A12

Vai al contenuto multimediale

Maria Orefice

I Big Data e gli effetti su privacy trasparenza e iniziativa economica

Aracne editrice

www.aracneeditrice.it
info@aracneeditrice.it

Gioacchino Onorati editore S.r.l. – unipersonale

www.gioacchinoonoratieditore.it
info@gioacchinoonoratieditore.it

via Vittorio Veneto, 20
00020 Canterano (RM)
(06) 45551463

ISBN 978-88-255-1655-5

I edizione: luglio 2018

A mamma e papà

Indice

Introduzione

Con il presente lavoro ci proponiamo di investigare in merito alla compatibilità del nuovo fenomeno dei *Big Data* con i diritti fondamentali.

Secondo la descrizione fornita dall'OCSE[1], per *Big Data* si intendono 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.

Qui analizzeremo le intersezioni di queste raccolte massive di dati con il valore costituzionale della trasparenza e con il diritto alla riservatezza, nonché 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 proposto è ancora poco conosciuto dalla dottrina pubblicistica italiana, ma a livello europeo - sia accademico che di Corti - è invece da tempo esplorato con attenzione, ne sia prova la multa comminata dalla Commissione Europea a *Google* il 27 giugno 2017 per abuso di posizione dominante sul mercato degli acquisti comparativi *online*[2] 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* 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.

[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.

[2] In http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740.

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.

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 adeguato alla loro *governance*, avanzeremo una serie di ipotesi sui formati e sulle politiche di apertura più adatte al paradigma della trasparenza.

A tale scopo guarderemo nell'ultimo capitolo, che chiude il cerchio dell'analisi, ricongiungendosi con il primo, alla risposta regolatoria proposta dalla Francia, nella cui capitale l'autrice ha svolto una parte della sua attività di ricerca, ripercorrendo le tappe legislative che hanno visto affermarsi una politica di apertura dei dati.

Si consideri che con l'affermazione delle nuove tecnologie, la concreta conversione della P.A. da soggetto autoritativo cartaceo a soggetto partecipativo digitale non produce solo effetti positivi in termini di riduzione dei costi, ma 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*.

Nel capitolo 1 ispezioneremo il terreno dei servizi che la Pubblica Amministrazione rende e potrebbe rendere attraverso Internet e dei diritti fondamentali che la pratica degli *e-services* e dell'*Internet of Things* intercetta, ponendo particolare attenzione al modello *openness*, presupposto non solo di un giudizio responsabile sull'operato dei go-

vernanti (e quindi del diritto di voto), ma anche di esercizio di altri diritti fondamentali.

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 automaticamente collegata all'installazione delle applicazioni sui dispositivi elettronici ed è condizione necessaria per la fruizione dei servizi offerti.

Tale trasferimento, in realtà, intaccherebbe la libertà degli individui perché il mercato non offre alternative agli utenti, i quali non hanno a disposizione un *carnet* di applicazioni con *privacy policy* differenti, ma il loro «consenso» viene coartato.

Le strategie commerciali *data driven*, infatti, 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 connotazione democratica di uno Stato.

Proprio per lo spiegarsi di nuovi fenomeni, delimitativi di inediti ambiti di tutela, ravvisiamo la necessità di indagare una definizione di *privacy* più calzante alla realtà interconnessa.

A tal fine, osserveremo 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* possano dirsi coperti dalla cd. «reasonable expec-

tation of privacy», elaborata dalla Corte Suprema USA 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 quindi rinunci all'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 scandalo "Cambridge Analytica", portato sotto i riflettori da alcuni articoli pubblicati su *The Observer*[3] e *The New York Times*[4], che hanno riferito sull'utilizzo di milioni di profili Facebook senza autorizzazione da parte della società di consulenza britannica - che ha guidato la campagna elettorale sulle piattaforme digitali di Trump - di una enorme quantità di dati prelevati da *Facebook*, ha messo in evidenza che gli utenti non intendono rinunciare alla loro aspettativa di *privacy* nemmeno sei i dati sono pubblicati in chiaro su un *social network*[5]. Ne è prova il movimento "#deletefa-

[3] I documenti sono consultabili in https://www.theguardian.com/news/series/cambridge-analytica-files.

[4] M. ROSENBERG, *Bolton Was Early Beneficiary of Cambridge Analytica's Facebook Data*, in *The New York Times*, 23 marzo 2018;

[5] Z. TUFEKCI, *Facebook's Surveillance Machine*, in *The New York Times*, March, 19, 2018; J. COBBE, *Reining in Big Data's Robber Barons*, April, 10, 2018, in http://www.nybooks.com/daily/2018/04/12/reining-in-big-datas-robber-barons/.

cebook"[6] generatosi dopo lo scandalo e dopo la notizia pubblicata sul *The Guardian*[7] relativa al fatto che *Facebook* era al corrente della violazione della sicurezza da circa due anni.

Lo studio prosegue con l'attento esame del contesto regolatorio europeo, precisamente con la specifica analisi delle modifiche introdotte dal nuovo Regolamento (GDPR) 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 se il Paese di destinazione 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 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*, falsando 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 rile-

[6] A. JENKINS, *These Companies Have Cut Their Ties With Facebook Amid the Cambridge Analytica Data Scandal*, in *Time.com*, March, 28, 2018.

[7] H. OSBORNE, *What is Cambridge Analytica? The firm at the centre of Facebook's data breach*, in *The Guardian*, March, 18, 2018.

vante, dal quale emergerebbe *ictu oculi* la condotta abusiva del dominante su una pluralità di servizi, apparentemente operanti su mercati diversi.

In dettaglio, 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 tanto più se consideriamo che un solo soggetto controlla *Facebook*, *Messenger, Whatsapp* e *Instagram*.

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.

Di conseguenza, un simile 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 «avrebbero acquisito 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 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* in Italia un'inversione di rotta nel perseguimento del risultato tra la diffusione indiscriminata dei dati personali (sotto forma di *Big Data*), i quali sfuggono, come ampiamente sarà esplicato nel prosieguo, dalle mani dei loro legittimi proprietari e la gelosa chiusura dei dati da parte delle

P.A., custode arcigna delle informazioni degli amministrati, veri generatori di dati, cui dovrebbero essere restituiti.

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

Da un esame così articolato e dal confronto con l'esperienza regolatoria francese si è evinto che il nuovo *habitat* delle libertà fondamentali invocherebbe un intervento normativo speciale che, attraverso un'interpretazione evolutiva delle Costituzioni nazionali e dalle Carte internazionali (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 e 42), recepisca i nuovi caratteri del mezzo, le nuove logiche di mercato e conseguentemente elabori nuovi paradigmi di *openness* e *competition* per consentire l'efficace tutela della trasparenza, della concorrenza e delle libertà, compresa la 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..

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 effettiva 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

1.1. 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*[1], per quest'ultima si intende la raccolta di dati, non necessariamente aperti, aggregati da soggetti indistintamente pubblici e privati[2].

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[3], la loro apertura rappresenterebbe, in altre parole, l'aspetto caratterizzante dell'*Open Government*[4]; per altri invece gli *Open Data* abbraccerebbero anche i dati generati, detenuti e pubblicati dai priva-

[1] 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.

[2] 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.

[3] *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.

[4] 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».

ti[5]. 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[6].

Nell'uno e nell'altro caso, per definire aperti i dati è necessario che posseggano alcuni requisiti: accessibili[7] attraverso la connessione a Internet, senza limitazioni collegate 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[8].

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*[9].

[5] 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..

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

[7] 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 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.

[8] 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).

[9] 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/

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[10].

In altre parole, l'apertura dei dati faciliterebbe l'esercizio dei diritti fondamentali e delle "vecchie" libertà trasferite nel nuovo *habitat* della Rete[11]:

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»[12] e diventerebbe strumento necessario per lo sviluppo economico, nonché amplificatore della partecipazione democratica alla *res pubblica*[13]. 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

3031518/Open_Source_Open_Access_ed_Open_Content_verso_sistemi_aperti_di_condivisione_della_conoscenza.

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

[11] 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 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.

[12] 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.

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

dettato costituzionale[14] e contribuisce alla creazione di un modello di «*see-through society*»[15].

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[16], in ossequio al dovere di trasparenza, *ex* artt. 1, 2, 21, 48, 97[17] 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 pubblica utilità in ragione del vincolo solidaristico»[18] 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*[19].

[14] 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.

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

[16] 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.

[17] 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.

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

[19] 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..