo scopo è quello di ovviare alla carenza di informazioni disponibili in un insieme di dati, in modo da permettere il loro collegamento con altri insiemi di dati provenienti da altri produttori.

L'aggiunta di un elemento supera la geolocalizzazione del dato, la cui informazione si riferisce a un territorio circoscritto e lo inserisce così in uno spazio di equivalenza comune per gli altri utilizzatori. In questo modo il dato potrà essere utilizzato in vari contesti: «est ainsi nécessaire pour ajouter cette information à la donnée afin de lui faire acquérir un caractère de généralité qui permettra d'étendre son domaine de validité»[754].

Queste operazioni di consolidamento possono essere eseguite dal produttore pubblico dei dati o da attori privati. Nel primo caso, l'*open data* non consiste più semplicemente nel mettere a disposizione i dati pubblici utilizzati ogni giorno, ma nel rielaborarli in modo che possano incontrare un uso esterno. È allora necessario ripensare all'infrastruttura informativa dei dati che deve essere integrata con queste nuove operazioni nel processo di produzione e di organizzazione tecnica. Queste operazioni richiedono un costo che è difficilmente sopportabile dalle comunità.

---

753 A. COURMONT, *ibid.*

754 ID., *ivi*, p. 47, cit.

Quando, invece sono gli attori privati responsabili del consolidamento essi si posizionano in un rango intermedio tra il produttore pubblico e i riutilizzatori dei dati.

Le aziende produttrici di mappe digitali sono, per esempio, *leader* storici nel settore intermedio. Oggi sono in concorrenza con attori dell'economia digitale, che sotto forma di piattaforme occupano una posizione centrale in crescita. Il rischio è che si trovino in una situazione di quasi-monopolio, determinando una redistribuzione del potere che apre la questione del controllo dei dati da parte delle autorità pubbliche.

3. La legge fondamentale sull'accesso: *la loi* CADA

Esamineremo qui la risposta regolatoria offerta negli anni dalla legislazione francese.

In Francia, in particolare, «on distinguera trois étapes entre accès aux documents administratifs, service public de diffusion du droit et 'libération' des données publiques»[755]. La cornice normativa è rappresentata dalla legge fondamentale sull'accesso all'ISP, la *loi CADA* del 1978, che ha sancito la libertà di chiunque di accedere ai «documenti amministrativi», ribaltando il principio del segreto che fino ad allora aveva informato la relazione tra amministrazione ed amministrati. La disciplina legislativa è completata da quella di cui al *décret n. 2005-1755 du 30 décembre 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi n° 78-753 du 17 juillet 1978* e dal *Code des relations entre le public et l'administration* (CRPA), entrato in vigore il 1 gennaio 2016.

Il CRPA costituisce la «*lex generalis* delle relazioni tra il pubblico e l'amministrazione. Comprende, pertanto, solo disposizioni trasversali, ad esclusione delle regole che concernono campi specifici dell'azione amministrativa e spesso, d'altronde, già

[755] D. BOURCIER (a cura di), *Open Data et Big Data, Nouveaux défis pour la vie privée*, Mare et Martin, Parigi, 2016, *passim* ; ID., *Tele-communs versus tele-services publics : vers des services publics collaboratifs en ligne*, in *Revue française d'aministration publique*, (n. 146), 2013, 271-284.

codificate. Tra le regole trasversali, il Codice include anche alcuni orientamenti giurisprudenziali che si è ritenuto opportuno, data la loro importanza, tradurre in un testo di rango legislativo»[756].

Quindi la *loi* CADA è confluita nel libro III del CRPA e ha continuato ad essere costantemente revisionata, si pensi che la *Loi Valter n. 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public* ha modificato gli articoli 10-19 del CADA.

Già con l'*ordonnance 2005/650*, che trasponeva *a maxima* la direttiva 2003/98/CE - anticipando le principali innovazioni normative introdotte a livello europeo dalla direttiva 2013/37/UE - l'ambito oggettivo di applicazione dell'accesso è stato esteso a quello del riutilizzo e quindi dello sfruttamento commerciale o non, armonizzandolo e consacrando fin dal 2005 il diritto al riutilizzo dell'informazione pubblica liberamente accessibile ed estendendone l'applicazione agli istituti d'istruzione e di ricerca e agli enti culturali, cui era riconosciuta la facoltà di adottare una disciplina derogatoria[757].

L'*ordonnance* del 2005 ha il merito di aver eliminato il divieto di riutilizzo commerciale di documenti acquisiti mediante l'esercizio del diritto di accesso.

Gli obblighi normativi posti in capo al riutilizzatore a tutela dell'integrità dell'informazione (art. 12), hanno rafforzato la tesi secondo cui riutilizzo e accesso garantiscono congiuntamente il diritto all'informazione. Infatti, «gli obblighi di integrità non sono posti a tutela dei diritti di proprietà intellettuale vantati dall'amministrazione sull'informazione oggetto di riutilizzo, ma del diritto del *quisque de populo* a godere di un prodotto informativo attendibile, soprattutto allorquando sia basato sul trattamento di informazioni pubbliche»[758]. Dunque l'esercizio del diritto di accesso non è condizionato ad alcun requisito di legittimazione.

---

[756] Rapport au Président de la République relatif à l'ordonnance n. 2015-1341 du 23 octobre 2015.

[757] «Les informations figurant dans des documents produits ou reçus par les administrations mentionnées à l'article 1er, quel que soit le support, peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus» - art. 10, c.1

[758] G. MANCOSU, *ivi,* p.176, cit. L'autore, a questo proposito, riporta come esempio eloquente una fattispecie di riutilizzo sanzionata dalla CADA ex art. 18: la società *France Quick* aveva realizzato nel 2008 una campagna pubblicitaria nella quale vantava le proprietà nutrizionali di un nuovo olio di frittura da essa realizzato, citando a suo vantaggio ed in maniera distorta le raccomandazioni dell'Agenzia francese di sicurezza sanitaria degli alimenti (AFSSA).

La disciplina del riutilizzo risultava però mitigata dalla facoltà riconosciuta all'amministrazione d'imporre tariffe e licenze (artt. 15 e 16). Non era tuttavia configurabile in capo all'amministrazione un obbligo di fornire il documento in un formato aperto e leggibile da una macchina, sia in risposta ad una richiesta di accesso (art. 4), sia in caso di diffusione (obbligatoria o facoltativa).

Inoltre ulteriori limitazioni erano rinvenibili nell'esclusione dall'ambito di applicazione della disciplina del riutilizzo delle informazioni contenute in documenti prodotti/ricevuti nello svolgimento di una *mission de service public à caractère industriel ou commercial* (SPIC) (art. 10); nella possibilità per le amministrazioni di prevedere tariffe superiori al costo marginale di diffusione (art. 15); nell'eterogeneità delle licenze di riutilizzo (correlata a quanto disposto dall'art. 16, c. 1), con nocumento dell'interoperabilità giuridica dei *dataset*; nell'inesistenza di un obbligo generale di diffusione dei «données-moyen» liberamente accessibili (art. 7); nell'inadempimento generalizzato dell'obbligo posto in capo alle amministrazioni di recensire l'ISP detenuta (art. 17).

Nel 2011 con la strategia OGD e in particolare con il *décret n. 2011-194 du 21 février 2011*[759], il *décret n. 2011-577 du 26 mai 2011*[760], la *circulaire du 26 mai 2011*[761] diversi punti di debolezza sono stati superati.

Sul diritto di accesso riconosciuto al *quisque de populo* vigila infatti un'Autorità indipendente autorevole, i cui orientamenti di *moral suasion* hanno guidato l'evoluzione dell'istituto nel contesto tecnologico e istituzionale, incentivando continui affinamenti normativi fino all'introduzione di una disciplina del riutilizzo all'avanguardia.

Nel 2012 viene esteso il principio di gratuità e rafforzato quello della diffusione del patrimonio informativo pubblico, a partire dai «données à fort impact sociétal (santé, éducation, etc.) et/ou à fort potentiel d'innovation sociale et économique»[762].

---

[759] che ha istituito l'Agenzia governativa *Etalab*, incaricata della creazione del portale nazionale OGD - *data.gouv.fr*.

[760] che ha inquadrato e ristretto il perimetro delle tariffe esistenti per il riutilizzo dell'ISP detenuta dallo Stato e dagli enti statali.

[761] che ha portato all'elaborazione da parte di *Etalab* di una licenza gratuita cui sottoporre il riutilizzo dell'ISP pubblicata sul portale data.gouv.fr e ha visto l'invito ad impiegare formati di rappresentazione dei dati che favoriscano l'interoperabilità dei sistemi informativi, la trasmissione e il riutilizzo dell'ISP.

[762] CIMAP del 18 dicembre 2012 in materia OGD.

Nel 2014 due *Missions d'information* presso il Senato hanno condotto alla formulazione di numerose e dettagliate raccomandazioni di carattere tecnico, organizzativo e giuridico sulla circolazione e la valorizzazione del patrimonio informativo pubblico. Il piano d'azione nazionale OGP 2015 ha rilanciato l'impegno del Governo nella direzione dell'apertura e della diffusione.

Il *projet de loi numérique* ha previsto ulteriori significative innovazioni, a partire dalla generalizzazione dell'obbligo di diffusione delle informazioni pubbliche, e del conseguente diritto civico, secondo uno *standard* aperto: «l'ultimo miglio» del processo di positivizzazione del modello OGD. Il diritto di ottenere dall'amministrazione la formazione di documenti o l'estrazione di informazioni mediante un *traitement automatisé d'usage courant* è stato riconosciuto anche dalla giurisprudenza amministrativa, che l'ha ritenuto implicito nella nozione di documento esistente: «Si l'administration ne détient pas le tableau nominatif des personnels salariés de la commune avec leur qualification et la qualification de leur poste de travail, mais peut l'obtenir grâce à un traitement automatisé d'usage courant, elle doit satisfaire la demande de communication»[763].

La sistematizzazione della diffusione avrebbe così avuto l'effetto di ridurre progressivamente le richieste di accesso, spingendo le amministrazioni a una gestione più consapevole ed accurata del loro patrimonio informativo, «aiutandole a percepirne l'apertura come un dovere istituzionale "trasversale" di rilevanza pari ai doveri istituzionali "caratterizzanti". Detto in altro modo, piuttosto che limitarsi a rispondere a richieste puntuali d'accesso ad uno specifico documento (nello "stato tecnologico" in cui si trova), l'amministrazione sarebbe costretta a farsi carico, anzitutto, di una ricognizione del proprio patrimonio informativo, e della programmazione di tutte quelle verifiche di affidabilità, accuratezza, completezza e (eventualmente) resistenza alla deanonimizzazione, preliminari alla diffusione»[764].

763 TA di Marsiglia, 2 novembre 2011, M.R., n. 1005828.

764 G. MANCOSU, *ivi*, p. 204, cit.

Il 28 settembre 2016 il Senato ha adottato le conclusioni della *Commission mixte paritaire* sul *projet de loi République numérique*[765], e ha avviato una consultazione sul *service public de la donnée*[766], tesa a semplificare e favorire l'apertura e la circolazione dei dati pubblici[767].

In conformità con gli impegni assunti dalla Francia nel quadro del partenariato per l'*Open Government*, il Segretario di Stato incaricato del digitale, Axelle Lemaire, ha voluto continuare l'approccio di cooperazione che ha già visto più di 21.000 partecipanti contribuire allo sviluppo e al miglioramento del testo originale[768].

In breve, il testo prevede che le PP.AA. possano avere accesso ai dati delle altre PP.AA., che rendano pubblici i codici sorgente e che informino i cittadini dei processi algoritmici attuati. Le informazioni pubbliche non saranno più oggetto di una domanda, ma saranno diffuse pubblicamente o perché esiste un *database* che le contiene oppure perché a loro pubblicazione è di interesse economico, sociale, sanitario o ambientale.

I dati saranno resi accessibili e riutilizzabili *sic et simpliciter*.

Potranno, altresì essere pubblicate e riutilizzate alcune informazioni pubbliche contenenti dati personali nel pieno rispetto della *privacy*.

Pertanto, dalla illustrazione del processo evolutivo del regime generale della circolazione e della valorizzazione delle informazioni, *de iure condito* e *de iure condendo,* nel panorama francese si evince chiaramente una maggiore sensibilità, coesione e solidità rispetto a quello italiano.

Per citare solo alcune delle concrete azioni del governo nazionale francese, si possono segnalare i due *software* che simulano l'applicazione del quadro normativo a una

---

765 La consultazione online si è servita della piattaforma: *https://www.republique-numerique.fr/*, in cui è disponibile ampia documentazione sull'evento. Si tratta della prima volta in cui il Governo sottopone a discussione pubblica la bozza di un progetto di legge prima di averla inviata al Consiglio di Stato e presentata in Consiglio dei Ministri.

766 Articolo 14 della *loi pour une République numérique*.

767 Secondo G. MANCOSU, *ivi*, p. 213 «La "rivoluzione copernicana" di cui la disciplina in esame si fa portatrice, presenta, ad avviso di chi scrive, almeno due punti di debolezza: l'obbligo di diffusione è condizionato alla disponibilità dei documenti in formato elettronico590, ma nulla è previsto a proposito dei tempi, dei modi, dei canali di finanziamento e dell'eventuale obbligatorietà della digitalizzazione dei documenti in formato cartaceo, magari a partire da quelli sui quali gli accedenti abbiano manifestato un particolare interesse; è fatto cenno all'anonimizzazione, ma nulla è previsto a proposito dei tempi, dei modi, dei canali di finanziamento e dell'eventuale obbligatorietà dell'anonimizzazione dei documenti contenenti dati personali, magari a partire da quelli sui quali la comunità dei riutilizzatori manifesti un particolare interesse».

768 I risultati della consultazione sono consultabili al *link*: *https://www.etalab.gouv.fr/consultation-spd*.

fattispecie concreta, i cui elementi rilevanti sono imputati dal cittadino. Questi strumenti hanno un duplice obiettivo informativo: di servizio, facilitando l'esercizio dei diritti del cittadino o l'adempimento dei propri doveri e di verifica democratica, in quanto alla comprensione dell'impatto pratico del quadro normativo corrisponde, una spiccata capacità del cittadino di misurare i risultati delle scelte compiute dai rappresentanti politici[769].

Un esempio sarà chiarificatore: *OpenFisca*[770] è un *software* di simulazione del sistema sociale e fiscale francese che consente di visualizzare le prestazioni sociali e le imposte pagate dalle famiglie e di simulare l'impatto delle riforme sul loro reddito, quindi i possibili risparmi. Analogamente il *software Mes-aides*[771] permette partendo dai dati relativi a uno specifico nucleo familiare, di conoscere le prestazioni sociali a cui esso ha diritto.

Il terzo strumento utilizzato in Francia, citato nel piano di azione OGP, è una piattaforma di visualizzazione concernente l'impiego dei fondi pubblici destinati all'aiuto allo sviluppo[772]. «Il sito contiene una presentazione georeferenziata dei progetti in corso di importo uguale o superiore a centomila euro e una maschera che ne consente l'esplorazione secondo differenti criteri di ricerca. Per ciascun progetto è presente una scheda che dettaglia: obiettivi, risultati attesi, calendario, stato di avanzamento, importo del finanziamento, operatori incaricati della realizzazione e beneficiari. I dati pubblicati sul sito sono liberamente e gratuitamente riutilizzabili ai sensi della *loi* CADA. Il sito include anche una funzione di monitoraggio civico dei progetti: un *form* consente a chiunque di fornire informazioni supplementari sulla loro realizzazione»[773].

---

769 G. MANCOSU, *ivi*, p. 229 ss.

770 *http://www.openfisca.fr/*.

771 *https://mes-aides.gouv.fr/*.

772 *http://www.transparence-aide.gouv.fr*.

773 G. MANCOSU, *ivi*, p. 230, cit.

4. Dall'*essential facility* all'*essential disclosure*

L'«essenzialità»[774] (*données essentielles*) delle informazioni nella dottrina francese, è intesa come prerequisito per l'esercizio dei diritti fondamentali di cittadini e stranieri.

Non un «minimum» fisso di informazioni, ma un insieme variabile di informazioni di interesse pubblico in ragione del momento storico tale da costituire la base di riutilizzo dell'informazione che genera nuovi contenuti utili alla collettività.

La dottrina dei dati essenziali ha preso le mosse dal rapporto Mandelkern[775] che si era posto lo scopo di definire un regime generale della circolazione dell'informazione pubblica, integrando nella *loi* CADA la disciplina della diffusione dei dati pubblici. Essa costituisce ancora oggi un riferimento d'avanguardia, a cui guardare per trarre «profitto democratico» dal modello OGD. Secondo questo Rapporto un regime particolarmente liberale doveva essere riservato ai «dati pubblici essenziali»[776]: «la notion de donnée essentielle est nécessairement évolutive. En effet, l'internet produit une dynamique propre qui pourrait conduire, de proche en proche, à élargir le contour des données gratuitement mises en ligne. D'une part, cet élargissement pourra résulter d'une volonté politique de transparence, ou d'une stratégie active de mise à la disposition du secteur privé de contenus […] Les données essentielles seraient alors définies comme les données publiques dont la

---

774 *Memorandum for the Heads of Executive Departments and Agencies* del 21 gennaio 2009, relativo all'applicazione del Freedom of Information Act, FOIA del 1966.

774 F. JUTAND, *Ouverture des données de transport. Paris: Ministère de l'écologie, du développement durable et de l'énergie*, in *http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/154000182.pdf*, 2015.

775 Così il Rapporto "Diffusion des données publiques et révolution numérique" del laboratorio diretto da Dieudonné Mandelkern che si si inserisce nel programma di governo per la società dell'informazione (PAGSI), annunciato dal Primo Ministro Lionel Jospin a Hourtin il 25 agosto 1997- adottato dal Comité interministériel pour la société de l'information il 16 gennaio 1998, che prevede il principio fondamentale della gratuità dei dati ritenuti essenziali, in *http://discours.vie-publique.fr/notices/973145007.html.*

776La loi CADA avrebbe dovuto contenere una disposizione simile : «Les services et établissements publics administratifs de l'Etat mettent gratuitement à la disposition du public, sur des sites accessibles en ligne, les données essentielles qui les concernent. Ces données peuvent être gratuitement utilisées et rediffusées, y compris à des fins commerciales, à condition qu'elles ne subissent pas d'altération et que leur source soit mentionnée». Il progetto di legge LSI prevedeva infatti anche la modifica del titolo della loi CADA in *Loi n° 78-753 du 17 juillet 1978 relative à l'accès aux documents administratifs et à la diffusion des données publiques*, tuttavia il progetto di legge LSI decadde e insieme ad esso l'illuminato disegno riformatore tracciato nel rapporto Mandelkern decadde alla fine della undicesima legislatura in *http://www.assemblee-nationale.fr/11/dossiers/societe_information.asp.*

mise à disposition est une condition indispensable à l'exercice des droits du citoyen, ainsi que de ceux des étrangers résidant sur notre sol»[777].

Viene anche fissato il criterio per definire l'essenzialità [778] e così proposta una definizione dinamica di «informazioni essenziali», che deve essere calata nel contesto politico e tecnologico, ma anche, e soprattutto, determinata rispetto al pubblico dei suoi fruitori. Da ciò deriva che l'amministrazione, non solo dovrà aprire i dati essenziali, ma anche adottare le misure atte a garantirne il godimento da parte dei cittadini. In altri termini, il rapporto Mandelkern precorre l'idea di una trasparenza essenziale irrinunciabile, basata sulla più ampia fruibilità dei significati delle informazioni più che una politica di diffusione di dati grezzi[779].

La nozione di essenzialità dei dati è mutuata dalla dottrina statunitense dell'*essential facility* e conduce all'obbligo di diffusione gratuita dei dati essenziali delle P.A. o degli enti privati incaricati di un pubblico servizio, essa risponderebbe all'esigenza di garantire la concessione d'uso dei dati a tutti, in un mercato concorrenziale[780].

In linea con la dottrina francese dell'essenzialità la nozione di informazione pubblica, il cui carattere oggettivo si ricava non solo dal lato dei suoi attributi qualitativi quali autenticità, integrità, certezza, ma soprattutto dalla suscettibilità a facilitare l'esercizio di altri diritti e il raggiungimento di altre finalità di pubblico interesse. Tali scopi sono sia estrinseci all'informazione, si pensi alla sicurezza dei trasporti potenziata dalla disponibilità di informazioni sul traffico, sulla condizione della rete, sulle condizioni meteorologiche, sia intrinseci, si pensi all'informazione come strumento diretto di trasparenza e di controllo democratico sull'esercizio del potere[781].

---

777 Rapporto "Diffusion des données publiques et révolution numérique" del laboratorio diretto da Dieudonné Mandelkern, p. 95, cit.

778 *Ibid.* «C'est finalement le critère de la finalité de l'usage des données publiques qui s'est imposé. Restait à savoir quelle finalité devait être privilégiée. Dans une approche économique, on aurait pu notamment donner au terme "essentiel" l'acception qui est la sienne dans le droit de la concurrence. La finalité économique n'a cependant pas paru devoir justifier la gratuité, qui traduit une action de redistribution. L'utilité pour la vie quotidienne est apparue trop extensive et floue. La seule utilité pour les démarches administratives est au contraire apparue en retrait de ce que proposait le PAGSI, qui va déjà au-delà des seuls formulaires administratifs. Conformément à l'esprit du PAGSI, c'est finalement la notion de citoyen qui s'est imposée», p. 96, cit.

779 G. MANCOSU, *op. cit.*, p. 185.

780 Cfr. con il § 3 del capitolo III di questa tesi.

781 ARENA G., *Trasparenza amministrativa*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 5945 ss.

La notevole compattezza e copertura fanno dell'informazione pubblica un *asset* economico e sociale strategico. È proprio per sfruttare le potenzialità delle infrastrutture tecnologiche attualmente disponibili e massimizzare le occasioni di riutilizzo che la dottrina francese ha invocato l'adozione di un regime che non sia restrittivo[782] mediante l'affermazione di un «modello di business» dei dati aperti e gratuiti[783].

Questi dati essenziali apparterrebbero alla stessa collettività cui andrebbero restituiti, se così non fosse ovvero se i dati non appartenessero al singolo cittadino o meglio se non fossero essenziali per la sua informazione quello stesso cittadino non potrebbe neanche richiederli perché verrebbe meno la titolarità del diritto all'accesso a quei dati.

5. L'apertura dei dati come *enjeu politique*: quale ruolo per il *policy maker*

La concentrazione delle informazioni rende le piattaforme pubbliche e private che utilizzano i dati incontrollabili e gli utilizzatori alla loro mercé[784]. La fase di consolidamento dei dati pubblici solleva questioni fondamentali sul ruolo dell'*acteur public* sulle politiche *open data.*

«Doit-il produire de la donnée uniquement pour ses propres besoins ou prendre en considération les besoins externes d'entreprises privées? Qui doit jouer le rôle de consolidateur des données afin de permettre leur usage dans la création de nouveaux services? L'acteur public doit-il laisser le champ à des entreprises privées au risque de se voir déposséder d'une situation d'intermédiaire?»[785].

Le risposte a queste domande sono cruciali perché determinano il confine pubblico/privato e la ricomposizione del ruolo dei governi.

---

782 G. MANCOSU, *op. cit.,* p. 53.

783 CHIGNARD S. – J. F. MARCHANDISE, *Open data, comprendre l'ouverture des données publiques*, Fyp éditions, 2012, p. 117.

784 S. FRENOT – S. GRUMBACH, *Des données à l'intermédiation, une révolution économique et politique*, *in* L. CALDERAN - P. LAURENT - H. LOWINGER - J. MILLET (dir.), *Big Data: nouvelles partitions de l'information,* Louvain-la-Neuve, De Boeck, coll. Information et stratégie, pp. 97-120, 2015.

785 A. COURMONT, *ibid.*

Simili interrogativi evidenziano, infatti, come le politiche di apertura dei dati richiedano una discussione politica aperta perché *la donnée n'est plus uniquement un instrument, elle devient un enjeu de gouvernement*. Aprire i dati significa trasformare l'infrastruttura informativa per accogliere tutti i loro possibili usi alternativi e considerare i dati stessi come oggetto di una politica di governo, non semplicemente strumenti di politica pubblica.

Esse non sono univoche, ma variabili in base ai settori di intervento pubblico, ai dati, ai metodi e agli attori coinvolti. Le politiche *open data* devono quindi essere considerate in funzione dei dati, dei settori e delle comunità nonché degli orientamenti politici.

Dall'esame dell'applicazione pratica del regime *open* francese si è evinto chiaramente che la dimensione politica dei dati fa di essi dei facilitatori di democrazia[786].

Uno Stato democratico e trasparente mostra i suoi dati al pubblico per rendere il suo operato visibile e dunque aprire le porte dell'amministrare ai cittadini operosi che vogliano partecipare alla cosa pubblica.

Le nuove questioni vedono confliggere però interessi diversi, per questo dovranno essere affrontate con cautela, tenuto conto che «l'ouverture des données publiques mise en oeuvre par les collectivités territoriales fait apparaître des défis imprévus: la donnée initiale n'est ni neutre ni brute et sa réutilisation exige des opérations d'ajustement et d'homogénéisation. Une question se pose, qui fait de l'open data un enjeu de politique publique: qui, des producteurs publics ou des acteurs privés en train de prendre une place dominante dans l'exploitation des data, va se charger de cette phase intermédiaire?»[787].

Resta da compiere un processo di assimilazione graduale dei canoni *open* da parte degli ordinamenti internazionali. Questa operazione richiede una griglia di valori e di priorità uniformi condivisi che orienti la costruzione di un diritto pubblico globale.

I programmi politici e i disciplinari che partono dal basso penetrano sempre più in profondità la relazione cittadino e P.A..

Le innovazioni tecnologiche esigono una conciliazione tra le differenti tradizioni giuridiche in materia e la Francia ben rappresenta, rispetto all'Italia, laboratorio

---

786 S. FRENOT – S. GRUMBACH, *op. cit., ibid.*

787 A. COURMONT, *Open data et recomposition du gouvernement urbain de la donnée comme instrument à la donnée comme enjeu politique*, in *Informations sociales*, 2015/5 (n. 191), pp. 40-50.

sperimentale di apertura dei dati per la definizione di un «diritto amministrativo cosmopolita dell'integrazione internazionale»[788].

Gli adeguamenti sul piano europeo dei diritti nazionali conseguenti alla trasposizione della direttiva 2013/37/UE si rivelano, nel complesso, modesti.

Il legislatore francese lavorando sui nuovi profili della trasparenza pubblica sarà destinato a influenzare i consessi internazionali cui pure aderiscono Francia e Italia.

Infatti, la tradizione giuridica e la riforma francesi, prima e in maniera più netta di quella italiana[789], esigono la diffusione di informazioni essenziali in un formato aperto rielaborabile; la generalizzazione di condizioni di riutilizzo compatibili con la definizione di conoscenza aperta e quindi la gratuità, l'ammissibilità di finalità commerciale e non commerciale; la definizione di accorgimenti giuridici e tecnologici atti a contemperare le esigenze di apertura con la protezione della riservatezza pubblica e privata.

È necessaria anche un'analisi del rapporto tra la qualità e la sostenibilità finanziaria delle misure attuative.

Tuttavia, fintanto che i canoni aperti non saranno pienamente integrati nei sistemi informativi in uso alle pubbliche amministrazioni e non saranno, in tal modo, pressoché azzerati i costi marginali dell'apertura delle informazioni, il diritto all'acquisizione di dati pubblici in formato aperto è destinato a restare «finanziariamente condizionato»[790].

Restano dunque aperti i problemi connessi all'esigibilità dei trattamenti di digitalizzazione, apertura e anonimizzazione e dell'apertura di *default* di quelle porzioni del patrimonio informativo pubblico ancora non investite da obblighi di pubblicazione o da richieste di accesso.

Una volta che i capisaldi *open* saranno stati in qualche modo riconosciuti a livello nazionale, è opportuno che per il loro consolidamento intervengano impegni assunti dai governi in sede internazionale che alimentino la «viralità della trasparenza», trasformandola in scelta predefinita.

---

788 G. MANCOSU, *op. cit.,* ivi, p. 239.

789 Per un esame delle criticità della normativa italiana sia consentito rinviare al § 3 del capitolo I di questa tesi.

790 G. MANCOSU, *op. cit.,* ivi, p. 240, cit.

Le peculiarità del dato richiede l'interoperabilità giuridica, tecnologica e semantica, ossia la standardizzazione di licenze e formati in grado di supportare l'integrazione di *dataset* di fonte eterogenea. La sostenibilità e l'efficacia dei processi di apertura passa attraverso una gestione nativa della produzione di informazioni, dati e documenti e del riutilizzo.

All'AgID in Italia e a Etalab in Francia è affidato il compito di vigilare sull'attuazione e sull'armonizzazione tecnologica del processo di apertura dei dati pubblici, attraverso la redazione di linee guida, la diffusione di *standard* e la promozione di buone prassi[791]. Un'autorità amministrativa indipendente[792] vigila sull'attuazione del dettato normativo e svolge un prezioso ruolo nomofilattico, tanto in sede consultiva quanto in sede precontenziosa.

La pubblicazione dei dati costituisce l'adempimento di un obbligo giuridico e di un impegno derivante dall'adesione a un atto di *soft law*. Nonostante ciò, il diritto giustiziabile alla *disclosure* è delimitato da confini oggettivi sempre meno stretti, in ragione dell'individuazione di nuove parti «essenziali» di informazioni[793].

La liberazione dei dati pubblici edifica una nuova trasparenza capovolgendo il profilo «unilaterale» che l'ha ridotta finora a un documento amministrativo custodito gelosamente dall'amministrazione che si è ben guardata dal fornirlo nei termini di legge.

Ora la dematerializzazione ha abilitato nuove forme di godimento di vecchi diritti e innescato nuovi processi di produzione della trasparenza.

In tale contesto è mutata la figura dell'amministrazione, sulla quale grava la garanzia dei «livelli essenziali» di trasparenza definiti dal legislatore nonché sfide organizzative e culturali.

L'informazione è stata finora gestita come un bene rivale dalla *manus* proprietaria dell'articolazione amministrativa che l'ha solo raccolta o registrata, mentre il nuovo modello *open* esalta il carattere non rivale del dato pubblico, il cui valore è direttamente

---

791 G. MANCOSU, p. 243.

792 ANAC.

793 *Ibid.*

proporzionale all'ampiezza e alla velocità della sua condivisione all'interno e all'esterno dell'amministrazione[794].

«A livello operativo, la messa a sistema del patrimonio informativo pubblico rende indispensabili la ricognizione, la bonifica e la normalizzazione delle basi di dati pubbliche, oltre a richiedere investimenti in risorse umane e tecnologiche specialistiche.

La complessità giuridica, tecnica ed organizzativa delle soluzioni necessarie all'implementazione del modello OGD spiega perché la sua emersione ed il suo progressivo radicamento continuino a trarre impulso più da una volontà di sperimentazione che dalla necessità di adempiere a un precetto normativo»[795]. È per questo che il *soft law* ha un ruolo preponderante rispetto all'*hard law*.

In conclusione, l'*Open Data* offre l'opportunità di radicare la propria cittadinanza su basi informative complete e affidabili. E ciò non tanto per vigilare su un'amministrazione, contemplandola dall'esterno, ma per rompere le pareti, entrare nella «casa di vetro», cancellando il *gap* tra cittadini e amministrazione ed esercitare la propria porzione di sovranità.

---

[794] G. MANCOSU, p. 246.

[795] *Ibid.*

Conclusioni

Da quanto fin qui argomentato si registra un parallelismo tra l'abuso di posizione dominante di *Google* nel mercato dei dati e l'abuso della dominanza delle PP.AA. nella gestione dei dati prodotti dai cittadini. Il primo è chiaramente un abuso finalizzato all'incremento del potere economico incontrastato di *Montain View*, e sprezzante della riservatezza dei singoli; il secondo, invece è diretto all'incremento del potere politico dei governi, ostili all'apertura e alla visibilità delle informazioni in loro possesso al pubblico.

A ciò si aggiunga che le contrastanti esigenze di chiusura (*rectius* controllo) dei dati, dettate dalla tutela della *privacy* e di condivisione degli stessi, domandate dall'efficace spiegarsi del principio di trasparenza, di libertà economica e di tutela della concorrenza vedono invertita la loro rotta: i dati personali, sotto forma di *big data*, sfuggono dalle mani dei loro legittimi proprietari per essere estratti e utilizzati abusivamente; l'*asset* strategico dei dati, rimane nascosto, perché ora è custodito gelosamente da una PA arcigna, ora diventa segreto d'impresa dei colossi della Rete, per niente intenzionati a condividere la fonte dei loro profitti.

Una soluzione comune potrebbe unire le due problematiche: i dati, in entrambi i casi, dovrebbero tornare nella loro forma grezza[796] a chi li produce, ma non i semplici dati anonimizzati e annacquati, ma i dati minimizzati e circostanziati, cioè dati relazionati ad altri dati mediante collegamenti *http,* che siano in grado di fornire, a chi li legge e usa, un'informazione utile e una fonte lucrativa senza identificare i soggetti a cui appartengono.

L'interesse allo sfruttamento dei *big data* può assumere come è emerso la consistenza delle libertà economiche, ma può acquisire un rango costituzionale anche più elevato, quando si pone al servizio dei diritti inviolabili, dell'uguaglianza e della concorrenza[797].

---

[796] «*Raw*» *data* secondo T. Berners Lee; *données «brutes»* secondo Simon Chignard.

[797] M. F. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale* collettiva, in *Pol. Dir.*, 4/2016.

La *privacy* diviene la «non-price dimension of competition»[798], essa in quanto tale può essere danneggiata se alcune aziende dispongono di un potere di mercato troppo elevato.

Le autorità *antitrust* non dovrebbero concentrarsi esclusivamente sull'impatto sulla concorrenza nei casi in cui gli accordi concorrenziali influiscano anche sulla tutela dei consumatori, ma dovrebbero invece includere effetti non concorrenziali nel bilanciare i costi e benefici. Esse, al contrario dovrebbero intervenire quando le aziende raggiungono il potere monopolistico traendo in errore i consumatori sulle loro politiche di raccolta dei dati[799].

La regolazione in materia dovrebbe tenere conto della tutela della *privacy*, nella sua accezione concorrenziale, perché essa può essere danneggiata se alcune aziende dispongono di un potere di mercato troppo elevato e allo stesso tempo può farsi strumento di concorrenza incoraggiando i *competitors* a fornire migliori tutele alla *privacy* nella gestione dei dati raccolti.

Tutela della *privacy* e concorrenza[800] si intrecciano quando le aziende raccolgono grandi quantità di dati personali[801]. In altre parole, il rischio per la vita privata si fa più elevato quando il possesso di grandi quantità di dati personali dà alle società più potere di mercato.

---

798 Kennedy richiama i 4 argomenti del commissario federale del commercio Maureen Ohlhausen e dell'avvocato Alexander Okuliar: 1. La privacy è una dimensione non tariffaria della concorrenza che può essere danneggiata se alcune aziende dispongono di un potere di mercato troppo elevato; 2. Le autorità antitrust non dovrebbero concentrarsi esclusivamente sull'impatto sulla concorrenza nei casi in cui gli accordi concorrenziali influiscano anche sulla tutela dei consumatori, ma dovrebbero invece includere effetti non concorrenziali nel bilanciare i costi e benefici; 3. Le autorità antitrust dovrebbero intervenire quando le aziende raggiungono il potere monopolistico traendo in errore i consumatori sulle loro politiche di raccolta dei dati. Cfr. J. KENNEDY, *op.cit*, *ivi,* p. 4, cit

799 Cfr. J. KENNEDY*, op. cit.,* p. 4; M. K. OHLHAUSEN – A. P. OKULIAR, *Competition, Consumer Protection, and The Right [Approach] to Privacy*, in *Antitrust Law Journal* 80 (2015), pp. 134–36. In rejecting attempts to incorporate privacy concerns into antitrust policy, the authors point to three major problems: 1) Antitrust deals with harm to competition, not to privacy harms; 2) Antitrust is concerned with market-wide effects whereas privacy policy focuses on the individual relationship between the company and the consumer; and 3) Antitrust remedies are inadequate to handle privacy concerns because companies can accomplish the same outcome through private contracts rather than a merger.

800 J. KENNEDY, *op.cit*, p. 20, cit.: «*Google*'s decision to acquire DoubleClick in 2007 gave the FTC its first public opportunity to study the intersection of antitrust policy and privacy». Anche se la FTC ha riconosciuto che la riservatezza può essere una dimensione non competitiva della concorrenza, ha anche rilevato che le leggi antitrust non consentono di bloccare una fusione solo per proteggere la privacy.

801 M. E. STUCKE – A. P. GRUNES,, *Big Data and Competition Policy,* p. 4.

Le aziende con grandi quantità di dati personali possono esercitare il loro potere di mercato per impedire l'ingresso di concorrenti in grado di offrire maggiore protezione della *privacy*.

Pertanto, la politica della concorrenza dovrebbe svolgere un ruolo più attivo per incoraggiare la concorrenza anche sul fronte della riservatezza.

Allo stesso modo, anche quando il potere di mercato non si traduce in un aumento dei prezzi perché i servizi sono in gran parte forniti gratuitamente, i consumatori possono ancora essere danneggiati perché una mancanza di concorrenza ridurrà la pressione sulle imprese alla sana competizione per i clienti.

Pertanto, il fatto che i servizi siano gratuiti non implica che la concorrenza non sia in pericolo o che le Autorità di tutela della concorrenza non debbano intervenire.

Quanto più dati si possono raccogliere, più il prodotto sarà migliore, ma anche più potente sarà il proprietario dei dati verso concorrenti e consumatori. Non è solo un problema di concorrenza, ma anche di *privacy*, proprietà di dati e sicurezza[802].

Anche se i consumatori sono più lassisti nella condivisione delle loro informazioni *online*, i responsabili di quei servizi non possono realmente conoscere le loro preferenze, a meno che gli utenti non siano pienamente informati sui costi e sui benefici delle loro azioni e che il mercato offre un «insieme competitivo» corrispondente alle loro preferenze di *privacy*[803].

Se la scelta è o tutti i tuoi dati o nessun servizio, il consenso non è libero.

Non ha rilievo il fatto che i consumatori preferiscano servizi gratuiti a quelli a pagamento[804] perché se la posta in gioco di quelli gratuiti è data dalla compressione dei diritti fondamentali la semplice cessione, seppure volontaria, degli stessi dati è nulla[805].

«The consensus is that the current notice-and-consent regiment [sic] is inadequate to safeguard privacy. Individuals are generally unaware who has access to their personal

---

802 Così la Commissaria Vestager in L.CROFTS – R. MCLEOD, *MLex Interview: Margrethe Vestager*, in *MLex*, January 2015, 5, *http://mlexmarketinsight.com/wp-content/uploads/2015/01/mlex-interview-vestager-22-01-151.pdf.*

803 M. E. STUCKE – A. P. GRUNES, *ivi,* p. 10.

804 La riflessione è di J. Kennedy, nell'articolo citato a p. 15. «Consumers voluntarily share enormous amounts of information *online* , policymakers cannot really know their preferences unless consumers are fully informed about the costs and benefits of their actions and the market offers a "competitive array" of options to match their privacy preferences».

805 C. PERLINGIERI - L. RUGGIERI (a cura di), *op. cit., ibidem.*

information, what data is being used, how the data is being used, when the data is used, and the privacy implications of the data's use»[806].

L'approccio civilistico[807] che richiede al singolo di invocare la nullità del contratto sarebbe eccessivamente oneroso per il privato, che non avrebbe la forza economica dell'*Over the Top*, per intentare un'azione legale e si tradurrebbe nella perpetrazione di condotte violative da parte del soggetto più forte.

L'autonomia negoziale incontra i limiti posti dai diritti inviolabili, che sono assoluti, ovvero garantiti verso chiunque, verso lo Stato, i privati e ogni forma di collettività, sono indisponibili, non cedibili, non rinunciabili, non trasferibili e imprescrittibili[808].

A questo punto si dovrebbe pensare a un intervento del *policymaker*, a una norma cogente internazionale che imponga a questi soggetti di non chiedere i dati personali come prezzo per i servizi offerti perché i dati, «nuovo nucleo essenziale dei diritti fondamentali»[809], non sono negoziabili. La semplice indisponibilità non sarebbe, in altre parole, sufficiente a impedire il loro trasferimento.

La Corte Costituzionale con sentenza del 9 marzo 1989 n. 103 ricorda i limiti convenzionali e legali posti dalla Costituzione all'autonomia negoziale: «proprio in virtù del precetto costituzionale di cui all'art. 41 della Costituzione, il potere di iniziativa dell'imprenditore non può esprimersi in termini di pura discrezionalità o addirittura di arbitrio, ma deve essere sorretto da una causa coerente con i principi fondamentali dell'ordinamento, e in specie non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà e alla dignità umana».

Se consideriamo l'articolo 41 e in particolare la funzione sociale per esempio dei servizi offerti da *Google*, è comunque il legislatore il primo protagonista nella gestione discrezionale dello spazio che esiste tra autonomia privata e funzione sociale, gestione comunque vincolata ai valori costituzionali, al principio di ragionevolezza, congruità e proporzione[810]. I diritti fondamentali sono strumenti ineludibili per un corretto

---

806 M. E. STUCKE – A. P. GRUNES, *op. cit.,* pp. 326-327, cit.

807 C. PERLINGIERI - L. RUGGIERI (a cura di), *Internet e Diritto civile*, in *Lezioni della Scuola di specializzazione in diritto civile dell'Università di Camerino*, XXXVII, Napoli, 2015.

808 *Supra* nota su diritti inviolabili.

809 M. OREFICE, *I Big Data. Regole e concorrenza*, in *Politica del diritto,* 4/2016.

810 cfr. con sentenza Corte Costituzionale del 23 aprile 1965, n. 30, seppure su altro tema.

bilanciamento di valori da parte del legislatore e poi anche per l'interpretazione dei precetti normativi in materia di autonomia negoziale.

Le aziende più ricche di dati spesso beneficiano degli effetti di rete e di scala: può essere difficile per i concorrenti più piccoli competere con un grande *incumbent* anche se loro hanno prodotti migliori, inoltre, l'accumulo di grandi quantità di dati crea barriere all'ingresso favorendo la concentrazione del mercato, la dominanza e l'abuso[811].

Anche se il costo marginale di un servizio di un nuovo cliente può essere molto basso, il costo per accumulare i dati necessari per servire il primo cliente può essere proibitivo, soprattutto a fronte di una determinata resistenza da parte di un *incumbent*.

Le economie di scala riducono i costi unitari, consentendo di migliorare più rapidamente la qualità del servizio e spingendo i fornitori a privilegiare la massimizzazione dei ricavi futuri. Ad esempio, un'azienda potrebbe negare ai concorrenti l'accesso alla propria piattaforma, limitare i dati a loro disponibili o proibire ai *partner* di trattare con loro. I dati diventano una barriera all'ingresso di nuovi concorrenti. Questa posizione dominante può quindi essere usata per eliminare la concorrenza su criteri diversi di concorrenza come la dimensione non tariffaria della privacy, come argomentato in precedenza.

A ciò si aggiunga che le conoscenze fornite dai dati danno alle aziende la comprensione di quello che sta accadendo sul mercato.

Per ragioni analoghe, poiché le aziende ottengono il maggior accesso alle informazioni, potranno stabilire una posizione dominante perché avranno raggiunto economie di scala significative[812].

Sul lato della domanda, gli effetti di rete assicurano che il valore di ciascun utente aumenti quando gli utenti utilizzano lo stesso servizio[813]. Le economie di scala e gli effetti di rete aumentano il benessere dei consumatori riducendo i costi e aumentando il valore.

---

811 ID., *op. cit.*, p. 7.

812 S. POTARAZU, *Why Obama's Crack Down on Corporate Mergers Is the Right Prescription for US Health Care*, in *FoxNews Opinion*, April 16, 2016, *http://www.foxnews.com/opinion/2016/04/16/why-obamas-crack-down-on-corporate-mergers-is-right-prescription-for-us-health-care.html.*

813 Si pensi che grazie agli effetti di rete il valore di *Facebook* è aumentato drammaticamente quando i primi miliardi di utenti si sono uniti. Ovviamente esso sarebbe diminuito se la metà degli amici, per esempio, erano ancora su *MySpace*.

Non reggono gli argomenti sulla non rivalità e non escludibilità dei dati[814], secondo cui i dati nelle mani di *Google* non escludono che gli stessi possano essere raccolti da altri, perché la minaccia per la concorrenza non sta nel fatto che i dati che possiede *Google*, per esempio, impediscono a un altro operatore di sviluppare applicazioni per raccoglierne altri, ma nel fatto che *Google* ha una piattaforma con una serie di servizi integrati che «obbligano» tutti gli utenti a utilizzare i suoi servizi, resi migliori dai dati di cui si è già appropriato.

Le analisi tradizionali *antitrust* possono effettivamente spingere gli *incumbent* a condividere i dati? È sufficiente multare l'*incumbent*, che non avrà certo problemi di portafoglio o serve un ripensamento delle vecchie categorie giuridiche *antitrust*, che dia la giusta rilevanza al mercato dei dati.

Un'altra argomentazione riguardante l'inadeguatezza delle leggi sulla *privacy* per tutelare il benessere dei consumatori è che la raccolta di grandi quantità di dati consente ai venditori di praticare la discriminazione dei prezzi per *bundle*, applicando ai consumatori diversi prezzi diversi a seconda della probabilità di acquistare un prodotto[815].

Con le aziende che raccolgono informazioni dettagliate sulle attività *online* e *offline* di consumatori, spesso senza conoscenza e consenso dei consumatori, aumenta il rischio di pratiche abusive. I consumatori potrebbero pagare prezzi più elevati a causa di errori nella raccolta di informazioni o nelle deduzioni effettuate da specifici algoritmi. Una simile *behavioural advertising* basata sui dati può determinare uno sfruttamento comportamentale, e spingere i più vulnerabili a determinati comportamenti o comunque a discriminazioni.

Ne deriva una minore capacità di scelta di beni o servizi, prezzi più elevati e una qualità minore, nonché maggiori disuguaglianze tra ricchi e poveri[816].

---

814 J. KENNEDY, *op. cit.,* p. 7: «There are several reasons why the possession of lots of data by itself does not confer an unassailable competitive advantage. First, the use of data is non-rivalrous, meaning that one person's use of it does not diminish its availability to other users. The value to one ad network of knowing a user's age and location is not affected by whether another ad network also has that information. *Google*'s use of open data for navigation services does not prevent Citymapper from building a popular app that uses the same data».

815 N. NEWMAN, *The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google*, in *William Mitchell Law Review*, 40, no. 2 (2014), *http://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1568&context=wmlr.*

816 M. E. STUCKE – A. P. GRUNES, *ivi, op. cit.,* p. 55

Anche l'argomento[817] secondo cui la discriminazione dei prezzi potrebbe avere effetti positivi[818] perché imporrebbe pezzi più alti a chi sarebbe disposto a pagarli e li più bassi per i consumatori più riluttanti agli acquisti (i consumatori a basso reddito sarebbero più reattivi al prezzo)[819], dovrà essere respinto perché chi e come potrebbe verificare se le discriminazioni vanno nel senso dell'uguaglianza? Di certo non il profitto.

Anche la tesi secondo la quale una regolazione soffocherebbe il grande valore sociale creato dalla raccolta dall'analisi, dalla condivisione dei dati e l'innovazione, perché senza grandi quantità di dati la tecnologia di auto-guida di Tesla (che affronta una maggiore concorrenza da parte di Google, automobilisti rivali e altri), la capacità di *IBM Watson* di diagnosticare la malattia medica e le previsioni meteorologiche di *Weather Company* sarebbero impossibili, è fallace. Al contrario i dati condivisi moltiplicherebbero i benefici, il gioco della concorrenza perché non solo *Google* saprebbe cosa stai cercando prima di finire di digitare la parola, non solo *Facebook* ti collegherebbe agli amici persi né solo *Waze* calcolerebbe il percorso migliore per i conducenti.

Il danno da fusioni e abusi di imprese dominanti potrebbe essere significativo. Il danno non solo comporta tassi di pubblicità più elevati. Gli abusi di potenti imprese tecnologiche possono causare un maggiore pregiudizio nella perdita di scelta, innovazione, *privacy*, autonomia e libertà individuali e fiducia dei cittadini in un'economia di mercato[820].

Per assicurare efficacia all'*enforcement* del diritto *antitrust*, si potrebbe pensare a un obbligo di *facere*, in capo all'impresa, come nel caso di pratiche escludenti, o a un ordine atipico del tipo di quelli che di regola si accompagnano alle concentrazioni vietate[821], per il fatto che indeboliscono in maniera significativa la concorrenza, creando o rafforzando una posizione dominante: quando, cioè la Commissione o l'Autorità *antitrust* nazionale, in

---

817 MANNE - SPERRY, *The Problems and Perils of Bootstrapping Privacy and Data Into an Antitrust Framework*, *CPI Antitrust Chronicle*, May 29, 2015, p. 7, *https://www.competitionpolicyinternational.com/the-problems-and-perils-of-bootstrapping-privacy-and-data-into-an-antitrust-framework/*. «It is inconsistent with basic economic logic to suggest that a business relying on metrics would want to serve only those who can pay more by charging them a lower price, while charging those who cannot afford it a larger one».

818 J. KENNEDY, *op. cit.,* p. 17 ss.

819 The White House, Big Data and Differential Pricing (Washington, DC: The White House, February 2015), 17, *https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf.*

820 M. E. STUCKE – A. P. GRUNES, *op. cit.*, p. 9.

821 Per uno studio approfondito delle concentrazioni si rimanda ancora a F. GHEZZI - G. OLIVIERI, *op. cit.*, pp. 253 ss.

luogo di ordinare la deconcentrazione, la ammette a determinate condizioni. Si potrebbe subordinare, allora, l'autorizzazione a specifiche condizioni, ossia a impegni concreti dell'impresa volti a evitare che la concorrenza venga falsata. L'impresa si potrebbe impegnare, ad esempio, a cedere una parte della sua attività o a dare in licenza una determinata «tecnologia» ad un altro operatore (qui più che una tecnologia penseremmo proprio all'accesso ai dati). Se la Commissione o l'Autorità *antitrust* nazionale è convinta che gli impegni possano mantenere o ristabilire la concorrenza sul mercato, la autorizza, salvo verificare poi che l'impresa rispetti le condizioni concordate; in caso contrario, può prendere ulteriori provvedimenti.

E, in questo contesto sarebbe pensabile un rimedio che consista nell'obbligo di condividere i dati con i terzi concorrenti. Proprio in questa direzione sembra si stia muovendo la Commissione Europea, che nella bozza della recente Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle Regioni «Building an European Data Economy»[822] ha individuato un generale «principle of free movement of data within the eu», dal quale deriva un «new data producer's right», ossia un diritto di utilizzo dei dati cui corrisponde una concessione in licenza d'uso di quei dati. Con questa soluzione non si vuole svincolare il controllo dei dati dall'osservanza di ogni limite, piuttosto nel liberare i dati occorrerebbe in via preventiva già definire uno *standard* di *privacy* del titolare del dato da trasmettere, e prevedere che l'obbligo di condivisione comporti per il beneficiario quello di adeguarsi alla *privacy policy* dell'«ordinario collezionatore del dato». Insomma, con il trasferimento da un dante causa a un avente causa le regole di fondo, quanto alla protezione dei dati, andrebbero mantenute invariate perché il dato, come ogni altro oggetto, può diventare un bene liberamente circolabile a condizione che siano fatti salvi i diritti della persona cui il dato pertiene, a prescindere da chi ne sia l'attuale detentore.

Per la ragione prima illustrata la *privacy policy* dell'ordinario collezionatore di dati andrebbe standardizzata, scritta in modo chiaro, resa conoscibile all'utente, e infine,

---

[822] La bozza della *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* «Building a European Data Economy» è stata pubblicata il 2/12/2016 sul sito *www.oeuractiv.com*.

informato questi della possibile cessione dei dati a terzi in condizioni di equivalenza[823]. Sul versante della tutela del consumatore, i danni per il consumatore, derivanti dal monopolio di *Google* sono evidenti e sottili. Il danno più grande, unitamente alla profilazione incontrollata, è la crescente disuguaglianza economica, come già evidenziato, il *profiling* da parte di *Google* dei suoi utenti per gli inserzionisti, se da un lato viola la *privacy* dell'utente monitorato, dall'altro dà avvio a possibili e probabili discriminazioni di prezzo e commercializzazioni predatorie.

Google è responsabile della diffusione di informazioni non eque tra i consumatori e gli inserzionisti aziendali, e per l'effetto la sua politica produrrebbe disparità di trattamento tra consumatori, il che contribuisce a creare ulteriori disuguaglianze. L'asimmetria informativa nella raccolta dei dati sbilancia il controllo dell'informazione a favore di pochi *players* (i gestori dei dati), distorce il mercato a danno dei consumatori, che non conoscono i termini di negoziazione dei propri dati e dimostra che il mercato da solo non riuscirà a frenare gli abusi monopolistici, tantomeno avvantaggerà il consumatore.

Pertanto, i dati possono divenire uno strumento di dominio, se il loro utilizzo tramite i *device* fa risparmiare agli utenti del tempo, quello stesso tempo sarà speso in ore di lavoro in più necessarie per pagare assicurazioni salate[824]; per esempio: i dati, «condensato delle loro vite sociali»[825], in assenza di un intervento normativo chiaro diventano la moneta dei poveri che li condannerà all'esposizione costante. Dunque, la *privacy* rischia così di diventare un privilegio[826]. Non tutti possono permettersi di rinunciare ai riflettori pagando un costo più alto per una transazione o un servizio, considerato che ogni dato è creditizio.

E allora, premesso che le soluzioni sono molteplici, è necessario che il legislatore sovranazionale intervenga o con una norma speciale che riveda completamente il diritto *antitrust* e la tutela dell'utente, alla luce dei cambiamenti tecnologici oppure mediante un'interpretazione elastica ed estensiva di quanto già scritto dal legislatore dell'analogico.

---

[823] Si badi bene le condizioni di equivalenza differiscono dalle condizioni di adeguatezza, attualmente richieste per il trasferimento dei dati, ai sensi degli articoli 45 e 46 del Regolamento Europeo 2016/679.

[824] Sul «dare potere agli utenti» e sul c.d. Socialismo sbagliato della Silicon Valley si legga E. MOROZOV, *Silicon Valley: i signori del silicio*, Torino, Codice edizioni, 2016, p. 9 ss.

[825] ID., *op. cit.*, p. 16; parla di organi umani M.G. RADIN, *Market-inalienability*, in *Harv. Law. Rev.*, 100, 1987, p. 174.

[826] Parla di *privacy* costosa E. MOROZOV, *op. cit.*, 50.

Tanto premesso, ad avviso di chi scrive tre potrebbero essere gli ulteriori e possibili rimedi, rivolti a frenare il controllo di *Google* sui dati personali degli utenti: *i.* si potrebbero adottare sistemi «*Do not track*» utili a nascondere l'attività degli utenti agli inserzionisti, purché il sito ospitato dal *browser* abiliti l'anti-tracciabilità, senza aggirare il divieto, cancellando dal solo terminale dell'utente la cronologia, e negando, per esempio l'accesso ai contenuti; *ii.* Una tecnica per correggere l'asimmetria informativa tra *Google* e i suoi utenti potrebbe essere quella di fornire maggiore trasparenza nel modo in cui *Google* monetizza i dati, come ad esempio mediante l'obbligo di pubblicazione di relazioni periodiche sul Costo per *click* e sul prezzo dei «pacchetti» degli utenti; *iii.* si potrebbe rendere effettivo un sistema di portabilità dei dati tra i servizi, che permetta di aumentare la concorrenza tra i prestatori di servizi e favorisca un mercato in cui gli utenti «*vote with their feet*»[827], cioè possano «dissentire», trattenendo tutti i loro dati. In particolare, in riferimento al punto *iii.* relativo alla portabilità dei dati è quantomeno utile il richiamo al diritto all'autodeterminazione informativa, proclamato dalla recente Dichiarazione dei diritti in Internet[828], la quale ben avrebbe potuto ispirare il legislatore sovranazionale[829].

Precisamente agli articoli 5 e 6, è riconosciuta la tutela dei dati personali nonché il diritto all'autodeterminazione informativa[830], che attribuisce all'utente il diritto di conoscere le modalità tecniche del trattamento dei propri dati e di accedere agli stessi,

---

827 N. NEWMAN, *op. cit.*, p. 67.

828 La Dichiarazione dei Diritti in Internet è stata approvata dalla Commissione per i diritti e i doveri relativi a Internet e pubblicata il 28 luglio 2015, in http:// www.camera.it/leg17/1179. Durante l'Internet Governance Forum 2015, inaugurato il 9 novembre a João Pessoa, cui l'autrice del saggio ha preso parte attiva, la Carta, «*The Italian Proposal for an Internet Bill of Rights*», è stata presentata e illustrata a istituzioni, *stakeholders* e società civile provenienti da tutto il mondo, e ha ottenuto il plauso dell'intera comunità internazionale.

829 Il 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 riconosce, nell'articolo 20, un diritto alla portabilità (*right to data portability*) che consente una più agevole trasmissione dei dati personali da un prestatore di servizi, ad esempio una rete sociale, ad un altro, tuttavia il Regolamento sembrerebbe mostrare diversi punti di debolezza: si pensi al sistema di trasferibilità del dato a un Paese terzo che richiede da parte dello Stato a cui i dati vengono trasferiti misure di sicurezza «adeguate» e non «equivalenti». Si richiama a questo punto l'art. 5, comma 4 della Dichiarazione dei diritti in Internet che stabilisce invece che «i dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa».

830 Con riferimento all'articolo 6, la De Minico ha ripetutamente sostenuto l'importanza del riconoscimento del diritto all'autodeterminazione informativa che ha guidato la stesura dell'articolo. Si leggano, a tal fine, i relativi Resoconti in part. n. 5, pp. 14-15, e n. 9. pp. 37-38.

modificarli, cancellarli, limitarne la raccolta e la conservazione al tempo necessario, al rispetto dei principi di finalità e di proporzionalità.

Allo scopo di consentire agli utenti di passare facilmente *online* da un servizio a un altro portando con sé tutti i dati (*e-mail*, video, audio, *social networking*, dati sanitari) è necessario definire almeno un prototipo di possibile sistema di portabilità dei dati.

Recependo quanto fin qui esposto, si potrebbe pensare a un'unica carta elettronica virtuale standardizzata, come quella che ha ispirato il progetto «cie» del Governo e da poco attuato[831], ma rispetto a quest'ultima integrata e implementata, che utilizzi un supporto fisico (per ragioni di sicurezza), riconoscibile da qualsiasi dispositivo elettronico mediante sistemi *contact less* o appositi adattatori, e su cui siano registrati tutti i dati dell'utente, da quelli sanitari a quelli di *social networking*. Tale *card* dovrebbe dare la possibilità all'utente, quando la utilizza, di spuntare i dati con cui intende accedere alla piattaforma. Per esempio, se l'utente intende prenotare una visita medica, spunterà la sola casella dei dati sanitari, sceglierà in questo modo cosa condividere e con chi.

Ma a tal fine è necessario che *Google*, i Governi e gli altri *Ott* diano agli utenti i dati che appartengono loro, in modo che possano utilizzarli, integrarli e incrociarli e così favorire l'esercizio di diritti fondamentali più robusti, come la Rete comanda.

In conclusione, torna più pressante la domanda di partenza: se sia necessario disciplinare i nuovi fenomeni *expressis verbis* affinché essi siano eterodiretti al *common good*, per scongiurare il presumibile rischio che i poteri economici forti occupino tutto lo spazio di manovra e di autogestione che desiderano, al solo fine di incrementare a dismisura il loro portafogli, in danno del principio di eguaglianza e avendo in spregio le libertà e i diritti dei singoli.

Una regolazione *well tailored* è richiesta per rendere agevolmente circolabili e accessibili, in un traffico interstatale i *dati*, al fine di creare un mercato unico dei *big data*, a vantaggio di tutti. La Strategia *Digital Single Market* (COM 2015-192) non potrà esaurirsi in una regolazione *ad hoc*, definita da ciascun Stato Membro con il rischio di un feudalesimo normativo e del reiterarsi – come già accaduto per il Regolamento UE 2015/2120, recante

[831] L'acronimo sta per carta d'identità elettronica. Il decreto del Ministro dell'Interno, è stato pubblicato in Gazzetta ufficiale il 30 dicembre 2015, in concerto con i ministeri della pa e dell'Economia, ha sbloccato dopo 20 anni l'iter della CIE.

misure riguardanti l'accesso a un'Internet aperta e che modifica la Direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica - dell'invito al legislatore statale a regolamentare in dettaglio il fenomeno in assenza di una disciplina sufficientemente compiuta a livello europeo.

L'Unione dovrebbe farsi carico dell'onere di disegnare una regolazione convergente che funga da *standard* minimo imposto, stante l'insufficienza, la parzialità e la contraddittorietà del Regolamento *Privacy*.

Un *DSM* implica anche la creazione e lo sviluppo contestuale di un *Data Single Market*. Una regolazione comune sufficientemente dettagliata per superare anche le "opache trasparenze italiane" e con pochi spazi alla discrezionalità normativa degli Stati membri? La misura di coesistenza che tenga insieme il *DSM* con le esigenze imposte dal binomio riservatezza-sicurezza, anche alla luce delle nuove disposizioni del *General Data Protection Regulation* sono date dalla nuova dimensione competitiva della *privacy*.

Lo scopo ultimo del legislatore internazionale sarà quello di elaborare una soluzione normativa calzante ai nuovi fenomeni tecnologici, ma, allo stesso tempo, rispondente alle esigenze commerciali delle industrie e ai bisogni sociali dei cittadini.

Su questa linea, andrebbe messo a punto un apparato di norme che tenga insieme il fine lucrativo e l'interesse dei cittadini alla tutela della *privacy* e della sicurezza, con lo scopo di mantenere integro il patto sociale. In questo modo, mediante l'agevole utilizzo dei dati, facilitato dal *single data market,* si rende più efficiente la gestione dei servizi offerti sul mercato digitale e allo stesso tempo viene soddisfatta la domanda di sicurezza dei cittadini e raggiunta una effettiva ed efficace tutela della *privacy* degli utenti della Rete. Ne derivano benefici sia per i singoli che per le imprese: si avvantaggiano da una parte gli utenti, utilizzatori di apparecchi intelligenti, i quali risulterebbero conformi alla piena protezione della sfera personale dei singoli, e l'industria che può avviare strategie remunerative più oculate e adattare, per esempio, i propri codici di condotta agli *standard* europei e alle convenzioni internazionali.

Dunque, ne consegue l'opportunità dell'adozione di un approccio globale non trascuri l'inadeguatezza della disciplina *antitrust* rispetto alla *new economy* e per questo riduca i vincoli nazionali specifici e cioè tutte quelle specificità e tutte quelle misure nazionali che

aumentano i costi, le complessità e gli ostacoli per gli sviluppatori che devono interfacciarsi con una pluralità di *framework* regolamentari.

Bibliografia

AA VV, E-government*, Profili teorici ed applicazioni pratiche del governo digitale*, in SARZANA F., DI IPPOLITO S. (a cura di), La Tribuna, Piacenza, 2003.

AA.VV., Dati sensibili e soggetti pubblici. Commento sistematico al D. lgs. n. 135/99*, Giuffrè, Milano, 2000.*

AA.VV., *Introduzione al tema*, in *L'amministrazione pubblica tra riservatezza e trasparenza,* Atti del XXXV Convegno di Studi di Scienza dell'Amministrazione - Varenna 1989, Milano, 1991.

AA.VV., *Società dell'informazione. Tutela della riservatezza*, Atti del congresso di Stresa, 16-17 maggio 1997, Giuffrè, Milano, 1998.

ABBAMONTE G., *La funzione amministrativa tra riservatezza e trasparenza. Introduzione sul tema,* in AA. VV., Atti del XXXV Convegno di studi di scienze dell'amministrazione, Milano, 1989.

ACCIAI R. (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice,* Maggioli, Rimini, 2004.

ACCIAI R., Le nuove norme in materia di *privacy*, decreto legislativo 28 dicembre 2001 n. 467, autorizzazioni generali al trattamento dei dati sensibili, codici deontologici, regole per i flussi di dati fuori dall'Unione europea, *Maggioli, Rimini, 2003.*

AGRIFOGLIO S., La trasparenza dell'azione amministrativa e il principio del contraddittorio: tra procedimento e processo, *in* Dir. proc. amm.*, 1991.*

AKRICH M., *The De-scription of Technical Objects*, *in* BIJKER W. E. - LAW J., *Shaping Technology/Building Society Studies in Sociotechnical Change,* MIT Press, Cambridge, 1992.

ALLEGRETTI U., L'amministrazione dall'attuazione costituzionale alla democrazia partecipativa, *Giuffré, Milano, 2009.*

ALPA G., *La disciplina dei dati personali, note esegetiche sulla legge 31 dicembre 1996 n. 675 e successive modifiche*, Seam, Roma, 1998.

ALPA G., *La normativa sui dati personali. Modelli di lettura e problemi esegetici,* in CUFFARO V. - RICCIUTO V. - ZENO-ZENCOVICH V. (a cura di), *Trattamento dei dati e tutela della persona,* Giuffrè*,* Milano, 1998.

AMORETTI F. - MUSELLA F., Policy *e* politics *del governo elettronico. L'esperienza europea,* in *Rivista Italiana di Politiche Pubbliche,* n. 3/2012.

ANDERSON J. - RAINIE L., *Main Report: An In-depth Look at Expert Responses,* in *Astrid,* 14 maggio 2014.

ARENA G. - CORTESE F. (a cura di), *Per governare insieme: il federalismo come metodo. Verso nuove forme della democrazia*, Cedam, Padova, 2011.

ARENA G. (a cura di), *La funzione di comunicazione nelle pubbliche amministrazioni*, Maggioli, Rimini, 2004.

ID., *Dalla trasparenza alla comunicazione nell'arco del decennio*, in *Riv. It. Di comunicazione pubblica,* Milano, n. 5, 2000.

ID.., E-government *e nuovi modelli di amministrazione*, in *Studi in onore di Gianni Ferrara*, Torino, 2006.

ID., *Trasparenza amministrativa e democrazia*, in BERTI G. - DE MARTIN G., *Gli istituti della democrazia amministrativa*, Giuffrè, Milano, 1996.

ID., *Trasparenza amministrativa*, in S. CASSESE (a cura di)*, Dizionario di diritto pubblico*, Milano, 2006, 5945 ss.

ARNÒ G., *La tutela della privacy nella rete internet,* Giappichelli, Torino, 2002.

ARRUABARRENA B., *Datavisualisation: des données à la connaissance*, in *I2D – Information, données & documents*, 2015/2, Vol. 52.

AURAY N. - VETEL B., *L'exploration comme modalité d'ouverture attentionnelle*, *Réseaux,* vol. 6, n. 182, 2013.

BACHIMONT B. *ET AL.*, *Enjeux et technologies: des données au sens*, in *Documentaliste-Sciences de l'Information*, 2011/4, Vol. 48.

BALDASSARRE A., *Diritto della persona e valori costituzionali*, Giappichelli, Torino, 1997.

ID., *Privacy e Costituzione. L'esperienza statunitense,* Bulzoni, Roma, 1974.

BANNISTER F. - CONNOLLY R., *The Trouble with Transparency: A Critical Review of Openness in e-Government,* in *Policy & Internet,*vol. 3, iss. 1, article 8, 2011, in *http://www.astrid-online.it/E-governme/Studi-e-ri/Bannister_Connolly_Policy-Internet_1_2011.pdf*.

BASILICA F., *"E-government": un'occasione per creare un nuovo modello di amministrazione*, in *Funzione pubblica*, fasc. 3, 2002.

BASSINI M. - POLLICINO O. (a cura di), *Verso un Internet Bill of Rights*, Aracne, Roma, 2015.

BASSINI M. - POLLICINO O., *Verso un Internet bill of rights*, Roma, Aracne, 2015.

BATINI C., *Un'introduzione ai servizi di e-Government,* in *Amministrare: rassegna internazionale di pubblica amministrazione*, 2013.

BAUDOT P.Y. *ET AL.*, *Encore une révolution informatique? Open et big data dans les organisations administratives*, in *Informations sociales*, 2015/5 (n. 191).

BAUME S. - D. J CARON. –COMEAU P.A., *Le principe de transparence en Suisse et dans le monde*, in M. PASQUIER (a cura di) Lausanne: Presses polytechniques et universitaires romandes, 2013.

BEANEY W. M., *The constitutional right to privacy in the Supreme Court*, in *Sup. Ct. Rev.*, 212, 1962.

BELLANGER P., *Les données personnelles : une question de souveraineté*, in *Le Débat* 2015/1 (n. 183), pp. 14-25.

BELLI L., *De la gouvernance à la régulation de l'Internet*, Editions Berger Levrault, 2016.

BENYAYER L.D. - CHIGNARD S., *Focus - Les enjeux économiques de l'ouverture des données : pas de marché, pas de valeur* , in *Informations sociales* 2015/5 (n. 191).

BERGUIG M. - COUPEZ F., *Faut-il réellement craindre l'Open data pour la protection de nos données personnelles?*, in *LEGICOM*, 2016/1 (n. 56).

BERNERS-LEE T., *Tim Berners Lee e il Web prossimo venturo*, in *www.ted.com*, marzo 2009.

BERTAILS A. *ET AL.*, *Le Web sémantique*, in *Annales des Mines – Réalités industrielles*,

2010/4 (Novembre 2010).

BEVIER L. R., *What privacy is not,* in *12 Harv. J. L. & Pub. Pol'y 99*, 1989.

BIANCA C. M., *Tutela della privacy. Note introduttive,* in *Nuove leggi civili commentate,* fascicoli 2-3, 1999.

BILOTTA F., *L'emersione del diritto alla privacy*, in Clemente A. (a cura di)*, Privacy*, Cedam, Padova, 1999.

BIN M., *Privacy e trattamento dei dati personali: entriamo in Europa* in *Contratto e impresa Europa*, 1997.

BIRKINSHAW P. J., '*Freedom of Information and Openness: Fundamental Human Rights*', in *Administrative Law Review*, 58(1).

ID., *Government and Information: The Law Relating to Access, Disclosure and their Regulation,* 3rd edn. Haywards Heath: Tottel. Birkinshaw, 2005.

BOLOGNINI L. - FULCO D. - PAGANINI P. (a cura di), *Next privacy: il futuro dei nostri dati nell'era digitale*, Etas, Collana Economia, 2010.

BOMBARDELLI M., *Fra sospetto e partecipazione: la duplice declinazione del principio di trasparenza,* in *Istituzioni del federalismo*, 3/4.2013.

BOUHADANA I. – GILLES W. – NGUYEN-DUY I., *Parliaments in the open government era*, Imodev Les èditions, Paris, 2016.

BOURCIER D. (a cura di), *Open Data et Big Data, Nouveaux défis pour la vie privée*, Mare et Martin, Parigi, 2016.

ID., *Tele-communs versus tele-services publics : vers des services publics collaboratifs en ligne*, in *Revue française d'aministration publique*, (n. 146), 2013.

BOWKER G. C. - BAKER K. - MILLERAND F. - RIBES D., *Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment*, *in* HUNSINGER J. - KLASTRUP L. - ALLEN M., *International Handbook of Internet Research,* Springer, Pays-Bas, 2010.

BRANDEIS L. - WARREN S., *The right to privacy,* in *Harward Law Review,* 4, 1890.

BRAUNSCHWEIG K. - EBERIUS J. - THIELE M. - LEHNER W., *The State of Open Data Limits of Current Open Data Platforms*, Technische Universität Dresden, Faculty of Computer Science, Dresden, Germany.

BRUGUIERE J.M., *Les données publiques et le droit.* Paris: Litec., 2002.

BUSIA G., voce *Riservatezza (diritto alla),* in *Digesto delle discipline pubblicistiche,* in *Digesto delle discipline pubblicistiche,* 2000.

BUTTARELLI G., *Banche dati e tutela della riservatezza,* Giuffrè, Milano, 1997.

CAILLOL H., *Ouverture des données de santé : l'expérience de l'Assurance maladie*, in *Informations sociales* 2015/5 (n. 191).

CALÌ D., *Dall'Amministrazione digitale all'Amministrazione 2.0,* in *Astrid,* 2008.

CAMMAROTA G., *L'erogazione on line di servizi pubblici burocratici*, in *Informatica e diritto, Studi e ricerche*, n. 2/2002.

CAMMAROTA G., *La nozione giuridica di servizio pubblico in rete. Note a margine dell'art.63 del Codice dell'amministrazione digitale*, in *Diritto amministrativo elettronico*, Quaderni DAE, Rivista di Diritto Amministrativo Elettronico, 2005.

CAMPILONGO D., *Privacy informatica: il regime degli esoneri e delle semplificazioni introdotte dal D. Lgs. N. 255 del 1997 di attuazione della L. delega n. 676/1996 sulla protezione dei dati personali*, in Fisco.

CANNADA BARTOLI E., *A proposito di tutela della riservatezza e trasparenza amministrativa*, in *Dir. proc. amm.*, 1999.

CARAVITA B., (a cura di), *I percorsi del federalismo*, in *federalismi.it*, Milano, 2004.

ID., *La Costituzione dopo la riforma del titolo V. Stato, regioni e autonomie fra Repubblica e Unione Europea*, Torino, 2000.

CARAVITA DI TORITTO B. (a cura di), *Una pagina web dedicata all'e-government*, in *Federalismi.it*, 11-06-2008.

CAREY P., *Data protection: a practical guide to U.K. and EU law,* Oxford University press, Oxford, 2004.

ID., *E-privacy and online data protection,* Butterworths, London, 2002.

CASSETTI L., *La democrazia locale e la rete: l'esperienza in Europa*, in *federalismi.it.*

CASTELLS M., *Information Tecnology, Globalization, Social Development*, Relazione per la UNRISD Discussion Paper No. 114, September, 1999.

ID., *La nascita della società in rete*, Università Bocconi, Milano, 2002.

CASTETS-RENARD C. - GANDON N., *Open data des données de la recherche publique: entre réformes législatives et retour d'expérience sur un guide pratique à destination des chercheurs*, in *LEGICOM*, 2016/1 (n. 56).

CASTETS-RENARD C., *Brève analyse du règlement général relatif à la protection des données personnelles*, in *Dalloz IP/IT*, 2016.

CATAUDELLA A., *Riservatezza (diritto alla),* I) *Diritto civile,* in *Enciclopedia giuridica,* XXVII, Roma, 1991.

CATE F.H. - MAYER-SCHÖNBERGER V., *Notice and Consent in a World of Big Data, in International Data Privacy Law*, 3, 2, 2012.

CERRI A., *Riservatezza (diritto alla),* III) *Diritto costituzionale,* in *Enciclopedia giuridica Treccani,* XXVII (aggiornamento), Roma, 1995.

CERRILLO I MARTINEZ A., *Fundamental interests and open data for re-use*, in 20 *Int'l J.L. & Info. Tech.*, 203, 2012.

CHEVALLIER J., *Le mythe de la transparence administrative,* in *CURAPP*, *Information et transparence administratives*, Paris: PUF, 1988.

ID., *Audition du 9 janvier. In C. Bouchoux, Refonder le droit à l'information publique à l'heure du numérique : un enjeu citoyen, une opportunité stratégique (Rapport*) (Vol. II, p. 7-13), Paris: Sénat, tratto da *http://www.senat.fr/rap/r13-589-2/r13-589-21.pdf*.

ID., *Le droit administratif entre science administrative et droit constitutionnel*, in J. CHEVALLIER - G. J. GUGLIELMI - D. LOCHAK & CURAPP (a cura di), *Le droit administratif en mutation*, Paris: PUF, 1993.

ID., *La transformation de la relation administrative : mythe ou réalité ? (à propos de la loi du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations)*, Recueil Dalloz (38), 2000.

ID., *Les pratiques administratives. Transparence et secret. Colloque pour le XXVe anniversaire de la loi du 17 juillet sur l'accès aux documents administratifs*, Paris: La Documentation française, 2003.

CHIEPPA R., *La trasparenza come regola della pubblica amministrazione*, in *Dir. econ.,* 1994.

CHIGNARD S., *Open data, comprendre l'ouverture des données publiques*, Fyp éditions, 2012.

CHITI M.P. - PALMA G. (a cura di), *I principi generali dell'azione amministrativa*, Napoli, 2006.

CIANCIO A. –DEMURO G. –DE MINICO G. - DONATI F. – VILLONE M. (a cura di), *Nuovi mezzi di comunicazione e identità: omologazione o diversità?,* Aracne, Roma, 2012.

CIFARELLI R., *La trasparenza amministrativa dalla legge n. 241/1990 all'accesso civico: spunti di riflessione,* in *Astrid*Rassegna, n. 16/2014.

CIMINO J. P., *Internet e la pubblica amministrazione: le infrastrutture e i processi*, in *Accademia.edu.it,* 11 maggio 2011.

CIMMINO L., *Dalla formazione del diritto alla privacy, alla libertà informatica*, in CIRILLO G. P. (a cura di), *Il codice sulla protezione dei dati personali*, Cedam, 2004.

CIRILLO G.P., *Il codice sulla protezione dei dati personali,* Giuffrè, Milano, 2004.

CLEMENTE A. (a cura di), *Privacy,* Cedam, Padova, 1999.

CLEMENT-FONTAINE M., *La régulation de l'Open data,* in *LEGICOM,* 2016/1, (n. 56).

CLUZEL-MÉTAYER L., *Les limites de l'open data*, in *AJDA,* 2016.COCOZZA A., *La riforma delle pubbliche amministrazioni: quale ruolo per la dirigenza?,* in COLOMBO F., *Il cittadino conta troppo poco con Internet conterà di più*, in *Teléma*, n. 19, burocrazia elettronica, società più civile, *www.baldo.fub.it/teléma*.

COHEN J. E., *What privacy is for*, in *126 Harv. L. Rev.*, 2012-13.

COHN B. L., *Data Governance: A Quality Imperative in the Era of Big Data, Open Data, and Beyond*, in 10 ISJLP, 811, 2014-2015.

COLLET-THIREAU K.. - THOMAS J.P., *Big Data et Open Data : quel impact pour les professionnels de l'information ?*, in *I2D – Information, données & documents*, 2015/4 (Volume 53).

COMANDÈ G., *Banche di dati giuridici e privacy*, in F. Di Ciompo (a cura di), Atti del Convegno *Il diritto del cittadino all'informazione giuridica*", CED della Corte di Cassazione, Roma,25 settembre 2000, *http://www.giustizia.it/cassazione/convegni/s25092000.htm.*

COMANDÈ G. - PASCUCCI G., *Diritto e informatica*, Giuffrè, Milano, 2002.

COMANDINI V. V., *Google e i mercati dei servizi di ricerca su Inernet*, in *Mercato concorrenza e regole*, a. XV, n.3.

CORASANTI G, *Codice per l'informatica. Internet, informatica nelle pubbliche amministrazioni, commercio elettronico, firma digitale, tutela del software, privacy*, Giuffrè, 2001.

CORSI M. - GULLO E. - GUMINA A., *L'impatto delle tecnologie dell'informazione sul settore delle amministrazioni pubbliche*, in *Economia Italiana*, n. 2/2002.

COSTANZO P. - DE MINICO G. - ZACCARIA R., *I «tre codici» della Società dell'informazione. Amministrazione digitale. Comunicazioni elettroniche Contenuti audiovisivi*, Torino, 2007.

COSTANZO P., *La democrazia elettronica (note minime sulla cd. E-democracy)*, in *Il diritto dell'informazione e dell'informatica*, Torino, 2003.

ID., *Le nuove forme di comunicazione in rete: Internet*, in *www.interlex.it*, 1997.

ID., *Profili costituzionali di Internet*, in TOSI E. (a cura di), *Diritto di Internet e di e-business*, Milano, 2003.

ID., *Nuove tecnologie e "forma" dell'amministrazione*, in COSTANZO P. – DE MINICO G. – ZACCARIA R. (a cura di), *I tre codici della società dell'informazione*, Torino, Giappichelli, 2007.

COTTIN S., *Les «données grises» des administrations publiques,* in *I2D – Information, données & documents*, 2015/1 (Volume 52).

COURMONT A., *Open data et recomposition du gouvernement urbain de la donnée comme instrument à la donnée comme enjeu politique*, in *Informations sociales*, 2015/5 (n. 191).

CUFFARO V. - RICCIUTO V. (a cura di), *La disciplina del trattamento dei dati personali,* Giappichelli, Torino, 1997.

CYTERMANN L., *Promesses et risques de l'open et du big data : les réponses du droit* , in *Informations sociales*, 2015/5 (n. 191).

DALBIN S. *ET AL.*, *Approches documentaires: priorité aux contenus*, in *Documentaliste-Sciences de l'Information*, 2011/4 (Vol. 48).

DARY M. – BENAISSA L.*, Privacy by Design : un principe de protection séduisant mais complexe à mettre en œuvre*, in *Dalloz IP/IT*, 2016.

DE CUPIS A., *Riservatezza e segreto (diritto a)*, in *Novissimo Digesto Italiano* XVI, Torino, 1969.

DE GIACOMO C., *Diritto, libertà e privacy nel mondo della comunicazione globale. Il contributo della teoria generale del diritto allo studio della normativa sulla tutela dei dati personali*, Giuffrè, Milano, 1999.

DE MINICO G., *Regole. Comando e consenso*, Giappichelli, Torino, 2005.

ID. (a cura di), *Dalla tecnologia ai diritti. Banda larga e servizi a rete,* Jovene, Napoli, 2010.

ID., *New European regulation on universal service and next generation networks of just a lifting of the old one?*, in *Computer and Telecommunications Law Review,* 2011.

ID., *Internet. Regola e anarchia*, Jovene, Napoli, 2012.

ID., *Uguaglianze e accesso a Internet*, in *Forum di Quaderni costituzionali*, 6 marzo 2013.

ID., *Gli* open data: *una politica "costituzionalmente necessaria?*, in www.forumcostituzionale.it, 12 giugno 2014.

ID., *Internet and fundamental rights in time of terrorism*, in *Rivista AIC* 4/2015, 6 novembre 2015.

ID., *Towards an Internet Bill of Rights*, in *Loyola of Los Angeles International and Comparative Law Review*, Vol. 37, No. 1, 2015.

ID., *Antiche libertà e nuova frontiera digitale*, Giappichelli, Torino, 2016.

ID., *Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016.

DE SIERVO U., *La nuova legislazione sulla tutela della riservatezza,* in *Orientamenti sociali,* 1997.

DE TULLIO M.F., *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, in *Politica del diritto,* 4/2016.

DEBET A. – MASSOT J. – METTALINOS N., *Informatique et libertés : la protection des données personnelles en droit français*, Lextenso, 2015.

DEBRAS B., *Focus - L'engagement de la branche Famille dans la démarche d'open data. S'inscrire dans un mouvement national et européen*, in *Informations sociales*, 2015/5 (n. 191).

DELL'AVERSANA F., *Le libertà economiche in Internet: competition, net neutrality e copyright*, Aracne, Roma, 2014.

DESFRICHES DORIA O., *Quels dispositifs numériques pour appréhender la datavisualisation?*, in *I2D – Information, données & documents*, 2015/2 (Volume 52).

DESROSIERES A., *La politique des grands nombres. Histoire de la raison statistique*, Paris, La Découverte, 1993.

DIDIER B. - PIAZZA P., *Les conséquences humaines de l'échange transnational des données individuelles*, in *Cultures & Conflits*, 76, 2009.

DIDIER E., *En quoi consiste l'Amérique ? Les statistiques, le New Deal et la démocratie*, Paris, La Découverte, 2009.

DONATI F., *I nuovi mezzi di comunicazione e la tutela dei principi costituzionali*, in CIANCIO A. - DE MINICO G. - DEMURO G. - DONATI F. - VILLONE M. (a cura di) *Nuovi mezzi di comunicazione e identità*, Aracne, Roma, 2013.

DONATI F., *Identità digitale e tutela dei diritti*, in POLLICINO O. - LUBELLO V. - BASSINI M. (a cura di), *Identità ed eredità digitali*, Aracne, Roma, 2016.

DOVE E. S., *Reflections on the concept of open data*, in *12 SCRIPTed*, 154, 2015.

DREXL J., *Economic efficiency versus democracy: on the potential role of competition policy in regulating digital markets in times of posttruth politics*, in *Max Planck Institute for Innovation and Competition Research*, Paper No. 16-16.

DUBREUIL C.A., *La démocratie et la transparence*, in *RFDA*, 2016.

DUNI G., *Teleamministrazione*, in *Enciclopedia Giuridica*, Vol. XXX, Roma, 1993.

ID., *Amministrazione digitale*, in *Enc. dir.*, Annali, Milano, 2007.

EDWARDS P. - JACKSON S. - BOWKER G. C. - WILLIAMS R., *Introduction: An Agenda for Infrastructure Studies*, in *Journal of the Association for Information Systems,* vol. 10, n. 5, 2009.

EDWARDS P., *A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming*, Cambridge, MIT Press, 2010.

ELLI G.- ZALLONE R., *Il nuovo codice della privacy (commento al decreto al d.lgs. 30 giugno 2003, n. 196) con la giurisprudenza del Garante),* Giappichelli, Torino, 2004.

EYNARD J., Les Données personnelles : quelle définition pour un régime de protection efficace ?, Editions Michalon, 2013.

FARO S., voce Trattamento dei dati personali e tutela della persona, in Digesto delle discipline pubblicistiche, Utet, Torino, 2000.

FILISTRUCCHI L., *A SSNIP test for two-sided markets: the case of Media*, in *Social Science Research Network*, 2008, in http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287442.

FINOCCHIARO G., *Una prima lettura della legge 31 dicembre 1996, n. 675 "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"*, in *Contratto e Impresa*, 1, 1997.

ID., *Diritto all'anonimato*, in FINOCCHIARO G. - DELFINI F. (a cura di), *Diritto dell'informatica*, Torino, 2014.

FIORETTI M., *Open data, Open Society, a research project about openness of public data in EU local administration,* Laboratory of Economics and Management of Scuola Superiore Sant'Anna, Pisa, 2010.

FISCHER P. E., *Will Privacy Law in the 21st Century be American, European or International?,* GRIN Verlag, Munich, 2012.

FLEETWOOD BARTEE A., *Privacy rights: cases lost and causes won before the Supreme Court*, 2006.

FLICHY P. - PARASIE S., *Présentation*, in *Réseaux*, 2013/2 (n. 178-179).

FOIS S., *Questioni sull'andamento costituzionale del diritto alla "identità personale"*, in ALPA G. - BESSONE M. - BONESCHI M. - CAIAZZA P. (a cura di), *L'informazione e i diritti della persona,* Jovene, Napoli, 1983.

FOREST D., *Droit des données personnelles,* Gualino éditeur, Paris, 2011.

FRANCESCHELLI U., *La tutela della privacy informatica: problemi e prospettive*, Giuffrè, Milano, 1998.

FRENOT S. - GRUMBACH S., *Des données à l'intermédiation, une révolution économique et politique*, *in* CALDERAN L. - LAURENT P. - LOWINGER H. - MILLET J. (dir.), *Big Data: nouvelles partitions de l'information,* Louvain-la-Neuve, De Boeck, coll. Information et stratégie, 2015.

FREUND P. A., *The Supreme Court of the United States: Its Business, Purposes and Performance*. Gloucester, MA: Peter Smith. 1972.

FROSINI T. E., *Banche dati, telematica e diritti della persona,* Cedam, Padova, 1981.

ID., *Tecnologie e libertà costituzionali*, in *Dir. Informatica*, 2003, 03, 487.

ID., *Tecnologie e libertà costituzionali*, in, *Il diritto dell'informazione e dell'informatica*, Torino, 2003.

ID., *Liberté Egalité Internet*, Editoriale Scientifica, Napoli, 2015.

FROSIO G., *Guida al Codice della Pubblica Amministrazione Digitale. La digitalizzazione della P.A. alla luce del D.lgs. 7 marzo 2005*, n. 82, Napoli, 2005.

GALETTA D. U., *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in *Rivista Italiana di Diritto Pubblico Comunitario*, fasc.5, 2016.

GARDINI G., *Le regole dell'informazione*, Giappichelli, Torino, 2014.

GHEORGHE-BADESCU I., *Le nouveau règlement général sur la protection des données, Quoi de neuf?*, in *Revue de l'Union européenne*, 2016.

GIACOBBE G., *Riservatezza (diritto alla),* in *Enciclopedia del diritto,* XL, Milano, 1989.

ID., *Il diritto alla riservatezza: da diritto di elaborazione giurisprudenziale a diritto codificato*, in *Iustitia*, 2, 1999.

GIANNANTONIO E., LOSANO G., ZENO-ZENCOVICH V., (a cura di), *La tutela dei dati personali. Commentario alla legge n. 675/96,* seconda edizione, Cedam, Padova, 1999.

GIANNINI M.S., *Atto amministrativo*, in *Enc. dir.,* IV, 1959, 178.

GITELMAN L. (dir.), *Raw Data Is an Oxymoron,* MIT Press, Cambridge, 2013.

GOËTA S., *Un air de famille : les trajectoires parallèles de l'open data et du big data*, in *Informations sociales*, 2015/5 (n. 191).

GRELLEY P., *Contrepoint - L'organisation de la statistique publique en France*, in *Informations* sociales, 2015/5 (n. 191).

GRIFFI F. P. *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza,* in *Federalismi.it,* 16 aprile 2013.

GRUTTEMEIER H. – HAMEAU T., *Accès aux données scientifiques et contraintes juridiques – une question d'équilibre*, in *I2D – Information, données & documents*, 2016/2 (Volume 53).

GUGLIELMI G., *Numérisation des données publiques et données publiques numériques*, in TEYSSIE B., *La communication numérique, un droit, des droits*. Paris: Editions Panthéon-Assas, 2013.

GURIN J., *Big Data and Open Data: How Open Will the Future Be?*, in 10 ISJLP 691 2014-2015.

GUTWIRTH S. - LEENES R. - DE HERT P., *Data protection on the move: current developments in ICT and privacy, data protection*, Springer, 2016.

HALPERT B., *Auditing cloud computing: a security and privacy guide,* Wiley, Hoboken, 2011.

HEALD D., *Pourquoi la transparence des dépenses publiques est-elle si difficile à atteindre?*, in *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78).

HELFTER C., *Contrepoint - La fétichisation du chiffre*, in *Informations sociales*, 2015/5 (n. 191).

HILDEBRANDT M., *Profiling and rule of law,* in *Vrije Universiteit Brussel*, Pleinlaan 2, B-1050 Brussel, Belgium, 1 marzo 2008.

HOLVAST J. (a cura di), *The global encyclopaedia of data protection regulations,* Kluwer Law International, London-Boston, 1999.

IRION K., *Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records*, in International Journal of Law and Information Technology, 2015, 23.

ITEANU O., *Quand le digital défie l'Etat de droit*, Eyrolles, 2016.

IZZO S., *Segretezza dei documenti e diritto comunitario*, in *Diritto Comunitario e scienza internazionale*, 2, 1997.

JAULT-SESEKE F. – ZOLYNSKI C., *Le règlement 2016/679/UE relatif aux données personnelles Aspects de droit international privé*, in *Recueil Dalloz*, 2016.

JUANALS B. - MINEL J.L., *Les stratégies institutionnelles des musées dans le web de données ouvert: la construction d'un espace muséal partagé en question*, in *Études de communication*, 46/2016.

JUTAND F., *Ouverture des données de transport. Paris: Ministère de l'écologie, du développement durable et de l'énergie*, in

http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/154000182.pdf, 2015.

KAMARCK E. C., *Government Innovation around the world*, Ash Institute for Democratic Governance and Innovation John F. Kennedy School of Government Harvard University, novembre 2003.

KENNEDY J., *The myth of data monopoly: why antitrust concerns about data are overblown*, in *Information Technology & Innovation Foundation*, march 2017.

KENNEDY J., *The myth of data monopoly: why antitrust concerns about data are overblown*, in *Information Technology & Innovation Foundation*, march 2017.

KENNEDY J., *The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown*, in *Information technology & innovation foundation*, march 2017.

KRANENBORG H. E VOERMANS W., *Access to Information in the European Union. A Compara tive Analysis of EC and Member State Legislation*, Groningen, 2006.

LAINEE F., *Responsable des données, un métier qui a le vent en poupe*, in *I2D – Information, données & documents*, 2015/1 (Volume 52).

LALLET A., *Documents administratifs: accès et réutilisation*, in *Répertoire de contentieux administratif*, Paris: Dalloz, 2009.

LASCHENA R. - PAJNO A., *Trasparenza e riservatezza nel processo amministrativo*, in *Dir. proc. amm.*, 1990.

LATTANZI R., *Dati sensibili: una categoria problematica nell'orizzonte europeo*, in *Europa e diritto privato*, 1998.

LESSING L., *Code and other laws of cyberspace,* Basic Books, New York, 1999.

LEVMORE S. - NUSSBAUM M. C., *The offensive Internet: speech, privacy, and reputation,* Harvard University Press, 2010.

LEYOUDEC L., *Reconstruire les conditions d'intelligibilité du document numérique patrimonial : mobilisations documentaire et sémiotique des Linked Open Data*, in *Les Enjeux de l'information et de la* communication, 2015/2 (n. 16/2).

LISI A., *La privacy in internet,* Esselibri Simone, Napoli, 2003.

LOCCHI G., *Il principio di trasparenza in Europa nei suoi risvolti in termini di Governance amministrativa e di comunicazione istituzionale dell'Unione,* in *Rivista elettronica di diritto pubblico,*

di diritto dell'economia e di scienza dell'amministrazione a cura del centro di ricerca sulle Amministrazioni pubbliche "Vittorio Bachelet", 2011.

LOIODICE A. - SANTANIELLO G., *La tutela della riservatezza,* Cedam, Padova, 2000.

LUCHETTA G.*, Google opera in un mercato a due versanti?*, in *Mercato concorrenza regole*, n.1, 2013.

LUNDQVIST B. - FORSBERG Y. - DE VRIES M. - MAGGIOLINO M., *Open data and competition law: some issues regarding access and pricing of raw data,* 9 *Masaryk U. J.L. & Tech.* 95, 2015.

LUNDQVIST B. - FORSBERG Y. - DE VRIES M. - MAGGIOLINO M., *Open data and competition law: some issues regarding access and pricing of raw data,* 9 *Masaryk U. J.L. & Tech.* 95, 2015.

MABI C., *La plate-forme « data.gouv.fr » ou l'open data à la française*, in *Informations sociales*, 2015/5 (n. 191).

MADDEN M. – GILMAN M. – LEVY K., MARWICK A., *Privacy, poverty and big data: a matrix of vulnerabilities for poor americans*, in *Washington University Law Review*, March 9, 2017.

MAIELLO R. *ET AL.*, *Droit de l'information*, in *Documentaliste-Sciences de l'Information*, 2014/2 (Vol. 51).

MANCOSU G., *Trasparenza amministrativa e open data: un binomio in fase di rodaggio*, in *Federalismi,* 17, 11 settembre 2012.

ID., *La transparence administrative en Italie face au défi de l'open data*, in *Federalismi.it*, 2013.

ID., *La transparence publique à l'ère de l'Open Data. Étude comparée Italie-France*, Université Panthéon-Assas (Paris 2), 2016.

MANENTI R., *La privacy: il rapporto tra CAD e D.Lgs n.196/2003*, in *Diritto amministrativo elettronico*, Quaderni DAE, Rivista di Diritto Amministrativo Elettronico, 2005.

MANGANARO F., *L'evoluzione del principio di trasparenza amministrativa,* in *Studi in memoria di Roberto Marrama*, Napoli, 2012.

MANSON S., *La mise à disposition de leurs données publiques par les collectivités territoriales,* in *AJDA*, 2016.

MARCHAND J., *Réflexions sur le principe de transparence. Revue du droit public et de la science politique en France et à l'Étranger*(3), 2014.

MARRAMA R., *La pubblica amministrazione tra trasparenza e riservatezza nell'organizzazione e nel procedimento amministrativo*, in *Dir. proc. amm.*, 1989.

ID., *La pubblica amministrazione tra trasparenza e riservatezza nell'organizzazione e nel procedimento amministrativo*, in C. S. COMO, *L'amministrazione pubblica tra riservatezza e trasparenza. Atti del XXXV Convegno di studi di scienza dell'amministrazione, Varenna, 21-23 settembre 1989*, 1991, Milano: Giuffré.

MASUCCI A., *Erogazione on line dei servizi pubblici e tele-procedure amministrative*, in *Diritto Pubblico,* n. 3/2003.

MATHER T., KUMARASWAMY S., LATIF S., *Cloud security and privacy,* O'Reilly Media, 2009.

MATTIONI A., *Informazione e riservatezza tra Convenzione Europea e Costituzione italiana*, in *Riv. int. dir. Dell'uomo,* n. 2/1990.

MATTIUZZO M., *Business models and big data: how google uses your personal information*, in https://itsrio.org/wp-content/uploads/2017/03/Marcela-Mattiuzzo-V-REVISADO.pdf.

MAYER SCONBERGER V. - CUKIER K. N., *Big Data. Una rivoluzione che trasformerà il modo di vivere e già minaccia la nostra libertà,* Garzanti, Milano, 2013.

MEIER A., *Edemocracy & egovernment: stage of a democratic Knowledge society,* New York, Springer, 2012.

MEIJER A. - RODRIGUEZ BOLIVAR M.P., *La gouvernance des villes intelligentes. Analyse de la littérature sur la gouvernance urbaine intelligente*, in *Revue Internationale des Sciences Administratives*, 2016/2 (Vol. 82).

MEIJER A. J. *ET AL.*, *La gouvernance ouverte: relier visibilité et moyens d'expression*, in *Revue Internationale des Sciences Administratives* 2012/1 (Vol. 78).

MELCHIONNA S., *La nuova privacy: semplificazioni senza rinunciare a regole e garanzie (D. lgs. 467/2001),* in *www.privacy.it, sezione saggi,* Roma, 23 gennaio 2002.

MERLONI F. - ARENA G.- CORSO G. - GARDINI G. - MARZUOLI C. (a cura di), *La trasparenza amministrativa*, Giuffré, Milano, 2008.

MERLONI F. (a cura di), *L'informazione delle pubbliche amministrazioni*, Maggioli, Rimini, 2002.

ID., *Introduzione all'e-government. Pubbliche amministrazioni e società dell'informazione*, Giappichelli, Torino, 2005.

ID., *Trasparenza delle istituzioni e principio democratico*, in MERLONI F- ARENA G.(a cura di), *La trasparenza amnministrativa*, Giuffré, Milano, 2008.

MESSINETTI D., voce *Personalità (diritti della)*, in *Enciclopedia del Diritto*, XXXIII, Giuffré, Milano, 1983.

MINAZZI F., *Il principio dell'open data by default nel codice dell'amministrazione digitale: profili interpretativi e questioni metodologiche,* in *Federalismi.it*, n. 23/2013, 20 novembre 2013.

MINICHIELLO F., *L'intérêt croissant pour l'ouverture des données publiques: des initiatives en éducation*, in *Revue internationale d'éducation de Sèvres*, 62, aprile 2013.

MONDUCCI J., *Diritti della persona e trattamento dei dati particolari,* Giuffrè, Milano, 2003.

MORELATO E., *Anonimato e protezione dei dati personali*, in FINOCCHIARO G. (a cura di) *Diritto all'anonimato*, Cedam, Padova, 2008.

MUCIO C., *Il diritto alla riservatezza nella pubblica amministrazione: dati sensibili, dati personali e diritto di accesso,* Ipsoa, Milano, 2003.

MUSIANI F., *Internet et vie privée en 40 pages*, Uppr Editions, 2016.

NAEGELEN P., *Vers un domaine public des données?*, in *I2D – Information, données & documents*, 2015/4 (Volume 53).

NEWMAN N., *The Cost of Lost Privacy: Search, Antitrust and the Economics of the Control of User Data*, in *SSRN: http://ssrn.com/abstract=2265026*, May 14, 2013.

NICOSIA F. M., *Principio di trasparenza dell'azione amministrativa ed obbligo di motivazione. Il diritto di accesso*, Napoli, 1992.

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

NOTARMUZI C., *DigitPA: la terza riorganizzazione dell'informatica pubblica,* commento al decreto legislativo 1 dicembre 2009, n. 177, in *Giornale di diritto amministrativo,* 2009.

NOUCHER M. – GAUTREAU P., *Le libre accès rebat-il les cartes? Nouvelles perspectives pour les données géographiques*, in *Les Cahiers du numérique*, 2013/1, (Vol. 9).

NOVA A., *La tutela del diritto alla riservatezza nel trattamento dei dati personali*, in *Aggiornamenti sociali,* 4, 1998.

NOVECK B. S., *Is Open Data the Death of FOIA?*, in *The Yale Law Journal FORUM*, November 21, 2016.

OLLION É., *L'abondance et ses revers. Big data, open data et recherches sur les questions sociales*, in *Informations* sociales, 2015/5 (n. 191).

OREFICE M., *Gli open data tra principio e azione: lo stato di avanzamento,* in *www.forumcostituzionale.it*, 25 maggio 2015.

OREFICE M., *I Big Data. Regole e concorrenza*, in *Politica del diritto*, 4/2016.

OSNAGHI A. - MESCHIA F. - PIANCIAMORE M., *La gestione dell'identità digitale,* in *Astrid*, 22 marzo 2011.

PACE A. - ZACCARIA R.- DE MINICO G. (a cura di), *Mezzi di comunicazione e riservatezza: ordinamento comunitario e ordinamento interno*, Napoli, Jovene, 2008.

PAGLIARULO G., *Il Codice sulla privacy: commento al D. lgs. 30 giugno 2003 n. 196*, Prime note Arial, Livorno, 2003.

PAJNO A., *Il principio di trasparenza alla luce delle norme anticorruzione*, in Astrid Rassegna, 2013, 17.

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* Giuffrè, Milano, 2003.

PATRONI GRIFFI F., *La trasparenza della Pubblica Amministrazione tra accessibilità totale e riservatezza*, in *www.federalismi.it*, 2013, 2.

PERIN M., *Il processo di digitalizzazione delle amministrazioni pubbliche*, in *Giustizia Amministrativa*, Rivista di Diritto Pubblico, n. 2-2003.

PIETRANGELO M., *Il diritto all'uso delle tecnologie nei rapporti con la pubblica amministrazione: luci ed ombre*, in *Diritto amministrativo elettronico*, Quaderni DAE, *Rivista di Diritto Amministrativo Elettronico*, 2005.

PIZZETTI F., *I diritti di libertà nel mondo della comunicazione globale,* in *Astrid,* 16 giugno 2014.

PLANTIN J.C. - VALENTIN J., *Données ouvertes et cartographie libre. Autour du cas de Montpellier*, in *Les Cahiers du numérique*, 2013/1 (Vol. 9).

POLLICINO O. - LUBELLO V. - BASSINI M. (a cura di), *Identità ed eredità digitali*, Aracne, Roma, 2016.

POLLICINO O. - ROMEO G., *The Internet and Constitutional Law. The protection of fundamental rights and constitutional adjudication in Europe*, Routledge, London, 2016.

PONTI B. (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33,* Rimini, 2013.

POZEN D., *Freedom of Information Beyond the Freedom of Information Act*, in *Columbia Public Law*, Research Paper No. 14-541 February 1, 2017.

RAGONE M., *L'open data: dal decreto "sviluppo" alla legge "anticorruzione", passando per il "crescita 2.0"*, in *IGED*, n. 4/12. *Rivista di diritto pubblico e scienze politiche*, 1997.

RIDEAU J., *La transparence dans l'Union européenne. Mythe ou principe juridique?* Paris: LGDJ, 1999.

ROCHÉ É., *Open data et business models*, in *LEGICOM*, 2016/1, (n. 56).

RODOTÀ S., Privacy *e costruzione della sfera privata. Ipotesi e prospettive*, in *Politica del diritto*, XXII, 1991.

ID., *Tecnologie e diritti,* Il Mulino, Bologna, 1995.

ID., *Controllo e riservatezza a garanzia della privacy ma senza i "lacci" della Burocrazia*, in *Guida al Diritto*, 1997.

ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 4, 1997.

ID., *Democrazia non solo telematica per una vera cittadinanza attiva*, in *Teléma*, n. 19, 1999.

ID., *Repertorio di fine secolo (la costruzione della sfera privata),* Laterza, Bari, 1999.

ID., *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione,* Editori Laterza, 2004.

ROMAN C., *Open data*, *ConLawNOW* 19, 2016.

ROMANO A. - L. MARASSO - MARINAZZO M., *Italia chiama e-government: molta tecnologia, poca innovazione, ancora troppa distanza dal cittadino*, Milano, Guerini, 2008.

RUBINO A., *E-government: reti, organizzazione e servizi*, in DE MINICO G., (a cura di) *Dalla tecnologia ai diritti. Banda Larga e Servizi a rete,* Napoli, Jovene, 2010.

SALAIS R., *La donnée n'est pas un donné. Pour une analyse critique de l'évaluation chiffrée de la performance*, in *Revue française d'administration publique*, 2010/3 (n. 135).

SALOMON D., *Data Privacy and Security,* Springer, 2003.

SANDULLI M. A. Il *d.l. 24 giugno 2014 n. 90 e i suoi effetti sulla giustizia amministrativa. Osservazioni a primissima lettura,* in *Federalismi.it,* 27 giugno 2014.

SANTANIELLO G., *La semplificazione delle regole nel Codice della privacy,* in *www.interlex.it,* sezione protezione dati personali, 19 gennaio 2004.

SARTOR G. - MONDUCCI J., *Il Codice in materia di protezione dei dati personali. Commentario sistematico al D. lgs. 30 giugno 2003 n. 196,* Cedam, Padova, 2004.

SAVINO M., *The Right to Open Public Administrations in Europe: Emerging Legal Standards,* Paris, Ocse-Sigma, 2010, in *http://www.oecd-ilibrary.org/fr/governance/sigma-papers20786 581*.

SELVADURAI N., *Not just a face in the crowd: addressing the intrusive potential of the online application of face recognition technologies*, in *International Journal of Law and Information Technology*, 2015, 23.

SEMENZATO S., *Internet come servizio pubblico*, in *www.interlex.it*, 1998.

SHIH RAY KU R., *Privacy is the problem,* in *19 Widener L.J. 873,* 2009-10.

SORRENTINO M., *Regolazione organizzativa e e-government, in Organizzazione, regolazione e competitività*, MERCURIO R. (a cura di), McGraw-Hill, Milano, 2006.

STUCKE M. E. – GRUNES A. P., *Big Data and Competition Policy*, New York: Oxford University Press, 2016.

STUCKE M. E. – GRUNES A. P., *Debunking the Myths Over Big Data and* Antitrust, in *CPI Antitrust Chronicle*, May 2015.

TALUKDER A., *Big Data Open Standards and Benchmarking To Foster Innovation*, in *10 ISJLP*, 799, 2014-2015.

TAMBOU O., *Protection des données personnelles: les difficultés de la mise en oeuvre du droit européen au déréférencement*, in *RTD Eur.*, 2016.

TANDA P., voce *Trasparenza* (*principio di*), in AA.VV., *Digesto delle discipline pubblicistiche*, Torino: UTET, 2008.

TASSO C. - OMERO P., *La personalizzazione dei contenuti web: e-commerce. i-access, e-government,* 2002.

TENE O. –POLONETSKY J., *Big Data for All: Privacy and User Control in the Age of Analytics*, in *Nw. J. Tech. & Intell. Prop.*, vol 11, n. 5, 2013.

TERESI L., *Exploitation des données publiques: le renouveau?*, in *LEGICOM*, 2011/2 (n. 47).

THEVENOT L., *Les investissements de forme,* in THEVENOT L. (dir.), *Conventions économiques*, Paris, Presses universitaires de France (Puf), 1986.

THIREAU K.C. - THOMAS J.P., *Big Data et Open Data: quel impact pour les professionnels de l'information?*, in *I2D – Information, données &* documents, 2015/4 (Volume 53).

TOLBERT C. J. - MOSSBERGER K., *The Effects of E-Government on Trust and Confidence in Government*, in *Public Administration Review*, May-June 2006.

TORRES L. – PINA V. - SONIA R., *E-government and the transformation of public administrations in EU countries: Beyond NPM or just a second wave of reforms?* in *Online Information Review*, vol. 29, n. 5, 2005.

TOSI E., *Il codice della privacy. Tutela e sicurezza dei dati personali: normativa nazionale e comunitaria,* La Tribuna, Piacenza, 2004.

TRIMARCHI BANFI F., *In tema di trasparenza amministrativa e di diritto alla riservatezza*, in AA.VV., Studi in onore di E. Casetta, I, Napoli, 2001.

TUGENDHAT M. - CHRISTIE I., *The law of privacy and the media: second cumulative supplement,* Oxford, Main Work and Second Cumulative Supplement, 2006.

UBERTAZZI T. M., *Il diritto alla privacy: natura e funzione giuridica,* Cedam, Padova, 2004.

VAYRE J.S., *Les tableaux de bord sur données massives, pour un nouveau management de l'innovation?* , *Innovations* 2015/2 (n. 47).

VERDIER H. - BAUDOT P.Y., *Au-delà de l'ouverture des données, ce qui est en jeu, c'est l'ouverture de la décision*, in *Informations sociales*, 2015/5 (n. 191).

VESPERINI G. (a cura di), *L'e-government*, Milano, Giuffrè, 2004.

VIGEVANI G. E., *Anonimato, responsabilità e trasparenza nel quadro costituzionale italiano*, in *AIC*, aprile 2014.

VOSS W.G., *Le concept de données à caractère personnel : divergences transatlantiques Safe Harbor et Priv acy Shield*, in *Dalloz IP/IT*, 2016.

VULBEAU A., *Contrepoint - L'infobésité et les risques de la surinformation*, in *Informations sociales*, 2015/5 (n. 191).

WRIGHT D. - DE HERT P. (a cura di), *Privacy impact assessment,* Springer-Verlag, 2012.

WYBER S., *Care.data: une expérience d'économie politique des données de santé en Angleterre*, *Informations sociales*, 2015/5 (n. 191).

YU H.– ROBINSON D., *The New Ambiguity of "Open Government"*, in *Ucla Law Review Discourse*, 2012.

ZARSKY T. Z., *Transparent predictions,* in University Of Illinois Law Review (4), 27 agosto 2013.

ZAZA O., *Vers un Open data visuel: le portail Open Data Paris*, in *I2D – Information, données & documents*, 2015/2 (Volume 52).

ZENO ZENCOVICH V., *I diritti della personalità dopo la legge sulla tutela dei dati personali,* in *Studium Iuris,* 1997.

ZENO ZENCOVICH V., *Personalità (diritti della)*, in *Digesto delle Discipline Privatistiche - Sez. civile*, vol. XIII**,** Utet, Torino, 1995.

ZENO ZENCOVICH V., Privacy *e informazioni a contenuto economico nel decreto legislativo n. 196 del 2003*, in *Studium Iuris,* fasc. 4, 2004.

ZHELEVA E. - TERZI E. - GETOOR L., *Privacy in Social Networks,* in *morganclaypool.com,* 2012.

ZICCARDI G., *Informatica giuridica,* Giuffrè, Milano 2012.

ZOFFOLI L., *La nuova amministrazione digitale*, in *Astrid,* maggio 2013.

ZOLLER É., *Le principe de transparence et les nouvelles technologies de l'information aux États-Unis. Conférence-débat du CDPC sur la transparence administrative et ses déclinaisons technologiques récentes*, Cycle « Les valeurs du droit public», Parigi, 2013, in *http://www.u-paris2.fr/CDPC0/0/fiche___pagelibre/*.

ZOLYNSKI C., *La Privacy by Design appliquée aux Objets Connectés : vers une régulation efficiente du risque informationnel?*, *in Dallo*z *IP/IT*, 2016.

ZUCCHETTI A.*, Privacy: dati personali e sensibili, sicurezza, regolamento, sanzioni: problemi e casi pratici*, Giuffrè, Milano, 2005.

ZUIDERVEEN BORGESIUS F. - GRAY J. - VAN EECHOUD M.*, Open data, privacy, and fair information principles: towards a balancing framework*, in *30 Berkeley Tech. L.J.*, 2073, 2015.