Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

Scienze giuridiche – PhD in Legal Studies

Ciclo XXX

Settore Concorsuale: 12/H3 – Filosofia del diritto

Settore Scientifico Disciplinare: IUS/20 – Filosofia del diritto

Curriculum: Diritto e nuove tecnologie

DATA SOCIETY.
GOVERNO DEI DATI E
TUTELA DEI DIRITTI NELL'ERA DIGITALE

Presentata da Fernanda Faini

Coordinatore Dottorato	**Supervisore**
Chiar.mo Prof. Andrea Morrone	Chiar.ma Prof.ssa Monica Palmirani

Esame finale anno 2018

INDICE

Data society. Governo dei dati e tutela dei diritti nell'era digitale

Abstract 6

Introduzione 8

Capitolo 1. *Digital society*. Governo aperto, cittadinanza digitale e nuovi diritti

1.1. Governare la *digital society* 13
1.2. L'amministrazione digitale e aperta: dall'*e-government* all'*open government* 23
1.2.1. Strategie in ambito internazionale ed europeo 29
1.2.2. Politiche di sviluppo e quadro normativo nazionale 32
1.3. La cittadinanza digitale e i diritti fondamentali nella rete 39
1.3.1. Le Carte costituzionali e le Carte dei diritti di Internet: il contesto internazionale e il caso italiano 45
1.3.2. I diritti digitali nella normativa nazionale vigente 63

Capitolo 2. La società della conoscenza. *Closed data* e trasparenza

2.1. La società della conoscenza 70
2.1.1. Caratteristiche, opportunità e rischi 70
2.1.2. Strumenti di conoscenza e forme di trasparenza (proattiva, reattiva, attiva) 78
2.2. *Closed data* e *disclosure* 81
2.3. L'evoluzione normativa del principio di trasparenza 83
2.3.1. Dalla legge 241/1990 al d.lgs. 33/2013 84
2.3.2. Trasparenza e *Freedom of Information Act* (FOIA) italiano: il d.lgs. 97/2016 nel quadro internazionale di riferimento 91
2.4. Principi e strumenti nella disciplina vigente 102

2.4.1. Il diritto alla conoscibilità, all'accessibilità e alla qualità dei dati 102
2.4.2. I diritti di accesso: documentale, civico semplice, civico generalizzato 107

Capitolo 3. La società dei dati e degli algoritmi. *Open data* e *big data*

3.1. *Open data*: principi e caratteristiche 120
3.1.1. La dimensione giuridica 125
3.1.2. La dimensione tecnica ed economica 133
3.2. Ecosistema *open data*: i profili sociali 137
3.3. I dati aperti nel quadro normativo vigente 142
3.4. Strategie e iniziative di *openness* 152
3.4.1. Iniziative a livello internazionale 152
3.4.2. Iniziative a livello nazionale e regionale 155
3.5. *Big data*: caratteristiche e aspetti tecnici 160
3.6. Finalità e valore dei *big data* 172
3.7. I profili relativi alla *digital economy*, i rischi e le implicazioni etico-sociali dei "grandi dati" 181
3.8. Le problematiche giuridiche poste dai *big data* 186
3.9. Iniziative e progetti a livello nazionale e internazionale 197

Capitolo 4. Tutela e bilanciamento dei diritti nel governo dei dati

4.1. Il diritto all'esistenza digitale e al governo dei dati 202
4.2. Il diritto alla conoscenza 207
4.3. Il diritto all'identità e il diritto all'oblio 213
4.3.1. Il diritto all'identità: identità personale e identità digitale 214
4.3.2. Il *right to be forgotten* 218
4.3.3. Bilanciamento tra diritti: *right to know*, identità, oblio 236
4.4. Il diritto d'autore nella *digital age* 241
4.4.1. La disciplina italiana del diritto d'autore online 243
4.4.2. Il contesto internazionale 257
4.4.3. La proprietà intellettuale nel governo dei dati 261
4.4.4. Diritto d'autore e *right to know*: alla ricerca dell'equilibrio 266

Capitolo 5. Protezione dei dati personali e *data governance*

5.1. Il diritto alla protezione dei dati personali nell'era digitale 273
5.1.1. Il fondamento del diritto e il sistema delle fonti 273
5.1.2. La disciplina di riferimento: il regolamento europeo 2016/679 e la normativa nazionale 286
5.2. La *data protection* nel governo dei dati 303
5.3. Privacy, trasparenza proattiva e apertura dei dati pubblici 308
5.3.1. *Data protection* e pubblicazione (obbligatoria e facoltativa) 308
5.3.2. I profili problematici del bilanciamento tra diritti: durata, indicizzazione e apertura (riutilizzo) 319
5.4. La protezione dei dati personali e la trasparenza reattiva realizzata con l'accesso civico generalizzato 334
5.5. Equilibri tra trasparenza, apertura e privacy 338
5.6. *Data protection* e *big data* 339

Capitolo 6. Dati, diritto e diritti: conclusioni e scenari futuri

6.1. La centralità della persona nel governo dei dati: una nuova etica digitale 356
6.2. Il cambiamento nell'articolazione del rapporto tra pubblico e privato 370
6.2.1. Pericoli di *closed government*, asimmetria, controllo e sorveglianza 370
6.2.2. Possibili rimedi: verso gli *open big data* e le tutele collettive dei diritti? 379
6.3. I nuovi equilibri tra diritti e la nuova fisionomia del diritto: suggestioni future 391

Bibliografia 405

Abstract

Data society. Governo dei dati e tutela dei diritti nell'era digitale

I dati formano il nostro "io" digitale e costituiscono il fondamento di ogni attività umana. Il governo della *data society* passa dal governo dei dati e il diritto, ontologicamente deputato a regolare la vita, è chiamato a disciplinare i volti assunti dai dati, dalle informazioni e dalla conoscenza nella contemporaneità e a tutelare i diritti che ne sono coinvolti.

In una realtà caratterizzata da amministrazioni aperte e cittadinanza digitale, il lavoro mira ad esaminare sotto la lente giuridica gli strumenti di conoscenza relativi alle diverse configurazioni dei dati, identificate nei *closed data* e nei relativi volti della trasparenza (proattiva e reattiva), negli *open data* e nei *big data*.

L'analisi degli strumenti di conoscenza permette di comprendere le questioni che si pongono al diritto: le connessioni intricate di dati rivelano connessioni intricate di diritti, da bilanciare con accuratezza al fine di tutelare la persona e, insieme a lei, la società democratica presente e futura. Il lavoro esamina la disciplina e le problematiche peculiari dei diritti maggiormente coinvolti nella *data governance*, in specifico *right to know*, identità, oblio, diritto d'autore e protezione dei dati personali, alla ricerca del bilanciamento tra gli stessi nelle diverse configurazioni assunte dai dati.

In conclusione il lavoro arriva a suggerire un bilanciamento tra diritti nel governo dei dati basato sulla centralità della persona, in particolare sulla dignità e sullo sviluppo della stessa, fondamenti sui quali convergono i diversi diritti oggetto di analisi. La tutela dei diritti può basarsi su un approccio preventivo e tecnologico *by default* e *by design* e sull'*accountability* dei soggetti, immaginando soluzioni capaci di innovare i paradigmi tradizionali e minimizzare i rischi di asimmetria, controllo e sorveglianza, come gli *open big data* e forme di tutela collettiva.

Un governo dei dati fondato su questa logica necessita del rinnovamento del diritto che passa da una costruzione di matrice globale e *multistakeholder* ed è guidato da un approccio etico, orientato verso la tutela dei diritti e lo sviluppo democratico.

Il ruolo del diritto e la forza dei diritti sono necessari al governo della *data society* e alla tutela della persona nell'era digitale: *ubi data society, ibi ius*.

******

Data society. Data governance and rights protection in the digital age

The data form our digital self and constitute the foundation of every human activity. The government of *data society* passes from data governance and the law, ontologically appointed to regulate life, is called upon to regulate the faces assumed by data, information and knowledge in contemporary society and to protect the rights that are involved.

In a reality characterized by open administrations and digital citizenship, this work aims to examine through the legal lens the tools of knowledge related to the different data configurations, identified in *closed data* and in the related faces of disclosure (proactive and reactive), in *open data* and in *big data*.

The analysis of the tools of knowledge makes it possible to understand the issues that arise in law: the intricate connections of data reveal intricate connections of rights, which must be accurately balanced in order to protect the individual and, together with it, the democratic society present and future. This work examines the discipline and the specific issues of the rights most involved in data governance, specifically right to know, identity, right to be forgotten, copyright and data protection, searching for the balance between these rights in the different data configurations.

In conclusion, the work suggests a balance between rights in data governance based on the central role of the individual, in particular on the dignity and the development of the individual himself, concepts on which the different rights under analysis converge. The protection of the rights can be based on a preventive and technological approach *by default* and *by design* and on the accountability of the subjects, imagining solutions capable of innovating the traditional paradigms and minimizing the risks of asymmetry, control and surveillance, such as *open big data* and forms of collective protection.

A data governance based on this logic requires the renewal of law through a global and multistakeholder construction that is guided by an ethical approach, oriented towards the protection of the rights and the democratic development.

The role of law and the force of rights are necessary for the governance of *data society* and for the protection of the individual in the digital age: *ubi data society, ibi ius*.

Introduzione

«Noi siamo le nostre informazioni»[1].

Nella società digitale il benessere e lo sviluppo umano hanno iniziato a dipendere in modo significativo dai servizi basati sui dati, dalla gestione del ciclo dell'informazione e dall'accesso al bene della conoscenza.

I dati formano il nostro "io" digitale e sui dati si basa ogni attività umana: i processi sono rappresentati da dati suscettibili di elaborazione e capaci di pervadere ogni aspetto dell'esistenza in modo ubiquo, integrandosi negli oggetti ed estendendo le capacità dell'uomo. I confini rassicuranti tra realtà digitale, cui accedere con il *login*, e realtà analogica, cui approdare con il *logout*, collassano nel concetto di realtà, i bit prendono il posto degli atomi, l'accesso ai dati e ai servizi scalza il paradigma della proprietà delle *res corporales*, si ridefiniscono sfera pubblica e privata, mutano le geometrie del potere in un mondo privo di frontiere e sovrani.

Nel presente lavoro la scelta è stata di definire la società contemporanea quale *data society*, una "società di dati", che non è soltanto fondata sui dati come nel suo avvento quale società dell'informazione e della conoscenza, ma ne è intimamente pervasa finendo per coinvolgere e plasmare l'uomo stesso come un *data subject*.

Alla luce della connotazione contemporanea della realtà, il governo della *data society* passa necessariamente dal governo dei dati e il diritto, deputato a regolare la vita, è chiamato a disciplinare il "diluvio di dati" che inonda l'esistenza contemporanea e a tutelare i diritti delle persone coinvolti dalle diverse declinazioni assunte dai dati, dalle informazioni e dalla conoscenza.

---

[1] «Il sé è concepito come un sistema informazionale complesso, costituito da attività, ricordi e storie in cui si esprime la nostra coscienza del sé. In questa prospettiva, noi siamo le nostre informazioni»: L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. it., Raffaello Cortina Editore, Milano, 2017, p. 78.

In specifico, il lavoro mira ad esaminare sotto la lente giuridica gli strumenti di conoscenza che attengono alle diverse configurazioni dei dati e i complessi bilanciamenti tra diritti diversi, che tali strumenti rendono necessari al fine di tutelare la persona e proteggere la società democratica presente e futura.

A tali fini, l'analisi relativa al governo dei dati si sofferma nel primo capitolo sui mutamenti indotti dalla rivoluzione digitale nella società, nelle istituzioni e nell'uomo.

Sotto la spinta della centralità dei dati, della circolazione delle informazioni e del valore della conoscenza, il rapporto tra governanti e governati diventa maggiormente orizzontale, connotandosi per l'emersione dei principi di trasparenza, partecipazione e collaborazione. Emergono, però, i rischi inversi di torsioni verso nuove asimmetrie di potere e inedite forme di controllo da parte dei "signori dei dati", costituiti non solo dai pubblici poteri, ma anche dai colossi del web, potenti controllori del pedaggio di accesso alla vita digitale.

Di conseguenza, la *data society* si connota, da un punto di vista soggettivo, per un profondo mutamento nella fisionomia e nel rapporto che lega i protagonisti del governo dei dati, da una parte amministrazioni digitali e aperte, ispirate a un modello di *open government*, e dall'altra la cittadinanza digitale, basata sulla nuova configurazione dei diritti e delle libertà resa possibile dalle tecnologie informatiche. Il primo capitolo è teso ad approfondire l'evoluzione che investe le amministrazioni digitali verso modelli di *open government*, che si affermano a livello internazionale e nazionale, e il parallelo mutamento che riguarda la cittadinanza digitale e i diritti fondamentali; a tal fine i diritti scaturenti dalla libertà informatica sono ricostruiti alla luce della Carta costituzionale, della Carta dei diritti in Internet e della normativa nazionale di riferimento, tenendo conto del contesto internazionale al riguardo.

La *data society*, da un punto di vista oggettivo, è caratterizzata da nuovi strumenti di conoscenza che attengono alle diverse configurazioni assunte dai dati, ossia *closed data* e trasparenza, *open data* e *big data*, oggetto di analisi nel secondo e nel terzo capitolo, che approfondiscono le caratteristiche principali, le problematiche e la disciplina giuridica che li connotano nell'ordinamento italiano, prestando attenzione anche al contesto europeo e internazionale di riferimento.

In specifico, nel secondo capitolo sono esaminati i *closed data* e i correlati volti della trasparenza, necessari per garantirne la *disclosure* e la relativa conoscenza da parte

della collettività: esaminata l'evoluzione normativa nel nostro ordinamento, l'analisi si concentra sulla trasparenza proattiva, che si realizza con la pubblicazione, e, in particolar modo, sulla trasparenza reattiva, in risposta alle istanze della collettività, che, a seguito della riforma recata dal d.lgs. 25 maggio 2016, n. 97, significativamente definito come il *Freedom of Information Act* italiano, prevede oggi accanto all'accesso documentale e all'accesso civico semplice lo strumento innovativo dell'accesso civico generalizzato, che dà forma e sostanza al *right to know* nei confronti delle istituzioni.

Sotto l'egida dell'*open government* e nell'affermarsi di nuovi modelli relazionali tra mondo pubblico e privato, la società dei dati si connota per il connubio tra *disclosure* e *openness* e la maturazione del concetto di trasparenza, che diventa "attiva" e si concreta nello strumento degli *open data* e nel diritto al riutilizzo. Gli *open data* sono trattati nel terzo capitolo nelle dimensioni caratterizzanti, nei profili sociali e negli aspetti giuridici, senza tralasciare le iniziative più significative a livello internazionale, nazionale e regionale.

La *data society* è dominata, anche, da un'altra configurazione di dati, i *big data*, caratterizzati dalla mole eterogenea di dati, dalla velocità degli algoritmi e dalla capacità di predizione, che costituiscono fenomeno peculiare del nostro tempo idoneo ad evolvere l'essenza stessa dei dati e dei loro utilizzi e a condurre a riflessioni inedite per l'uomo. I *big data* sono analizzati nel terzo capitolo: ne sono approfondite caratteristiche, finalità, implicazioni sociali e problematiche giuridiche, dando conto anche in tal caso di significative iniziative internazionali e nazionali al riguardo.

L'analisi degli strumenti di conoscenza del secondo e del terzo capitolo è necessaria al fine di comprendere le questioni che si pongono al diritto e i bilanciamenti da realizzare tra diritti.

Il governo dei dati, infatti, necessita del diritto e dei poteri pubblici, ontologicamente tenuti a proteggere i diritti della persona e responsabili di difficili equilibri nelle diverse configurazioni assunte dai dati nella contemporaneità. L'analisi del quarto e del quinto capitolo si concentra, di conseguenza, sulla tutela e sul bilanciamento dei diritti nel governo dei dati; l'analisi è attenta, in particolare, al rapporto che lega pubblici poteri e collettività, ma anche al mondo privato dei giganti della rete, in considerazione del ruolo dominante che rivestono nella *data governance* e nel bilanciamento tra diritti.

In considerazione della centralità dei dati, il diritto all'esistenza digitale, parte integrante e indistinguibile dell'esistenza *tout court*, metaforico ombrello sotto cui ospitare i diversi diritti scaturenti dalla libertà informatica, è anche diritto al governo dei dati, da intendersi proprio come tutela delle libertà e dei diritti nelle diverse fasi di gestione e nelle diverse conformazioni dei dati. Nella *data governance*, di conseguenza, garantire effettiva tutela alla persona significa affrontare complessi bilanciamenti tra diritti che si intrecciano e confliggono, mossi da tensioni diverse: il diritto alla conoscenza e il diritto ad essere correttamente o a non essere più conosciuti (il diritto all'identità e il diritto all'oblio); il diritto all'informazione e alla condivisione da una parte e il diritto d'autore e il riconoscimento della proprietà intellettuale dall'altra; il *right to know* e il diritto al riutilizzo da un lato e il diritto alla protezione dei dati personali dall'altro. Le connessioni intricate di dati sono anche connessioni intricate di diritti indivisibili e difficilmente gerarchizzabili, da bilanciare con accuratezza al fine di tutelare la persona e, insieme a lei, la stessa società di riferimento.

Il lavoro esamina la disciplina e le problematiche che connotano i diritti maggiormente coinvolti nel governo dei dati: nel capitolo quarto, oltre al diritto all'esistenza digitale, sono oggetto di analisi il diritto alla conoscenza, il diritto all'identità, il diritto all'oblio e il diritto d'autore, mentre il capitolo quinto è dedicato alla protezione dei dati personali nella *data governance*, con particolare attenzione all'approccio e agli strumenti previsti dal regolamento europeo 2016/679. In relazione a ogni diritto esaminato, oltre alla disciplina di riferimento e alle peculiari problematiche che si pongono nel governo dei dati, l'analisi affronta, in specifico, le diverse sfumature, intensità e gradazioni dei problemi da risolvere e degli equilibri da trovare nei diversi strumenti di conoscenza afferenti alle differenti conformazioni dei dati esaminate nei primi capitoli (trasparenza, *open data*, *big data*).

Il sesto capitolo è dedicato alle conclusioni e agli scenari futuri in merito a dati, diritto e diritti. In particolare, l'analisi svolta in merito ai diritti maggiormente coinvolti nel governo dei dati e ai loro difficili bilanciamenti mostra che tutti poggiano e convergono sulla centralità della persona, in specifico sulla dignità e sullo sviluppo della stessa, condivisi fondamenti costituzionali: la persona nella sua identità, ampiamente intesa, funge da prisma i cui riflessi sono costituiti dai diversi diritti in gioco.

La ricerca conduce a ritenere che il bilanciamento "mobile" tra diritti possa essere centrato, allora, sulla tutela della persona e fondato sulla qualità dei dati, sulla presenza di metadati e di adeguate licenze, possa avvalersi della tecnica per un approccio preventivo, proattivo e tecnologico *by default* e *by design* e responsabilizzare i soggetti, confinando efficaci repressioni prevalentemente al momento successivo delle sanzioni.

Dall'analisi e dalle criticità emerse nella tutela dei diritti esaminati, al fine di affermare tale approccio di tutela, emergono possibili soluzioni capaci di innovare i paradigmi tradizionali e minimizzare i rischi di controllo e sorveglianza, riequilibrando le asimmetrie a favore della collettività grazie all'apertura dei *big data* (*open big data*) e proteggendo in modo efficace la persona con forme di tutela collettiva dei diritti, capaci di coadiuvare quelle individuali; a tali fini è opportuno immaginare, altresì, autorità sovranazionali dedicate al governo dei dati indipendenti da quei poteri che possono avere svariati interessi a orientarlo verso specifiche direzioni (poteri pubblici e mercato).

Al fine di realizzare un governo dei dati fondato su questa logica sono necessarie regole giuridiche e, al riguardo, emerge l'opportunità di costruire un rinnovato diritto, di matrice globale e *multistakeholder*, capace di guidare altri sistemi di regole e guidato da un approccio etico, idoneo a orientare la *data society* verso la direzione della tutela dei diritti e dello sviluppo democratico: un "nuovo diritto" può trovare forma in una condivisa Dichiarazione dei diritti.

Ubi data society, ibi ius: arrivando a innovare il noto brocardo, le conclusioni portano a ritenere che il governo dei dati necessita del ruolo del diritto e della forza dei diritti per riuscire a proteggere la persona nell'era digitale e disegnare il presente e il futuro della democrazia.

Capitolo 1

Digital society.
Governo aperto, cittadinanza digitale e nuovi diritti

SOMMARIO: 1.1. Governare la *digital society*. – 1.2. L'amministrazione digitale e aperta: dall'*e-government* all'*open government*. – 1.2.1. Strategie in ambito internazionale ed europeo. – 1.2.2. Politiche di sviluppo e quadro normativo nazionale. – 1.3. La cittadinanza digitale e i diritti fondamentali nella rete. – 1.3.1. Le Carte costituzionali e le Carte dei diritti di Internet: il contesto internazionale e il caso italiano. – 1.3.2. I diritti digitali nella normativa nazionale vigente.

1.1. Governare la *digital society*

L'esistenza contemporanea è dominata dalla realtà digitale.

Le tecnologie informatiche[2], che nel loro avvento hanno assunto il ruolo di strumento e ausilio delle attività umane, in breve tempo sono riuscite a determinare profondi mutamenti sociali e l'emersione di nuove opportunità, inedite esigenze, problematiche sconosciute.

La "rivoluzione digitale" ha prodotto ed esercita incessantemente un impatto profondo, ormai irreversibile, sulla vita degli individui e delle organizzazioni, incidendo sulle attività quotidiane, sulle relazioni e sulle modalità di partecipazione alla vita pubblica, influenzando il progresso scientifico, sociale ed economico, espandendo le possibilità dell'agire umano e le capacità stesse dell'uomo.

La realtà digitale evolve costantemente.

Il web ha avuto uno sviluppo in senso dinamico e partecipativo nel passaggio dal *web 1.0* al *web 2.0*: da mero strumento, che consentiva un'interazione limitata all'utente

[2] Il termine è usato per riferirsi alle *Information and Communication Technologies* (ICT), ossia le tecnologie dell'informazione e della comunicazione, dette anche "nuove tecnologie".

e offriva servizi in modo unilaterale, la rete si è sviluppata nel *web 2.0*, che garantisce un ruolo significativo all'utente, cui è assicurato un alto livello di interazione e la possibilità di contribuire in modo sostanziale ad arricchire il web stesso[3]. Insieme al ruolo del singolo aumentano le capacità stesse dell'uomo di ricercare, memorizzare, interagire e partecipare: si realizza una vera e propria estensione umana nella realtà digitale; già Frosini definiva il computer «protesi elettronica dell'intelligenza umana»[4]. Mutano le relazioni e le possibilità comunicative, evolvono le formazioni sociali, fondate ora sulla comunanza di interessi e non su aggregazioni territoriali: i confini geografici collassano nella rete globale.

Il digitale plasma l'esistenza in modo evidente negli ulteriori passaggi al *web 3.0* e al *web 4.0*, quando la rete si integra negli oggetti (*Internet of Things*) e acquisisce ubiquità e piena pervasività sulla realtà (*Internet of Everything*)[5]. Le potenzialità del mondo digitale arrivano a sostituire prerogative umane grazie a connessioni, algoritmi e intelligenza artificiale, capaci di svolgere al posto dell'uomo i suoi compiti e le sue attività. Sotto la pressione dei byte salta la barriera fra "interno" ed "esterno" alla rete, si

---

[3] Negli anni 2000 avviene l'evoluzione dal *web 1.0*, costellato da siti statici, servizi offerti in modo unilaterale e interazione limitata dell'utente (motori di ricerca ed email) al *web 2.0*, che non si differenzia dal *web 1.0* da un punto di vista tecnologico e architetturale (stessi protocolli di trasmissione e stesso linguaggio), ma è caratterizzato da una serie di applicazioni e servizi che garantiscono un alto livello di interazione e si avvalgono in maniera sostanziale del ruolo degli utenti. Il web diventa testo "riscrivibile", alla cui evoluzione tutti possono partecipare fornendo il proprio contributo, grazie a strumenti come i *social network* (es. Facebook, Twitter, LinkedIn), le piattaforme per la condivisione di contenuti (es. YouTube, Flickr), *wiki* (es. Wikipedia), *blog*, *forum, chat,* messaggistica istantanea (es. WhatsApp, Telegram), etc. In relazione allo sviluppo del web, E. GIOVANNINI*, Scegliere il futuro. Conoscenza e politica al tempo dei Big Data*, Il Mulino, Bologna, 2014, p. 93 evidenzia «la trasformazione dell'utente da "navigatore" a "cercatore" e da *consumer* a *prosumer*, cioè da puro utilizzatore dell'informazione ad aggregatore e a produttore di informazione originale».

[4] V. FROSINI, *Il diritto dell'informatica negli anni ottanta*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 1984, p. 396.

[5] Secondo S. RODOTÀ*, Il diritto di avere diritti,* Laterza, Roma-Bari, 2012, p. 323 il *web 3.0* «descrive un mutamento di paradigma all'interno della rete di portata tendenzialmente superiore a quello descritto parlando di Web 2.0. Qui, infatti, si era in presenza di un passaggio dall'Internet degli individui a quello delle reti sociali, rimanendo comunque la rete centrata unicamente sulle persone. Si profila ora una separazione tra il mondo delle persone e un mondo degli oggetti dotato di una propria, crescente autonomia».

svuota la realtà "analogica" e si riempie quella "digitale" in un'inedita migrazione contemporanea di massa[6]; muta lo stesso corpo che ora è anche "elettronico" (si pensi ai *device* indossabili che monitorano la condizione fisica). Il confine stesso tra essere umano e mondo digitale diventa sempre più impercettibile: realtà analogica e digitale arrivano a coincidere nel concetto semplice di realtà[7].

In questa evoluzione capace di sfumare non solo i confini geografici, ma anche i limiti dell'essere umano e delle sue capacità cognitive, i dati rivestono un ruolo centrale.

I dati e le relative informazioni, parte integrante di ogni attività umana, possono essere rappresentati in byte suscettibili di elaborazione: i processi "analogici" sono sostituiti da rappresentazioni informatiche; la digitalizzazione arriva a pervadere ogni aspetto della vita. Non a caso la società contemporanea, basata sul ruolo decisivo delle nuove tecnologie e sulla centralità dell'informazione, viene definita "società dell'informazione" o "società dell'informazione e della conoscenza"[8]: il fondamento e

---

[6] Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, trad. it., Codice edizioni, Torino, 2012, p. 3 ss., per il quale stiamo «sperimentando una *quarta rivoluzione*, che si manifesta nel processo di dislocazione e ridefinizione dell'essenza della nostra natura e del ruolo che rivestiamo nell'universo» (p. 14).

[7] Cfr. S. RODOTÀ*, Il diritto di avere diritti,* cit., pp. 25 e 26, che parla di un «ridisegno complessivo dei luoghi tradizionali e delle distinzioni che li sostengono - nazionale/globale, pubblico/privato, individuale/sociale, reale/virtuale, interno/esterno, identità/alterità». Secondo L. FLORIDI, *La rivoluzione dell'informazione*, cit. «l'infosfera sta progressivamente assorbendo ogni altro spazio» (p. 20) e «le ICT non stanno soltanto ricostruendo il nostro mondo: lo stanno *riontologizzando*» (p. 13). Per F. DI CIOMMO, *La responsabilità civile in Internet: prove di governo dell'anarchia tecnocratica*, in *La Responsabilità Civile*, fasc. 6, 2006, pp. 548-563 la rivoluzione digitale «in breve tempo ha cambiato il modo in cui l'uomo si relaziona con i prodotti, con le informazioni, con i suoi simili e con se stesso; in definitiva essa ha cambiato il modo in cui l'uomo abita la terra, sublimando quel concetto di ambiente tecnologico», dove non esistono più le dimensioni dello spazio e del tempo. Secondo R. BRIGHI, *Dati informatici e modelli dei dati. Verso "una nuova dimensione della realtà"*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, p. 281 ss. «le tecnologie informatiche forniscono quella che si può definire una "nuova dimensione della realtà" poiché, aggregando e combinando (e quindi "creando") dati, trasformano la realtà e riducono la distinzione tra essa e la sua rappresentazione digitale». Sull'impatto delle tecnologie digitali sulla vita umana cfr. N. NEGROPONTE*, Essere digitali,* trad. it., Sperling & Kupfer, Milano, 1995.

[8] In merito alla società dell'informazione cfr., *inter alia*, M. CASTELLS, *The Information Age: Economy, Society and Culture,* Blackwell, 3 tomi, Cambridge-Oxford, 1996-1998; A. MATTELART, *Storia*

l'essenza della *digital society* sono costituiti dai dati e dalle informazioni, risorse essenziali per lo sviluppo economico, sociale e culturale[9].

L'informazione è dotata di caratteristiche finora inedite nella storia umana: la quantità (di informazioni facilmente disponibili)[10], la diffusione e la velocità (di accesso, elaborazione, integrazione), la varietà, la durata o persistenza[11]. Il mutamento dell'informazione induce cambiamenti nella conoscenza: evolvono gli utilizzi, le condivisioni e le connessioni tra informazioni, l'accesso alla conoscenza diventa rapido, economico e semplice; la rete e la conoscenza si elevano a beni comuni.

Tutto questo evidenzia che il governo della *digital society* passa necessariamente dal governo dei dati, che chiama in causa il diritto. Il cambiamento pervasivo determinato dallo sviluppo delle tecnologie informatiche e dalla centralità assunta dai dati investe i complessi equilibri tra diritti e libertà, il bilanciamento tra interessi contrapposti, il rapporto tra poteri e la tenuta dei principi democratici fondamentali, determinando le condizioni di giustizia e progresso e influenzando fortemente le direttrici culturali ed etiche del futuro. Dal momento che la funzione del diritto consiste nel regolare la vita, il diritto è chiamato a disciplinare le tecnologie digitali e il "diluvio di dati" che connotano l'esistenza contemporanea. In specifico, il diritto deve essere capace di dettare regole, tracciare principi e valori condivisi, disciplinare i comportamenti, definire le responsabilità, tutelare i diritti e sanare i conflitti che scaturiscono dall'esistenza digitale, parte integrante e indistinguibile della vita reale.

---

della società dell'informazione, trad. it., Einaudi, Torino, 2002; G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Giappichelli, Torino, 2010, p. 1 ss.

[9] Cfr. P. MARSOCCI, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista AIC*, fasc. 1, 2015, p. 3: «La Rete ha inoltre, almeno al momento, una peculiare caratteristica generale: ad essere immessi, usati, scambiati, memorizzati sono sempre informazioni, ossia dati che contengono elementi di conoscenza».

[10] Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 7, che parla di «una "democratizzazione" dell'informazione senza precedenti: più persone posseggono più dati di quanto sia mai successo prima».

[11] Al riguardo cfr. V. FROSINI, *Il diritto dell'informatica negli anni ottanta*, cit., p. 395 ss., che sottolinea anche come l'informazione non sia più vincolata fisicamente al supporto materiale. Riguardo all'informazione R. BORRUSO, voce *Informatica giuridica*, in *Enciclopedia del diritto*, agg., I, Milano, 1997, p. 640 ss. pone tra le conseguenze della società postindustriale l'«avere non tanto una massa enorme di informazioni, quanto piuttosto solo quelle che servono, nel momento in cui servono, "*ad libitum*" del "*quisque de populo*"».

Nello svolgere la sua funzione il diritto è esposto a mutamenti che scaturiscono dalle caratteristiche stesse della società digitale[12].

Innanzitutto, l'oggetto di regolazione è costituito da beni intangibili, diversi dai beni materiali cui il diritto è abituato da sempre: non emerge più la produzione di beni materiali, tipica della società industriale, ma la generazione e l'utilizzo di *res incorporales*, i dati. Parallelamente viene svuotato il paradigma della proprietà, rimpiazzato dall'accesso ai dati, ai servizi, alla rete, alla propria esistenza digitale: non contano gli atomi, ma le sequenze di bit[13], i beni si trasformano in servizi[14], il concetto di proprietà cede di fronte al concetto di accesso[15].

L'oggetto della regolazione rileva sotto un altro profilo, che richiama il complesso rapporto tra diritto e tecnica: le tecnologie sono disciplinate da istruzioni, codici e regole informatiche, capaci di condizionare il comportamento dell'uomo, dal momento che tecnicamente rendono possibili o meno determinate azioni, definendo modi e vincoli, e,

---

12 V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, p. 89 ss.: «se il diritto si atteggia alla società come un guanto alla mano, è inevitabile che la diffusione delle tecnologie informatiche influenzi il diritto».

13 Cfr. G. PASCUZZI, *Dematerializzazione*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, p. 341 ss.: «I referenti della disciplina giuridica non sono atomi (parti fondamentali della materia e delle cose) ma sequenze di bit che rilevano in quanto costitutivi di beni (ad esempio software) o di rapporti (ad esempio lo *streaming* di brani musicali via rete)».

14 Si pensi al fenomeno del *car sharing* o alla fruizione di contenuti in *streaming*. Cfr. G. PASCUZZI, *Dematerializzazione*, cit., p. 342: «Non è più corretto parlare di situazioni di proprietà e di possesso bensì di titolarità e di legittimazione».

15 Cfr. J. RIFKIN, *L'era dell'accesso. La rivoluzione della new economy*, trad. it., Mondadori, Milano, 2000; S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 105 ss.; P. SAMMARCO, *I nuovi contratti dell'informatica: sistema e prassi*, in F. GALGANO (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Cedam, Padova, 2006, p. 177 ss.; V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, cit., p. 89 ss., che sottolinea come per secoli il giurista si sia confrontato con "la forza delle cose", di cui il paradigma è la proprietà. Secondo V.M. SBRESCIA, *Le comunicazioni elettroniche tra tecnologia e regolazione*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 5, 2011, p. 1207 ss. nella contemporanea "età della tecnica" o "età tecnologica" «la civiltà delle macchine sembra cedere il passo alla società della conoscenza»; secondo l'Autore «l'accesso sembra costituire una sorta di chiave di volta del sistema di fruizione di beni e servizi» e assume «una valenza non solo simbolica (sintetizzata dall'espressione "era dell'accesso") ma anche sostanziale e densa di contenuti reali (accesso alle reti, alle informazioni, ai servizi, in definitiva, accesso ai mercati)».

di conseguenza, condizionano ogni altra forma di regolazione, anche quella giuridica; si parla al riguardo di *lex informatica* o *digitalis*[16]. Ma le regole informatiche sono prodotte dall'uomo, che, pertanto, può intervenire su queste per mezzo delle regole giuridiche[17]. Di conseguenza il diritto deve essere capace di non rendere tutto ciò che è tecnologicamente possibile, solo per questo, giuridicamente legittimo[18] e tracciare un difficile equilibrio che permetta alla tecnica di non prevalere sul diritto, ma neppure al diritto di limitare le potenzialità della tecnologia[19].

L'oggetto di regolazione incide anche sotto un altro aspetto significativo, legato alla dimensione temporale: la tecnica evolve con estrema rapidità, mentre il diritto è strutturalmente "più lento", in quanto frutto di scelte e bilanciamenti tipici del processo democratico[20].

Accanto al tempo, anche la dimensione dello spazio è investita dalla rivoluzione digitale e influisce, di conseguenza, sul diritto. Nella storia le libertà si sono evolute nel segno di una pluralità di ordinamenti relativi ai diversi Stati, che hanno fornito le regole all'interno dei propri territori. I confini nazionali sono oggi superati dalla società digitale connotata dalla dimensione globale, che esige soluzioni giuridiche armonizzate e omogenee per essere effettive. Le attività, gli acquisti, le relazioni non scontano più il

---

16 Cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, cit., p. 37 ss. e G. SARTOR, *Internet e il diritto*, in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli, Torino, 2013, p. 1 ss. Al riguardo cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, 1999, pp. 501-546, che nel governo del ciberspazio delinea quattro fattori fondamentali: regole giuridiche, regole sociali, mercato e "il codice" (*lex informatica*). Sul rapporto tra diritto e *lex informatica* cfr. E. MAESTRI, Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars Interpretandi*, fasc. 6, 2017, pp. 15-28.

17 Il diritto può arrivare ad affiancare alla tutela giuridica la previsione di misure tecnologiche idonee a disabilitare o a rendere impossibili tecnicamente azioni illecite (è il caso delle misure tecnologiche di protezione previste dalle norme a tutela del diritto d'autore, in specifico nell'art. 102-quater, legge 22 aprile 1941, n. 633). Cfr. G. SARTOR, *Internet e il diritto*, cit., p. 15 ss.

18 Cfr. S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. CONTI, Laterza, Roma-Bari, 2005.

19 Cfr. G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2012, p. 831 ss.; V. FROSINI, *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981; N. IRTI - E. SEVERINO, *Dialogo su diritto e tecnica*, Laterza, Roma-Bari, 2001; V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, cit., p. 89 ss.

20 Cfr. V. M. SBRESCIA, *op. cit.*, p. 1207 ss.

limite geografico e questo determina la necessità che, parallelamente alle questioni oggetto di regolazione, le risposte giuridiche abbiano una connotazione sovranazionale per non creare una discrasia inevitabile tra la connotazione globale delle fattispecie e la configurazione territoriale delle norme da applicare alle stesse.

Internet si pone come il più grande spazio pubblico, *agorà* non tangibile, decentrata e aterritoriale, capace di ridefinire le attività e i processi, reinterpretare il singolo e le formazioni sociali; è uno spazio su cui nessuno può vantare un potere esclusivo[21]. La "navigazione in rete", priva di riferimenti terreni, di frontiere e di "sovrani", pone difficoltà a individuare il diritto applicabile proprio come il mare[22].

La dimensione globale della *digital society* conduce, di conseguenza, a un ripensamento del potere nazionale e a un'erosione dei monopoli statali[23].

Allo stesso tempo la sovranità statale è minacciata anche dal ruolo assunto dai poteri privati, che, a differenza degli Stati, grazie alla rilevanza nel mercato hanno conquistato la dimensione globale, regolando l'accesso ai servizi e alle utilità della rete, incidendo così sui diritti e sulle libertà dei singoli[24]. Google, Facebook, Amazon, nel porre le condizioni generali di servizio e i termini di accesso e utilizzo, di fatto producono regole, seppur privi di legittimazione democratica e guidati non dall'interesse pubblico, ma dal profitto economico: si tratta di una nuova "legge" costituita da regole ampiamente accettate, seppur più o meno consapevolmente, capaci

---

21 Tali caratteristiche hanno portato alcuni a vedere Internet come "spazio senza legge"; in proposito si può ricordare la «*Declaration of the Indipendence of Cyberspace*» di J. Barlow nel 1996 (*www.eff.org/cyberspace-independence*); *infra*, § 3.

22 Cfr. S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 378 ss. e G. PELLERINO, *I rischi del diritto nella Rete globale*, in *Informatica e diritto*, fasc. 1, 2009, p. 262 ss., che, in relazione al diritto dei naviganti, sottolinea trattarsi di «una *lex mercatoria*, una norma a carattere consuetudinario, di origine prettamente sociale, nella formazione della quale era determinante l'influenza dei destinatari delle norme».

23 Cfr. E. MAESTRI, Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, cit., p. 19: «Il diritto digitale segna irreversibilmente la crisi della sovranità dello Stato: la rigidità del diritto statale si rivela incapace di regolare le nuove modalità delle azioni umane; la destatualizzazione produce un diritto flessibile, che si adatta al modello reticolare del mondo digitale».

24 Cfr. P. MARSOCCI, *op. cit.*, p. 5: «il dato dell'arretramento dell'azione politica degli Stati, unito sia alla tendenza all'autoregolamentazione dal basso sia all'appropriazione da parte dei poteri economici forti, ha determinato una sfida inedita per i sistemi giuridici contemporanei».

di influire sulla vita quotidiana e sulle attività degli individui quanto le norme con efficacia vincolante prodotte dagli Stati.

La società degli algoritmi, se lasciata all'autoregolazione e al mercato, rischia una torsione atta ad assegnare il potere nelle mani di pochi, detentori di dati e conoscenza[25]. I colossi del web, fuori da ogni controllo istituzionale, diventano i controllori del pedaggio di accesso alla vita digitale: la libertà degli individui è apparente, perché il passaggio è obbligato per accedere e godere di servizi, relazioni e possibilità[26]. Ugualmente apparente è la gratuità dell'accesso concesso, dal momento che il pedaggio è pagato con la moneta dei dati personali, che rischiano una mercificazione che incrina diritti e libertà[27].

In questo processo sono depotenziati i legislatori e arretra lo spazio giuridico pubblico, soppiantato dal ruolo svolto dal mercato, frenato a sua volta soltanto dall'opera delle giurisdizioni delle Corti sovranazionali[28]: il potere giurisdizionale finisce per assolvere un ruolo suppletivo che non è suo proprio, dovendo compiere *ex post* complessi bilanciamenti tra interessi diversi che il potere legislativo non ha

---

25 R. CAZZANTI, *Open data e nativi digitali. Per un uso intelligente delle tecnologie,* libreriauniversitaria.it edizioni, Padova, 2016, p. 12 avverte sulla «deriva mercantilistica della società che confonde la pace con il benessere materiale perseguendolo con l'abbassamento della consapevolezza individuale e collettiva».

26 Cfr. B.C. HAN, *La società della trasparenza,* trad. it., Nottetempo, Roma, 2014, p. 76 ss.: «L'intero globo evolve oggi in un panottico. Non c'è alcun esterno rispetto al panottico, che diventa totale. Nessun muro separa l'interno dall'esterno. Google e i social network, che si presentano come spazi di libertà, assumono forme panottiche. La sorveglianza oggi non si realizza, come si ritiene normalmente, nella forma di un *attacco alla libertà*. Piuttosto, ciascuno si consegna *volontariamente* allo sguardo panottico. *Si collabora* intenzionalmente al panottico digitale, svelando ed esponendo se stessi. Il detenuto del panottico digitale è, al tempo stesso, carnefice e vittima. In ciò consiste la dialettica della libertà. La libertà si rivela controllo» (p. 83).

27 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 413 ss. e A. MASERA - G. SCORZA, *Internet, i nostri diritti*, Laterza, Roma-Bari, 2016, p. 38 ss. Secondo P. MARSOCCI, *op. cit.*, p. 7: «la digitalizzazione ha aumentato la fragilità di ciascuno di noi non meno di quella delle nostre nazioni».

28 Tale fenomeno viene spiegato da P. OTRANTO, *Internet nell'organizzazione amministrativa. Reti di libertà*, Cacucci editore, Bari, 2015, p. 68: «la rapidità con la quale internet si evolve nelle sue applicazioni e nella sua diffusione, fa sì che la regola giuridica sempre più si formi nelle Corti, perché tra tempo del diritto, inteso come disciplina dei fenomeni sociali, e tempo della produzione normativa in senso formale, è presente una discrasia assai rilevante».

preventivamente regolato[29]. Questo rischia di minare il principio costituito dalla certezza del diritto, dal momento che gli individui hanno bisogno di conoscere come sono regolate le fattispecie per agire in modo lecito, evitare conflitti e conseguenti contenziosi.

La società digitale ridefinisce, dunque, la sfera pubblica e privata, ridistribuisce e disegna nuove geometrie di potere. La rivoluzione dell'informazione colpisce il processo democratico, condizionato dalla circolazione e dalla diffusione di informazioni, capaci di influire sulla capacità di giudizio dei cittadini, sulla partecipazione consapevole, sulla formazione di una coscienza civica e sul concetto stesso di rappresentanza[30]. Il ruolo della rete e della condivisione di dati e informazioni risulta evidente in forme temporanee di mobilitazione e protesta, come le cosiddette "primavere arabe", nelle campagne elettorali[31] e, altresì, nel rinnovamento o nella formazione di nuovi soggetti politici[32].

---

[29] Esemplificativamente si pensi all'impatto della sentenza della Corte di Giustizia dell'Unione europea del 13 maggio 2014, causa C-131/12, cosiddetta *Google Spain*, a seguito della quale Google ha assunto di fatto la funzione di arbitro e detentore della luce e dell'ombra sui dati personali nel web per mezzo dell'indicizzazione o deindicizzazione dei contenuti. Più ampiamente al riguardo, *infra*, cap. 4 § 3.2.

[30] Cfr. T.E. FROSINI, *Liberté, Egalité, Internet*, Editoriale Scientifica, Napoli, 2015, p. 40 ss. In merito alle molteplici informazioni messe a disposizione dalla rete M. CUNIBERTI, *Nuove tecnologie della comunicazione e trasformazioni della democrazia*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, Milano, 2008, p. 360 ss. sottolinea la libertà apparente e i fenomeni di "polarizzazione" e "balcanizzazione" dell'opinione pubblica, per effetto dei quali il soggetto che entra in rete finisce per rafforzare le sue convinzioni di partenza. Al riguardo secondo B.C. HAN*, op. cit.*, p. 60 ss. «i social media e i motori di ricerca personalizzati edificano nella rete uno *spazio di prossimità* assoluto, dal quale l'*esterno* è eliminato. Lì si ha modo di incontrare soltanto se stessi e i propri eguali. […] Questa *prossimità digitale* propone al partecipante soltanto quei frammenti di mondo che gli *piacciono*. Di conseguenza, abolisce la dimensione pubblica, la coscienza pubblica, davvero *critica*, e privatizza il mondo».

[31] Si pensi alla campagna presidenziale di Barack Obama e, successivamente, a quella di Donald Trump negli Stati Uniti.

[32] È il caso dei Partiti Pirata nel Nord Europa. Cfr. G. AZZARITI, *Internet e Costituzione,* in *Costituzionalismo.it,* fasc. 2, 2011, p. 1 ss.; P. COSTANZO, *Quale partecipazione politica attraverso le nuove tecnologie comunicative in Italia*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2011, p.

Il cambiamento investe e forza il rapporto tra governanti e governati che, sotto la spinta della centralità dei dati, della circolazione delle informazioni e del valore della conoscenza, diventa maggiormente orizzontale, connotandosi per l'emersione dei principi di trasparenza, partecipazione e collaborazione e caratterizzandosi per un possibile maggiore controllo democratico[33]; al tempo stesso si pone, però, il rischio inverso di scivolare verso nuove asimmetrie informative e inedite forme di controllo sociale, rese possibili dalla sconcertante disponibilità dei dati e da rapporti di interesse tra pubblici poteri e giganti del web[34].

La tecnologia può essere orientata in un senso o nell'altro: la sua regolamentazione giuridica involge la stessa questione democratica, la fisionomia da offrire alla società che si staglia all'orizzonte e in larga parte è già presente, i bilanciamenti da disegnare e la tutela da offrire ai diritti[35]. Utilizzando le parole di Rodotà, il bisogno di diritti è anche bisogno di diritto[36].

La *digital society*, basata sui dati, sulle informazioni e sulla conoscenza, provoca un profondo mutamento nel volto e nel rapporto che lega i protagonisti della società

---

19 ss.; M. CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, p. 275 ss.

33 G. PELLERINO, *op. cit.*, p. 257: «Internet rappresenta uno strumento di accrescimento delle conoscenze e della libertà, portando con sé un ampliamento degli strumenti di governo non autoritativi e consensuali cui corrisponde una riduzione di quelli di tipo autoritativo».

34 Cfr. G. AZZARITI, *op. cit.*, pp. 4-5 e A. MASERA - G. SCORZA, *op. cit.*, p. 60 ss.: i *transparency report* di Facebook e Twitter rivelano come i governi ricorrano ai responsabili delle piattaforme per ottenere dati personali o la cancellazione o rimozione di contenuti, senza alcun provvedimento del giudice. M. CUNIBERTI, *Nuove tecnologie della comunicazione e trasformazioni della democrazia*, cit., p. 364 ss. ritiene che lo spontaneismo sociale, ONG e associazionismo siano l'unico contrappeso al potere economico delle imprese: «utilizzando un linguaggio che ha avuto un certo successo, si può dire che, tra il "privato" delle imprese e il "comune", rappresentato dall'accesso e dall'utilizzo diffuso, quello che scompare è il "pubblico", inteso come gestione organizzata di beni collettivi, attraverso scelte politiche sottoposte a controllo parlamentare» (p. 368).

35 Cfr. R. BORRUSO, voce *Informatica giuridica*, cit.: «l'uso del computer – che come la scrittura e la stampa sta permeando di sé tutte le nostre attività e quindi anche il diritto – può essere volto tanto a rendere la vita più umana, più giusta, più democratica, quanto a disumanizzarla rendendola arida e opprimente».

36 S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 3 ss.

contemporanea, con un cambiamento che tocca anche le denominazioni: si parla da una parte di *e-government* e governo aperto e dall'altra di cittadinanza digitale.

1.2. L'amministrazione digitale e aperta: dall'*e-government* all'*open government*

Le tecnologie evolvono e insieme al loro sviluppo muta la società con i suoi modelli relazionali.

La rete, come visto, matura nel passaggio dal *web 1.0* al *web 2.0* da mero strumento "statico" di consultazione a spazio dinamico di partecipazione, da mezzo unilaterale a piattaforma collaborativa e "riscrivibile" che garantisce a chiunque la possibilità di contribuire attivamente; sotto i nostri occhi la rete evolve ancora inarrestabile verso la pervasività e l'ubiquità del *web 3.0* e *4.0*, promettendo e realizzando nuove possibilità di interazione non solo tra gli esseri umani, ma anche tra gli esseri umani e gli oggetti, tra gli esseri umani e le macchine. La rete diventa il più grande spazio pubblico di condivisione, sviluppo e aggregazione di informazioni e servizi, basato saldamente sull'utilizzo dei dati.

L'evoluzione delle tecnologie informatiche e della rete coinvolge la società stessa, che viene pervasa dal principio di *openness*, da un approccio "a rete" in grado di creare sinergie inedite tra dati, ma anche tra soggetti diversi, consentendo in tal modo di generare nuove soluzioni: le *keywords* della contemporaneità coincidono con i concetti di partecipazione, condivisione e collaborazione ed emerge il concetto di intelligenza collettiva[37]. La rinnovata fisionomia della società contemporanea, innescata

[37] L'intelligenza collettiva secondo P. LÉVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Feltrinelli, Milano, 1996, p. 34 ss. è «un'intelligenza distribuita ovunque, continuamente valorizzata, coordinata in tempo reale, che porta a una mobilitazione effettiva delle competenze. […] Lungi dal fondere le intelligenze individuali in una sorta di magma indistinto, l'intelligenza collettiva è un processo di crescita, di differenziazione e di mutuo rilancio delle specificità. L'immagine dinamica che emerge dalle sue competenze, dai suoi progetti e dalle relazioni che i suoi membri intrattengono all'interno dello Spazio del sapere, costituisce per un collettivo una nuova modalità di identificazione, aperta, viva e positiva». Come rileva F. DI DONATO, *Lo stato trasparente. Linked open data e cittadinanza attiva*, Edizioni ETS, Pisa, 2010, p. 82 l'intelligenza collettiva è prodotta dalla

dall'ingresso e dall'evoluzione delle tecnologie informatiche e caratterizzata dal ruolo centrale assunto dai dati e dalla conoscenza, determina una conseguente modifica nelle relazioni e nello sviluppo di nuovi modelli di governo; di conseguenza muta il volto dell'amministrazione pubblica, attore protagonista dei processi di riferimento della società[38].

Il profondo sviluppo della società tecnologica è, dunque, all'origine dell'evoluzione dell'amministrazione pubblica nel senso della digitalizzazione e dell'apertura, sviluppo necessario per essere in grado di rispondere efficacemente alle esigenze della società e acquisire la capacità di parlarne lo stesso linguaggio. Del resto la *mission* delle istituzioni consiste nel perseguimento dei diritti di cittadini e imprese e nella realizzazione del benessere della collettività: a tali fini, nello svolgimento delle funzioni e nell'erogazione dei servizi, le amministrazioni devono ontologicamente essere capaci di comprendere le esigenze della collettività, interagire con le modalità relazionali più idonee e realizzare la soddisfazione degli utenti[39]; per compiere in modo adeguato il proprio ruolo, i poteri pubblici devono necessariamente evolvere insieme alla società di riferimento, trovandosi pertanto chiamati a guidare, governare e promuovere lo sviluppo digitale[40].

«compresenza della massima accessibilità dell'informazione e della massima libertà di accrescere la massa di queste informazioni».

38 Cfr. R. CARPENTIERI, *L'Agenda digitale italiana (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 225-233, secondo la quale l'innovazione digitale «non è più solo una priorità, ma un pre-requisito per lo sviluppo del Paese e del relativo sistema produttivo, con importanti implicazioni per il prodotto interno lordo, l'occupazione e la crescita» (p. 225). La sfida della digitalizzazione, quale asse portante delle riforme amministrative, è comune a diversi Stati; al riguardo, si veda l'analisi di G. NAPOLITANO, *Le riforme amministrative in Europa all'inizio del ventunesimo secolo*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 2015, pp. 611-640.

39 Cfr. E. D'ORLANDO, *Profili costituzionali dell'amministrazione digitale,* in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2011, p. 213 ss.

40 Cfr. P. OTRANTO, *op. cit.*, p. 104, secondo cui i poteri pubblici, nel guidare lo sviluppo digitale della società, devono creare «le condizioni più favorevoli per l'attuazione, attraverso la rete, del principio personalista nella sua nuova e sempre più complessa dimensione». Secondo S. CALZOLAIO, Digital (and privacy) by default. *L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, fasc. 31, 2016, p. 186 la digitalizzazione delle attività e dei servizi pubblici è decisiva «non solo in vista della progressiva digitalizzazione del "settore pubblico", ma ai fini della digitalizzazione

Negli ultimi anni, di conseguenza, tale evoluzione ha interessato anche le istituzioni e, in particolare, il modello di amministrazione digitale (*e-government*), ossia l'organizzazione delle attività dell'amministrazione pubblica fondata sull'adozione estesa e integrata delle tecnologie informatiche nello svolgimento delle funzioni e nell'erogazione dei servizi[41].

Il concetto di amministrazione digitale si riferisce all'innovazione in senso ampio come evoluzione dell'amministrazione pubblica attivata dalle tecnologie informatiche, che in queste non si esaurisce, ma si esplica altresì in un conseguente cambiamento di logiche e processi dell'*agere* pubblico. Non significa una semplice automazione dei procedimenti, ma implica riorganizzazione, razionalizzazione, reingegnerizzazione delle attività e la configurazione di un nuovo rapporto con la cittadinanza, a sua volta "digitale"; si tratta di un profondo ripensamento di relazioni, attività e processi, in cui le tecnologie informatiche non costituiscono il fine ultimo, ma rappresentano lo strumento idoneo a raggiungere gli obiettivi che caratterizzano l'azione pubblica.

Le motivazioni e gli obiettivi principali della costruzione della pubblica amministrazione digitale trovano radici, infatti, proprio nelle finalità dell'azione pubblica: efficacia ed efficienza, migliore qualità dei servizi, maggiore soddisfazione

---

della società e, con essa, della determinazione dei caratteri fondamentali delle democrazie europee e della cittadinanza nazionale ed europea».

41 Sulla pubblica amministrazione digitale cfr., *inter alia*, G. CASSANO - C. GIURDANELLA (a cura di), *Il codice della Pubblica Amministrazione digitale. Commentario al D.lgs. n. 82 del 7 marzo 2005*, Giuffrè, Milano, 2005; E. BELISARIO, *La nuova Pubblica Amministrazione Digitale. Guida al Codice dell'Amministrazione Digitale dopo la Legge n. 69/*2009, Maggioli, Rimini, 2009; E. ZUANELLI, *Amministrazione digitale e innovazione tecnologica: analisi, riflessioni, proposte*, Aracne, Roma, 2013; L. DE PIETRO (a cura di), *Dieci lezioni per capire ed attuare l'e-government*, Marsilio Editori, Venezia, 2011; M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014; F. TROJANI, *Il nuovo Codice dell'amministrazione digitale dopo il d.lgs. 179/2016 e il Regolamento eIDAS,* Maggioli, Rimini, 2017; M. DI FRANCESCO TORREGROSSA, *La pubblica amministrazione nella società digitale,* Editoriale scientifica, Napoli, 2017. Sia consentito, altresì, il rinvio a F. FAINI, *L'evoluzione del modello di amministrazione digitale,* in *Rivista elettronica di Diritto, Economia e Management*, n. 1, 2014, pp. 184-210; F. FAINI, *Informatica e Pubblica Amministrazione*, in G. TADDEI ELMI (a cura di), *Corso di Informatica giuridica*, IV ed., Edizioni Giuridiche Simone, Napoli, 2016, pp. 179-243; F. FAINI, *L'amministrazione digitale e aperta*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 149-194: l'analisi condotta in questo paragrafo sviluppa le riflessioni contenute nei contributi richiamati.

degli utenti, semplificazione e conseguente riduzione dei tempi, partecipazione dei cittadini. Tra collettività e amministrazioni può prendere forma una relazione diretta e collaborativa di fiducia, che poggia sui principi di trasparenza e di ascolto e permette di ridurre gli squilibri[42].

Sotto la spinta evolutiva della *digital society*, negli ultimi anni il governo digitale matura nell'*open government*, modello secondo cui le amministrazioni devono essere capaci di essere trasparenti a tutti i livelli e di rendere le proprie attività aperte e disponibili per favorire azioni maggiormente efficaci, rispondere alle istanze della società e garantire il controllo pubblico del proprio operato mediante le nuove tecnologie[43].

Il modello di *open government*, basato sulla centralità attribuita ai cittadini, si caratterizza, in parallelo alla società aperta, per l'importanza strategica assunta dai dati e dalle informazioni e per l'emersione del valore della conoscenza nel rapporto fra governanti e governati. L'informazione pubblica assurge a bene comune, aperto alla massima fruizione dei cittadini attraverso le tecnologie[44].

Il governo aperto, di conseguenza, promette di garantire pieno e universale accesso al patrimonio informativo pubblico e assicurare la partecipazione consapevole e

---

42 Cfr. B. CAROTTI, *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa (commento alla legge 7 agosto 2015, n. 124)*, in *Giornale di diritto amministrativo*, fasc. 5, 2015, pp. 625-629, che sottolinea come «la "sostanza digitale" possa contribuire a un "rinnovato patto" tra singolo e poteri pubblici».

43 Sull'*open government* cfr., *inter alia*, D. LATHROP - L. RUMA (a cura di), *Open government: Collaboration, Transparency, and Participation In Practice,* O'Reilly Media, Sebastopol, 2010; E. CARLONI (a cura di), *L'amministrazione aperta. Regole strumenti e limiti dell'open government*, Maggioli, Rimini, 2014; F. DI DONATO, *op. cit.*; L. SARTORI, *Open government: what else?*, in *Istituzioni del federalismo*, fasc. 3-4, 2013, pp. 753-775; sia consentito, altresì, il rinvio a F. FAINI, *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in *Ciberspazio e diritto*, fasc. 2, 2013, pp. 213-238. In merito T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, in G. PERUGINELLI - M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, Napoli-Roma, 2014, p. 581 sottolinea come il paradigma del governo aperto sia anteriore e indipendente rispetto alle tecnologie della rete: è finalizzato alla trasparenza, alla responsabilità e al controllo delle azioni da parte dei cittadini.

44 Cfr. P. OTRANTO, *op. cit.*, p. 108, che sottolinea l'emersione del ruolo dell'informazione pubblica nell'evoluzione dell'ordinamento amministrativo verso la digitalizzazione.

informata, al fine di gestire in modo dinamico e collaborativo l'interazione tra sistema pubblico e privato. Il controllo democratico, che permette di acquisire, confrontare e valutare le informazioni, diventa strumento di partecipazione e collaborazione dei cittadini per favorire il buon andamento, l'*accountability* e l'imparzialità, finalità tipiche dell'agire pubblico.

I pilastri dell'*open government* sono costituiti dai principi stessi su cui il modello si fonda:

1. la trasparenza, che si basa sulla disponibilità e condivisione di dati, informazioni e documenti e promuove, in tal modo, l'*accountability* delle istituzioni;
2. la partecipazione, che si fonda sul coinvolgimento dei cittadini nel sistema decisionale e consente a ciascuno di fornire il proprio apporto di conoscenze, idee ed esperienze per il miglioramento delle politiche pubbliche;
3. la collaborazione, che può essere intesa come cooperazione tra i diversi livelli di governo e gli attori privati[45].

L'*open government* porta le amministrazioni pubbliche a un ripensamento dei processi decisionali tradizionali, in particolare sotto il profilo degli strumenti e delle modalità attraverso cui si esplica la relazione con la collettività. Il metodo di governo è orizzontale e flessibile, idoneo a rispondere agli impulsi e alle esigenze della collettività e il processo decisionale scaturisce dal dialogo e dal confronto: in questa nuova configurazione è possibile governare con l'apporto fattivo dei diversi portatori di interesse. In tal modo il modello di *open government* permette di diminuire le asimmetrie informative e rafforzare la fiducia verso le amministrazioni pubbliche, incidendo favorevolmente sulla qualità dei servizi e della stessa democrazia[46].

Nel nuovo paradigma si attualizzano, pertanto, i principi di trasparenza e

---

[45] Cfr. L. SARTORI, *op. cit.*, p. 755: «I pilastri dell'Opengov sono individuabili nella trasparenza e nella partecipazione, cui va aggiunta la collaborazione, quale meccanismo di raccordo tra le due precedenti».

[46] In tal senso cfr. L. SARTORI, *op. cit.*, p. 754 ss.: «Le istituzioni possono agire nell'ottica dell'Opengov per diverse ragioni: ideali (per rinnovare il patto democratico), politiche (per ottenere credito elettorale) o procedurali (per rendere più efficaci le politiche). La richiesta di uno stile di governo più partecipativo e *accountable* emerge quindi sia da parte dei cittadini (che vogliono poter esprimere la loro voce per contribuire alla gestione del bene pubblico) che da parte dei politici (che vogliono rimediare al forte *disengagement*)» (p. 756).

partecipazione che caratterizzano anche la rete dinamica e interattiva: evolve il modo di intendere, condividere e utilizzare i dati, che diventano indipendenti dai titolari pubblici e possono essere utilizzati, aggregati, sviluppati da cittadini e imprese, generando così nuovi servizi. Strumento significativo del governo aperto sono, infatti, gli *open data*, nei quali trovano attuazione i principi fondanti dell'*open government*[47].

In linea con la configurazione della rete, il governo diventa una piattaforma comune (*government as a platform*), fondata sulla facile reperibilità e sulla riutilizzabilità dei dati, centrata sul coinvolgimento e sulla responsabilizzazione degli utenti e capace, in tal modo, di generare un vero e proprio mutamento culturale[48].

Pertanto i nuovi strumenti offerti dalla società tecnologica possono essere proficuamente impiegati nelle politiche e nelle azioni pubbliche, per mezzo di un atteggiamento caratterizzato dalla condivisione e dalla collaborazione delle istituzioni con altre istituzioni, cittadini, associazioni e imprese. Questo presuppone un profondo cambiamento delle istituzioni stesse sia nelle relazioni fra le diverse amministrazioni, che devono basarsi sullo scambio e sulla condivisione di dati e informazioni e su un approccio unitario ed omogeneo[49], sia nei rapporti del sistema istituzionale con la società, sviluppando una proficua "contaminazione" tra mondo pubblico e privato nelle attività e nei servizi pubblici.

L'*open government* prende forma nel volto aperto di istituzioni pronte a recepire l'apporto della società, capaci insieme di attivare innovazione, creatività e competitività e proiettate alla revisione dei modelli di azione nell'ottica suggerita dall'Europa, che prevede come priorità l'*empowerment* di cittadini e imprese, ossia il coinvolgimento e la produzione collaborativa di servizi[50].

In questo processo di apertura delle istituzioni i principi di digitalizzazione e

---

47 *Infra*, cap. 3.

48 Cfr. A. CASINELLI, *L'e-government (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 234-239.

49 Secondo S. CALZOLAIO, *op. cit.*, p. 195 ss. i processi di digitalizzazione necessitano del coordinamento e di un governo unitario, per evitare altrimenti il rischio concreto di creare «"realtà digitalmente impermeabili", dei veri e propri feudi digitali» (p. 195).

50 Per *empowerment* si intende la responsabilizzazione dell'utente tesa a incrementare nei cittadini, nelle imprese e nelle altre organizzazioni la capacità di essere proattivi nella società mediante il ricorso ai nuovi strumenti tecnologici.

trasparenza si collegano strettamente fino a fondersi, come basi principali su cui poggia il nuovo modello di governo, come emerge dalle strategie internazionali e dall'evoluzione normativa italiana.

1.2.1. Strategie in ambito internazionale ed europeo

Il modello di *open government* nasce in America.

Dopo una campagna elettorale fortemente basata sulla partecipazione dei cittadini[51], con il *Memorandum on Transparency and Open Government* del 21 gennaio 2009 e l'*Open Government Directive* dell'8 dicembre 2009 il Presidente degli Stati Uniti Barack Obama prescrive alle istituzioni i pilastri del governo aperto, costituiti da trasparenza, partecipazione e collaborazione, e individua negli *open data* uno strumento strategico di partecipazione della collettività: i dati pubblici sono considerati risorsa da aprire e le tecnologie informatiche sono interpretate come strumenti idonei ad assicurare questo processo di apertura[52]. Tale strategia coniuga trasparenza e apertura, impegnando al riguardo le istituzioni americane, al fine di rafforzare la fiducia pubblica, promuovere l'efficienza delle istituzioni e fortificare la democrazia. In merito è significativo anche il *Memorandum Freedom of Information Act*, emanato anch'esso il 21 gennaio 2009, che pone una sorta di presunzione di apertura, imponendo nei casi dubbi di permettere l'accesso[53]. Questi atti dell'amministrazione Obama pongono le fondamenta di un

---

51 Cfr. L. SARTORI, *op. cit.*, p. 758 ss.

52 Cfr. B. OBAMA, *Memorandum for the Heads of Executive Departments and Agencies on Transparency and Open Government* del 21 gennaio 2009 e *Open Government Directive* dell'8 dicembre 2009, accessibili al link *obamawhitehouse.archives.gov/open/about/policy*, che hanno dato vita all'*Open Government Initiative.*

53 Cfr. V. LUBELLO, *L'*Open Government *negli Stati Uniti d'America tra il* Freedom of Information Act *e il* bazar, in *Informatica e diritto*, nn. 1-2, 2011, p. 387, secondo cui «le politiche di *Open Government* intraprese dalla presidenza Obama sono, anzitutto, una risposta politica alla fase di "chiusura" che ha caratterizzato l'amministrazione precedente nella divulgazione dei dati pubblici» e «i *memoranda* dell'*Open Government* e le iniziative che ne fanno da corollario sono la presa di coscienza dell'avvento di un Web 2.0 nel quale gli utenti possono farsi essi stessi carico di una più efficace e diretta comunicazione delle informazioni». Cfr. B. COCCAGNA - G. ZICCARDI, *Open data, trasparenza elettronica e codice aperto*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e*

government as a platform[54].

La strategia del Presidente Obama porta alla creazione nel 2009 del portale *open data*, *data.gov*, modello seguito negli anni successivi da molti Paesi europei: nello stesso anno viene lanciato il portale *data.gov.uk* del Regno Unito, seguono la Francia con *data.gouv.fr*, la Spagna con *datos.gob.es* e la Germania con *govdata.de.* Pochi anni dopo arrivano anche i portali europei *European Union Open Data Portal* (*data.europa.eu/euodp/en/data*) ed *European Data Portal* (*www.europeandataportal.eu*)[55].

Il percorso strategico europeo, che ha dato impulso anche alle politiche e all'evoluzione normativa italiana, nasce in modo diverso rispetto agli Stati Uniti. In tal caso, in coerenza stessa col modello, l'*openness* origina "dal basso" per mezzo della dichiarazione aperta sui servizi pubblici europei promossa nel 2009 da un insieme di cittadini e associazioni, che pongono all'attenzione degli organi europei l'importanza dei principi di trasparenza, partecipazione ed *empowerment*, pilastri fondanti del governo aperto[56]. I contenuti del documento sono fatti propri dalla dichiarazione di Malmö del 2009[57], che fissa tra gli obiettivi per il 2015 il coinvolgimento della società civile e degli *stakeholder* nello sviluppo di servizi *user-centric*, l'aumento della disponibilità e il riuso di dati pubblici, la trasparenza dei processi e la promozione della partecipazione attiva.

Oggi la cornice strategica è fornita dalla *Digital Agenda for Europe* e dai relativi

---

diritto delle nuove tecnologie, Utet giuridica, Milano, 2012, p. 398 ss. In merito L. SARTORI, *op. cit.*, p. 758 ss. sottolinea che la strategia di *open government* di Obama riesce ad imporsi come priorità politica e strategica grazie a un percorso istituzionale e culturale, fatto di diverse tappe significative fra le quali il *Freedom of Information Act* (1966) e il *Privacy Act* (1974), dove già emergono i valori dell'*open government*, dell'*accountability* e della responsabilità.

54 V. LUBELLO, *op. cit.*, p. 383 vede in questo «un vero e proprio elemento prodromico alla più suggestiva entità della cyberdemocrazia teorizzata da Lévy». Secondo B. COCCAGNA - G. ZICCARDI, *op. cit.*, p. 398 ss., nell'attuare un'efficace politica di *open data*, il primo passo da compiere è «quello di immaginare il governo come una piattaforma, ovvero come un *provider* di dati e servizi liberamente implementabili da parte dei terzi» (p. 401).

55 Sulla misurazione dello stato di realizzazione e avanzamento dell'*open government* nel mondo cfr. L. SARTORI, *op. cit.*, p. 763 ss.

56 Cfr. *eups20.wordpress.com/the-open-declaration.*

57 La Dichiarazione è resa nella V Conferenza ministeriale sull'E-government.

piani d'azione.

L'Agenda digitale europea si pone significativamente come una delle sette iniziative "faro" individuate nella più ampia Strategia Europea 2020[58], che mira a realizzare una crescita intelligente, sostenibile e inclusiva: in specifico la *Digital Agenda for Europe*, nella realizzazione di un *digital single market* europeo[59], conferisce un ruolo chiave alle tecnologie informatiche per raggiungere gli obiettivi ed è finalizzata a sfruttare al meglio il potenziale delle tecnologie per favorire l'innovazione, la crescita economica, la competitività e il progresso[60].

All'Agenda digitale europea si collegano i relativi piani d'azione: dopo il piano d'azione europeo per l'*e-government* 2011-2015, adottato nel 2010[61], che riflette le priorità della dichiarazione di Malmö[62], si pone in coerenza l'attuale Piano d'azione

---

58 Comunicazione della Commissione europea «*Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva*» - COM(2010) 2020 del 3 marzo 2010.

59 Al riguardo risulta particolarmente significativa la comunicazione della Commissione europea «*A Digital Single Market Strategy for Europe*» - COM(2015) 192 final del 6 maggio 2015.

60 Comunicazione della Commissione europea «*Un'agenda digitale europea*» - COM(2010) 245 definitivo/2 del 26 agosto 2010. L'Agenda digitale europea arriva dopo un lungo percorso di politiche europee di sviluppo delle tecnologie informatiche e dell'*e-government*, che nasce nel programma *Esprit* del 1984, nel c.d. Rapporto Delors del 1993 e nel c.d. Rapporto Bangemann del 1994; poi sono stati approvati l'iniziativa «*eEurope - Una Società dell'Informazione per tutti*» del 2000 e i relativi piani di azione *eEurope 2002* del 2001 e *eEurope 2005* del 2002, seguiti nel 2005 dall'iniziativa «*i2010 – Una società europea dell'informazione per la crescita e l'occupazione*» e dal relativo Piano d'azione *e-government*, presentato nel 2006. Cfr. D.A. LIMONE, *Politica e Normativa Comunitaria per la Società dell'Informazione (1990-2010)*, in *Rivista elettronica di Diritto, Economia, Management*, n. 1, 2010.

61 Comunicazione della Commissione europea «*Il piano d'azione europeo per l'eGovernment 2011-2015 - Valorizzare le TIC per promuovere un'amministrazione digitale intelligente, sostenibile e innovativa*» - COM(2010) 743 def. del 15 dicembre 2010.

62 L'obiettivo del Piano consiste nel facilitare la transizione verso una nuova generazione di servizi di amministrazione digitale aperti e flessibili a livello locale, regionale, nazionale ed europeo. A tale scopo, fra le priorità di azione, sono previsti *l'empowerment* degli utenti, lo sviluppo di servizi inclusivi progettati per rispondere alle esigenze dell'utenza, la produzione collaborativa di servizi (ad esempio con strumenti del *web 2.0*), il riutilizzo di informazioni nel settore pubblico e il coinvolgimento di cittadini e imprese nei processi decisionali (*e-democracy*).

dell'UE per l'*eGovernment* 2016-2020[63], che conferisce centralità ai principi di trasparenza e apertura, declinati nella possibilità di accesso, controllo e correzione dei propri dati da parte degli utenti e nel coinvolgimento delle parti interessate nella progettazione e nella prestazione dei servizi[64].

Nel percorso di genesi americano ed europeo del paradigma di *open government*, alle strategie e alle politiche istituzionali si coniugano i movimenti dal basso tesi ad affermare, da una parte, il diritto all'informazione con l'approvazione e la valorizzazione dei *Freedom of Information Act* e, dall'altra, l'apertura con il suo strumento più caratterizzante costituito dagli *open government data*: tali movimenti si basano e condividono la centralità e il valore dei dati per la crescita economica, culturale e sociale[65].

1.2.2. Politiche di sviluppo e quadro normativo nazionale

Nella direzione dell'*openness* è particolarmente interessante quanto compiuto dall'Italia a livello strategico e normativo[66].

Le strategie di "apertura" si affermano negli ultimi anni, in conformità

---

63 Comunicazione della Commissione europea recante il «*Piano d'azione dell'UE per l'eGovernment 2016-2020. Accelerare la trasformazione digitale della pubblica amministrazione*» - COM(2016) 179 final del 19 aprile 2016.

64 La finalità del Piano consiste nell'accelerare la trasformazione digitale della pubblica amministrazione: a tal fine, prevede, quali priorità strategiche, di modernizzare la pubblica amministrazione con le tecnologie digitali, agevolare la mobilità transfrontaliera con servizi pubblici interoperabili e favorire l'interazione digitale fra amministrazioni e cittadini/imprese per servizi pubblici di qualità. Accanto ad apertura e trasparenza, il Piano prevede tra i principi di base, "digitale per definizione", inclusività e accessibilità, interoperabilità e sicurezza.

65 Cfr. L. SARTORI, *op. cit.*, p. 758 ss.

66 In Italia il termine *open government* si affaccia già nella direttiva 105/2010, *Linee guida per la predisposizione del Programma triennale per la trasparenza e l'integrità,* di CiVIT (Commissione per la Valutazione, la trasparenza e l'integrità delle amministrazioni pubbliche – oggi Anac, Autorità Nazionale Anticorruzione), dove si fa richiamo all'esperienza statunitense: il concetto di accessibilità totale presuppone l'accesso da parte dell'intera collettività a tutte le informazioni pubbliche, secondo il paradigma della "libertà di informazione" dell'*open government* di origine statunitense.

all'esaminato contesto internazionale di riferimento: si innestano e permettono l'evoluzione del modello di amministrazione digitale, cui, a sua volta, sono state dedicate nel corso degli anni, accanto alle norme, strategie che hanno preso forma prima nei piani di azione per l'*e-government* e, più di recente, nell'Agenda digitale italiana, nelle strategie per la banda ultralarga e per la crescita digitale 2014-2020, nel Piano triennale per l'informatica nella pubblica amministrazione 2017-2019[67].

In specifico, in relazione all'affermazione del paradigma dell'*openness* nelle amministrazioni pubbliche, il Governo italiano ha aderito all'iniziativa internazionale *Open Government Partnership* (OGP), promossa nel 2011 e tesa a favorire la trasparenza e l'apertura dei governi attraverso l'*accountability* e la partecipazione attiva dei cittadini, delle associazioni e delle imprese, al fine di creare una cittadinanza attiva e governi più efficaci, aperti e responsabili[68]: nel 2012 l'Italia ha predisposto il suo primo

---

[67] La prima fase inizia nel 2000 ed è caratterizzata dal piano d'azione nazionale per l'*e-government*: dal 2003 comincia la seconda fase, caratterizzata dalla strategia comune tra Stato, Regioni e Autonomie locali «*L'e-government per un federalismo efficiente: una visione condivisa, una realizzazione cooperativa*», per arrivare poi al *Piano e-gov* 2012, presentato nel dicembre 2008. Successivamente l'Agenda digitale italiana viene prevista nell'art. 47 del d.l. 9 febbraio 2012, n. 5, convertito con modificazioni dalla legge 4 aprile 2012, n. 35 (c.d. decreto Semplificazioni) con l'obiettivo di modernizzare i rapporti tra pubbliche amministrazioni, cittadini e imprese attraverso azioni coordinate dirette a favorire lo sviluppo di domanda e offerta di servizi digitali innovativi, potenziare l'offerta di connettività a larga banda, incentivare cittadini e imprese all'utilizzo di servizi digitali e promuovere la crescita di capacità industriali adeguate a sostenere lo sviluppo di prodotti e servizi innovativi. Per il perseguimento degli obiettivi dell'Agenda digitale, la Presidenza del Consiglio, insieme al Ministero dello sviluppo economico, all'Agenzia per l'Italia Digitale e all'Agenzia per la Coesione, ha adottato nel 2015 la «Strategia italiana per la banda ultralarga» e la «Strategia per la crescita digitale 2014-2020»; in tale quadro strategico si inserisce, altresì, l'Agenda per la semplificazione 2015-2017 (prevista dal d.l. 24 giugno 2014, n. 90, convertito con modificazioni dalla legge 11 agosto 2014, n. 114). Il Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, previsto nell'art. 14-bis del d.lgs. 7 marzo 2005, n. 82, introdotto dal d.lgs. 26 agosto 2016, n. 179 e modificato dal d.lgs. 13 dicembre 2017, n. 217, è stato approvato nel maggio 2017 (il sito dedicato è *pianotriennale-ict.italia.it*). Cfr. E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Giornale di diritto amministrativo*, fasc. 2, 2015, p. 148 ss.

[68] Il lancio formale dell'iniziativa è avvenuto nel settembre 2011: in specifico, aderendo all'*Open Government Declaration* gli Stati si sono impegnati ad accrescere la disponibilità delle informazioni pubbliche, supportare la partecipazione, implementare elevati standard d'integrità nella gestione della cosa pubblica e aumentare il ricorso alle nuove tecnologie a fini di apertura e *accountability*.

action plan 2012-2014, che dopo essere stato sottoposto a consultazione pubblica è stato presentato al primo *meeting* di OGP a Brasilia[69]; il secondo piano d'azione 2014-2016 è stato presentato nel dicembre 2014. Il terzo piano d'azione 2016-2018 viene pubblicato il 20 settembre 2016 nella sua versione definitiva, a conclusione dell'attività di consultazione pubblica[70]: per elaborarlo è stato costituito dal Governo il 6 giugno 2016 l'*Open Government Forum*, formato da rappresentanti della società civile, del mondo universitario, delle imprese e delle associazioni di tutela dei consumatori, per garantire un confronto ampio e partecipato sui temi dell'*open government*[71].

Le strategie italiane, in coerenza con gli altri Paesi europei, si caratterizzano nel corso degli anni per il lancio del portale nazionale di *open data* (*dati.gov.it*) e per la realizzazione di una serie di portali istituzionali tematici e territoriali dedicati ai dati aperti, esperienze accompagnate anche da una serie di iniziative civiche "dal basso". L'apertura viene garantita da un movimento duplice e sincrono da parte delle istituzioni e della collettività, pervadendo la relazione tra governanti e governati[72].

Accanto alle politiche di sviluppo dell'*open government*, è particolarmente significativa l'evoluzione normativa, costellata negli ultimi anni dall'approvazione di importanti interventi[73].

---

69 Il primo *meeting* si è svolto a Brasilia il 17 e 18 aprile 2012.

70 La consultazione pubblica si è svolta dal 16 luglio al 31 agosto 2016.

71 Il sito dedicato è *open.gov.it*.

72 L. SARTORI, *op. cit.*, p. 773 ss. «L'efficacia dei meccanismi di Opengov dipende – come tutti i fenomeni complessi e *multistakeholder* – da un insieme di fattori quali l'atteggiamento dei cittadini (più o meno fiducioso), l'esistenza di organismi indipendenti di monitoraggio (tra istituzioni e cittadini), dirigenti pubblici motivati che introducono pratiche innovative, la qualità della pratica democratica e la volontà politica della classe dirigente» (p. 773); «le sue potenzialità sono quindi piuttosto chiare, ma potranno dare i frutti desiderati solo se consapevoli delle facili scorciatoie (scambiare gli Open data per Opengov), degli ostacoli (una tradizionale cultura organizzativa della p.a. unita a una scarsa volontà della classe politica) e delle sinergie necessarie (tra cittadini, imprese, istituzioni e governi)» (p. 775).

73 Al riguardo, cfr. F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, p. 227 ss.: «Le difficoltà applicative del disegno originariamente concepito e più volte manipolato dal legislatore, hanno reso permeabile il modello incompiuto dell'amministrazione digitale verso nuovi paradigmi, che sono stati importati (ed in parte letteralmente trasposti in disposizioni di legge) senza la necessaria meditazione in ordine alla loro compatibilità con il tessuto normativo esistente, con il nostro modello costituzionale di amministrazione e

La normativa in materia di amministrazione digitale e aperta trova indiretta fonte costituzionale nell'art. 97, comma 1, Cost., dal momento che la digitalizzazione e l'*openness* si pongono quali strumenti per garantire il buon andamento della pubblica amministrazione[74].

In materia è considerata come una sorta di vera e propria *Magna Charta* il Codice dell'amministrazione digitale (di seguito anche CAD), il d.lgs. 7 marzo 2005, n. 82[75], oggetto di ripetute modifiche e integrazioni nel corso degli anni, anche molto recenti[76], alcune delle quali particolarmente incisive: è il caso del d.lgs. 4 aprile 2006, n. 159, del d.lgs. 30 dicembre 2010, n. 235 e del d.lgs. 26 agosto 2016, n. 179[77], seguito dal cosiddetto "decreto correttivo", il d.lgs. 13 dicembre 2017, n. 217[78].

---

con le altre leggi fondamentali dell'ordinamento» e, di conseguenza, «sebbene risulti chiaro il ruolo strumentale delle tecnologie rispetto ai principi dell'amministrazione aperta le modalità adesive del governo italiano al programma di *open government* si incentrano soprattutto sull'uso delle tecnologie dell'informazione (*open data*, pubblica amministrazione 2.0 e *government cloud*)».

74 Ai sensi dell'art. 97 C. «*i pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione*». Cfr. E. D'ORLANDO, *op. cit.*, p. 213 ss. e P. OTRANTO, *op. cit.*, p. 105 ss.

75 Il d.lgs. 82/2005 è stato approvato in virtù della delega contenuta nell'art. 10 della legge 29 luglio 2003, n. 229 insieme al d.lgs. 28 febbraio 2005, n. 42 (che ha istituito il sistema pubblico di connettività e la rete internazionale della pubblica amministrazione), abrogato dal d.lgs. 159/2006 e incluso nei suoi contenuti nel d.lgs. 82/2005: il CAD ha acquisito piena centralità come atto di riferimento in materia. Dagli anni '90 fino al 2005, anno di approvazione del CAD, numerose norme si sono occupate di amministrazione digitale, tra le quali la legge 23 ottobre 1992, n. 421 e il d.lgs. 12 febbraio 1993, n. 39, la legge 15 marzo 1997, n. 59 e il d.p.r. 10 novembre 1997, n. 513, il d.p.r. 20 ottobre 1998, n. 428 fino ad arrivare al d.p.r. 28 dicembre 2000, n. 445 e poi al d.lgs. 23 gennaio 2002, n. 10 e al relativo d.p.r. 7 aprile 2003, n. 137.

76 Sono stati oltre venticinque gli interventi normativi di modifica del d.lgs. 82/2005.

77 In merito alla riforma del d.lgs. 235/2010 cfr. E. CARLONI, *La riforma del Codice dell'amministrazione digitale (commento al Decreto legislativo 30 dicembre 2010, n. 235)*, in *Giornale di diritto amministrativo*, fasc. 5, 2011, pp. 469-476. Sulla riforma del d.lgs. 179/2016 cfr. B. CAROTTI, *L'amministrazione digitale. Le sfide culturali e politiche del nuovo Codice (commento al d.lgs. 26 agosto 2016, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 1, 2017, pp. 7-18.

78 Si tratta del decreto legislativo recante disposizioni integrative e correttive al d.lgs. 179/2016, che ha riformato il Codice dell'amministrazione digitale, d.lgs. 82/2005. Nell'iter di approvazione, lo schema di decreto correttivo è stato sottoposto a consultazione pubblica (*open.gov.it/partecipa/consultazioni-attive/consultazione-pubblica-cad-2017/*).

In particolare, nel senso di garantire apertura, dopo la profonda riforma del d.lgs. 235/2010[79], sono state approvate norme rilevanti come il cosiddetto decreto Semplificazioni[80], che ha previsto l'Agenda digitale italiana, e il cosiddetto decreto Sviluppo 2012, contenente significative disposizioni sull'"amministrazione aperta" e sulla *governance* digitale con l'istituzione dell'Agenzia per l'Italia Digitale (AgID)[81]. L'evoluzione normativa verso l'*open government* si è sostanziata poi nelle pervasive modifiche all'amministrazione digitale del cosiddetto decreto Crescita 2.0, che ha fatto entrare nel Codice gli *open data*[82].

L'ultima profonda riforma che ha interessato il CAD, realizzata con la legge delega 7 agosto 2015, n. 124, il relativo d.lgs. 179/2016 e il d.lgs. "correttivo" 217/2017, di recente approvazione, ha previsto tra i criteri ispiratori, accanto ai principi *digital by default* e *digital first*[83], proprio la «*realizzazione di un'amministrazione*

---

79 Al riguardo sia consentito il rinvio a F. FAINI, *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 263-286.

80 D.l. 9 febbraio 2012, n. 5, convertito con modificazioni dalla legge 4 aprile 2012, n. 35.

81 D.l. 22 giugno 2012, n. 83, convertito con modificazioni dalla legge 7 agosto 2012, n. 134. Prima di diventare Agenzia per l'Italia Digitale, l'istituzione ha vissuto diverse riorganizzazioni: con il d.lgs. 39/1993 viene istituita l'Autorità per l'informatica nella Pubblica Amministrazione (AIPA), che diventa il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), ai sensi dell'art. 176 del d.lgs. 30 giugno 2003, n. 196, e successivamente DigitPA, a seguito del riordino avvenuto con d.lgs. 1° dicembre 2009, n. 177.

82 D.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 22; sul provvedimento normativo cfr. L. FIORENTINO (*et al.*), *Il decreto "crescita 2.0" (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 223-264.

83 L' art. 1, comma 1, lett. b), legge 124/2015 prevede la ridefinizione e la semplificazione dei procedimenti amministrativi, in relazione alle esigenze di celerità, certezza dei tempi e trasparenza nei confronti dei cittadini e delle imprese, mediante una disciplina basata sulla loro digitalizzazione e per la piena realizzazione del principio «innanzitutto digitale» (*digital first*). Al riguardo, secondo S. CALZOLAIO, *op. cit.*, p. 194 ss., E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, cit., p. 153 ss. e C. LEONE, *Il principio "digital first": obblighi e diritti in capo all'amministrazione e a tutela del cittadino. Note a margine dell'art. 1 della legge 124 del 2015*, in *GiustAmm.it*, fasc. 6, 2016, p. 1 ss. il principio di *digital first*, che si pone come principio guida del processo di digitalizzazione, si distingue dal principio di esclusività digitale (ossia un vero e proprio *switch off* verso l'esclusivo utilizzo di modalità digitali), da considerare come ipotesi eccezionale che necessita di un'esplicita previsione normativa (è il caso dell'art. 5-bis del d.lgs. 82/2005 che prevede

digitale e aperta»[84], che ha declinato nel rafforzamento dei principi di trasparenza, partecipazione e collaborazione; la riforma espressamente pone come propria finalità principale garantire a cittadini e imprese «*il diritto di accedere a tutti i dati, i documenti e i servizi di loro interesse in modalità digitale*»[85].

Nonostante l'assoluta centralità in materia, l'amministrazione digitale non esaurisce le proprie disposizioni di riferimento nel CAD, ma rilevano ulteriori disposizioni: alcune trasversali, in coerenza con la trasversalità della tematica, come la legge 7 agosto 1990, n. 241 sul procedimento amministrativo e sul diritto di accesso documentale e il d.p.r. 28 dicembre 2000, n. 445 sulla documentazione amministrativa, sul protocollo informatico e sulla gestione dei flussi documentali, altre maggiormente settoriali[86]. I principi giuridici recati dalle norme si realizzano nelle regole di carattere tecnico, fondamentali per l'attuazione delle disposizioni di rango primario[87]: particolarmente significative in tale ambito sono, pertanto, la normazione secondaria e le regole tecniche, che, a seguito delle modifiche introdotte dal d.lgs. 217/2017, saranno costituite da linee guida adottate dall'AgID secondo il procedimento previsto nell'art. 71 del d.lgs. 82/2005, invece che da decreti come è stato finora[88].

---

comunicazioni esclusivamente digitali tra amministrazioni e imprese). Il d.lgs. 217/2017, che ha riformato il d.lgs. 82/2005, ricorre in più occasioni al principio di esclusività digitale e al relativo meccanismo di *switch off*, la cui previsione viene rimessa a specifici d.p.c.m.: è il caso della previsione di comunicazioni esclusivamente digitali tra i soggetti ai quali si applica il CAD e i cittadini (art. 3-bis, comma 3-bis, d.lgs. 82/2005) e dell'utilizzo esclusivo da parte dei soggetti ai quali si applica il CAD delle identità digitali (afferenti al Sistema Pubblico per la gestione delle Identità Digitali di cittadini e imprese - SPID) ai fini dell'identificazione degli utenti dei propri servizi online (art. 64, comma 3-bis, d.lgs. 82/2005).

84 Art. 1, comma 1, lett. n), legge 124/2015.

85 Art. 1, comma 1, legge 124/2015.

86 È il caso ad esempio della normativa dedicata alla posta elettronica certificata (d.p.r. 11 febbraio 2005, n. 68 e relativo d.m. 2 novembre 2005).

87 Cfr. A. MAGGIPINTO, *Amministrazione digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, pp. 283-284.

88 Si pensi alle regole tecniche in materia di firme elettroniche avanzate, qualificate e digitali (d.p.c.m. 22 febbraio 2013, pubblicato in *G.U.* 21 maggio 2013, n. 117), quelle sui documenti informatici (d.p.c.m. 13 novembre 2014, pubblicato in *G.U.* 12 gennaio 2015, n. 8), le regole tecniche per il protocollo informatico e quelle in materia di sistema di conservazione (entrambi d.p.c.m. 3 dicembre 2013, pubblicati in *G.U.* 12 marzo 2014, n. 59). Le regole tecniche restano efficaci fino all'eventuale

In particolare, sotto il profilo dell'*open government*, il Codice dell'amministrazione digitale è integrato dalla normativa sulla trasparenza e, in particolare, dal d.lgs. 14 marzo 2013, n. 33[89]: nell'art. 1 del d.lgs. 33/2013 viene esplicitamente chiarito che la trasparenza concorre alla realizzazione di un'amministrazione aperta, al servizio del cittadino[90].

Il connubio tra trasparenza e digitalizzazione è *in nuce* al concetto stesso di *disclosure*, dal momento che gli strumenti digitali ed in particolare il web, con le sue caratteristiche intrinseche di ubiquità, semplicità e immediatezza nella diffusione, favoriscono ontologicamente la trasparenza.

Questo collegamento tra le due anime emerge particolarmente nell'ultima riforma di riorganizzazione delle pubbliche amministrazioni, recata dalla cosiddetta legge Madia (legge 124/2015), che contiene al suo interno sia la delega alle modifiche e integrazioni del CAD (art. 1), attuata con il d.lgs. 179/2016 e il d.lgs. "correttivo" 217/2017[91], sia la delega alla riforma del d.lgs. 33/2013 (art. 7), attuata con il d.lgs. 25 maggio 2016, n. 97, cosiddetto *Freedom of Information Act* italiano[92].

La connessione tra le due direttrici di riforma della pubblica amministrazione, costituite dalla digitalizzazione e dalla trasparenza, discende dalla centralità assunta dai

---

modifica o abrogazione da parte delle linee guida di cui all'art. 71 d.lgs. 82/2005, come modificato dal d.lgs. 217/2017 (art. 65, comma 10, d.lgs. 217/2017).

89 Il d.lgs. 33/2013 è stato approvato in attuazione della legge 6 novembre 2012, n. 190 (cosiddetta legge Anticorruzione) e ha riordinato le disposizioni in materia di pubblicità, trasparenza e diffusione delle informazioni. Secondo S. CALZOLAIO, *op. cit.*, pp. 190-192 la disciplina sulla trasparenza «non è che la più rilevante e vistosa etero-disciplina dell'amministrazione digitale rispetto al CAD».

90 Cfr. F. CARDARELLI, *op. cit.*, p. 227 ss., che sottolinea come per la prima volta in un testo normativo venga richiamato l'*open government*.

91 L'art. 1 della legge 124/2015 prevede, nel comma 1, la delega al Governo all'adozione di uno o più decreti legislativi, che ha portato all'approvazione del d.lgs. 179/2016, e, nel comma 3, la possibile adozione da parte del Governo, entro 12 mesi, di uno o più decreti legislativi integrativi e correttivi, che ha condotto all'approvazione del d.lgs. 217/2017.

92 Cfr. S. CALZOLAIO, *op. cit.*, p. 185 ss. Al riguardo, secondo F. CARDARELLI, *op. cit.*, p. 227 ss. un «nucleo normativo su cui poggia l'amministrazione digitale si è articolato sulla declinazione positiva ed applicativa del principio di trasparenza».

dati, che a sua volta chiama in causa la protezione e la sicurezza dei dati stessi[93], che non è più disciplinata principalmente dalla normativa italiana (d.lgs. 30 giugno 2003, n. 196), ma vanta oggi la forte tutela europea assicurata dal regolamento (UE) 2016/679[94]. Il processo di digitalizzazione, *disclosure* e apertura realizza, infatti, anche un enorme fenomeno di trattamento di dati[95].

Sotto tale lente, la rilevanza dei dati e dei connessi processi di digitalizzazione e apertura che investono, insieme alla società, le amministrazioni pubbliche, portano più ampiamente a dover volgere l'attenzione all'impatto sulla cittadinanza digitale e sulla tutela dei diritti dei soggetti.

1.3. La cittadinanza digitale e i diritti fondamentali nella rete

L'evoluzione delle tecnologie è capace di cambiare il volto dei protagonisti della società, i paradigmi relazionali e i modelli di governo.

---

93 S. CALZOLAIO, *op. cit.*, p. 189 sottolinea che, in relazione al bilanciamento tra protezione dei dati e trasparenza, «il vero nodo problematico non risiede principalmente nella trasparenza amministrativa dell'informazione in quanto tale, ma nelle infinite potenzialità diffusive tipiche della rete internet (e quindi nelle modalità digitali della trasparenza amministrativa *online*)».

94 Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati): il Regolamento si applica in via diretta dal 25 maggio 2018. Secondo S. CALZOLAIO, *op. cit.*, p. 185 ss. dall'interazione tra i due processi di riforma costituiti da una parte dalla digitalizzazione, dalla semplificazione amministrativa e dalla trasparenza (c.d. legge Madia) e dall'altra dalla protezione e sicurezza dei dati (il nuovo "pacchetto europeo" di protezione dei dati personali) «emerge l'identità costituzionale dell'amministrazione digitale»; pertanto «la digitalizzazione delle amministrazioni pubbliche dell'Unione europea costituisce un processo che incide direttamente sul rapporto di cittadinanza e sulla tutela dei diritti fondamentali dei cittadini dei singoli Stati dell'Unione europea» (p. 186).

95 Per S. CALZOLAIO, *op. cit.*, p. 199 la valutazione di impatto sulla sicurezza e sulla protezione dei dati si configura «non solo come una irrinunciabile garanzia dei diritti individuali dei singoli, ma costituisce condizione di libertà dello Stato e nello Stato».

Le istituzioni diventano digitali, pervase dai concetti di trasparenza e *openness*, capaci di instaurare relazioni orizzontali, basate sulla partecipazione e sulla collaborazione dei cittadini.

Sotto lo sviluppo inarrestabile della realtà digitale, inevitabilmente muta, insieme ai pubblici poteri, il concetto di cittadinanza.

La stessa riforma del Codice dell'amministrazione digitale, recata dalla legge 124/2015, significativamente sceglie per l'art. 1 la rubrica «*Carta della cittadinanza digitale*»[96], che, a seguito delle modifiche del d.lgs. 217/2017, diventa la rubrica anche della sezione II del capo I del d.lgs. 82/2005, dedicata proprio ai diritti[97]. La locuzione vuole richiamare l'evoluzione che interessa il concetto stesso di cittadinanza, che nella realtà digitale non è ancorata in modo rassicurante a un territorio e ai suoi confini, ma si riferisce allo spazio - non spazio di Internet. È una configurazione dinamica come lo è lo sviluppo delle tecnologie e allo stesso tempo è indivisibile nei diritti e nelle libertà che vuole definire, esattamente come inestricabili sono gli intrecci di byte nella società digitale[98]. Si tratta, a ben vedere, più di una nuova dimensione della nostra vita, che si salda fino ad essere indistinguibile dalla cittadinanza "analogica". Di conseguenza, seppur il mancato ancoraggio ai confini territoriali, l'espansione e la pervasività del concetto rendano difficile definirla puntualmente, nel suo nucleo concettuale profondo la cittadinanza digitale identifica la configurazione stessa dei diritti dei cittadini nei confronti delle istituzioni, resa possibile dalle nuove tecnologie[99].

---

96 B. CAROTTI, *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa,* cit., p. 11 sottolinea che in sede di esercizio della delega non è stato definito il concetto di "cittadinanza digitale", su cui si basa la riforma.

97 Prima della riforma recata dal d.lgs. 217/2017 la sezione aveva la rubrica «*Diritti dei cittadini e delle imprese*».

98 Cfr. S. RODOTÀ*, Il diritto di avere diritti*, cit., p. 384 ss., secondo cui l'idea di cittadinanza digitale «è per sua natura dinamica, accompagna la persona nel suo essere nel mondo e, di conseguenza, integra la sua dotazione di diritti tutte le volte che questo suo ampliamento viene sollecitato dall'incessante mutamento prodotto dall'innovazione scientifica e tecnologica, e soprattutto dalle dinamiche sociali che così si determinano» (p. 385). Per l'Autore, inoltre, si assiste ad una indivisibilità dei diritti, dal momento che «i diritti in rete non sono gerarchizzabili, perché è la rete stessa che rifiuta la gerarchie, e così promuove una cittadinanza sempre più "orizzontale"» (p. 394).

99 Cfr. S. RODOTÀ*, Il diritto di avere diritti*, cit., p. 384 ss., secondo cui più ampiamente il tema della cittadinanza digitale, seppur ancora nebuloso, «consente di ricondurre alla persona un insieme di

Il concetto di cittadinanza digitale richiama più ampiamente l'attenzione alla tutela dei diritti e delle libertà nella *digital society*[100].

Al riguardo, fin dagli anni '80, la dottrina parla di una nuova forma di libertà generata dall'impatto delle nuove tecnologie, la "libertà informatica", evoluzione della libertà personale che si connota come una libertà *di* e non solo *da*[101]; tale libertà assume allo stesso tempo, infatti, la connotazione "negativa" come *right to be let alone* e protezione della propria sfera autonoma, ma altresì quella "positiva" e "attiva" quale diritto di controllo relativo alle informazioni e ai dati sulla propria persona. Le tecnologie espandono quindi i confini delle libertà umane: si parla di un diritto all'*habeas data*, sviluppo dell'*habeas corpus*, da cui è originata la libertà personale[102].

L'evoluzione ed espansione del diritto stesso di libertà, frutto delle possibilità inedite consentite dalle tecnologie e composto da un insieme di diritti, si declina in senso individuale e sociale, prende forma in due aspetti che si integrano reciprocamente

---

situazioni che concorrono a definirne la condizione nel cyberspazio». P. MARSOCCI, *op. cit*., p. 12: «Appare chiaro oggi che non si tratta solo di disciplinare un mezzo tecnologico, ma di ripensare i modi di affrontare le grandi politiche pubbliche dove si sperimenta in concreto la capacità di esercitare i diritti civili, politici e sociali».

[100] Sui diritti umani nell'era digitale è interessante la lettura di OXFAM ITALIA (*et al.*), *Realtà virtuale, diritti concreti. Diritti umani nell'Era della Cittadinanza Digitale*, libro-dossier realizzato in occasione del XX Meeting sui diritti umani, 13 dicembre 2016.

[101] Cfr. T.E. FROSINI, *Costituzionalismo 2.0*, in *Rassegna parlamentare*, fasc. 4, 2016, pp. 678-679, che qualifica la cosiddetta libertà informatica come «una pretesa di libertà in senso attivo, non libertà *da* ma libertà *di*, che è quella di valersi degli strumenti informatici per fornire e ottenere informazioni di ogni genere. È il diritto di partecipazione alla società virtuale, che è stata generata dall'avvento degli elaboratori elettronici nella società tecnologica: è una società dai componenti mobili e dalle relazioni dinamiche, in cui ogni individuo partecipante è sovrano nelle sue decisioni».

[102] Questa dicotomia riproduce anche la distinzione fra libertà negative e positive, per le quali cfr. R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, V ed., Cedam, Padova, 2011, p. 1 ss.: «Nella dinamica del progressivo coagularsi di libertà giuridicamente riconosciute e tutelate all'interno delle legislazioni dei singoli Stati non si può prescindere da una scansione concettuale che progressivamente muove dalle cosiddette libertà negative, cioè le libertà *dallo* Stato, consistenti in una sostanziale assenza di divieti, costrizioni o impedimenti, per poi approdare alle libertà positive, che si attuano come libertà *nello* Stato, e consentono la partecipazione attiva alla formazione del potere politico e quindi la traduzione in prassi dei principi di rappresentanza e di cittadinanza».

e trovano entrambi il presupposto necessario nel diritto di accesso a Internet, prodromico alla possibilità di sviluppo degli altri diritti della persona.

L'anima individuale involge il concetto di libertà personale, mentre l'anima "sociale" è maggiormente collegata alla dimensione pubblica e politica dell'uomo, ai nuovi modelli di governo e al processo democratico e, di conseguenza, si traduce nella pretesa soggettiva a prestazioni pubbliche[103]: nelle due anime si innesta anche il concetto di cittadinanza digitale.

La connessione inestricabile tra le due anime di questa nuova libertà permette di rileggere e reinterpretare molti diritti e libertà, alla luce dell'impatto pervasivo delle tecnologie sui diversi aspetti dell'esistenza dell'uomo: di conseguenza, è difficile separare i diversi profili che la compongono[104].

Nella fusione delle due anime che la costituiscono, la libertà informatica si traduce in una sorta di meta-diritto di accesso allo svolgimento della propria esistenza digitale, che condiziona e permette l'esercizio dei diritti individuali e sociali e il rapporto con i pubblici poteri[105]. L'impatto delle tecnologie informatiche riesce a superare la propria essenza ontologica di "strumento", per assurgere a valore che informa l'esercizio dei diritti e delle libertà: non consente soltanto l'esercizio di uno o più diritti legati a una dimensione specifica dell'esistenza, ma permette più ampiamente di svolgere la propria esistenza stessa, quella digitale, parte integrante e sempre più significativa della vita reale[106].

---

103 Cfr. G. PELLERINO, *op. cit.*, p. 255 ss.

104 T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 47 ss.: «rimane altresì problematico separare le diverse libertà per giungere semmai a un modello olistico di libertà: d'altronde, chi accede a Internet si esprime, corrisponde, naviga, si unisce e si riunisce, in forme variabili e lasciate alla scelta individuale. Le diverse libertà vengono quindi esercitate con lo stesso mezzo che è la rete, e nello stesso tempo o in tempi assai ravvicinati» (p. 50); cfr., altresì, S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 384 ss.

105 Cfr. S. RODOTÀ*, Il diritto di avere diritti*, cit., p. 394 ss. e T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 17 ss. *Infra*, cap. 4, § 1.

106 G. SCORZA, *Accedo ergo sum,* in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011, p. 126: «Accedere, nella società dell'informazione, per un cittadino significa esistere. In difetto dell'accesso si è, inesorabilmente e rapidamente, esclusi dall'appartenenza alla comunità globale, privati della possibilità di fruire di esperienze di relazione,

L'accesso alla propria vita digitale è vincolato fortemente non solo dalla possibilità effettiva di poter concretamente accedere a Internet, ma anche dall'azione dei controllori del pedaggio per l'accesso alle autostrade digitali, i colossi del web.

La protezione della libertà informatica e dei diritti digitali si pone come l'unico reale freno alle pretese di potere agite dagli Stati[107] e dai giganti della rete e assurge a questione ineludibile della società contemporanea, per scongiurare il rischio di rimettere la tutela al soggetto stesso, parte debole nel rapporto sia con gli uni che con gli altri[108].

Nella difficile regolazione dovuta al travalicamento dei confini territoriali e alla necessità di nuove forme di tutela il rischio è che i poteri pubblici "si voltino dall'altra parte", lasciando campo libero alle forze del mercato[109]. Il pericolo concreto della *digital society* consiste, dunque, nella possibilità che i poteri pubblici abdichino alla protezione di diritti e libertà, indulgendo nella quotidianità alla possibilità della loro violazione e lasciando al singolo e alla sua consapevolezza la capacità e la forza di proteggersi. L'individuo si trova in una condizione di apparente libertà, dovendo mettere in campo continuamente un supplemento di attenzione, preoccupazione, strumentazione e azione, senza poter abbassare la guardia e fruire con semplicità delle prerogative della propria esistenza digitale[110]. L'eventuale rinuncia dei poteri pubblici a

---

mercato e politica e, soprattutto, dell'esercizio di ogni diritto e libertà che abbia, per presupposto, l'interazione con lo Stato o con gli altri membri della comunità di appartenenza».

[107] Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 378 ss., secondo cui, anche se gli Stati hanno la pretesa aggressiva di far valere le proprie prerogative anche su Internet, «non possono stabilire una sovranità sul cyberspazio» (p. 379).

[108] Secondo S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 3 ss. la lotta per i diritti «si presenta come la sola in grado di contrapporsi alla volontà di imporre al mondo una nuova e invincibile legge naturale, quella del mercato, con la sua pretesa di incorporare e definire anche le condizioni per il riconoscimento dei diritti» (pp. 7-8).

[109] S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 3: «Diritti senza terra vagano nel mondo globale alla ricerca di un costituzionalismo anch'esso globale che offra loro ancoraggio e garanzia. Orfani di un territorio che dava loro radici e affidava alla sovranità nazionale la loro concreta tutela, sembrano ora dissolversi in un mondo senza confini dove sono all'opera poteri che appaiono non controllabili».

[110] Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 398 ss., che sottolinea il supplemento di azioni richieste al soggetto, come le tecniche di *opting-out*, che «affidano la garanzia dei dati personali alla sola vigilanza dell'interessato, tenuto a una interminata serie di atti difensivi, mentre dall'altra parte i signori delle informazioni, già in condizione di esercitare sugli utenti varie forme di pressione, possono limitarsi

svolgere la loro stessa funzione si traduce in una sconfitta in campo digitale e nel rischio di una sorta di privatizzazione della rete, dominata dalla regola del più forte e caratterizzata dall'atmosfera fosca del tramonto dell'età dei diritti[111].

Finisce per sbiadire il confine e la distinzione tra la dimensione pubblica sovrana e quella privata degli interessi particolari; la realtà digitale rischia di diventare il territorio del dominio dei *big player* e il mondo della solitudine reale di individui deboli e indeboliti, lasciati soli dall'incapacità dei pubblici poteri di difenderli.

Di conseguenza, anche se può risultare difficile definire puntualmente i concetti di libertà informatica e di cittadinanza digitale, è semplice trovare l'aggettivo che deve accompagnarli: si tratta di una dimensione "costituzionale", in quanto riguarda diritti e libertà; in considerazione dei rischi appena esaminati, garantire i diritti e le libertà nel ciberspazio costituisce la sfida costituzionale del nostro tempo[112].

Pertanto l'espressione, lo sviluppo e la tutela delle libertà e dei diritti e della connessa cittadinanza nella società tecnologica richiama necessariamente la Costituzione "specchio e sintesi della società"[113], atto fondamentale propriamente teso a

---

a una attesa che consente loro di beneficiare di una situazione che, per ragioni di tempo o di insufficiente informazione, induce alla passività» (pp. 399-400).

111 Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 2 ss.

112 Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 413 ss.: «La rete ha cambiato la società, ma è quest'ultima che agisce per determinarne le modalità di funzionamento, e dunque essa stessa cambia la rete» (p. 414). Cfr. T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 673 ss., che reputa il costituzionalismo come un «plebiscito che si rinnova ogni giorno: perché sviluppa nuove forme di valorizzazione e di tutela della libertà dell'individuo. La sfida che nel Ventunesimo secolo attende il costituzionalismo è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica e i suoi derivati in punto di diritto» (p. 675); l'Autore si riferisce a questo costituzionalismo digitale con il termine di "costituzionalismo 2.0" e ritiene che nel ventunesimo secolo si stagli l'«orizzonte giuridico dell'Internet», di cui parlava V. FROSINI, *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2000, p. 271 ss. Per tali motivi secondo T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 16 «si deve ingaggiare una lotta per il diritto di libertà a Internet. Ecco perché oggi il motto e la missione è: *Liberté*, *Egalité*, *Internet*».

113 Così T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 677.

fornire tutela ai diritti e alle libertà, che dispone al più alto grado in merito ai principi fondamentali, ai diritti e ai doveri dei cittadini e alla divisione dei poteri[114].

1.3.1. Le Carte costituzionali e le Carte dei diritti di Internet: il contesto internazionale e il caso italiano

Nella riflessione costituzionale che riguarda Internet e, più ampiamente, la realtà digitale rilevano le caratteristiche della rete stessa, in particolare l'approccio decentrato e il superamento delle barriere geografiche, che conducono alla necessità di soluzioni sovranazionali adatte alla nuova dimensione globale di riferimento[115].

Sotto tale profilo non sono mancate le teorie che qualificano Internet come ordinamento giuridico autonomo: è il caso della «*Declaration of Independence of Cyberspace*» di John Perry Barlow del 1996[116]. La rete viene interpretata come uno spazio spontaneo e libertario dotato della regolazione offerta dalla *lex informatica*, basata sulla *self-regulation* degli utenti e sulla *co-regulation* tra gli Stati[117].

---

114 Cfr. T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 673 ss., che, tra le tante, reputa maggiormente convincente la definizione del costituzionalismo come "tecnica della libertà" «che si declina nella separazione dei poteri, nelle garanzie costituzionali e nella tutela dei diritti fondamentali, che sono, infatti, delle tecniche per l'affermazione della libertà dell'individuo, ovvero rappresentano il modo attraverso il quale svolgere una continua ricerca sul come affermare e garantire il diritto di libertà individuale» (p. 673).

115 S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 7 parla di un «nuovo costituzionalismo, che porta in primo piano la materialità delle situazioni e dei bisogni, che individua nuove forme dei legami tra le persone e le proietta su una scala diversa da quelle che abbiamo finora conosciuto».

116 Sulla libertà e autonomia di Internet si esprime in modo efficace la Dichiarazione fin dal suo *incipit*: «Governi del mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo»; cfr. *www.eff.org/cyberspace-independence*.

117 Cfr. T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 79 ss. e S. RODOTÀ*, Il diritto di avere diritti*, cit., p. 378 ss. Sulla *co-regulation* cfr. L. LESSIG*, Code and Other Law of Cyberspace*, Basic Books, New York, 1999.

Seppur non sia condivisibile la soluzione di uno spazio di diritto e di una conseguente struttura giuridica autonoma di Internet per la sua intrinseca debolezza anche teorica, indubbiamente le caratteristiche della rete pongono il problema della capacità dei singoli ordinamenti di regolare diritti e libertà, che nella *digital society* per essere efficacemente tutelati hanno bisogno di soluzioni di dimensione globale.

Tale constatazione porta a volgere lo sguardo agli atti sovranazionali, capaci di produrre effetti sui diversi Stati e guidare l'interpretazione delle norme, per comprendere se ci siano significativi riferimenti idonei a offrire fondamento alle nuove libertà e all'ampliamento di quelle esistenti.

Sotto la lente delle libertà digitali, a livello internazionale, la Dichiarazione universale dei diritti umani, adottata dalle Nazioni Unite il 10 dicembre 1948, descrive il diritto di libertà alla manifestazione del pensiero come diritto di «*cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere*» (art. 19), con una qualificazione che si adatta anche alla società tecnologica; la Dichiarazione pone attenzione, altresì, alla tutela della riservatezza dell'individuo (art. 12). Nello stesso senso rileva l'art. 19 del Patto internazionale sui diritti civili e politici, adottato dalle Nazioni Unite il 19 dicembre 1966 ed entrato in vigore nel 1976[118]. La conferma di tale interpretazione evolutiva viene dal richiamo fatto a questi atti dal Consiglio per i diritti umani delle Nazioni Unite (Unhrc) nel Rapporto Frank La Rue presentato nel 2011 e in una risoluzione del 2012[119]: Internet è qualificato come condizione necessaria e strumento fondamentale per garantire il pieno esercizio della libertà di espressione e degli altri diritti fondamentali[120].

In senso analogo, la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 4 novembre 1950, successivamente modificata

---

[118] L'art. 19 prevede una libertà di espressione «*senza riguardo a frontiere*», attraverso qualsiasi mezzo a scelta dell'individuo.

[119] «*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*», presentato all'Assemblea generale Onu il 16 maggio 2011 e «*The promotion, protection and enjoyment of human rights on the Internet*», 29 giugno 2012.

[120] Cfr. L. CUOCOLO, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, fasc. 2-3, 2012, p. 263 ss., secondo cui il Rapporto ONU non qualifica mai l'accesso a Internet come diritto umano in sé considerato, ma ritiene l'utilizzo della rete strumentale all'esercizio di diritti umani.

e ampliata, parla di libertà di espressione «*senza limiti di frontiera*», che può essere sottoposta solo alle limitazioni legali necessarie, in una società democratica, a proteggere una serie di interessi tutelati (art. 10); la Corte europea ha affermato più volte che tale libertà deve essere tutelata anche in Internet e nella realtà digitale[121].

Nella Carta dei diritti fondamentali dell'Unione europea[122], altresì, trovano spazio alcuni principi e diritti che possono costituire fondamento a livello interpretativo delle libertà dell'era digitale, quali lo sviluppo della dignità umana, la protezione dei dati personali e la libertà di espressione e informazione[123].

La necessità di tutelare diritti e libertà nella società tecnologica viene espressa dall'Europa anche attraverso atti, risoluzioni e raccomandazioni: l'Unione europea nel 2006 ha affermato il ruolo di Internet per esercitare la libertà di espressione, rafforzare la democrazia e contribuire allo sviluppo economico e sociale[124], nel 2008 ha riconosciuto l'impatto di Internet sui diritti dell'uomo[125] e nel 2009 ha chiarito la necessità di un «*rafforzamento della sicurezza e delle libertà fondamentali su Internet*», che «*dà pieno significato alla libertà di espressione*», sancita dall'art. 11 della Carta di Nizza[126].

---

121 In modo esemplificativo si pensi alla sentenza della Corte europea dei diritti dell'uomo *Yldirim v. Turchia* del 18 dicembre 2012, ricorso n. 3111/10, che ha constatato la violazione dell'art. 10 della Convenzione da parte della Turchia nell'oscuramento di un sito web.

122 La Carta, proclamata nel 2000 a Nizza, è divenuta giuridicamente vincolante in occasione dell'entrata in vigore nel 2009 del Trattato di Lisbona del 2007, che nell'art. 6 le ha attribuito lo stesso valore dei Trattati.

123 La dignità umana è qualificata come valore inviolabile e quindi fondamentale canone interpretativo (art. 1), la protezione dei dati di carattere personale si configura quale diritto autonomo e "dinamico" (art. 8), separato da quello al rispetto della propria vita privata e familiare (di cui all'art. 7), e la libertà di espressione e d'informazione viene connotata «*senza limiti di frontiera*» (art. 11).

124 Risoluzione del Parlamento europeo del 6 luglio 2006 sulla libertà di espressione su Internet.

125 Risoluzione del Parlamento europeo del 10 aprile 2008 su un'agenda europea per la cultura in un mondo in via di globalizzazione.

126 Raccomandazione del Parlamento europeo del 26 marzo 2009 sul rafforzamento della sicurezza e delle libertà fondamentali su Internet. Cfr. F. BADOCCO, *Riflessioni sul diritto di accesso a Internet nell'ambito del diritto dell'Unione europea*, in *Informatica e diritto*, fasc. 1, 2009, p. 153 ss. e T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 47 ss.

Nell'*incipit* della «*Guida dei diritti umani per gli utenti di Internet*» del 2014, l'Europa chiarisce che gli Stati sono tenuti a garantire a ogni persona i diritti umani e le libertà fondamentali sanciti dalla Convenzione europea dei diritti dell'uomo: tale obbligo vale anche nel contesto di Internet, al quale si applicano, altresì, le altre convenzioni e gli altri strumenti europei di tutela dei diritti; di conseguenza, i diritti umani e le libertà fondamentali devono trovare applicazione in egual misura online e offline, con la conseguente necessità di aiutare gli utenti a comprendere i diritti di cui godono e ad esercitarli effettivamente[127].

Degni di attenzione anche gli atti europei relativi alle comunicazioni elettroniche[128] e, di recente, il regolamento UE 2015/2120 del 25 novembre 2015, la cui applicazione, tranne eccezioni, decorre dal 30 aprile 2016. Il regolamento UE 2015/2120 stabilisce misure riguardanti «*l'accesso a un'Internet aperta*» e disciplina il principio di neutralità della rete: in specifico, come precisato nel primo considerando, «*mira a definire norme comuni per garantire un trattamento equo e non discriminatorio del traffico nella fornitura dei servizi di accesso a Internet e tutelare i relativi diritti degli utenti finali*»[129].

Pertanto sulle libertà nel ciberspazio non mancano riferimenti sovranazionali importanti, ma l'incapacità attuale a regolare da soli i diritti degli individui lascia alle Carte costituzionali, ancora oggi, il ruolo di atto fondamentale che regola la vita negli

---

127 Raccomandazione CM/Rec(2014)6 del Comitato dei Ministri agli Stati membri, adottata il 16 aprile 2014, che riconosce il valore di servizio pubblico a Internet e disciplina nel suo allegato diritti e libertà costituzionali, affrontando le seguenti tematiche: accesso e non discriminazione; libertà di espressione e di informazione; riunione, associazione e partecipazione; protezione della vita privata e dei dati personali; istruzione e conoscenze generali; bambini e giovani; vie di ricorso effettive.

128 In specifico, il "pacchetto" di direttive europee del 2002 (direttiva "accesso" 2002/19/CE, direttiva "autorizzazioni" 2002/20/CE, direttiva "quadro" 2002/21/CE e direttiva "servizio universale" 2002/22/CE) e il c.d. "Pacchetto Telecom" del 2009.

129 Il regolamento 2015/2120 del 25 novembre 2015, modificando la direttiva 2002/22/CE e il reg. 531/2012, è teso a riconoscere e a salvaguardare agli utenti finali l'accesso a informazioni e contenuti e la loro diffusione, nonché l'utilizzo e la fornitura di applicazioni e servizi e l'utilizzo di apparecchiature terminali di loro scelta, indipendentemente dalla sede o dalla localizzazione, dall'origine o dalla destinazione, tramite il servizio di accesso a Internet (art. 3).

Stati e porta, di conseguenza, al loro esame per trovare fondamento ai nuovi diritti e libertà[130].

Nella configurazione della libertà informatica e della cittadinanza digitale, l'interrogativo che emerge è se le tecnologie siano capaci di creare nuovi diritti e libertà o se siano strumento ed espansione di diritti e libertà esistenti e, in modo correlato e conseguente, se sia necessario intervenire sulle Costituzioni integrandole con nuove disposizioni o se sia sufficiente l'interpretazione ermeneutica di quelle esistenti[131].

In una prospettiva comparata, coerente col carattere globale della rete, sono diverse le risposte che gli Stati odierni danno agli interrogativi posti dalla società tecnologica, anche in considerazione del momento di emanazione delle relative Carte costituzionali[132].

---

130 Cfr. M. CUNIBERTI, *La libertà della comunicazione nello scenario della convergenza*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, Milano, 2008, p. 18. Secondo P. MARSOCCI, *op. cit.*, p. 3 «anche se la Rete mal sopporta la regolamentazione riferita allo spazio, inteso come territorio, che invece è la principale *ambizione* delle Costituzioni, questo non vuol dire che i diversi tentativi di organizzare una sua *governance* si pongano in contrapposizione con i sistemi costituzionali» e, di conseguenza, «la regolamentazione dell'uso della Rete resta un tema di diritto costituzionale costituito e non coinvolge (e travolge) la legittimazione stessa delle Costituzioni». Secondo F. AMORETTI - E. GARGIULO, *Dall'appartenenza materiale all'appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, in *Politica del diritto*, fasc. 3, 2010, pp. 353-389 «le costituzioni sovrastatali non sono ancora riuscite, di fatto, a vincolare gli attori statali al rispetto dei diritti fondamentali delle *persone*. La condizione di cittadino è rimasta la via d'accesso privilegiata, se non unica, a tali diritti».

131 La presente analisi del contesto costituzionale internazionale e italiano muove dalle riflessioni contenute in F. FAINI, *Diritti digitali. Libertà costituzionali e tecnologie informatiche*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 67-110.

132 Sul rapporto tra libertà costituzionali e tecnologie informatiche si rinvia alla vastissima dottrina in materia: cfr., *inter alia*, T.E. FROSINI - O. POLLICINO - E. APA - M. BASSINI (a cura di), *Diritti e libertà in Internet*, Mondadori education - Le Monnier Università, Milano, 2017; M.R. ALLEGRI, *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a internet (o al ciberspazio?)*, in *Rivista AIC*, fasc. 1, 2016, p. 1 ss.; G. AZZARITI, *op. cit.*, p. 1 ss.; P. COSTANZO, voce *Internet (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, IV ed., Appendice, Utet, Torino, 2000, p. 347 ss.; P. COSTANZO, *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, in *Consulta OnLine*, 2012, p. 1 ss.; G. DE MINICO, *Diritti, Regole, Internet*, in *Costituzionalismo.it*, fasc. 2, 2011, p. 1 ss.; E. D'ORLANDO, *op. cit.*, p. 213 ss.; T.E. FROSINI, *Liberté, Egalité, Internet*, cit.; L. NANNIPIERI, *Costituzione*

Le Costituzioni maggiormente recenti hanno potuto assorbire l'impatto delle tecnologie e alludere o prevedere questa nuova libertà, mentre le Costituzioni anteriori alla rivoluzione digitale hanno dovuto tutelare la nuova realtà per mezzo dell'introduzione di nuove norme o per mezzo di un'interpretazione evolutiva di quelle esistenti, talvolta accompagnata da previsioni contenute in leggi che disciplinano esplicitamente i diritti.

Tra le Costituzioni recenti o di recente modifica, che si riferiscono all'*habeas data* e alle libertà digitali, si spazia dalle Carte costituzionali dell'America Latina, come Brasile[133], Paraguay[134], Venezuela[135], Ecuador[136] e Messico[137], alla Costituzione della Federazione di Russia del 1993, a quella della Repubblica del Sudafrica del 1996[138] fino

---

e nuove tecnologie: profili costituzionali dell'accesso ad Internet, in *www.gruppodipisa.it*, 2013; M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011; O. POLLICINO - E. BERTOLINI - V. LUBELLO (a cura di), *Internet: regole e tutela dei diritti fondamentali*, Aracne, Roma, 2013; S. RODOTÀ, *Una Costituzione per Internet?*, in F. AMORETTI (a cura di), *Diritti e sfera pubblica nell'era digitale,* numero speciale in *Politica del diritto,* fasc. 3, 2010, p. 337 ss.; S. RODOTÀ, *Il diritto di avere diritti*, cit.

[133] La Costituzione della Repubblica Federale del Brasile del 1988, come successivamente riformata, disciplina l'*habeas data* nell'art. 5, comma 72.

[134] La Costituzione della Repubblica del Paraguay del 1992 disciplina il diritto di accesso agli strumenti elettronici e gli aspetti fondamentali dell'*habeas data* negli artt. 30, 33 e 135.

[135] La Costituzione della Repubblica Bolivariana del Venezuela del 1999 nell'art. 28 tratta di diritto di accesso alle informazioni e ai dati, che riguardano il soggetto o comunità e gruppi di persone, e nell'art. 108 prevede l'impegno dello Stato a garantire, anche attraverso reti informatiche, l'accesso universale all'informazione.

[136] La Costituzione ecuadoreña del 2008 prevede il diritto di «accesso universale alle tecnologie dell'informazione e della comunicazione» in capo a tutte le persone, individualmente e collettivamente, anche in chiave partecipativa (art. 16); la disposizione è seguita da altre di maggior dettaglio, gli artt. 17 e 18.

[137] La legge di revisione costituzionale dell'11 giugno 2013 ha integrato l'art. 6 della Costituzione messicana con nuovi commi che, prevedendo il diritto in capo a tutti di accedere liberamente alle informazioni attraverso qualsiasi mezzo, impongono allo Stato di garantire il diritto di accesso alle tecnologie di informazione e comunicazione, incluso Internet in banda larga. Sulle Costituzioni dell'America Latina, cfr. T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 17 ss.

[138] Nella Costituzione russa rilevano gli artt. 23, 24 e 29 e nella Costituzione del Sudafrica rileva il combinato disposto degli artt. 14 (privacy), 16 (libertà di espressione) e 32 (accesso all'informazione).

all'Europa, con la Costituzione portoghese[139], la Costituzione spagnola[140], la Costituzione della Svizzera del 1999[141] e la revisione costituzionale del 2001 in Grecia[142]. Altri Paesi hanno preferito esplicitare in legge diritti legati alle nuove tecnologie, come l'Estonia[143], la Finlandia[144] e, anche, la Spagna[145]. Nel contesto internazionale assume grande rilevanza il *Marco Civil* approvato nel 2014 in Brasile, *Magna Charta* dei diritti e doveri dei cittadini in rete[146].

Diversamente, altri ordinamenti regolati da Costituzioni risalenti a un'epoca antecedente alla rivoluzione digitale, per offrire tutela alla libertà informatica si sono affidati all'interpretazione evolutiva delle norme esistenti. In proposito sono significative la sentenza americana della Corte Suprema U.S. del 1997, *Reno v. American Civil Liberties Union* (ALCU)[147] e la decisione del *Conseil Constitutionnel*

---

139 Nella Costituzione portoghese rileva l'art. 35, che allude alla libertà informatica.

140 Nella Costituzione spagnola del 1978 l'art. 18, comma 4, dispone la previsione di limiti da parte della legge all'uso dell'informatica per salvaguardare il diritto all'onore e all'intimità, personale e familiare, e il pieno esercizio dei diritti dei cittadini.

141 Nella Costituzione Federale della Confederazione Svizzera rilevano gli artt. 13 (protezione della sfera privata), 16 (libertà d'opinione e d'informazione) e 17 (libertà dei media).

142 L'art. 5a della Costituzione greca prevede il diritto di accesso alla rete e un corrispettivo esplicito obbligo a carico dei pubblici poteri di garantirne l'effettiva realizzazione.

143 Il *Telecommunications Act* del 9 febbraio 2000, in particolare l'articolo 5, ha posto il diritto a Internet fra gli obblighi di servizio universale, da garantire a tutti, a prescindere dalla posizione geografica e «a un prezzo uniforme». L'Estonia è anche il Paese che ha sperimentato e fatto ampio ricorso all'utilizzo della rete per le operazioni di voto.

144 Rilevano il *Communications Market Act* (393/2003) e il decreto 732/2009, in vigore dal 1° luglio 2010. La Finlandia prevede il diritto legale di accesso a Internet, ritenendo diritto elementare una connessione a banda larga di alta qualità a un prezzo ragionevole e impegnando i fornitori a garantire una velocità di *download* di almeno un *megabit* al secondo.

145 La *Ley de Economía sostenible* n. 2/2011 collega l'accesso a Internet al concetto di servizio universale e la *Ley* n. 9/2014, *General de Telecomunicaciones*, pone la banda larga tra gli obblighi del servizio universale, garantendo a ogni cittadino una connessione minima da un *megabit* al secondo.

146 *Infra*, più avanti in questo paragrafo. Cfr. M.R. ALLEGRI, *op. cit.*, che accanto al *Marco Civil* ricorda il caso di un altro *Internet Bill of Rights*, approvato dalle Filippine nel 2013, la *Magna Charta for Philippine Internet Freedom, Cybercrime Prevention and Law Enforcement, Cyberdefense and National Cybersecurity*.

147 Cfr. S.C. U.S., *Reno*, *Attorney General of the United States*, *et al.* v. *American Civil Liberties Union et al.*, no. 96-511, *Argued March* 19, 1997 - *Decided June* 26, 1997. La sentenza ha dichiarato

francese del 2009[148], richiamata espressamente dalla *Sala Constitucional de la Corte Suprema de Justicia* della Costa Rica nella sentenza n. 12790 del 30 luglio 2010[149].

Nel variegato quadro internazionale relativo al rapporto tra libertà costituzionali e realtà digitale, si pone la Costituzione italiana, che non contiene riferimenti espliciti alle tecnologie informatiche e a Internet, dal momento che la sua emanazione si colloca in un momento antecedente alla rivoluzione digitale e le revisioni costituzionali non hanno toccato il profilo. Di conseguenza, si pone anche per la Carta fondamentale del nostro Paese il quesito se sia necessaria la previsione di nuovi diritti e libertà e, quindi, nuove norme o sia sufficiente l'interpretazione evolutiva delle disposizioni e delle statuite libertà.

Al riguardo è intenso il dibattito dottrinale, accompagnato anche da alcuni significativi disegni di riforma costituzionale. La riflessione si concentra in modo

---

incostituzionale per contrasto con il primo emendamento della Costituzione degli Stati Uniti il *Communication Defency Act* del 1996, che vietava i contenuti di carattere indecente su Internet. La Corte Suprema collega le tecnologie informatiche all'esercizio delle libertà fondamentali, riconosce Internet «quale mezzo di comunicazione umana a livello mondiale unico e assolutamente nuovo», capace di accrescere le libertà, e ritiene che «l'interesse a stimolare la libertà di espressione in una società democratica è superiore a qualunque preteso, non dimostrato, beneficio della censura».

148 La sentenza del *Conseil Constitutionnel* francese n. 2009-580 DC del 10 giugno 2009 riguardava il controllo preventivo di legittimità costituzionale della legge *Création et Internet*, cosiddetta legge *Hadopi* (dal nome dell'Autorità amministrativa istituita dalla legge stessa, ossia la *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*), che, in caso di reiterate violazioni dei diritti di proprietà intellettuale, prevedeva un meccanismo sanzionatorio, in particolare la disconnessione forzata da Internet, a seguito di una decisione dell'autorità amministrativa e senza nessun controllo giurisdizionale, rimettendo a un soggetto amministrativo un ampio margine di apprezzamento in merito alla restrizione di diritti fondamentali. La sentenza, nel dichiarare incostituzionale la legge in diversi aspetti, individua l'accesso a Internet quale presupposto della libertà di comunicazione e di espressione, richiamando con interpretazione evolutiva l'art. 11 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789. Secondo L. CUOCOLO, *op. cit.*, p. 273 ss. non è chiaro se nella sentenza il diritto di accesso a Internet sia considerato come diritto in sé oppure come situazione giuridica che va protetta in quanto funzionale all'esercizio della libertà di comunicazione.

149 La sentenza designa Internet quale presupposto e strumento primario per agevolare l'esercizio dei diritti fondamentali relativi alla sfera privata e pubblica e, di conseguenza, si spinge a richiedere ai governanti di promuovere e garantire in forma universale l'accesso alle tecnologie. La sentenza riconosce nell'accesso a Internet un diritto fondamentale; cfr. L. CUOCOLO, *op. cit.*, p. 275.

particolare sul diritto di accesso a Internet, presupposto necessario per svolgere in rete tutti gli altri diritti, ma non ha mancato di espandersi anche a tutte le altre libertà che la rete genera o consente di esercitare in modo diverso.

Da una parte c'è chi ritiene sufficiente l'interpretazione della Carta costituzionale e dei diritti ivi previsti per dare fondamento alle nuove libertà.

A sostegno di tale tesi, in un approccio più risalente nel tempo, si richiamano l'art. 15 Cost., relativo alla libertà e alla segretezza della corrispondenza, e il primo comma dell'art. 21 Cost., che prevede la libertà di espressione con «*ogni mezzo di diffusione*», comma interpretato evolutivamente come diritto passivo e attivo, libertà non solo *di* informazione, ma *alla* informazione[150], che presuppone la possibilità di accedere a Internet per poter essere esercitata pienamente[151].

Tale interpretazione però finisce per equiparare le tecnologie informatiche a mezzo di comunicazione teso a garantire la libertà di espressione e informazione, in una configurazione limitata rispetto alle reali possibilità, che più ampiamente involgono una serie di attività umane che trovano il collante nell'esercizio della libertà individuale, nello sviluppo della persona e nell'effettiva partecipazione alla vita politica, economica

---

150 Cfr., *inter alia*, sentenze Corte cost., 15 giugno 1972, n. 105 e Corte cost., 30 maggio 1977, n. 94. Più ampiamente cfr. D. MULA, *Libertà di manifestazione del pensiero in rete*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, p. 1 ss. e P. OTRANTO, *op. cit.*, p. 19 ss.

151 L'art. 15 Cost. si riferisce a una comunicazione interpersonale rivolta a un numero di soggetti determinati, a differenza dell'art. 21 Cost. relativo all'informazione a destinatari illimitati o comunque non identificabili; P. PASSAGLIA, *Internet nella Costituzione italiana: considerazioni introduttive*, in *Consulta OnLine*, 2013, p. 10 rileva come Internet consenta un tipo di comunicazione diversa: mentre l'art. 15 si riferisce ad un'interazione "uno a uno" e l'art. 21 a un modello comunicativo "uno a molti", Internet si basa sul paradigma della comunicazione "molti a molti". La ricostruzione del diritto di accesso in seno agli artt. 15 e 21 Cost. afferisce alle prime riflessioni negli anni '90; cfr. A. VALASTRO, *Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011, p. 45 ss.

e sociale. Il diritto di accesso a Internet, strumentale all'esercizio di tutti gli altri[152], configura al tempo stesso un diritto della persona afferente alla sfera privata, che permette l'esercizio della propria libertà di manifestazione del pensiero, ma anche un diritto sociale relativo alla sfera pubblica, quale pretesa soggettiva a prestazioni a carico dello Stato per esercitare la propria cittadinanza digitale, dotata di chiaro impatto sul funzionamento del sistema democratico stesso; si configura, insomma, come un servizio universale da garantire per permettere a ciascuno di sviluppare la propria personalità, svolgere la propria esistenza digitale ed esercitare i diritti e le libertà costituzionalmente tutelati[153].

A ben vedere la realtà digitale finisce per riguardare lo svolgimento della propria personalità e l'impianto intero dei diritti e delle libertà della Costituzione[154].

Sotto tale lente, di conseguenza, parte della dottrina condivisibilmente fonda i nuovi diritti collegati alle tecnologie informatiche sui principi fondamentali della nostra Carta costituzionale, contenuti nei primi articoli, e, in particolare, l'art. 2, che richiama il concetto ampio di "svolgimento della personalità" sia come singolo, sia nelle formazioni sociali[155], e l'art. 3, che tutela «*il pieno sviluppo della persona umana*», la

---

[152] Al riguardo, P. MARSOCCI, *op. cit.*, p. 2 distingue, seppur logicamente connessi, il tema dell'esercizio dei diritti nel ciberspazio da quello dell'accesso a Internet, relativo alla natura di tale posizione soggettiva e della sua conseguente protezione.

[153] Cfr., *inter alia*, M. BETZU, *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista AIC*, fasc. 4, 2012, p. 1 ss.; G. DE MINICO, *Diritti, Regole, Internet*, cit., p. 1 ss.; T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 11 ss.; L. NANNIPIERI, *op. cit.*, p. 1 ss.; A. VALASTRO, *op. cit.*, p. 45 ss.

[154] Cfr. P. PASSAGLIA, *Internet nella Costituzione italiana: considerazioni introduttive*, cit., p. 12 e P. PASSAGLIA, *Diritto di accesso a Internet e giustizia costituzionale. Una (preliminare) indagine comparata*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli - Roma, 2011, p. 59 ss., secondo cui condivisibilmente «l'accesso ad Internet prescinde da ogni specifico interesse, per il semplice fatto che l'interesse è presupposto della stessa configurazione di Internet come sede di estrinsecazione della personalità. Più che di un *interesse all'accesso*, dunque, nel caso di Internet può parlarsi di un *accesso all'interesse*, cioè di un accesso rivolto a realizzare un interesse, quale è quello dello sviluppo della propria personalità nella dimensione ulteriore offerta dalla rete».

[155] «*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale*».

«*pari dignità sociale*» e l'uguaglianza non solo formale, ma sostanziale (2° comma), richiamando i poteri pubblici a rimuovere gli ostacoli di ordine economico e sociale (si pensi nel contesto del ciberspazio al *digital divide*)[156]; la rete consente anche forme inedite di esercizio della sovranità popolare, di cui all'art. 1 C.[157].

Attraverso l'interpretazione evolutiva degli artt. 2 e 3 della Costituzione è possibile includere le molteplici libertà coinvolte dalle tecnologie informatiche, libertà di carattere personale, sociale e politico, previste negli altri articoli della Costituzione[158]. Inoltre sui concetti di dignità umana e sviluppo della persona, quali fondamentali canoni interpretativi scaturenti dai primi articoli della Costituzione[159], anche in combinato

---

[156] La Repubblica ha il compito di «*rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese*». Cfr., *inter alia*, G. DE MINICO, *Diritti, Regole, Internet*, cit.; T.E. FROSINI, *Liberté, Egalité, Internet*, cit.; P. MARSOCCI, *op. cit.*, p. 8 ss.; L. NANNIPIERI, *op. cit.*; R. RAZZANTE, *op. cit.*, p. 1 ss.; A. ROSSETTI, *È necessario il diritto all'accesso alla rete?*, in M. PIETRANGELO (a cura di), *op. cit.*, p. 89 ss.; A. VALASTRO, *op. cit.*, p. 45 ss.; P. PASSAGLIA, *Internet nella Costituzione italiana: considerazioni introduttive*, cit., p. 27 ss., che propone la ricostruzione della comunità degli utenti di Internet quale formazione sociale ai sensi dell'art. 2 Cost.

[157] In merito P. MARSOCCI, *op. cit*., p. 8 ss. porta gli esempi delle applicazioni e dei servizi web. L'Autrice sottolinea che è coinvolto dall'impatto della rete anche il principio lavorista di cui agli artt. 1 e 4.

[158] In particolare il principio di democrazia e sovranità popolare (art. 1), la libertà personale (art. 13), la libertà di comunicazione (art. 15), la libertà di riunione (art. 17), la libertà di associazione (art. 18), la libertà di informazione (art. 21), la libertà di iniziativa economica (art. 41) e, ancora, il diritto alla cultura (artt. 9 e 33), il diritto alla salute (art. 32), il diritto all'istruzione (art. 34), il diritto al lavoro (art. 35) e le libertà politiche. Al riguardo, è degna di nota la sentenza della Corte costituzionale, 21 ottobre 2004, n. 307, che ha qualificato un intervento di alfabetizzazione informatica corrispondente a «finalità di interesse generale, quale è lo sviluppo della cultura, nella specie attraverso l'uso dello strumento informatico, il cui perseguimento fa capo alla Repubblica in tutte le sue articolazioni (art. 9 della Costituzione) anche al di là del riparto di competenze per materia fra Stato e Regioni di cui all'art. 117 della Costituzione».

[159] T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 100: «È il principio fondamentale della dignità […] che costituisce il fondamento costituzionale di tutti i diritti strettamente connessi allo sviluppo della persona». Secondo R. RAZZANTE, *op. cit.*, p. 21 ss. i diritti e doveri del cittadino previsti negli articoli dal 13 al 54 Cost. «non rappresentano un'elencazione tassativa e chiusa in se stessa […]. In questo senso l'art. 2 costituisce il tessuto connettivo tra i "vecchi" e i "nuovi" diritti di libertà, tra le ipotesi di libertà

disposto con altre norme costituzionali (artt. 13, 15, 21), è possibile fondare libertà e diritti che emergono in modo inedito nella rete, come l'anonimato, l'identità digitale, la protezione dei dati personali, da leggere come "diritto ad essere lasciati soli" (*right to be let alone*), ossia più propriamente diritto alla riservatezza, ma anche come diritto all'autodeterminazione informativa[160] e il correlato diritto all'oblio (*right to be forgotten*)[161], il principio di *net neutrality*[162] e la qualificazione della rete quale bene comune[163].

Altra parte della dottrina, diversamente da chi rinviene nella nostra Costituzione gli spazi per una rilettura estensiva dei principi e delle libertà previste, auspica un riconoscimento esplicito attraverso un'integrazione della Costituzione stessa, alla luce della specificità della rete e dei diritti che viene a creare e dell'esigenza di responsabilizzare i pubblici poteri nella loro tutela. Ad avviso di tale dottrina, l'interpretazione evolutiva della Carta, infatti, finisce per attribuire un significato nuovo e diverso da quello originario del testo scritto e rigido, che rischia di sfociare in una forzatura del dettato costituzionale e, in ogni caso, non riesce pienamente a cogliere l'essenza delle nuove libertà, rischiando di favorire l'autoregolamentazione e la

---

espressamente sancite nella Costituzione formale e quelle che gradualmente, con il moto dell'evoluzione storica, si affacciano sul proscenio della Costituzione materiale e sostanziale […]. L'art. 2 della Costituzione è una norma che fissa un fine da raggiungere, vale a dire lo sviluppo della persona umana, astenendosi invece dal predeterminare i mezzi, e lasciando pertanto la porta sempre aperta all'ingresso di nuove libertà costituzionalmente garantibili oltre quelle testualmente indicate».

160 S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 394 ss. e S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997 (nuova ed. 2004).

161 T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 94 ss.

162 Il principio di *net neutrality* indica il divieto per i fornitori di operare discriminazioni tra gli utenti in relazione alla qualità o alla velocità di connessione, alle applicazioni o ai servizi; cfr. G. DE MINICO, "*Net neutrality" come diritto fondamentale di chi verrà*, in *Costituzionalismo.it*, fasc. 1, 2016, p. 1 ss. Al riguardo, secondo A. MASERA - G. SCORZA, *op. cit.*, p. 25 «si può definire la *net neutrality* come "la versione digitale del principio di uguaglianza"».

163 Cfr. S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 389 ss., che reputa diritto di accesso e neutralità della rete «gli strumenti necessari per rendere possibile il "contributo creativo" di una platea sterminata di soggetti che guardano alla conoscenza in rete come a una continua, interminata costruzione collettiva, sottratta alla regola del profitto e così volta verso l'apertura di spazi "comuni" sempre più larghi, di "non-market commons"» (p. 391). Cfr. A. MASERA - G. SCORZA, *op. cit.*, p. 18.

concentrazione del potere nelle mani dei più forti[164] e di tradursi in una tutela più debole dei diritti digitali rispetto ai diritti offline da parte della giurisprudenza[165].

Secondo questo orientamento è pertanto necessaria una revisione costituzionale, che si è tradotta in alcuni disegni di legge, che, in coerenza con le due anime dicotomiche e connesse della libertà informatica, individuale e sociale, hanno evidenziato l'una o l'altra.

Una proposta di revisione costituzionale, che valorizza il diritto di accesso come libertà individuale e libera manifestazione del pensiero, seppur contenga anche l'aspetto della pretesa soggettiva di prestazioni a carico dei pubblici poteri, riguarda l'inserimento di un art. 21-bis nella Costituzione o l'integrazione dell'art. 21 Cost.[166].

Un'altra proposta di riforma costituzionale, invece, privilegiando il carattere di diritto sociale dell'accesso alle tecnologie informatiche, ha previsto l'inserimento di un art. 34-bis in Costituzione[167].

---

164 G. AZZARITI, *op. cit*., p. 3 ss.

165 Si mostrano favorevoli ad una revisione costituzionale, *inter alia*, P. COSTANZO, *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, cit. e M.R. ALLEGRI, *op. cit.*, secondo cui la revisione della Carta costituzionale eviterebbe di declassare i diritti del ciberspazio, attualmente condizionati alla "riserva del possibile" rimessa al legislatore e alle esigenze di disponibilità economiche, in base all'art. 81 C.

166 La proposta deriva da quella avanzata dal prof. Rodotà all'*Internet Governance Forum* a Roma nel 2010 e va nella direzione di ampliare i principi costituzionali riguardanti l'uguaglianza e lo sviluppo della persona. La proposta di Stefano Rodotà consisteva nell'inserimento in Costituzione di un art. 21-bis di tale tenore: «Tutti hanno eguale diritto di accedere alla rete Internet, in condizioni di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale». La proposta ha visto diverse formulazioni nel corso degli anni e si è tradotta in svariati disegni di revisione costituzionale: il d.d.l. cost. 2485 del 6 dicembre 2010, presentato al Senato, sull'introduzione dell'art. 21-bis; il d.d.l. cost. 2922 del 22 settembre 2011, presentato al Senato, recante modifiche all'art. 21; successivamente, il d.d.l. cost. 1058 del 27 maggio 2013 e il d.d.l. cost. 1244 del 20 giugno 2013, presentati alla Camera, che proponevano un art. 21-bis e il d.d.l. cost. 1317 del 17 febbraio 2014, presentato al Senato, recante modifiche all'art. 21. Cfr. S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, p. 13 ss.

167 Il d.d.l. cost. 1561 del 10 luglio 2014, presentato al Senato, e il d.d.l. cost. 2816 del 14 gennaio 2015, presentato alla Camera, prevedono l'introduzione di un art. 34-bis, con tale formulazione: «Tutti hanno eguale diritto di accedere alla rete internet, in modo neutrale, in condizione di parità e con modalità tecnologicamente adeguate. La Repubblica promuove le condizioni che rendano effettivo l'accesso alla

In dottrina, tra i fautori della revisione costituzionale alcuni ritengono che l'intervento dovrebbe riguardare, invece, i principi fondamentali della Costituzione e in particolare proprio i canoni interpretativi della dignità umana e del principio di uguaglianza, di cui agli articoli 2 e 3, comma 2, Cost., per non rischiare di effettuare un intervento che può rivelarsi limitato al momento dell'applicazione e coprire, invece, in modo aperto l'insieme di diritti e libertà coinvolti dalla rivoluzione digitale[168].

La profonda riflessione e l'acceso dibattito italiano hanno portato a un significativo riconoscimento istituzionale, a una Carta delle libertà digitali, che non ha carattere costituzionale e neppure legislativo: la Dichiarazione dei diritti in Internet, detta anche *Internet Bill of Rights* italiana.

L'iniziativa italiana si colloca nell'alveo dei tentativi di emanare un *Internet Bill of Rights* a livello sovranazionale[169]. Le iniziative legate a una ridefinizione delle libertà e a un "costituzionalismo digitale" trovano matrice nella stessa rivoluzione informatica e nei cambiamenti causati nell'esistenza dell'uomo e negli assetti di potere. La dimensione globale delle questioni rischia, infatti, di sottrarre l'effettiva tutela dei diritti alle necessarie garanzie e ai tradizionali processi giudiziari, consegnando il potere nelle mani dei soggetti più forti in un terreno di conquista conteso da «Stati invadenti e imprese prepotenti»[170]. Nonostante le intenzioni e gli sforzi in questa direzione, non si è

---

rete internet come luogo ove si svolge la personalità umana, si esercitano i diritti e si adempiono i doveri di solidarietà politica, economica e sociale».

168 In tal senso P. MARSOCCI, *op. cit.*, p. 8 ss., secondo cui l'inserimento in Costituzione può «"rivitalizzare" il principio di eguaglianza sostanziale, così come anche contribuire a contrastare il diffondersi dell'idea di un'economia sovrana distaccata dagli Stati e dalle loro leggi (come anche dagli ordinamenti internazionali), proprio sul nodo della ricchezza e della sua distribuzione»; P. PASSAGLIA, *Internet nella Costituzione italiana: considerazioni introduttive*, cit., p. 37 ss., che, in caso di intervento costituzionale, propone l'introduzione di un art. 2-bis o di un art. 3-bis, anche se a suo avviso è preferibile conservare l'impianto originario e neutrale della Costituzione, offrendo tutela per via ermeneutica; M.R. ALLEGRI, *op. cit.*, che propone in modo più ampio di integrare gli artt. 2 e 3, comma 2, Cost. con l'inciso «tanto nello spazio fisico quanto nel ciberspazio».

169 Nel 2005, in occasione del *World Summit on Information Society* organizzato dall'ONU a Tunisi, il professor Rodotà rileva la necessità di una Carta dei diritti digitali, al fine di proteggere le libertà e i diritti umani nella rete.

170 S. RODOTÀ, *Prefazione*, in A. MASERA - G. SCORZA, *op. cit.*, p. V ss.; S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 417 ss. sottolinea come l'*Internet Bill of Rights* debba originare da una negoziazione e

ancora giunti all'emanazione di un vero e proprio *Internet Bill of Rights* a livello internazionale, ma non mancano iniziative e movimenti in tal senso da parte di coalizioni e gruppi spontanei[171] e anche da parte di singoli Stati, che non hanno mancato di istituire Commissioni istituzionali dedicate a tali temi[172].

In particolare, a questo proposito rileva il cosiddetto *Marco Civil da Internet*, ossia la legge 12.965 del 23 aprile 2014 del Brasile, approvata a seguito di un'intensa e lunga consultazione pubblica basata su un paradigma partecipativo e pluralista: la Carta nei suoi 32 articoli «*stabilisce princìpi, garanzie, diritti e doveri per l'uso di Internet in Brasile*» (così l'articolo 1). La legge brasiliana garantisce i diritti che caratterizzano la realtà digitale, quali il diritto di accesso a Internet, la libertà di espressione e la protezione dei dati personali; il *Marco Civil* cerca di promuovere, altresì, l'accesso all'informazione e alla conoscenza, la partecipazione alla vita culturale e alla gestione della cosa pubblica, la neutralità, il mantenimento della stabilità, della sicurezza e della funzionalità della rete e della sua natura libera, aperta e partecipativa, la responsabilizzazione degli agenti e la libertà economica[173]. Nella consapevolezza della particolarità dell'oggetto della regolazione, l'art. 6 del *Marco Civil* pone quale criterio interpretativo della legge stessa la considerazione, «*unitamente ai fondamenti, ai principi e agli scopi previsti*» di una serie di elementi: «*la natura di internet, i suoi particolari usi e costumi e la sua importanza per la promozione dello sviluppo umano, economico, sociale e culturale*».

---

da un impegno *multistakeholder* e *multilevel*, ossia da un modello e una procedura diversi da quelli tradizionali.

171 Un esempio significativo è la Carta dei Diritti Umani e dei Principi di Internet elaborata da una *dynamic coalition* e presentata all'*Internet Governance Forum* di Vilnius del 2010. S. RODOTÀ, *Prefazione*, cit., p. V ss. parla dei «quasi cento *Internet Bill of Rights* che è possibile trovare in rete, e che sono il prodotto del lavoro spontaneo di gruppi, "*dynamic coalitions*", imprese, singoli (il 60% successivi al 2012)». G. AZZARITI, *op. cit.*, p. 7 riconosce alle Carte dei diritti della società civile globale in Internet, oltre al valore culturale, anche un valore giuridico «sul piano persuasivo, quello proprio dell'argomentazione. Con un'incidenza sul ragionamento giuridico che può essere anche decisiva»; il valore simbolico e la finalità intrinseca di queste Carte per l'Autore motivano la forzatura semantica.

172 Nel 2013 la Gran Bretagna istituisce una Commissione sulla democrazia digitale, nel 2014 la Germania istituisce una Commissione parlamentare permanente sulla *Digital society* e nello stesso anno la Francia istituisce una Commissione sui diritti e sulle libertà digitali.

173 Artt. 2, 3, 4 del *Marco Civil da Internet*.

L'Italia, ispirata anche dal modello brasiliano del *Marco Civil*, non ha scelto però di approvare un atto di natura legislativa[174], ma una Dichiarazione.

La Camera dei deputati, il 28 luglio 2014, ha nominato una Commissione per i diritti e i doveri relativi ad Internet, composta in modo misto da parlamentari, studiosi ed esperti, promossa e presieduta dalla Presidente Laura Boldrini e coordinata da Stefano Rodotà[175], col fine esplicito di elaborare una Dichiarazione dei diritti in Internet. La bozza di Dichiarazione, prodotta dalla Commissione l'8 ottobre 2014, dopo un percorso partecipativo di consultazione pubblica, come nel caso del *Marco Civil*[176], è approdata al testo definitivo, approvato dalla Commissione e pubblicato il 28 luglio 2015[177].

Il documento indica principi e direzioni per possibili sviluppi normativi nei diversi livelli nazionale e internazionale[178] ed è stato presentato all'*Internet Governance Forum* 2015 in Brasile, in coerenza con la mozione "Quintarelli e altri" n. 1-01031 e la mozione "Caparini e altri" n. 1-01052 del 3 novembre 2015, approvate dalla Camera dei deputati e volte a impegnare il Governo ad attivare ogni iniziativa utile per la promozione e l'adozione dei principi della Dichiarazione a livello nazionale, europeo e internazionale[179].

---

174 Cfr. M.R. ALLEGRI, *op. cit.*, p. 17 e A. MASERA - G. SCORZA, *op. cit.*, p. 87 ss.

175 La Commissione è stata composta da 23 membri tra i quali deputati, esperti del settore, rappresentanti delle imprese, delle associazioni e della società civile, partecipanti a titolo gratuito.

176 La consultazione, durata cinque mesi, è iniziata il 27 ottobre 2014 e si è conclusa il 31 marzo 2015: si è svolta grazie a una piattaforma online e attraverso le audizioni dei portatori di interesse.

177 Il testo definitivo della Dichiarazione e la documentazione relativa ai lavori della Commissione sono consultabili al seguente link: *www.camera.it/leg17/1179*.

178 Cfr. A. MORELLI, *I diritti e la Rete. Notazioni sulla Bozza di Dichiarazione dei diritti in Internet*, in *federalismi.it*, focus TMT, n. 1, 2015, p. 2 ss.; G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015, p. 73 ss.; A. MASERA - G. SCORZA, *op. cit.*, p. 87 ss.

179 Le mozioni definiscono Internet «uno strumento imprescindibile per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale». Il 28 settembre 2015 è stata firmata una dichiarazione congiunta fra la Presidente della Camera dei deputati Laura Boldrini e il Presidente dell'Assemblea nazionale francese Claude Bartolone, quali Presidenti delle rispettive Commissioni di studio: nella dichiarazione congiunta Internet viene qualificato come bene comune mondiale e vengono condivisi molti principi presenti nella Dichiarazione dei diritti italiana.

In merito al valore sul piano del diritto positivo, nonostante il preambolo richiami la necessità di dare fondamento costituzionale sovranazionale ai diritti digitali[180], la Dichiarazione risulta priva di forza giuridica vincolante e prescrittiva, ma, seppur per tale ragione non sia stata esente da critiche[181], svolge una significativa funzione di *moral suasion*. Si pone, infatti, quale documento di indirizzo per il Governo, dotato di un esplicito valore culturale e politico, oltre che della necessaria flessibilità per adeguarsi all'evoluzione digitale: sotto tale profilo può costituire un eventuale significativo riferimento per il legislatore e un elemento utile nel complesso lavoro ermeneutico delle Corti giurisdizionali nel bilanciamento tra diritti[182]. Inoltre rappresenta l'esito finale di un percorso partecipato e orizzontale, una sorta di modello "*wiki*", lontano dai metodi tradizionali "calati dall'alto" e coerente con la società digitale e con la rete stessa, che si arricchisce costantemente del contributo della collettività[183].

---

180 Nel preambolo della Dichiarazione è chiarito esplicitamente che «una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale».

181 In tal senso cfr. M.R. ALLEGRI, *op. cit.*, p. 10; T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 131 ss.; A. MORELLI, *I diritti e la Rete. Notazioni sulla Bozza di Dichiarazione dei diritti in Internet*, cit., p. 1 ss.; C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, il Mulino, Bologna, 2015, p. 151 ss., che ritiene siano trascurati nella Dichiarazione gli aspetti di innovazione e crescita legati ai *big data* (sul piano tecnologico ed economico) e quelli di sicurezza (sul piano politico e di difesa) e, di conseguenza, reputa l'operazione compiuta dalla Dichiarazione «fortemente a favore dei diritti umani ma essenzialmente priva di una solida base scientifica che permetta *realisticamente* di proteggerli».

182 Così S. RODOTÀ, *Prefazione*, cit., p. V ss. Al riguardo, secondo P. OTRANTO, *op. cit.*, p. 128 ss., seppur i principi della Dichiarazione siano recessivi rispetto a norme primarie statali o norme di carattere pattizio dotate di forza cogente, «in difetto di contrasto con esse, potrebbero contribuire a fondare l'argomentazione delle Corti e per tal via risultare decisive nel lento, ma costante, processo di creazione del diritto per via giurisprudenziale, influenzato anche dal dialogo tra giudici appartenenti a diversi ordinamenti» (p. 131).

183 Cfr. S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 417 ss. e S. RODOTÀ, *Prefazione*, cit., p. V ss., che, in relazione alla creazione di regole nel mondo digitale, parla di un processo per accumulazione, in coerenza con la natura partecipativa e dialogica di Internet. Secondo M. OREFICE, *I big data. Regole e concorrenza*, in *Politica del diritto*, fasc. 4, 2016, p. 740 la Dichiarazione «si pone come un catalogo mite, nato da un processo di formazione pseudo-eteronomo, promosso in sede politica, ritornato al basso e sottoposto alle osservazioni di cittadini e operatori e infine approvato in sede istituzionale. Ha così

La Dichiarazione, composta da un preambolo e da 14 articoli e tesa esplicitamente al riconoscimento e alla garanzia dei diritti (art. 1), interpreta la libertà informatica nelle sue dimensioni di libertà individuale, ma anche di diritto sociale: in tale ottica disciplina i diritti fondamentali della rete, che possono essere distinti in tre macro-aree[184].

Una macro-area riguarda i diritti legati alla possibilità stessa di fruire liberamente della rete, quali il diritto di accesso a Internet, diritto "madre" prodromico agli altri, il diritto alla cultura digitale[185], che si collega strettamente al primo, il diritto alla neutralità della rete e il governo della rete stessa. Un secondo insieme di diritti definisce e regola i principi afferenti all'identità e alla tutela della persona: vi rientrano il diritto all'identità, la protezione dell'anonimato e i diritti più specificamente legati alla privacy, come la tutela dei dati personali, il diritto all'autodeterminazione informativa e il diritto all'oblio. Infine la Dichiarazione prevede una terza macro-area relativa alla sicurezza e alla garanzia del soggetto, che prevede il diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici, i trattamenti automatizzati, i diritti e le garanzie delle persone sulle piattaforme e la sicurezza in rete[186].

La Dichiarazione, pur non costituendo atto normativo, è significativa della riflessione in atto e della tensione istituzionale odierna verso il riconoscimento delle libertà e dei diritti in rete.

---

assunto il tipico valore politico di impegno del Governo […]. Resta fermo che la semplice capacità orientativa dei *bill* rispetto alla discrezionalità del legislatore è variabile in ragione del contesto e quindi del consenso radicato nel tessuto sociale della comunità ovvero della ponderatezza del contenuto delle sue previsioni».

184 S. RODOTÀ, *Prefazione*, cit., p. V ss. evidenzia come la Dichiarazione sia dedicata in particolare ai principi legati al funzionamento di Internet.

185 La Dichiarazione parla di conoscenza ed educazione in rete.

186 Per l'analisi della Dichiarazione cfr. A. MASERA - G. SCORZA, *op. cit.*; G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 73 ss.; P. OTRANTO, *op. cit.*, p. 128, che sottolinea come siano richiamati principi riconosciuti e tutelati dal diritto interno (anzitutto di rango costituzionale) ed europeo e dalla giurisprudenza nazionale e sovranazionale.

1.3.2. I diritti digitali nella normativa nazionale vigente

Se a livello costituzionale l'impatto della realtà digitale si traduce in interpretazioni evolutive delle garanzie previste e in tentativi di revisione della Carta fondamentale, rimasti al momento solo disegni di legge costituzionale, nella normativa di rango primario si trovano riferimenti significativi che riguardano le libertà e i diritti in rete.

In particolare la legislazione si occupa della cosiddetta cittadinanza digitale e, quindi, della configurazione dei diritti dei cittadini nei confronti delle istituzioni, resa possibile dalle nuove tecnologie[187]. Alla luce di quanto esaminato, si può ritenere che tali disposizioni di rango primario trovino copertura costituzionale nei principi fondamentali e nei canoni interpretativi contenuti in particolare negli artt. 2 e 3 C., anche in combinato disposto con un insieme di ulteriori norme e relative libertà costituzionali, e, altresì, nell'art. 97 C. che permette di leggere la digitalizzazione delle amministrazioni quale strumento per assicurare il buon andamento delle stesse[188].

Già nella legge 9 gennaio 2004, n. 4, cosiddetta "legge Stanca", recante «*Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*» si trova nell'art. 1 un riferimento significativo al diritto di accesso alla rete e «*a tutte le fonti di informazione e ai relativi servizi»*, che emerge quale diritto sociale derivante dal principio di eguaglianza sostanziale di cui all'art. 3 della Costituzione[189].

---

187 Secondo F. AMORETTI - E. GARGIULO, *op. cit.*, p. 353 ss. la cittadinanza elettronica è «una nuova opportunità di esercizio di diritti – civili, politici e sociali – già entrati a far parte della dotazione di ogni cittadino» e «un non-cittadino, tramite l'accesso alla rete, è in grado di agire dei diritti che, in un'arena non elettronica, gli sarebbero preclusi».

188 Cfr. E. D'ORLANDO, *op. cit.*, p. 213 ss. «Se, infatti, si parte dall'assunto per cui le tecnologie rappresentano un fattore moltiplicatore e di crescita delle libertà e si conviene con il fatto che la missione dell'Amministrazione è il servizio ai diritti dei cittadini, tutte le opzioni normative e le prassi amministrative necessarie per realizzare le politiche di *e-Government* possono ritenersi assistite da una presunzione di costituzionalità/legittimità».

189 «*La Repubblica riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione e ai relativi servizi, ivi compresi quelli che si articolano attraverso gli strumenti informatici e telematici. È tutelato e garantito, in particolare, il diritto di accesso ai servizi informatici e telematici*

Da un punto di vista normativo, è il Codice dell'amministrazione digitale il provvedimento che si occupa di disciplinare i diritti digitali di cittadini e imprese nei confronti delle pubbliche amministrazioni, in particolare nelle prime disposizioni (art. 3 e ss.), a conferma della centralità che deve essere riservata agli utenti nell'azione pubblica[190]. Tale aspetto è stato ulteriormente rafforzato dalla recente riforma recata dalla cosiddetta legge Madia: l'art. 1 della legge delega 124/2015 e i relativi d.lgs. 179/2016 e d.lgs. 217/2017 esprimono l'intenzione del legislatore di fortificare e rendere effettivi i diritti digitali nei confronti delle amministrazioni pubbliche[191]. Il d.lgs. 217/2017, oltre a rubricare la sezione II del capo I del CAD proprio con l'espressione «*Carta della cittadinanza digitale*», modifica e integra ulteriormente il Codice dell'amministrazione digitale nella direzione del rafforzamento dei diritti.

Il Codice declina il rapporto con i pubblici poteri nei termini della cittadinanza digitale e configura il diritto di accesso come precondizione per l'esercizio dei diritti dei cittadini e l'assolvimento dei doveri delle istituzioni[192].

La cittadinanza digitale si basa sul diritto all'uso delle tecnologie nei rapporti tra cittadini e soggetti pubblici, espressamente disposto dall'art. 3, d.lgs. 82/2005, che presuppone necessariamente anche il diritto di accesso a Internet[193]. La norma è ampia,

---

della pubblica amministrazione e ai servizi di pubblica utilità da parte delle persone disabili, in ottemperanza al principio di uguaglianza ai sensi dell'articolo 3 della Costituzione».

190 E. D'ORLANDO, *op. cit.*, p. 213 ss. parla di «statuto del cittadino digitale contenuto nel CAD», che si pone come «la risultante di una pluralità coerente di declinazioni di un diritto di libertà informatica costituzionalmente derivabile».

191 Fin dall'inizio della relazione illustrativa di accompagnamento allo schema del d.lgs. 179/2016 viene esplicitata la *ratio* della riforma che consiste nello spostamento della prospettiva dal processo di digitalizzazione delle amministrazioni alla cittadinanza digitale.

192 T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 61: il d.lgs. 82/2005 «individua una sorta di statuto del cittadino digitale (sia per le persone fisiche che giuridiche)», basato «sul diritto di pretendere dai pubblici uffici l'interazione in modalità digitale, al quale corrisponde l'obbligo dell'amministrazione di adeguarsi sotto il profilo tecnico e organizzativo per soddisfare la pretesa dell'utente».

193 Art. 3, comma 1: «*Chiunque ha il diritto di usare, in modo accessibile ed efficace, le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2* [ossia i soggetti cui si applica il Codice]*, anche ai fini dell'esercizio dei diritti di accesso e della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute*». L'art. 3 del d.lgs. 82/2005 è stato oggetto di profonda modifica da parte del d.lgs. 179/2016 e del d.lgs. 217/2017, che lo hanno fortificato e ne hanno ampliato la portata.

riguarda ogni fase del rapporto tra istituzioni e collettività e valorizza la dimensione sociale di accesso e partecipazione: per la sua effettività presuppone non solo l'introduzione delle tecnologie, ma la riorganizzazione e la reingegnerizzazione dei processi della macchina pubblica. La disposizione, di contenuto precettivo e immediatamente applicabile, in caso di violazione è munita della relativa tutela giurisdizionale davanti al giudice amministrativo[194]. Al riguardo è significativa la sentenza del TAR Basilicata, 23 settembre 2011, n. 478, che ha riconosciuto espressamente il diritto di cittadini e imprese all'utilizzo delle tecnologie informatiche, a cui corrisponde un correlato dovere della pubblica amministrazione di renderlo concretamente attuabile ed esercitabile.

Il diritto di accesso a Internet viene poi declinato sotto l'aspetto culturale nell'art. 8 del d.lgs. 82/2005 (*Alfabetizzazione informatica dei cittadini*), che evidenzia la necessità di competenze per poter utilizzare l'accesso messo tecnicamente a disposizione e coglierne le opportunità e i rischi[195].

È opportuno leggere gli artt. 3 e 8 in combinato disposto con i relativi obblighi posti a carico delle amministrazioni: da questo punto di vista rileva l'art. 2, comma 1, d.lgs. 82/2005, che impegna le istituzioni ad assicurare la possibilità di fruire e utilizzare le tecnologie informatiche[196]. Sotto tale profilo le istituzioni sono ontologicamente tenute a realizzare le soluzioni necessarie per mezzo di azioni positive, specifiche e

---

194 Art. 3, comma 1-ter, d.lgs. 82/2005. Cfr. F. CARDARELLI, *op. cit.*, p. 227 ss., secondo cui il diritto all'uso delle tecnologie è qualificabile come una posizione giuridica soggettiva strumentale verso la pubblica amministrazione, accostabile al paradigma dell'interesse legittimo.

195 Lo Stato e i soggetti cui si applica il Codice sono tenuti a promuovere «*iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo*». Anche questa norma, come l'art. 3, ha subito modifiche tese ad ampliare e a fortificare il disposto normativo da parte del d.lgs. 179/2016, che ha anche introdotto l'art. 8-bis, teso a favorire la connettività alla rete Internet negli uffici e luoghi pubblici, a beneficio degli utenti.

196 «*Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione*».

concrete, mirate a creare le condizioni per l'esercizio dei diritti nel ciberspazio e il pieno sviluppo della persona umana. Nell'attuazione della normativa, pertanto, deve essere costante l'impegno dei poteri pubblici nel contrasto al *digital divide*[197], declinazione della disuguaglianza, nuova forma di analfabetismo, il cui superamento è necessario per affermare i nuovi diritti, lo sviluppo della persona e gli inediti volti della democrazia.

Il diritto all'uso delle tecnologie costituisce la norma "madre" e disciplina il diritto fondamentale in capo ai privati, affiancato nel CAD da una serie di diritti "derivati" legati al procedimento[198] e altri diritti "derivati" relativi specificamente alle comunicazioni, afferenti a determinate tipologie di soggetti[199] o a specifici strumenti di esercizio del diritto[200].

La cittadinanza "digitale" si esplica poi in una serie di diritti che trovano la loro matrice nel modello di *open government*, che informa la normativa, e in particolare nei principi di trasparenza, partecipazione e collaborazione, come il diritto ai servizi online e alla loro qualità (*customer satisfaction*)[201] e il diritto alla partecipazione democratica

---

197 Il *digital divide* configura il divario tra chi accede, fruisce e utilizza le tecnologie informatiche e chi ne è escluso, in modo parziale o totale. Sono diverse le motivazioni di esclusione: geografiche e infrastrutturali (aree remote e rurali, assenza delle infrastrutture), culturali, anagrafiche, economiche, inerenti a disabilità.

198 È il caso del diritto all'effettuazione dei pagamenti online (art. 5, d.lgs. 82/2005) e del diritto a trovare online, per ogni tipologia di procedimento a istanza di parte, gli atti e i documenti da allegare all'istanza e la modulistica necessaria, nonché gli uffici ai quali rivolgersi (art. 35, comma 1, lett. d) e comma 2, d.lgs. 33/2013).

199 È il caso del diritto all'identità digitale e al domicilio digitale (art. 3-bis) e del diritto delle imprese alle comunicazioni telematiche con le istituzioni (art. 5-bis).

200 È il caso del domicilio digitale (art. 6) e dei pubblici elenchi contenenti gli indirizzi telematici, quali l'indice nazionale dei domicili digitali (INI-PEC) delle imprese e professionisti (art. 6-bis), l'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA) (art. 6-ter) e l'indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato, non tenuti all'iscrizione in albi professionali o nel registro delle imprese (art. 6-quater; i domicili digitali contenuti in tale elenco saranno trasferiti dall'AgID nell'ANPR – Anagrafe nazionale della popolazione residente, di cui all'art. 62, al momento del suo completamento). La consultazione e l'accesso a tali elenchi sono regolati dall'art. 6-quinquies del d.lgs. 82/2005, introdotto dal d.lgs. 217/2017.

201 Art. 7, d.lgs. 82/2005, che, a seguito delle modifiche del d.lgs. 217/2017, prevede la significativa rubrica «*Diritto a servizi on-line semplici e integrati*»: anche le modifiche della disposizione vanno in tal senso. Il d.lgs. 217/2017 ha integrato, altresì, l'art. 64-bis con il comma 1-bis, al fine di rendere effettiva

elettronica (*e-democracy*)[202]. La libertà informatica si declina, infatti, non solo in senso individuale, ma anche nella dimensione sociale e politica dell'uomo, legata al processo democratico e ai nuovi assetti istituzionali. L'*e-democracy* fa riferimento proprio all'utilizzo delle tecnologie informatiche nelle diverse fasi del processo democratico, al fine di garantire e favorire la partecipazione alla sfera pubblica, il coinvolgimento nei processi decisionali, il controllo democratico e le iniziative dirette dei cittadini, nella logica del governo aperto.

Alla previsione dei diritti digitali corrisponde il dovere di renderli effettivi da parte delle istituzioni, tenute ad attivare gli strumenti necessari a una concreta cittadinanza digitale e chiamate, altresì, a rispondere in caso di mancato rispetto delle disposizioni[203]. In direzione di garantire effettività ai diritti dei cittadini possono essere interpretate, altresì, le figure deputate a "traghettare" le istituzioni italiane verso il

---

la disposizione di cui all'art. 7: «*i soggetti di cui all'articolo 2, comma 2, i fornitori di identità digitali e i prestatori dei servizi fiduciari qualificati, in sede di evoluzione, progettano e sviluppano i propri sistemi e servizi in modo da garantire l'integrazione e l'interoperabilità tra i diversi sistemi e servizi e con il servizio di cui al comma 1, espongono per ogni servizio le relative interfacce applicative e, al fine di consentire la verifica del rispetto degli standard e livelli di qualità di cui all'articolo 7, comma 1, adottano gli strumenti di analisi individuati dall'AgID con le Linee guida*».

[202] Art. 9, d.lgs. 82/2005: i soggetti cui si applicano le disposizioni del Codice «*favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili e migliorare la qualità dei propri atti, anche attraverso l'utilizzo, ove previsto e nell'ambito delle risorse disponibili a legislazione vigente, di forme di consultazione preventiva per via telematica sugli schemi di atto da adottare*». Cfr. F. CARDARELLI, *op. cit.*, p. 227 ss.

[203] I dirigenti rispondono dell'osservanza e attuazione delle disposizioni del CAD ai sensi e nei limiti degli artt. 21 (responsabilità dirigenziale) e 55 (responsabilità disciplinare) del d.lgs. 165/2001, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme. Inoltre, l'attuazione delle disposizioni è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa e individuale dei dirigenti (art. 12, comma 1-ter, d.lgs. 82/2005). Su questi profili sta crescendo l'attenzione della giurisprudenza; cfr., *inter alia*, sentenza del TAR Trento, 15 aprile 2015, n. 149, che riconosce la responsabilità della pubblica amministrazione in relazione al funzionamento delle piattaforme e degli strumenti informatici: in specifico, in caso di anomalie, la responsabilità è sia di chi li ha predisposti senza considerare tali conseguenze, sia, quale responsabilità almeno omissiva, del dipendente che, tempestivamente informato, non si è adoperato per svolgere, secondo i principi di legalità e imparzialità, tutte quelle attività che, in concreto, possano soddisfare le legittime pretese dell'istante; cfr. G. SGUEO, *L'amministrazione digitale*, in *Giornale di diritto amministrativo*, fasc. 1, 2016, p. 114 ss.

modello di amministrazione digitale e aperta, previste sia a livello di singola amministrazione, quale il responsabile per la transizione digitale[204], sia a livello nazionale, come il difensore civico per il digitale[205], il Commissario straordinario per l'attuazione dell'Agenda digitale[206] e l'Agenzia per l'Italia Digitale (AgID)[207]. Peraltro l'AgID ha anche il compito di pubblicare sul proprio sito una guida di riepilogo dei diritti di cittadinanza digitale previsti dal CAD[208].

Pertanto, alla luce di tale analisi, il Codice dell'amministrazione digitale si pone come la fonte normativa principale che ospita la cittadinanza digitale e i diritti che fondano il rapporto fra istituzioni e cittadini.

I diritti digitali afferenti, invece, maggiormente alla sfera personale del soggetto e particolarmente rilevanti nel governo dei dati trovano allocazione in provvedimenti normativi diversi, spesso dedicati puntualmente a uno specifico diritto.

Il diritto a conoscere è, infatti, regolato dal d.lgs. 33/2013, nel testo scaturente dalle profonde modifiche apportate dal d.lgs. 97/2016[209], il diritto alla protezione dei

---

204 Al responsabile di tale ufficio, dotato di adeguate competenze tecnologiche, manageriali e di informatica giuridica, è affidata «*la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità*»: con riferimento ai compiti relativi alla transizione alla modalità digitale, il responsabile risponde direttamente all'organo di vertice politico (art. 17, commi 1, 1-ter e 1-sexies, d.lgs. 82/2005).

205 Art. 17, comma 1-quater, d.lgs. 82/2005. Il d.lgs. 217/2017 ha previsto l'istituzione presso l'AgID di questa figura, originariamente prevista per ogni singola amministrazione.

206 Il Commissario, la cui nomina è stata prevista con la riforma del d.lgs. 179/2016 per un periodo non superiore a tre anni, svolge un ruolo di coordinamento, allo scopo di disegnare il "sistema operativo" del Paese. Al Commissario è assegnata una struttura di supporto (Team per la trasformazione digitale) e sono attribuiti poteri di impulso e di coordinamento nei confronti dei soggetti pubblici, ivi inclusa l'AgID, nonché il potere sostitutivo in caso di inadempienze (art. 63, d.lgs. 179/2016). Il sito dedicato al Commissario e al Team per la trasformazione digitale è *teamdigitale.governo.it*.

207 All'AgID, preposta alla realizzazione degli obiettivi dell'Agenda digitale italiana e alla promozione dell'innovazione digitale nel Paese, sono attribuite funzioni di programmazione, coordinamento e monitoraggio, l'emanazione di linee guida recanti regole e standard, la vigilanza e il controllo sull'attuazione e sul rispetto delle norme, la realizzazione di progetti e lo svolgimento di compiti di natura tecnica (artt. 14, comma 2, e 14-bis, d.lgs. 82/2005).

208 Art. 17, comma 1-quinquies, d.lgs. 82/2005.

209 *Infra*, cap. 2 e cap. 4, § 2.

dati personali trova fonte nazionale nel d.lgs. 196/2003 e, oggi, fonte europea nel regolamento UE 2016/679[210] e la protezione della proprietà intellettuale e del diritto d'autore è disciplinata nella legge 22 aprile 1941, n. 633, come scaturente dalle modifiche e integrazioni che ha avuto nel corso degli anni, anche a seguito della normativa europea[211].

Il bilanciamento dell'insieme complesso dei diritti che formano la persona e il cittadino digitale è reso particolarmente difficile dal ruolo assunto dai dati e dai loro intrecci, che connotano la società digitale sempre più come *data society* o società della conoscenza. La società contemporanea è, infatti, caratterizzata da nuovi strumenti e da inedite configurazioni dei dati (*closed data*, *open data* e *big data*)[212], che necessitano del ruolo dei poteri pubblici e di forme di tutela idonee a proteggere i diritti della persona, chiamati a difficili equilibri.

---

210 *Infra*, cap. 5.

211 *Infra*, cap. 4, § 4.

212 La società della conoscenza, dei dati e degli algoritmi e i relativi strumenti saranno oggetto dell'analisi svolta nei capitoli 2 e 3.

Capitolo 2

La società della conoscenza. *Closed data* e trasparenza

SOMMARIO: 2.1. La società della conoscenza. – 2.1.1. Caratteristiche, opportunità e rischi. – 2.1.2. Strumenti di conoscenza e forme di trasparenza (proattiva, reattiva, attiva). – 2.2. *Closed data* e *disclosure*. – 2.3. L'evoluzione normativa del principio di trasparenza. – 2.3.1. Dalla legge 241/1990 al d.lgs. 33/2013. – 2.3.2. Trasparenza e *Freedom of Information Act* (FOIA) italiano: il d.lgs. 97/2016 nel quadro internazionale di riferimento. – 2.4. Principi e strumenti nella disciplina vigente. – 2.4.1. Il diritto alla conoscibilità, all'accessibilità e alla qualità dei dati. – 2.4.2. I diritti di accesso: documentale, civico semplice, civico generalizzato.

2.1. La società della conoscenza

2.1.1. Caratteristiche, opportunità e rischi

Solo in epoca recente il benessere e lo sviluppo umano hanno iniziato a dipendere in modo significativo dalla gestione del ciclo dell'informazione, dai servizi basati sui dati e dall'accesso al bene della conoscenza.

La società odierna, dominata dai dati e dall'informazione, si muove nello spazio pubblico comune di Internet caratterizzato dal paradigma della conoscenza: l'economia stessa oggi è basata sui dati, come da anni chiariscono con consapevolezza anche i documenti dell'Unione europea[213].

[213] In tal senso diverse comunicazioni della Commissione europea, quali «*Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*», COM(2011) 882 def. del 12 dicembre 2011, «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014 e «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017, che interpreta i dati quale «risorsa essenziale per la crescita economica, la creazione di posti di lavoro e il progresso sociale. L'analisi dei dati facilita l'ottimizzazione di processi e decisioni, l'innovazione e la predizione di eventi futuri».

Di conseguenza, la società postindustriale viene definita, come esaminato, quale società "dell'informazione e della conoscenza". I due termini dell'endiadi, lungi dall'essere sinonimi, si differenziano: se nell'esordio della società contemporanea prevale il primo, negli sviluppi che si delineano emerge come tratto caratterizzante e valore da perseguire il secondo, la conoscenza rispetto all'informazione[214].

Le informazioni sono definite generalmente come dati, formati in base a una sintassi, dotati di significato (informazione = dati + significato)[215]. La conoscenza si basa su informazioni, ma necessita di ulteriori fattori, quali il processo cognitivo e l'elaborazione "intelligente", la comprensione e l'applicazione all'esperienza: di conseguenza, si colloca a un livello gerarchico superiore e possiede un maggiore valore rispetto al dato e all'informazione. Il solo insieme di informazioni non è necessariamente sinonimo di conoscenza[216].

---

214 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 130 ss. e G. BOMBELLI, *Tecnologia, diritto, antropologia: appunti sull'*Information (Knowledge) Society, in M. MEGALE (a cura di), *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2012, p. 22 ss., secondo cui l'informazione (*information*) non coincide con la conoscenza (*knowledge*) e la società della conoscenza riposa su presupposti teorici più impegnativi della società dell'informazione, relativi a un modello antropologico e a un'idea di società.

215 Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 3 ss., secondo cui il dato «è riducibile, in ultima analisi, a una mancanza di uniformità» (p. 27). I dati digitali possono essere definiti anche come dati binari, in quanto di regola codificati in *bit* (*binary digit*), l'unità minima di informazione, che consiste nella presenza o assenza di un segnale, 0 o 1 (una serie di 8 *bit* forma il *byte – by eight*); la quantità di *byte* è calcolata dal sistema binario. L'informazione consiste in differenti tipologie di dati (primari, secondari, metadati, operativi, derivati) e assume diverse qualificazioni (ambientale, matematica, semantica, fisica, biologica, economica). Dello stesso avviso U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014, p. 35: i dati possono essere intesi come mancanza di uniformità nel mondo reale, a cui viene attribuito un significato determinato; l'informazione semantica si basa su dati dotati di significato.

216 Cfr. B. C. HAN, *op. cit.*, p. 9 ss.: «Un mondo che consistesse solo di informazioni e che definisse comunicazione la loro circolazione indisturbata, assomiglierebbe a una macchina» (p. 11). Secondo l'Autore «un aumento di informazioni non porta necessariamente a scelte migliori. L'*intuizione*, per esempio, trascende le informazioni disponibili e segue una propria logica. A causa della crescente, e anzi esorbitante massa di informazioni, si atrofizza la capacità superiore di giudizio. Spesso un *meno* di sapere e di informazione implica un *più*» (pp. 14-15). Cfr. E. GIOVANNINI, *op. cit.*, p. 59 ss., che in relazione

Per prendere decisioni occorre conoscere, secondo il famoso adagio «conoscere per deliberare» di Einaudi[217]. Più ampiamente, è necessario conoscere per vivere il proprio spazio decisionale, economico e sociale[218] e per esercitare consapevolmente i propri diritti e libertà. Pertanto l'accesso alla conoscenza manifesta un legame saldo con la persona e i suoi diritti: è determinante per garantire le libertà fondamentali nella nuova realtà digitale e si salda fortemente con altri diritti quali la libertà di informazione, lo sviluppo culturale e più ampiamente lo svolgimento stesso della personalità. *A contrario*, di conseguenza, la mancata conoscenza può arrivare a minare le fondamenta del modello democratico[219].

Il web stesso nella sua evoluzione diventa *web of data*, che collega dati piuttosto che documenti, e *web semantico*, che permette di conoscere e facilita la conoscenza[220].

---

all'informazione statistica per trasformare i dati in conoscenza sottolinea l'importanza di alcuni fattori quali la quantità di dati prodotti, il ruolo dei *media* nella diffusione e presentazione, la rilevanza per gli utenti e la fiducia nel produttore dei dati; accanto a questi «l'aumento di conoscenza dipende anche dalla capacità degli individui di trattare dati statistici e di trarre da questi ultimi elementi concreti di conoscenza» (p. 59). Di conseguenza l'Autore sottolinea la complessità della relazione tra informazione statistica e conoscenza, individuale e collettiva: produrre informazione statistica non si traduce necessariamente in avanzamento della conoscenza collettiva, dato che «la catena di comportamenti che lega la produzione del dato e l'accrescimento della conoscenza è articolata e complessa, e coinvolge numerosi soggetti, portatori di interessi particolari, per quanto legittimi. E tutto questo può diventare pericoloso per il funzionamento di una società» (p. 63).

217 L. EINAUDI, *Prediche inutili. Dispensa 1: Conoscere per deliberare*, Einaudi, Torino, 1956, pp. 3-14.

218 Cfr. E. GIOVANNINI, *op. cit.*, p. 83.

219 Cfr. E. GIOVANNINI, *op. cit.*, p. 87 ss.

220 T. AGNOLONI, Linked Open Data *nel dominio giuridico*, in *Informatica e diritto*, nn. 1-2, 2011, p. 411 ss. riporta la convinzione di Tim Berners Lee, inventore del *Semantic Web*, che consiste nel fatto che l'evoluzione di Internet è rappresentata dal passaggio da una rete di documenti a una rete di dati. Secondo la definizione di Tim Berners Lee il *Semantic Web* consiste in un'evoluzione del web in cui le informazioni hanno un preciso significato e in cui computer e utenti lavorano in cooperazione; si tratta di un web in cui agiscono applicazioni in grado di comprendere il significato delle risorse in rete e guidare pertanto l'utente o sostituirsi allo stesso nello svolgimento di alcune operazioni. Secondo G. MODESTI, *Open data e privacy. La creazione di un programma aziendale per governare il processo di gestione dei dati*, in *Quaderni amministrativi*, fasc. 2-3, 2016, p. 29 il *web semantico* indica un «insieme di modelli e standard Web in cui le risorse vengono descritte e correlate fra loro in modo formale attraverso l'uso opportuno di metadati. In questo modo si abilitano gli agenti automatici a comprendere il significato dei

Dunque si parla di società della conoscenza per voler connotare uno stadio evolutivo (ancora da raggiungere, a dire il vero) capace di andare oltre il rumore e il caos prodotto dal flusso continuo di dati e informazioni e di approdare all'ordine della conoscenza, che porta con sé pluralismo informativo, consapevolezza, indipendenza e democrazia[221]. A tal fine la società contemporanea deve essere capace di "ascoltare", leggere e usare i dati e le informazioni[222].

Tutto questo si avvalora ulteriormente nelle evoluzioni significative e recenti che riguardano il cambiamento del rapporto tra mondo dei beni e delle persone[223]: il digitale si diffonde negli oggetti e fa saltare la soglia rassicurante tra mondo digitale (cui si accede con il *login*) e mondo analogico (dove si approda dopo il *logout*)[224], a favore dell'ubiquità di ambienti intelligenti e di un mondo che assume i connotati

---

dati e delle informazioni». G. RIZZO - F. MORANDO - J.C. DE MARTIN, Open Data: *la piattaforma di dati aperti per il* Linked Data, in *Informatica e diritto*, nn. 1-2, 2011, p. 493 ss.: il passaggio dal documento al dato grezzo «permette di separare in modo embrionale il contenuto di un artefatto in tante parti, potendo collegare tra loro o con altre informazioni i dati presenti all'interno dell'artefatto stesso, al fine di inferire nuove informazioni o creare nuovi artefatti» (p. 494); nel *web of data*, quale spazio di condivisione globale dei dati grezzi (*raw*), è possibile strutturare i dati della risorsa in modo da leggerli separatamente e aggregarli con altri, a richiesta dell'utente. Strumento del *web of data* sono i *linked open data*, per i quali *infra*, cap. 3.

221 S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 135, secondo cui la conoscenza si pone quale «fondamento del processo democratico di decisione e come precondizione per la partecipazione e il controllo».

222 Cfr. B.C. HAN, *op. cit.*, p. 21: «L'iper-informazione e l'iper-comunicazione dimostrano proprio la *mancanza di verità*, anzi la *mancanza d'essere*. Più informazione, più comunicazione non eliminano la fondamentale *opacità del tutto*. Piuttosto la accrescono» e V. MAYER-SCHÖNBERGER - K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Garzanti, Milano, 2013, p. 9 ss.: i dati non sono più un patrimonio statico, ma una materia prima, un input d'importanza vitale, capace di creare una nuova forma di valore, che se riusati intelligentemente possono essere trasformati in fonte d'innovazione e di nuovi servizi; di conseguenza «la vera rivoluzione non sta nelle macchine che elaborano i dati, ma solo nei dati in sé e nel modo in cui li usiamo» (p. 17). Secondo E. GIOVANNINI, *op. cit.*, p. 132 la quantità straordinaria di informazioni a disposizione ha bisogno di una qualità ugualmente straordinaria nel leggerle «distinguendo i "segnali", cioè i fenomeni veramente rilevanti, dal "rumore" prodotto dallo scroscio ininterrotto dei dati […]».

223 S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 109: «Diritti fondamentali, accesso, beni comuni disegnano una trama che ridefinisce il rapporto tra il mondo delle persone e il mondo dei beni».

224 Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 20 ss.

dell'"infosfera", usando il termine di Floridi[225]. I dati permettono di configurare l'uomo come "agente informazionale", di rendere gli oggetti capaci di interazione (*Internet of Things*)[226] fino a generare nuove soggettività con l'intelligenza artificiale. Gli esseri umani, gli oggetti intelligenti, i robot si basano, elaborano e scambiano dati, conoscono e si conoscono grazie alle informazioni[227].

In questo scenario di sviluppo presente e futuro, i regolatori pubblici e il diritto sono tenuti ad occuparsi necessariamente dei dati e della conoscenza, che assurgono a materie prime essenziali della stessa esistenza umana, come aria e acqua: l'oro della contemporaneità sono i dati che permettono di generare quella conoscenza[228].

---

225 Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 10 ss., che definisce quale "infosfera" «l'ambiente informazionale costituito da tutti i processi, i servizi ed entità informazionali che includono gli agenti informazionali così come le loro proprietà, interazioni e relazioni reciproche» (p. 11); gli uomini, quali *inforg* (organismi informazionali interconnessi), condividono l'infosfera con agenti biologici e artefatti ingegnerizzati. L'influenza delle ICT, sottolinea Floridi, è «sia estroversa, sia introversa, modificando non solo la nostra interazione con il mondo ma anche la comprensione di noi stessi» (p. 11): l'infosfera «diventerà progressivamente *sincronizzata* (tempo), *delocalizzata* (spazio) e *correlata* (interazioni)» (p. 22).

226 L. AGRÒ, *Internet of Humans*, Egea, Milano, 2017, p. 21: «l'Internet of Things, l'Internet degli Oggetti, è un'incredibile opportunità per consentire di aggiungere un'"anima di software" praticamente in qualsiasi cosa»; l'Autore distingue tra tecnologie passive (frigorifero), tecnologie reattive (Siri o Cortana) e proattive (bilancia pesapersone che motiva i soggetti).

227 Cfr. L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 19: «le ICT stanno tanto cambiando il nostro mondo quanto creando nuove realtà. La soglia tra il *qui* (analogico, di carbonio, offline) e il *là* (digitale, di silicio, online) diviene rapidamente impercettibile ma ciò va tanto a favore del *là* che del *qui*. Il digitale si sta diffondendo nell'analogico e confondendo con esso. Questo fenomeno recente è variamente definito nei termini di *ubiquità computazionale*, *ambiente intelligente*, *internet delle cose* o *Web-augmented things*». Cfr. J.C. DE MARTIN, *Le evoluzioni delle licenze* Creative Commons, in G. CONCAS - G. DE PETRA - G.B. GALLUS - G. GINESU - M. MARCHESI - F. MARZANO, *Contenuti aperti, beni comuni. La tecnologia per diffondere la cultura*, McGraw-Hill, Milano, 2009, p. 11, secondo cui la digitalizzazione della conoscenza «rimuove un formidabile ostacolo alla collaborazione, dal momento che rende la conoscenza ancora più nettamente non rivale di quanto già non fosse per sua natura […]».

228 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 112, che individua quali beni necessari per la soddisfazione dei diritti inerenti alla costituzionalizzazione della persona «quelli essenziali per la sopravvivenza (l'acqua, il cibo) e per garantire eguaglianza e libero sviluppo della personalità (la conoscenza)».

La "democratizzazione" dell'informazione, di cui parla Floridi, ha portato oggi più persone al possesso di più dati di quanto mai successo nella storia[229]. Ma più la conoscenza è diffusa più ci sono torsioni per limitarne l'utilizzabilità grazie anche all'ausilio di norme, non perfettamente adeguate alla società di riferimento. E quindi sulla scena della contemporaneità compaiono nuovi squilibri: pochi soggetti hanno in mano i dati e dunque la correlata conoscenza, che finisce per essere posta al centro di un conflitto. Il rischio è che la società possa scivolare in derive popolate da nuove asimmetrie, mancata protezione dei diritti, disuguaglianza e controllo.

I "signori dei dati" sono poteri pubblici e nuovi grandi poteri privati[230]. Se i secondi sono mossi dalla logica economica del profitto, i primi sono ontologicamente tenuti a garantire i diritti fondamentali e a stabilire, di conseguenza, i principi e le direttrici del governo dei dati. Per garantire i diritti di cittadinanza digitale è essenziale che i pubblici poteri si adoperino per mettere in campo i beni e gli strumenti necessari alla loro soddisfazione; tra questi, al fine di garantire il libero sviluppo della persona, il dispiegamento delle potenzialità umane e l'uguaglianza sostanziale, si pone proprio il bene della conoscenza, visto come bene comune globale, privo di proprietari o gestori, esercitabile da chiunque in condizioni di parità, il cui uso non ammette limitazioni[231].

La conoscenza costituisce un bene peculiare, che nella sua essenza possiede le caratteristiche della non escludibilità e della non rivalità, ma rischia di perderle laddove l'utilizzo da parte di alcuni possa portare difficoltà di accesso da parte di altri e conseguenti asimmetrie nella fruizione: questo si verifica nell'incontro col mondo privato del mercato e, in modo quasi contraddittorio, anche nella tutela offerta da parte del diritto (si pensi alla proprietà intellettuale e alla normativa sul diritto d'autore)[232]. In

---

229 L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 6 ss.

230 A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2012, p. 135: i detentori delle risorse informative e di calcolo «dispongono di un notevole potere informativo derivante dal controllo sulla gestione dei dati, tale da evocare la nozione di signoria».

231 Cfr. L. GALLINO, *Tecnologia e democrazia. Conoscenze tecniche e scientifiche come beni pubblici*, Einaudi, Torino, 2007. Sulla qualificazione di Internet quale bene comune e, più ampiamente, sulla riflessione giuridica relativa ai beni comuni cfr. P. OTRANTO, *op. cit.*, p. 249 ss.

232 La disciplina del diritto d'autore lascia salve le idee, che, di conseguenza, sono sottratte alla relativa disciplina. Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 131 ss.: «Più la conoscenza si dilatava

tal modo, nella strada delle disposizioni normative riemerge quella logica proprietaria tanto cara al diritto e così lontana dalla dinamica dell'accesso. Il concetto di accesso, infatti, non si collega necessariamente e strumentalmente alla proprietà[233]: ciò non significa sia diretto a qualcosa di vuoto, ma si tratta di accesso alla conoscenza che permette relazioni, attività, il controllo democratico del potere[234]. È un bene globale, a titolarità diffusa, su cui nessuno deve poter vantare diritti esclusivi e che per tali ragioni non può essere sottoposto a logiche di tipo proprietario o di mercato che da bene sono capaci di trasformarlo in merce[235].

L'accesso rischia concretamente di essere mediato da forme di pagamento in denaro o in dati personali, foriere di una nuova insidiosa disuguaglianza travestita da apparente gratuità e simulata libertà[236]; l'informazione e la correlata conoscenza da bene globale, comune o pubblico, rischia di diventare bene giuridico dotato di utilità e valore economico[237]. In questa direzione la concentrazione del controllo e le diseguaglianze

---

e diveniva accessibile, più si ricorreva a strumenti che, come il diritto d'autore, limitavano l'utilizzabilità di conoscenze prima liberamente disponibili» e P. OTRANTO, *op. cit.*, p. 272 ss., che riporta la dottrina secondo la quale per parlare di conoscenza quale bene comune bisogna distinguere tra i contenuti in pubblico dominio, che si configurano come beni pubblici, e quelli sottoposti a regimi di privativa dalle norme sulla proprietà intellettuale.

233 S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 108: «Accesso e proprietà si presentano come categorie autonome e, in diverse situazioni, potenzialmente o attualmente in conflitto. Si può accedere a un bene, e goderne delle utilità, senza assumere la qualità di proprietario».

234 Cfr. V. M. SBRESCIA, *op. cit.*, p. 1207 ss.; L. FLORIDI, *La rivoluzione dell'informazione*, cit., p. 10 ss.: «Porre minore enfasi sulla natura fisica di oggetti e processi implica che il diritto di uso sia giudicato almeno tanto importante quanto il diritto di proprietà» (p. 15).

235 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 113 ss., secondo cui «la logica del "comune" obbliga a progettazioni istituzionali adeguate alle caratteristiche del bene considerato, e ribadisce un nesso evidente con la necessità di politiche adatte alla realtà di un mondo in cui le interdipendenze crescenti individuano spazi ormai concretamente comuni, che attendono istituzioni che li sottraggano a imprese variamente distruttive» (p. 125).

236 S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 133 sottolinea come le logiche del mercato vengano a intaccare la natura di *common* della rete: «l'accesso mediato da forme di pagamento apre la via più insidiosa tra le diseguaglianze digitali, quella che istituisce un rapporto tra reddito e accesso alla conoscenza».

237 P. SAMMARCO, *op. cit.*, p. 177 ss. sottolinea come in tal modo l'informazione acquisisca la fisionomia di un prodotto commerciale.

nell'accesso alla conoscenza possono arrivare a inficiare il progresso, lo sviluppo e la coesione sociale[238].

Si tratta in modo palese di una sfida che mette in gioco i valori costituzionali della tutela dei diritti fondamentali, dell'uguaglianza e della stessa democrazia, che rischia di essere travolta da asimmetrie informative che già esistono e potrebbero nel lungo periodo divenire insanabili. Il rischio dunque consiste nello *human divide*, di cui parlava Rodotà, una disuguaglianza radicale che investe lo stesso essere umano, le sue prerogative, la sua natura, la sua ontologia e il suo ruolo, ridefiniti grazie alle tecnologie e alla centralità dei dati: in un percorso di disuguaglianza insieme all'uomo sono travolti i suoi diritti e le sue libertà[239].

In considerazione della loro funzione sono le istituzioni che hanno il difficile compito di sottrarre i dati e la conoscenza a questo potenziale destino, sono i regolatori pubblici che hanno la responsabilità verso le generazioni presenti e future di sottrarre al mercato e alle sue logiche redistributive questi beni globali, costitutivi dell'uomo contemporaneo e dei suoi diritti[240]. Per questo, quando si parla di dati e conoscenza, vengono in gioco i pubblici poteri: sono i soggetti deputati al governo dei dati.

---

238 Cfr. G. PASCUZZI, *Dematerializzazione*, cit., p. 344: «Lo scenario che vedesse la concentrazione della proprietà e del controllo della conoscenza potrebbe mettere in discussione le stesse forme di governo democratico».

239 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 138, secondo cui, proiettata su scala globale, «la relazione tra diritti fondamentali e beni comuni si presenta come una decisiva opportunità per affrontare la questione essenziale di uno "human divide", di una diseguaglianza radicale che incide sulla stessa umanità delle persone, mettendo in discussione la dignità e la vita stessa». Cfr. B.C. HAN, *op. cit.*, p. 79 ss., secondo cui si configura «un'illuminazione reciproca. Il controllo non si esercita solo dall'alto verso il basso, ma anche dal basso verso l'alto. Ciascuno espone ogni altro alla visibilità e al controllo, addirittura fin dentro la sfera privata. Questa sorveglianza totale degrada la "società trasparente" a una disumana società del controllo. Ognuno controlla l'altro» (p. 79); di conseguenza «il controllo totale annienta la libertà d'azione e conduce, alla fine, a un livellamento. La fiducia, che produce liberi spazi d'azione, non può essere facilmente rimpiazzata dal controllo» (p. 79) e, secondo l'Autore, si genera una società della sfiducia, nella quale «l'auto-illuminazione è più efficace dell'illuminazione che proviene da un altro, perché si unisce a un sentimento di libertà» (p. 81).

240 Cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 137, secondo cui «i beni comuni affrancano i diritti di cittadinanza dalle politiche redistributive».

Se le istituzioni sono il soggetto deputato a svolgere quest'opera, lo strumento per farlo, il sapere chiamato in causa è il diritto, al fine di fornire regole idonee a governare i dati e la correlata conoscenza.

Chi ha accesso alla conoscenza? A quali condizioni? La quantità di informazioni e dati, oggi resa possibile, si traduce in conoscenza? Il *web semantico* e ubiquo ci permette di conoscere di più o affidarsi agli algoritmi e ai numeri può dare vita a nuove manipolazioni? E, ancora, come limitare squilibri e asimmetrie, preservando la libertà del mercato e lo sviluppo economico[241]?

Per poter rispondere a tali domande è necessario esaminare gli strumenti di conoscenza e il relativo quadro normativo, esaminando il ruolo dei poteri pubblici nel governo dei dati, le problematiche giuridiche e la protezione da fornire ai diritti fondamentali del singolo negli inediti bilanciamenti tra interessi diversi cui è chiamata la società contemporanea[242].

2.1.2. Strumenti di conoscenza e forme di trasparenza (proattiva, reattiva, attiva)

Nel parlare di società della conoscenza emerge una caratteristica fondamentale che la connota, uno strumento essenziale per permettere alla società della conoscenza di essere tale: la trasparenza[243].

---

241 Cfr. J.C. DE MARTIN, *Prefazione*, in L. FLORIDI, *La rivoluzione dell'informazione*, cit., pp. XI-XII: «In particolare, la questione cruciale di chi avrà accesso a quali informazioni e a quali condizioni, e di quanto ampia sarà la libertà dell'individuo di comunicarle determinerà, a seconda degli esiti, infosfere radicalmente diverse tra loro, con enormi potenziali benefici per l'umanità e per il pianeta, ma anche con rischi di segregazione, sfruttamento e oppressione senza precedenti. Il modo in cui evolverà la rivoluzione dell'informazione dipenderà da noi».

242 L'analisi di tali aspetti costituisce sostanzialmente l'oggetto del presente lavoro e sarà affrontata in questo e nei prossimi capitoli, dedicati agli strumenti di conoscenza (capitoli 2 e 3) e alla tutela e al bilanciamento tra diritti (capitoli 4 e 5).

243 B.C. HAN, *op. cit.*, p. 75: «Il *vento digitale* della comunicazione e dell'informazione pervade ogni cosa e rende tutto trasparente. Soffia attraverso la società della *trasparenza*».

Come nel caso del termine "società dell'informazione e della conoscenza" anche quando si parla di trasparenza e conoscenza non si deve indulgere alla tentazione di interpretarli come sinonimi[244]. Non manca chi definisce la società attuale come società della trasparenza, ma nonostante questo il concetto differisce da quello di conoscenza. La trasparenza, che espone e "illumina" dati e informazioni, a ben vedere è strumento che può consentire la conoscenza, ma da sola, "nuda", non consente di eliminare aloni di opacità e il rumore della massa di informazioni rese disponibili[245].

La *disclosure*, valore del nostro tempo, che, come si vedrà più avanti, informa l'evoluzione normativa e l'azione dei pubblici poteri, assurge a fattore fondamentale della società proprio per il suo essere strumentale alla conoscenza e, altresì, per riuscire a creare una simmetria e un rapporto orizzontale fra governanti e governati, permettendo controllo e partecipazione "dal basso" e contrastando squilibri tra i "signori dei dati" pubblici e la collettività[246].

La trasparenza assume volti diversi e si traduce in strumenti differenti nella vigente normativa di riferimento italiana, oggetto precipuo di analisi, seppur esaminata nel contesto internazionale di riferimento.

La "trasparenza proattiva" (*proactive disclosure*), che si realizza con la pubblicazione di documenti, informazioni e dati da parte delle istituzioni, è accompagnata dalla "trasparenza reattiva" (*reactive disclosure*), che, invece, si ottiene in risposta alle istanze di conoscenza avanzate dagli interessati, dalla collettività di

---

244 B.C. HAN, *op. cit.*, p. 68: «La società della trasparenza è una società dell'informazione. L'informazione è, *in quanto tale*, un fenomeno della trasparenza, perché le manca ogni negatività. È un linguaggio positivizzato, operazionale».

245 B.C. HAN, *op. cit.*, p. 70: «Un semplice aumento di informazioni e di comunicazione non *rischiara* il mondo. Neppure l'evidenza agisce rischiarando. La massa di informazioni non produce alcuna *verità*. Più informazioni vengono liberate, meno intelligibile diviene il mondo. L'iper-informazione e l'iper-comunicazione non gettano alcuna *luce* nella tenebra». Al riguardo L. SARTORI, *op. cit.*, p. 773 ss. mette in guardia sul "lato oscuro della trasparenza" e sul fatto che il principio non debba diventare «un concetto fine a se stesso, adottato acriticamente come valore in sé, perché altrimenti si svuoterebbe velocemente di significato rimanendo lettera morta» (p. 774).

246 Al riguardo G. ZICCARDI, *Internet, controllo e libertà*, cit., p. 21 si chiede «La trasparenza è veramente il miglior disinfettante per il settore pubblico e per la democrazia in genere, o i problemi che pone in concreto, soprattutto se viene interpretata come trasparenza *radicale* e senza controllo, potrebbero rivelarsi maggiori dei possibili vantaggi?».

riferimento[247]. Nell'odierno contesto digitale la trasparenza si collega, altresì, in modo significativo con l'apertura: non è sufficiente una conoscenza "passiva" delle informazioni, dei dati e dei documenti resi disponibili, ma si configura una trasparenza "attiva", realizzata con il riutilizzo dei dati messi a disposizione, grazie agli *open data*.

In particolare l'analisi si concentrerà sugli strumenti di conoscenza, che attengono alle diverse configurazioni assunte dai dati nella contemporaneità e sono forieri di peculiari problematiche giuridiche e di complessi bilanciamenti tra diritti. È, infatti, necessario esaminare e capire in cosa consistono le diverse tipologie di dati che costituiscono gli strumenti di conoscenza della contemporaneità per comprendere le questioni che si pongono al diritto e i bilanciamenti da realizzare tra diritti[248].

Al fine di analizzare il governo dei dati e la tutela offerta ai diritti, l'analisi giuridica sarà attenta in particolare al ruolo dei pubblici poteri nel rapporto con la collettività, ma altresì al mondo privato e al potere dei giganti del web, che insieme alle istituzioni pubbliche rivestono il ruolo di "signori dei dati" della contemporaneità.

L'analisi spazierà, dunque, tra le diverse configurazioni di dati, che si traducono nei relativi strumenti di conoscenza: *closed data*, *open data*, *big data*.

I dati chiusi, i *closed data*, hanno bisogno della trasparenza proattiva e reattiva per essere svelati e garantire la conoscenza della collettività, gli *open data* danno significato al concetto di trasparenza attiva, garantendo il riutilizzo dei dati per crearne di nuovi, generare servizi e prodotti e, infine, i *big data*, fenomeno peculiare del nostro tempo, che si configura nelle caratteristiche della quantità, varietà e velocità, sono capaci di evolvere l'essenza stessa dei dati e dei loro utilizzi e condurre a riflessioni e a problematiche inedite[249].

---

247 In tal senso il Consiglio di Stato nel parere sullo schema di quello che sarebbe diventato il d.lgs. 97/2016, reso nell'adunanza di sezione 18/02/2016 (n. 515 del 24/02/2016).

248 Come sottolineano R. BORRUSO - S. RUSSO - C. TIBERI, *L'informatica per il giurista. Dal bit a Internet*, III ed., Giuffrè, Milano, 2009, prefazione, p. XXVII per comprendere il diritto è «innanzitutto indispensabile conoscere i fatti di vita, i fenomeni, i comportamenti che il diritto vuole disciplinare. Altrimenti non si è giuristi, ma semplici legulei». Mentre *closed data* e trasparenza saranno oggetto di questo capitolo, il capitolo 3 sarà dedicato a *open data* e *big data*.

249 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 15, secondo i quali i dati hanno cominciato ad accumularsi in misura tale da creare un fenomeno nuovo e peculiare. «Il cambiamento di dimensione

2.2. *Closed data* e *disclosure*

Il principio di trasparenza[250] costituisce lo strumento fondamentale per mettere a disposizione della collettività il patrimonio informativo pubblico, un insieme vastissimo di dati che altrimenti costituirebbero *closed data* nelle mani dei poteri pubblici[251].

I *closed data*, in specifico, sono sottoposti a un'operazione di *disclosure* e "visibilità del potere", presupposto per la "comprensibilità" dell'attività amministrativa[252], che avviene in due modi: l'amministrazione tramite un'azione positiva pubblica i dati, rendendosi parte attiva, in genere in conseguenza di espliciti obblighi di pubblicazione previsti dalla normativa di riferimento (trasparenza proattiva - *proactive disclosure*) oppure la collettività e, in specifico, chi è interessato a conoscere

---

ha prodotto un cambiamento di stato. Il cambiamento quantitativo ha prodotto un cambiamento qualitativo».

250 Sulla trasparenza amministrativa è presente una vastissima letteratura; cfr., *inter alia*, oltre agli autori citati nel corso della trattazione, G. ARENA, *Trasparenza amministrativa* (voce), in S. CASSESE (diretto da), in *Dizionario di diritto pubblico*, vol. VI, Giuffrè, Milano, 2006; F. MERLONI (a cura di), *La trasparenza amministrativa*, Giuffrè, Milano, 2008; M. OCCHIENA, *I principi di pubblicità e trasparenza*, in M. RENNA-F. SAITTA, (a cura di), *Studi sui principi di diritto amministrativo*, Giuffrè, Milano, 2012, p. 141 ss. L'analisi contenuta in questo lavoro tiene in considerazione, altresì, le riflessioni contenute in F. FAINI, *Trasparenza, apertura e controllo democratico dell'amministrazione pubblica,* in *Ciberspazio e diritto*, fasc. 1, 2014, pp. 39-70; F. FAINI - M. PALMIRANI, *The Right to Know Trough the Freedom of Information and Open Data,* in M. DEČMAN - T. JUKIĆ (a cura di), *Proceedings of the 16th European Conference on e-Government*", ACPI, 2016, pp. 54-62; F. FAINI, *Internet e il diritto a conoscere nei confronti delle pubbliche amministrazioni*, in P. PASSAGLIA - D. POLETTI (a cura di), *Nodi Virtuali, legami informali: Internet alla ricerca di regole*, Pisa University press, 2017, pp. 337-350.

251 Cfr. A. MONEA, *Pubblica amministrazione, vera "casa di vetro"?*, in *Azienditalia - il Personale*, fasc. 6, 2015, p. 311: «per "trasparenza" si può intendere, in prima approssimazione, la "visibilità di un corpo" e, nel caso di un'Organizzazione pubblica, la qualità di un corpo amministrativo di lasciarsi attraversare, per far vedere nitidamente, la sua azione e i suoi effetti. Trasferendo tale concetto nel mondo giuridico e, in specie in quello amministrativo, un'Organizzazione pubblica si può ritenere "trasparente" quando si rende aperta alla conoscenza di altri, quando pone in essere atti, procedimenti e condotte visibili, chiari, aperti e palesi ai più».

252 G. ARMAO, *Considerazioni su amministrazione aperta e protezione dei dati personali*, in *Amministrativ@mente*, fasc. 3-4, 2015, p. 8 ss.

alcuni dati li richiede alla pubblica amministrazione, che di conseguenza li rende conoscibili a seguito di un'istanza, come risposta quindi a una richiesta proveniente dalla società (trasparenza reattiva - *reactive disclosure*)[253].

Nel mettere a "nudo" informazioni, dati e documenti, in modo proattivo o reattivo, la *disclosure* assicura in mano alla collettività un significativo potere di controllo democratico sull'operato delle istituzioni, che si coordina con l'esigenza di una pubblica amministrazione capace di garantire all'utente un ruolo attivo di partecipazione e di promuovere allo stesso tempo l'*accountability* degli amministratori pubblici[254]. Lo stesso modello di *open government* trova fondamento nella trasparenza e nell'apertura, esplicitamente finalizzate, accanto all'efficacia dell'azione pubblica, al controllo democratico, capace peraltro di prevenire e contrastare fenomeni di illiceità e corruzione[255].

---

253 Cfr. E. FURIOSI, *L'accesso civico generalizzato, alla luce delle Linee Guida ANAC*, in *GiustAmm.it*, fasc. 4, 2017. Al riguardo cfr. F. MERLONI, *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Maggioli, Rimini, 2013, p. 18: «ad assicurare la trasparenza concorrono due strumenti, non necessariamente tra loro alternativi. L'accesso ai documenti e alle informazioni delle pubbliche amministrazioni e la pubblicità, oggi soprattutto grazie alle tecnologie dell'informazione, nella forma della pubblicazione di documenti e informazioni nei siti informatici delle pubbliche amministrazioni». Diversamente, secondo C. CUDIA, *Appunti su trasparenza amministrativa e diritto alla conoscibilità*, in *GiustAmm.it*, fasc. 12, 2016, p. 1 ss. «se l'aspirazione all'informazione diviene suscettibile di essere frustrata per effetto del confronto con altri interessi (pubblici o privati che siano), tale pretesa esula dall'ambito del principio di trasparenza-pubblicità»; per tale motivo l'Autrice distingue quali veri e propri strumenti di trasparenza e pubblicità la pubblicazione e il diritto di accesso civico semplice, che definisce "proprio", per i quali il legislatore ha risolto in via preliminare e in modo definitivo il problema dell'emersione di eventuali contro-interessi; mentre secondo l'Autrice le forme di accesso documentale e civico generalizzato, che definisce "improprio" o parziale, si configurano come rimedi all'assenza di trasparenza, dove si configura un bilanciamento con interessi diversi e si affaccia il potere discrezionale dell'amministrazione.

254 Cfr. F. MERLONI, *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, cit., p. 17 ss.

255 Cfr. F. MERLONI, *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, cit., p. 18: «Perché i cittadini, singoli e associati possano svolgere il loro compito di controllori dell'esercizio dei poteri che in loro nome la legge attribuisce alle amministrazioni e ai loro organi, occorre che ad essi sia consentita una conoscenza diffusa dell'azione, anche relativamente ai suoi principali risultati, gli atti adottati». E. TEDESCHI, *Il diritto di accesso: il nuovo dovere di collaborazione*

2.3. L'evoluzione normativa del principio di trasparenza

Il principio di trasparenza ha conosciuto un crescente interesse nei suoi confronti da parte della normativa italiana, particolarmente accentuato negli ultimi anni, che non si è tradotto solo nel mettere a disposizione un maggior numero di informazioni, ma ha mutato in modo profondo il principio stesso ampliandolo e arrivando, di recente, ad un autentico *right to know*, in linea con molti altri Paesi[256]. Nell'evoluzione normativa la trasparenza si atteggia sempre più come valore immanente all'ordinamento, allo stesso tempo finalistico, quale espressione di democrazia, e strumentale, in quanto idoneo ad assicurare la conoscenza[257].

Al fine di cogliere pienamente la configurazione della trasparenza nel nostro

---

dell'amministrazione (nota a TAR Lazio – Roma, sez. II ter, 15 marzo 2016, n. 3287), in *Giornale di diritto amministrativo*, fasc. 6, 2016, pp. 805-814 sottolinea che la trasparenza degli aspetti inerenti la gestione del bene pubblico è vista in dottrina come strumento essenziale per il rafforzamento della democrazia partecipativa.

256 G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.: la recente introduzione del Freedom Act of Information (FOIA) nell'ordinamento italiano*, in *GiustAmm.*it, fasc. 3, 2017, p. 1 ss.: «Nel percorso normativo della trasparenza è possibile individuare diverse fasi evolutive, ciascuna delle quali caratterizzata dal diverso rapporto tra la trasparenza e la forma di realizzazione della medesima, accesso o pubblicità di dati, documenti ed informazioni». Il Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA, parla della trasparenza come «uno dei gangli del diritto pubblico maggiormente soggetto all'evoluzione politica, sociale e tecnologica».

257 Cfr. F. PATRONI GRIFFI, *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *federalismi.it*, fasc. 8, 2013, p. 1 ss. M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, in *Informatica e diritto*, nn. 1-2, 2011, p. 256 parlano di «una dirompente maturazione del canone costituzionale della trasparenza, il quale non può essere più soltanto uno strumento finalizzato al controllo del procedimento amministrativo, bensì un vero e proprio risultato dell'azione amministrativa, che, pur arrivando direttamente dall'Unione Europea, è stata prontamente recepita dal legislatore italiano»; in tal senso anche Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA, che parla della trasparenza non più solo come un criterio informatore, ma anche come un obiettivo dell'azione amministrativa.

ordinamento e i relativi strumenti, è necessario esaminarne l'evoluzione normativa[258].

2.3.1. Dalla legge 241/1990 al d.lgs. 33/2013

La trasparenza, quale strumento atto a garantire il buon andamento e l'imparzialità della pubblica amministrazione, già costituisce principio informatore dell'attività amministrativa nella legge 7 agosto 1990, n. 241, come modificata nel 2005[259]. In specifico si pone come garanzia di accesso per coloro che ne hanno diritto[260], ma nell'evoluzione normativa si pone, altresì, come accessibilità che prescinde dalla sfera giuridica di determinati soggetti ed è tesa ad assicurare una conoscenza diffusa e generale delle informazioni. Emerge fin dalla genesi l'anima eterogenea del principio di trasparenza, che è al tempo stesso proattiva per mezzo della pubblicazione e reattiva in conseguenza di istanze di accesso[261].

Ben presto la trasparenza incontra influenti alleati nel suo cammino: le tecnologie informatiche e, in particolare, la rete sono capaci di rendere l'informazione disponibile a un numero indefinito di soggetti e consultabile in ogni momento da luoghi fisici diversi, permettendo una diffusione inedita e pervasiva, prima inarrivabile, capace di abbattere i confini geografici e i vincoli della fisicità. La conferma del connubio tra tecnologie

---

258 D.U. 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 *Rivista Italiana di Diritto Pubblico Comunitario*, fasc. 5, 2016, pp. 1019-1065 definisce la trasparenza quale «concetto polivalente e dai contenuti indefiniti», dietro al quale si nascondono significati molto diversi.

259 Art. 1, comma 1, legge 241/1990, come modificato dalla legge 11 febbraio 2005, n. 15, che pone il principio accanto ai criteri di economicità, efficacia, imparzialità (inserito dalla legge 18 giugno 2009, n. 69) e pubblicità. Al riguardo M.C. CAVALLARO, *Garanzie della trasparenza amministrativa e tutela dei privati*, in *Diritto amministrativo*, fasc. 1, 2015, p. 121 ss. sottolinea che il principio di pubblicità si pone come *species* del *genus* della trasparenza, quale "modo di essere dell'amministrazione" negli ultimi tempi cruciale per il corretto esercizio dei poteri pubblici, al fine di realizzare una dimensione più partecipata e imparziale volta ad assicurare la "visibilità del potere" e limitare l'opacità del processo decisionale.

260 Il Capo V (art. 22 e seguenti) della legge 241/1990 è dedicato al diritto di accesso ai documenti amministrativi.

261 L'aspetto di comunicazione e pubblicazione del patrimonio informativo pubblico viene ampiamente trattato dalla legge 7 giugno 2000, n. 150.

informatiche e *disclosure* arriva nel Codice dell'amministrazione digitale, il d.lgs. 82/2005, dove la trasparenza è finalità principale capace di caratterizzarne molte disposizioni; è stata poi fortificata da successivi interventi normativi, che non si sono limitati ad aumentare le informazioni oggetto di pubblicazione obbligatoria sui siti istituzionali, ma hanno dato valore alla pubblicazione online come la legge 18 giugno 2009, n. 69: gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti web da parte delle amministrazioni e, parallelamente, le pubblicazioni effettuate in forma cartacea cessano di avere effetto di pubblicità legale[262].

Un passaggio significativo si realizza con la c.d. Riforma Brunetta (di cui alla legge delega 4 marzo 2009, n. 15 e al relativo d.lgs. 27 ottobre 2009, n. 150), dal momento che, con particolare riferimento all'organizzazione e alla gestione del personale pubblico, viene previsto il concetto di *total disclosure*, accessibilità totale delle informazioni coniugata alla finalità di forme diffuse di controllo del rispetto dei principi di buon andamento e imparzialità[263]. Il concetto è simbolicamente significativo e sicuramente eccedente rispetto a quanto espresso dalle disposizioni, che lungi dal disporre un'accessibilità totale prevedono la pubblicazione di una serie determinata di

---

[262] Art. 32, legge 69/2009. La previsione decorre dal 1° gennaio 2011 e, nei casi previsti dall'art. 32, comma 2, dal 1° gennaio 2013 e lascia ferma la possibilità per le amministrazioni e gli enti pubblici, in via integrativa, di effettuare la pubblicità sui quotidiani a scopo di maggiore diffusione, nei limiti degli ordinari stanziamenti di bilancio (art. 32, comma 5, legge 69/2009). La disposizione fa salva la pubblicità nella Gazzetta Ufficiale dell'Unione europea, nella Gazzetta Ufficiale della Repubblica italiana e i relativi effetti giuridici e negli altri casi specifici previsti (art. 32, comma 7, d.lgs. 69/2009).

[263] In specifico, la normativa si riferisce alle informazioni concernenti ogni aspetto dell'organizzazione delle pubbliche amministrazioni, agli indicatori relativi agli andamenti gestionali e all'utilizzo delle risorse per il perseguimento delle funzioni istituzionali, ai risultati dell'attività di misurazione e valutazione svolta in proposito dagli organi competenti. Si tratta in particolare dell'art. 4, comma 7, legge 15/2009 e dell'art. 11, comma 1, d.lgs. 150/2009 (l'art. 11 del d.lgs. 150/2009 è stato abrogato dal d.lgs. 33/2013). D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 4 ss. sottolinea la convivenza nel decreto Brunetta di due obiettivi della trasparenza: l'efficienza della pubblica amministrazione e la prevenzione della corruzione, quest'ultima linea direttrice su cui si colloca il d.lgs. 33/2013.

informazioni, puntualmente specificata dalle disposizioni[264].

Nel corso degli anni, la trasparenza si configura come un principio che pervade norme, regole, direttive e linee guida e definisce caratteristiche e contenuti del sito web, porta di accesso digitale al patrimonio informativo delle amministrazioni pubbliche[265]; le riforme del Codice dell'amministrazione digitale incidono sugli strumenti con cui si garantisce la trasparenza, ampliandoli e cercando di conferire loro maggiore effettività[266].

Le disposizioni si succedono e talvolta si sovrappongono nel corso degli anni, fino a che non approdano nel corposo e auspicato riordino degli obblighi di pubblicità, trasparenza e diffusione delle informazioni compiuto dal cosiddetto decreto Trasparenza, il d.lgs. 14 marzo 2013, n. 33, in attuazione della cosiddetta legge Anticorruzione (legge 6 novembre 2012, n. 90)[267]. Come si deduce dalla legge delega da

---

264 G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit. sottolinea che con la riforma Brunetta mutano sia l'oggetto della trasparenza (non più i documenti, ma le informazioni), sia gli strumenti necessari alla sua realizzazione (non più l'accesso, ma la pubblicazione delle informazioni). M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento (commento a d.lgs. 25 maggio 2016, n. 97)*, in *Giornale di diritto amministrativo*, fasc. 5, 2016, p. 593 ss.: «L'euforia per la prodigiosa estensione a colpi di legge dell'area del conoscibile via internet traspariva dalle enfatiche formule che affioravano nella normativa di settore: su tutte, quella della "accessibilità totale", che tale non poteva essere, giacché le informazioni pubbliche (accessibili online) erano soltanto quelle corrispondenti alle ipotesi di pubblicazione doverosa».

265 Senza pretesa di esaustività, la direttiva 8/2009 per la riduzione dei siti web delle pubbliche amministrazioni e per il miglioramento della qualità dei servizi e delle informazioni online al cittadino, le relative *Linee guida per i siti web della PA* del 2010, aggiornate nel 2011, la delibera 105/2010 della Commissione Indipendente per la Valutazione, la Trasparenza e l'Integrità delle amministrazioni pubbliche (CiVIT, oggi diventata Anac) e le linee guida della CiVIT, oggi Anac, prodotte nel corso degli anni. Alle Linee Guida sui siti web hanno fatto seguito una serie di Vademecum sull'albo online (2011), su PA e *social media* (2011), sugli *open data* (2011), sulla misurazione della qualità dei siti web (2012), etc.

266 È il caso della profonda modifica al d.lgs. 82/2005, recata dal d.lgs. 235/2010, sulla quale sia consentito il rinvio a F. FAINI, *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 263-286.

267 Il d.lgs. 33/2013, recante «*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*» è stato adottato a seguito della delega di cui all'art. 1, commi 35 e 36, della legge 190/2012.

cui deriva, nel d.lgs. 33/2013 il principio di trasparenza si basa sulla centralità degli obblighi di pubblicazione ed è finalizzato al contrasto preventivo della corruzione e dei fenomeni di *maladministration*[268]. Proprio il decreto Trasparenza, come si vedrà, è stato oggetto della significativa recente riforma, recata dal d.lgs. 25 maggio 2016, n. 97, approvato in attuazione della legge 7 agosto 2015, n. 124, che "rivoluziona" il principio di trasparenza.

Il d.lgs. 33/2013 ha tentato di ovviare alle problematiche relative alla normativa in materia di trasparenza emerse nel corso degli anni: in particolare, le disposizioni e le meritevoli enunciazioni di principio che caratterizzano i diversi provvedimenti normativi, come lo stesso concetto di accessibilità totale, sono risultati spesso privi di forti meccanismi di *enforcement* e caratterizzati da frammentarietà e ridondanza insieme a un alto tasso di inosservanza[269].

A tal fine, il d.lgs. 33/2013, oltre ad aumentarli considerevolmente, ha riordinato gli obblighi di pubblicazione, che si erano sommati nel tempo, suddividendoli in macro-ambiti concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, l'uso delle risorse pubbliche, le prestazioni offerte e i servizi erogati e, infine, i "settori speciali"[270].

Le tecnologie informatiche diventano la strada maestra per garantire la

---

[268] Cfr. F. PATRONI GRIFFI, *op. cit.*, p. 5 e M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, in *Giornale di diritto amministrativo*, 2013, fasc. 8-9, p. 795 ss. Secondo E. CARLONI, *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, in *Rassegna Astrid*, fasc. 4, 2016 il d.lgs. 33/2013 riversa sulla pubblicità, quale obbligo di pubblicazione, le esigenze di controllo diffuso e di riconoscimento di un diritto a conoscere slegato dal possesso di particolari situazioni legittimanti, esigenze che altrove, di norma, sono incanalate come libertà di informazione nei *Freedom of Information Act*.

[269] Cfr. M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit., p. 795 ss.

[270] Tra i settori speciali rientrano i contratti pubblici di lavori, servizi e forniture, le attività di pianificazione e governo del territorio, il servizio sanitario nazionale, etc. Seppur il decreto Trasparenza compia un corposo riordino degli obblighi di pubblicazione, alcuni obblighi non sono compresi nel d.lgs. 33/2013, ma sono previsti da norme vigenti, precedenti e successive: a titolo di esempio gli obblighi di pubblicazione previsti in materia di *class action* dagli art. 1, comma 2, e art. 4, commi 2 e 6, d.lgs. 20 dicembre 2009, n. 198. Per un quadro maggiormente esaustivo degli obblighi di pubblicazione in capo alle amministrazioni cfr. la delibera CiVIT (oggi Anac) n. 50 del 4 luglio 2013, «*Linee guida per l'aggiornamento del Programma triennale per la trasparenza e l'integrità 2014-2016*» e relativi allegati.

trasparenza[271]: per pubblicazione, infatti, si intende esplicitamente quella «*nei siti istituzionali delle pubbliche amministrazioni dei documenti, delle informazioni e dei dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, cui corrisponde il diritto di chiunque di accedere ai siti direttamente ed immediatamente, senza autenticazione ed identificazione*»[272]. L'amministrazione, in tal caso, in attuazione della normativa, pubblica quanto previsto dalle disposizioni senza attendere un'istanza specifica di accesso: si tratta di trasparenza realizzata grazie alla pubblicazione sui siti istituzionali di documenti, informazioni e dati indicati dalla legge e, dunque, di trasparenza proattiva.

Il decreto, proprio per rendere la trasparenza effettiva e di semplice fruizione, conferisce volto omogeneo alle pubbliche amministrazioni grazie alla previsione di contenuti organizzati in una veste grafica comune: viene disciplinata la specifica sezione "Amministrazione Trasparente" nella *home page* del sito web istituzionale[273]. Di conseguenza, vengono fortificati e uniformati gli obblighi di pubblicazione delle amministrazioni, tenute a rivedere i propri processi per garantire un'informazione completa e aggiornata, perseguibile solo preoccupandosi della pubblicazione fin dal momento della produzione del dato, nell'ottica di vere e proprie case di vetro digitali.

Alle previsioni del d.lgs. 33/2013 si collega espressamente e fedelmente il provvedimento normativo "alleato" costituito dal Codice dell'amministrazione digitale: i siti istituzionali, ai sensi dell'art. 54 del d.lgs. 82/2005, devono contenere i dati di cui al d.lgs. 33/2013, ossia quelli oggetto di pubblicazione obbligatoria ai sensi della

---

271 Nel d.lgs. 33/2013 l'uso dell'informatica e, in particolare, la pubblicazione sul web diventano la strada obbligata per realizzare la trasparenza, a differenza della Riforma Brunetta in cui la pubblicazione sul sito web istituzionale era uno degli strumenti possibili per assicurare la trasparenza: ai sensi dell'art. 11 del d.lgs. 150/2009 (abrogato dal d.lgs. 33/2013), infatti, «*la trasparenza è intesa come accessibilità totale, anche attraverso lo strumento della pubblicazione sui siti istituzionali delle amministrazioni pubbliche* […]».

272 Art. 2, comma 2, d.lgs. 33/2013.

273 Art. 2, comma 2, e art. 9, comma 1, d.lgs. 33/2013, secondo cui le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente". L'allegato A del d.lgs. 33/2013 dettaglia struttura e organizzazione dei contenuti della sezione "Amministrazione Trasparente" dei siti web istituzionali.

normativa[274].

Al fine di eliminare aloni di opacità, il decreto Trasparenza ha previsto significativi meccanismi di *enforcement*, quali gli strumenti di vigilanza sull'attuazione delle disposizioni e le sanzioni relative al mancato rispetto delle norme[275]. In particolare, al fine di permettere il controllo dei cittadini, agli obblighi di pubblicazione viene collegato un istituto, l'accesso civico (art. 5, già nella formulazione precedente alla riforma del d.lgs. 97/2016), ossia il diritto di chiunque di richiedere all'amministrazione documenti, informazioni e dati oggetto di pubblicazione obbligatoria, nei casi in cui sia omessa la loro pubblicazione, senza nessuna limitazione quanto alla legittimazione soggettiva, senza necessità di motivazione e gratuitamente[276].

Lo strumento dell'accesso civico si pone come un rimedio in caso di inadempimento, che ne costituisce il presupposto perché possa essere agito: di

---

274 Il d.lgs. 217/2017 ha integrato l'art. 54 del d.lgs. 82/2005 prevedendo come contenuto dei siti, oltre ai dati di cui al d.lgs. 33/2013, quelli ulteriori previsti dalla legislazione vigente.

275 In particolare Capo VI (art. 43 e ss.) del d.lgs. 33/2013. La vigilanza sull'attuazione delle disposizioni viene affidata a una serie di soggetti interni ed esterni all'amministrazione, quali il Responsabile della trasparenza, gli Organismi Indipendenti di Valutazione (OIV) e l'Autorità Nazionale Anticorruzione (Anac). L'inadempimento delle disposizioni costituisce elemento di valutazione della responsabilità dirigenziale, è eventuale causa di responsabilità per danno all'immagine dell'amministrazione e comporta comunque una valutazione ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili (art. 46, d.lgs. 33/2013); sono previste inoltre sanzioni per casi specifici (art. 47, d.lgs. 33/2013).

276 L'accesso civico è previsto all'art. 5 del d.lgs. 33/2013: per M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit., p. 795 ss. l'istituto si pone come «"pungolo" al corretto adempimento degli obblighi di pubblicazione da parte delle amministrazioni, più che come strumento di potenziamento della cittadinanza attiva». M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo*, cit., p. 593 ss. rileva come lo strumento dell'accesso civico nella prassi sia rimasto pressoché lettera morta: «l'astuzia che aveva partorito, nel 2013, l'accesso civico ne ha condizionato anche la sorte. Ridotto a strumento di *enforcement* di obblighi di legge e limitato nella sua estensione da una logica dirigista che affida al legislatore la scelta su cosa debba essere d'interesse dei cittadini, quel diritto è stato ignorato dai suoi legittimi titolari». Cfr., altresì, F. MERLONI, *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, cit., p. 27, che considera importanti passi avanti del d.lgs. 33/2013 «da un lato l'opera di "codificazione" degli obblighi di pubblicazione che gravano sulle pubbliche amministrazioni, dall'altro le misure volte a dare a questi obblighi una sicura effettività».

conseguenza, il d.lgs. 33/2013, prima della riforma del d.lgs. 97/2016, si affida esclusivamente a un meccanismo di pubblicità obbligatoria di specifici documenti, dati e informazioni, garantiti dalla possibilità di azionare il diritto di accesso civico, che permette un effettivo controllo democratico sul rispetto delle norme.

Pertanto nella disciplina, prima dell'ultima riforma, l'oggetto della pubblicità è normativamente predeterminato[277]: per tutto ciò che non è oggetto di pubblicazione obbligatoria la trasparenza è facoltativa, a seguito della scelta discrezionale dell'amministrazione[278], e la disciplina di riferimento resta quella del diritto di accesso documentale già previsto dalla legge 241/1990. Secondo la legge del 1990 il diritto di accesso può essere esperito solo in presenza di un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso, e deve essere accompagnato da una motivazione[279]; non siamo

---

277 Cfr. G. MANCOSU, *Trasparenza amministrativa e* open data*: un binomio in fase di rodaggio*, in *federalismi.it*, fasc. 17, 2012, p. 10, secondo cui «il rischio è quello di "ipertrofia" della pubblicità con esiti destinati ad essere perennemente inappaganti».

278 Art. 4, d.lgs. 33/2013 (poi abrogato con il d.lgs. 97/2016 e divenuto con modifiche l'art. 7-bis). In tal senso E. CARLONI, *I principi del codice della trasparenza (artt. 1, commi 1 e 2, 2, 6)*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Maggioli, Rimini, 2013, p. 29 ss. Secondo M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit., p. 795 ss. viene posta dall'ordinamento italiano una distinzione fra la pubblicità necessaria (prevista dalle norme sugli obblighi di pubblicazione) e quella facoltativa: «la pubblicità, essendo effettiva (e azionabile) solo se e nei limiti in cui è imposta dalla legge, finisce per operare come una regola di stretto diritto positivo», contrariamente all'enfatico e astratto principio di accessibilità totale; non si configura pertanto prima della riforma del d.lgs. 97/2016 un diritto fondamentale a conoscere (*right to know*) come nei sistemi FOIA, in cui può essere fatto valere in assenza di norme, caratterizzandosi come un valore-guida. G. GARDINI, *Il codice della trasparenza: Un primo passo verso il diritto all'informazione amministrativa?*, in *Giornale di diritto amministrativo*, fasc. 8-9, 2014, pp. 875-891: «La pubblicità è considerata regola di stretto diritto positivo, non un principio generale, ed è garantita nella misura in cui sia prevista da una norma».

279 Art. 22 e ss. della legge 241/1990: il diritto si esercita con la visione e l'estrazione di copia dei documenti amministrativi. Sulle differenze relative ai due istituti si sofferma la circolare n. 2 del 19 luglio 2013 della Presidenza del Consiglio dei ministri – Dipartimento della Funzione Pubblica, *D.lgs. n. 33/2013 – Attuazione della trasparenza*, in *www.funzionepubblica.gov.it* e si esprime anche la giurisprudenza, in particolare TAR Lombardia, Sezione Quarta, sentenza n. 1904, depositata in data 18 luglio 2013; Consiglio di Stato, in sede giurisdizionale, Sezione Sesta, sentenza n. 5515, depositata il 20 novembre 2013; TAR Lazio, Sezione Terza Bis, sentenza n. 233, depositata in data 9 gennaio 2014; TAR Lazio, Sezione Terza Quater, sentenza n. 3017, depositata in data 8 marzo 2016.

di fronte a un vero e proprio diritto all'informazione, ma piuttosto a una trasparenza di tipo procedimentale e a un diritto alla conoscenza condizionato dalla presenza di una legittimazione soggettiva e di una motivazione[280].

Prima del d.lgs. 97/2016 il *right to know* non viene tutelato in se stesso, ma nella misura in cui coincide con gli obblighi di pubblicazione che fanno scattare l'accesso civico ai sensi del d.lgs. 33/2013 o alla presenza delle condizioni legittimanti per azionare il diritto di accesso documentale di cui alla legge 241/1990.

2.3.2. Trasparenza e *Freedom of Information Act* (FOIA) italiano: il d.lgs. 97/2016 nel quadro internazionale di riferimento

In considerazione dei limiti della normativa e alla luce del contesto internazionale che offre tutela al *right to know* nei cosiddetti *Freedom of Information Act* in molti Paesi del mondo, è stato approvato il decreto legislativo 25 maggio 2016, n. 97 anche a seguito delle sollecitazioni della società civile, come quelle provenienti dall'iniziativa Foia4Italy[281]: in virtù della delega di cui all'art. 7 della legge 7 agosto 2015, n. 124 (c.d. legge Madia), il provvedimento ha modificato il d.lgs. 33/2013, al fine di garantire un autentico "diritto a conoscere" della collettività nei confronti delle istituzioni[282].

Il cambiamento di prospettiva è evidente fin dal concetto stesso di trasparenza, finalizzata alla tutela dei diritti, alla partecipazione e al controllo democratico: si parla di «*accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli*

---

280 Cfr. M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit., p. 795 ss. e G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit.

281 Il sito di riferimento dell'iniziativa, che ha coinvolto più di 30 associazioni attive in materia di diritti civili, trasparenza, libertà di informazione e *open government*, è *www.foia4italy.it*; nel sito è presente anche la proposta di legge elaborata dalle associazioni di Foia4Italy.

282 G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit., p. 1 ss.: «La riforma si è resa necessaria per tutelare il *right to know*, ossia il diritto di conoscere dei cittadini, per controllare le istituzioni, come sana espressione del principio di democrazia, a prescindere da qualsiasi forma di tutela precontenziosa o contenziosa».

interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche»[283].

Gli obiettivi delineati sono perseguiti dal d.lgs. 97/2016 con profonde modifiche e integrazioni al d.lgs. 33/2013 che incidono sotto diversi profili: viene ampliato l'ambito soggettivo di applicazione[284], sono razionalizzati e resi più sostenibili gli obblighi di pubblicazione[285], sono rafforzati gli obblighi in materia di spesa pubblica, contratti pubblici e personale[286], viene fortificato il ruolo dell'Anac[287] e sono ampliate responsabilità e sanzioni[288].

---

283 Art. 1, comma 1, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016.

284 Il d.lgs. 97/2016 ha introdotto l'art. 2-bis nel d.lgs. 33/2013 dedicato all'ambito soggettivo di applicazione delle disposizioni, che comprende tutte le amministrazioni di cui all'art. 1, comma 2, del d.lgs. 165/ 2001, comprese le autorità portuali, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione (comma 1); le disposizioni si applicano anche, in quanto compatibili, agli enti pubblici economici, agli ordini professionali, alle società in controllo pubblico (escluse le società quotate) e alle associazioni, alle fondazioni e agli enti di diritto privato ad essi assimilati e previsti nel comma 2 e, limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea, alle società in partecipazione pubblica e agli altri enti di diritto privato assimilati di cui al comma 3.

285 La semplificazione degli obblighi di pubblicazione si pone come conseguenza del riconoscimento del *right to know* come diritto fondamentale; cfr. M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «quanto agli obblighi di pubblicazione, perno della precedente strategia di promozione della trasparenza, il legislatore delegato ha interpretato in modo prudente il mandato, operando una razionalizzazione leggera, che però dischiude la prospettiva di una più incisiva semplificazione affidata alla pubblicazione di banche dati centrali e all'Autorità nazionale anticorruzione (Anac)».

286 Artt. 4-bis, 14 e 37, d.lgs. 33/2013.

287 Art. 3, comma 1-bis e comma 1-ter, e art. 8, comma 3-bis.

288 Questi obiettivi del d.lgs. 97/2016 sono precisati dalla stessa relazione illustrativa di accompagnamento al provvedimento normativo. Tra le misure introdotte, a fini di semplificazione, concentrazione e riduzione degli oneri, viene prevista la possibilità di adempiere agli obblighi di pubblicazione relativi a una serie di banche dati dettagliate nell'allegato B del d.lgs. 33/2013 mediante la comunicazione dei dati, delle informazioni o dei documenti detenuti e con la pubblicazione del collegamento ipertestuale alla banca dati contenente i relativi dati, informazioni e documenti (art. 9-bis, comma 2, d.lgs. 33/2013, introdotto dal d.lgs. 97/2016). Per un'analisi dei meccanismi di razionalizzazione e semplificazione degli obblighi di pubblicazione, attivati dalla normativa cfr. M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss. Più

Le novità più significative, però, riguardano proprio l'ampiezza del diritto a conoscere. Sotto tale profilo il d.lgs. 97/2016 non impatta sulla legge 241/1990 e sul diritto di accesso documentale ivi previsto, che pertanto rimane strumento vigente[289], ma incide sul diritto di accesso civico disciplinato nel d.lgs. 33/2013.

Accanto al già previsto diritto di accesso civico "semplice", la riforma prevede il diritto di accesso civico "generalizzato", che permette a chiunque (senza bisogno di alcuna legittimazione soggettiva) senza motivazione di accedere ai dati e ai documenti detenuti dalla pubblica amministrazione ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti[290].

In tal modo si concretizza il passaggio a quella logica orizzontale che deve caratterizzare il rapporto tra pubblici poteri e cittadini nel modello di *open government*[291] e che è conforme alle modalità relazionali della società digitale, rispetto

---

ampiamente, per un commento sistematico del d.lgs. 33/2013, a seguito della riforma del d.lgs. 97/2016, cfr. B. PONTI (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Maggioli, Rimini, 2016.

289 L'art. 5, comma 11, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, esplicitamente afferma che restano ferme le diverse forme di accesso degli interessati previste dal capo V della legge 241/1990.

290 Secondo P. FALLETTA, *Il* freedom of information act *italiano e i rischi della trasparenza digitale*, in *federalismi.it*, fasc. 23, 2016, p. 4 ss. si attua un rovesciamento di logica rispetto alla legge 241/1990, imponendo il versante attivo della trasparenza rispetto a quello passivo della legge sul procedimento.

291 S. VACCARI, *Il difficile bilanciamento tra* favor *per la trasparenza e (necessaria) tutela della riservatezza nel d.lgs. 33/2013*, in *Il diritto dell'economia*, fasc. 1, 2015, p. 154 ss. «Attraverso tale forma di attuazione della "visibilità del potere" e dell'amministrazione aperta si cerca di perseguire lo scopo di promuovere la partecipazione e la "demarchia" dei cittadini nell'ottica di favorire forme diffuse di controllo sull'esercizio delle funzioni istituzionali e sulle modalità di utilizzo delle risorse pubbliche, facendo acquisire alla trasparenza un carattere di servizio rispetto a principi e finalità primarie dell'ordinamento (si veda il comma 2 dell'art. 1 del d.lgs. 33/2013), quali il principio democratico, l'imparzialità, il buon andamento, l'efficacia ed efficienza nell'utilizzo di risorse pubbliche, la responsabilità e l'integrità e la lealtà nel servizio alla nazione». Il concetto di demarchia o democrazia partecipativa fa riferimento a «un modello di amministrazione paritaria e condivisa con il cittadino al quale, nell'esercizio della funzione amministrativa, viene conferito il ruolo di co-amministrante dotato di posizioni di libertà attiva nei confronti della p.a. detentrice del potere d'impero con la quale dialoga all'interno di un mutato rapporto con i pubblici poteri caratterizzato in senso collaborativo più che conflittuale».

alle resistenti impostazioni ancora verticali e autoritative quali le modalità di accesso documentale e gli obblighi di pubblicazione[292]. Sotto tale profilo, nell'evoluzione normativa esaminata il principio di trasparenza e la disciplina che ne è espressione si stagliano come elementi significativi dei processi di digitalizzazione e apertura della pubblica amministrazione[293].

Di conseguenza, nell'ordinamento giuridico italiano attuale convivono diversi strumenti di accesso, quali strumenti di "trasparenza reattiva" che permettono alla collettività di conoscere il patrimonio informativo pubblico: l'accesso documentale ai sensi della legge 241/1990, l'accesso civico "generalizzato" ai sensi del d.lgs. 33/2013, che viene introdotto dal d.lgs. 97/2016, e l'accesso civico "semplice", che in realtà costituisce più propriamente una risposta all'inadempimento degli obblighi di pubblicazione[294].

---

[292] Cfr. P. FALLETTA, *op. cit.*, p. 5: tale visione mette al centro il destinatario del servizio pubblico innovando lo stesso diritto amministrativo che non deve esaurirsi nel c.d. "diritto autoritativo", ma deve articolarsi anche nel c.d. "diritto convenzionale". Secondo S. LA PISCOPIA, *Italian Freedom of Information Act: approcci interpretativi e dottrinari*, in *Periodico di Diritto e Procedura Penale Militare*, fasc. 5, 2016, p. 2 ss. la riforma configura «la trasformazione epocale del limitato diritto all'informazione amministrativa, da una generale strumentalità *uti cives,* ad un diritto *uti singuli* per la protezione di un bene fondamentale o della vita: quello all'informazione trasparente del singolo, chiunque egli sia. Si passa quindi, ora sì, dal *need to know* al *right to know* procedendo ad un superamento della stringente selettività dell'informazione soggettivamente fruibile. […] L'informazione diventa un "bene della vita" che può essere funzionale anche alla tutela di interessi patrimoniali del cittadino, superando la concezione dell'informazione come mero oggetto di conoscenza garantito da generali finalità d'interesse pubblico»; la riforma incarna per alcuni versi «l'antico spirito partecipativo della *res publica* ciceroniana».

[293] Secondo S. CALZOLAIO, *op. cit.*, p. 187 ss. la trasparenza amministrativa sul web rappresenta «quanto di più vicino possa immaginarsi al *digital by default standard*, poiché si tratta di obblighi di pubblicazione naturalmente pensati per la rete internet e di una forma di accessibilità garantita in modo sostanzialmente esclusivo attraverso il web» (p. 188): i fini della normativa sulla trasparenza non sono esplicitamente tesi alla digitalizzazione pubblica, ma la trasparenza può realizzarsi solo attraverso un uso massivo del web. Secondo B. CAROTTI, *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa,* cit., p. 625 ss. la trasparenza procede di pari passo con la digitalizzazione, che è a sua volta strumentale al perseguimento della *disclosure*.

[294] S. VILLAMENA, *Il c.d. FOIA (o accesso civico 2016) ed il suo coordinamento con istituti consimili*, in *federalismi.it*, fasc. 23, 2016, p. 1 ss. muove critiche alla generica denominazione "accesso civico" da parte del legislatore per riferirsi a due istituti diversi, sottolineando il cattivo coordinamento tra la vecchia e la nuova stesura del d.lgs. 33/2013.

L'intervento del d.lgs. 97/2016 si è reso necessario per tutelare pienamente la libertà di conoscere nel nostro Paese e ha fatto parlare del provvedimento normativo in termini di *Freedom of Information Act* italiano[295].

Sotto tale profilo è interessante uno sguardo oltre confine per esaminare come si atteggiano al riguardo alcune significative discipline di altri ordinamenti, per poi concentrarsi sull'analisi del principio di trasparenza e del diritto di accesso civico generalizzato nella nostra normativa, a seguito della riforma del 2016.

Nel contesto internazionale, sotto tale punto di vista, è particolarmente significativo il caso degli Stati Uniti d'America, che già nel 1966 adottano il *Freedom of Information Act* (FOIA), emendato successivamente numerose volte, anche per esigenze di adeguamento alle pronunce giurisprudenziali[296]: particolarmente rilevante in proposito l'*Electronic Freedom of Information Act* (c.d. EFOIA) del 1996, che ha adeguato il testo alle possibilità offerte dalle nuove tecnologie e ha costituito un importante cambio di paradigma prevedendo la pubblicazione obbligatoria online di una

---

[295] G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit.: «Con la riforma il legislatore ha ridefinito il rapporto tra mezzo (obbligo di pubblicazione) e fine (diritto di accedere ai dati e ai documenti), che nel D. Lgs. 33 del 2013 non era ancora in linea con la maggior parte dei modelli di accesso alle informazioni adottati a livello europeo ed internazionale ed aderenti al modello FOIA. Nella disciplina di cui al D. Lgs. 33 del 2013, infatti, l'esercizio del diritto di accesso è stato previsto come strumentale all'adempimento dell'obbligo di pubblicazione, mentre nei sistemi liberali che si sono ispirati al FOIA, il fine è rappresentato dalla libertà di accedere alle informazioni e tale fine si persegue e si realizza soprattutto facendo ricorso al mezzo della pubblicazione delle informazioni, dei dati e dei documenti delle pubbliche amministrazioni». Il *right to know* nei modelli FOIA persegue finalità di *accountability*, *participation* e *legitimacy*; cfr. M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit.

[296] Il FOIA viene adottato come emendamento all'*Administrative Procedure Act* del 1946. Per un'analisi delle origini e dell'evoluzione del FOIA statunitense cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., secondo la quale il FOIA statunitense «è universalmente considerato (in modo talora del tutto acritico) come "il" modello di riferimento ed è, più in generale, usato di regola quale metro di paragone per la valutazione delle legislazioni nazionali in materia di trasparenza». Secondo P. FALLETTA, *op. cit.*, p. 2 la riforma italiana ha mutuato essenzialmente tre profili dal modello americano di FOIA: «il "doppio binario" tra obblighi di pubblicazione e richieste di accesso civico; l'accessibilità, in linea di principio, totale ai documenti delle amministrazioni statali; il riconoscimento dell'accesso anche a chi non dimostri la titolarità di un interesse specifico alla conoscenza degli atti».

grande quantità di dati[297].

Nel FOIA americano la trasparenza si caratterizza come accessibilità totale e il regime di accesso è *open to all*: i documenti e le informazioni detenuti da ogni *Federal Agency*, indipendentemente dal supporto utilizzato, sono accessibili da chiunque senza bisogno di una specifica legittimazione; grava sull'amministrazione dover provare l'esistenza di ragioni che impediscano di soddisfare la richiesta[298]. La normativa prevede un elenco tassativo di nove *exemptions*, quali il segreto nell'interesse della difesa nazionale o della politica estera, i segreti industriali e la violazione della privacy e tre leggi speciali di esclusione; al riguardo è importante precisare che la giurisprudenza ha elaborato un'interpretazione piuttosto restrittiva sulla possibilità di fare ricorso alle eccezioni[299].

Gli USA accompagnano la regolamentazione del diritto di accesso, che dà sostanza alla trasparenza reattiva, con la previsione di un'ampia trasparenza proattiva: il FOIA prescrive a ogni *Federal Agency* di pubblicare sul *Federal Register*, nelle cosiddette *online reading room*, una serie di informazioni relative all'assetto organizzativo e alle regole sostanziali e procedurali. Nel corso degli anni sono aumentati i documenti che devono essere resi disponibili al pubblico ed è stata prevista la pubblicazione obbligatoria per mezzo di strumenti informatici di tutti quelli adottati dopo il 1° novembre 1996.

È, altresì, previsto un interessante meccanismo di collegamento fra trasparenza reattiva e proattiva (c.d. *user-driven proactive transparency*): si prevede la messa a disposizione dei documenti oggetto delle richieste, laddove per la natura delle

---

297 Cfr. A. BONOMO, *Informazione e pubbliche amministrazioni. Dall'accesso ai documenti alla disponibilità delle informazioni*, Cacucci, Bari, 2012 e V. LUBELLO, *op. cit.*, p. 371 ss.

298 La richiesta deve individuare ragionevolmente l'oggetto dell'accesso e deve essere fatta in ottemperanza alla normativa; il tempo ordinario di risposta è previsto in 20 giorni lavorativi. Le istituzioni non sono tenute a creare dati, per rispondere alle istanze, ma devono attingere solo ai dati già a disposizione. Ogni *Federal Agency* deve rendere noto l'importo degli eventuali oneri applicabili; la documentazione deve essere fornita senza costo o ad un costo ridotto, qualora la divulgazione sia fatta nell'interesse del pubblico e non sia fatta principalmente per interesse commerciale.

299 Cfr. A. BONOMO, *op. cit.*

informazioni, la *Federal Agency* ritenga che sia diventata o sia in procinto di diventare oggetto di successive richieste sostanzialmente identiche[300].

Il FOIA del 1966 è stato emendato nel 2007 dall'*Open Government Act*[301], prevedendo l'istituzione di uno *Chief FOIA Officer* in ogni Agenzia federale e dell'*Office of Government Information Services* (OGIS)[302], organismo che dal 2009 svolge funzioni quali la verifica del rispetto del FOIA, la formulazione di raccomandazioni e la mediazione nelle controversie[303].

Il sistema statunitense si caratterizza, pertanto, per un ampio livello di accessibilità, che permette ai cittadini di esercitare un controllo diffuso sull'attività governativa e di servirsi dell'informazione come strumento di partecipazione democratica[304].

Il FOIA, insieme ad altri atti significativi, quali il *Federal Advisory Committee Act* del 1972, il *Privacy Act* del 1974, il *Government in the Sunshine Act* del 1976 e il *Paperwork Reduction Act* del 1984, caratterizza le amministrazioni per la diffusione delle informazioni pubbliche e il principio di trasparenza: in linea con questi atti, i provvedimenti del Governo Obama hanno dato vita al modello di *open government*. A tale proposito sono particolarmente rilevanti il *Memorandum "Freedom of Information Act"* del 2009[305] e il *FOIA Improvement Act* del 2016: la prospettiva adottata è quella di

---

300 Cfr. M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit. In merito A. BONOMO, *op. cit.* sottolinea che il sistema mostra attenzione anche alla qualità delle informazioni: nel 2002 sono state pubblicate le *Guidelines* finalizzate a garantire che le informazioni prodotte, utilizzate e diffuse siano conformi a elevati standard di qualità, attraverso la previsione di specifiche procedure di riesame.

301 In specifico, l'*Openness Promotes Effectiveness in our National Government Act* o *Open Government Act*.

302 Cfr. *ogis.archives.gov*.

303 Cfr. A. MARCHETTI, *Il diritto di accesso: modelli di enforcement e cause di exemptions nella prospettiva comparata*, in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale Scientifica, Napoli, 2012, p. 209 ss. e S. VACCARI, *op. cit.*, p. 154, che sottolinea come negli Stati Uniti i documenti sui quali è previsto l'accesso sono interpretati come proprietà collettiva, sulla quale il cittadino, per mezzo del diritto di accesso, fa valere una posizione equiparabile a un diritto reale su un bene di tipo immateriale.

304 Cfr. A. BONOMO, *op. cit.*

305 Secondo V. LUBELLO, *op. cit.*, p. 380 il Memorandum può essere visto come una sorta di interpretazione autentica del FOIA stesso.

una *presumption of openness* a causa della quale può essere negato l'accesso solo con adeguata motivazione in presenza di un divieto posto da una norma o per la sussistenza di un interesse protetto da una delle cause di esenzione[306].

Trova ispirazione nel modello statunitense il Regno Unito, che ha adottato recentemente, nel 2000, il *Freedom of Information Act* (FOIA) e, nel 2002, lo speculare *Freedom of Information (Scotland) Act*. A ciascuna persona viene riconosciuto il diritto di accedere alle informazioni, detenute in ogni forma, in possesso di amministrazioni e autorità pubbliche, senza limitazioni di tipo soggettivo e senza obbligo di motivazione[307]. Si prevede un ampio elenco di *exemptions*, alcune assolute, per le quali non si applica il *public interest test* (es. sicurezza o informazioni personali di terzi), altre che implicano la sottoposizione al *public interest test*, ossia la valutazione dell'amministrazione se prevalga l'interesse a diffondere o a mantenere segreta l'informazione (es. difesa nazionale e relazioni internazionali): in entrambi i casi l'amministrazione conserva il potere discrezionale di non applicare le *exemptions*[308].

La normativa, a differenza di altri ordinamenti, non prevede un elenco di informazioni oggetto di pubblicazione obbligatoria, ma dispone che le amministrazioni realizzino e rendano noti dei *publications schemes*, indicando le tipologie di informazioni che saranno pubblicate, la forma di pubblicazione ed eventuali costi, tenendo conto nella loro elaborazione dell'interesse ad accedere dei cittadini[309].

In direzione di effettività l'attuazione dei FOIA inglese e scozzese è stata prevista nel 2005 per dare tempo alle amministrazioni di organizzarsi in vista dell'applicazione, adottare i propri *publications schemes* e studiare le ipotesi ricadenti nelle esclusioni.

---

306 Cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., che osserva come per lunghissimo tempo il livello di implementazione del FOIA sia stato a livelli bassissimi con un sostegno molto scarso delle corti statunitensi (anche grazie all'ampiezza delle deroghe) e sia migliorato con le diverse riforme nell'arco degli anni. Secondo V. LUBELLO, *op. cit.*, p. 379 i tre *memoranda* dell'amministrazione Obama si collocano «nella dimensione "politica" del FOIA; non si tratta di emendamenti legislativi dell'atto stesso, ma di provvedimenti amministrativi volti ad organizzare e migliorare la diffusione delle informazioni generate e raccolte nella sfera pubblica».

307 La richiesta di accesso deve descrivere le informazioni desiderate, di norma è priva di costi e l'amministrazione ha un termine ordinario di 20 giorni lavorativi per rispondere.

308 Cfr. A. BONOMO, *op. cit.* e A. MARCHETTI, *op.cit*.

309 Cfr. G. GARDINI, *op. cit.*, p. 875 ss.

L'ordinamento britannico pone a presidio della normativa un'autorità, l'*Information Commissioner's Office* (ICO), che ha la funzione di promuovere il rispetto della normativa e la predisposizione degli schemi di pubblicazione, sensibilizzare i cittadini, adottare raccomandazioni ed esaminare i ricorsi per diniego di accesso[310].

Oltre agli ordinamenti di *Common Law*, l'attenzione alla *freedom of information* e al *right to know* è diffusa in molti altri Stati del mondo[311] e trova impulso anche nella normativa e nelle strategie dell'Unione europea, che garantisce e regola il principio di trasparenza e il diritto di accesso[312].

In particolare, l'art. 1 del Trattato dell'Unione europea (TUE) dispone che «*le decisioni siano prese nel modo più trasparente possibile* […]» e l'art. 15 del Trattato sul funzionamento dell'Unione europea (TFUE) (ex art. 255 TCE) ribadisce il principio di trasparenza e contiene le disposizioni in materia di accesso, confluite nel testo dopo il

---

310 Cfr. *ico.org.uk*.

311 Sono oltre 100 gli Stati nel mondo che hanno adottato normative relative alla *freedom of information*: la Svezia già nel 1766 (la disciplina negli anni è stata aggiornata) ha adottato una legislazione sulla libertà di informazione, simile agli attuali FOIA e va considerata come modello di riferimento in materia di trasparenza; al riguardo D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss. sottolinea come la normativa svedese rischi di trascurare quasi del tutto le opposte esigenze di riservatezza, ponendo problemi di compatibilità col nuovo Regolamento (UE) 2016/679. Per un'analisi comparata cfr., *inter alia*, J.M. ACKERMAN - I.E. SANDOVAL-BALLESTEROS, *The Global Explosion of Freedom of Information Laws*, in *Administrative Law Review*, vol. 58, n. 1, 2006, p. 85 ss.; D. BANISAR, *Freedom of Information Around The World 2006*. *A Global Survey of Access to Government Information Laws*, 2006, *www.humanrightsinitiative.org*; A. BONOMO, *op. cit.*; H. KRANENBORG - W. VOERMANS*, Access to Information in the European Union. A comparative Analysis of EC and Member State legislation*, Europa Law Publishing, Groningen, 2005; T. MENDEL, *Freedom of Information: A Comparative Legal Survey*, UNESCO, Parigi, 2008; M. SAVINO, *The Right to Open Public Administrations in Europe: Emerging Legal Standards*, Ocse, Sigma papers, Paris, 2010, pp. 1-40; R. TARCHI, *Il diritto d'accesso nella prospettiva comparata* e A. MARCHETTI, *op.cit*., entrambi in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale scientifica, Napoli, 2012, p. 141 ss.

312 Cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss.: fin dal Libro Bianco del 2001 sulla *governance* europea la Commissione individua quali principi fondamentali, tra gli altri, il principio di apertura e il principio di partecipazione, entrambi finalizzati a rendere l'Europa più trasparente.

Trattato di Lisbona[313]; anche nell'art. 42 della Carta dei diritti fondamentali dell'Unione europea si sancisce il diritto di accesso[314]. In specifico, ai sensi della normativa europea, ogni cittadino dell'Unione nonché ogni persona fisica o giuridica che risieda o abbia la sede sociale in uno Stato membro ha il diritto di accedere ai documenti delle istituzioni, degli organi e degli organismi dell'Unione, a prescindere dal loro supporto.

Le modalità e le condizioni di esercizio del diritto di accesso ai documenti del Parlamento europeo, del Consiglio e della Commissione sono contenute nel regolamento n. 1049 del 2001: non è necessario motivare la domanda, la risposta è prevista di norma in 15 giorni lavorativi e sono disposte una serie di eccezioni atte a tutelare altri interessi protetti, quali la sicurezza pubblica, la difesa, le relazioni internazionali, gli interessi commerciali di un terzo, la vita privata e l'integrità di un individuo. Ciascuna istituzione, per facilitare l'accesso, deve rendere accessibile un registro di documenti, in forma elettronica.

A livello internazionale, degna di nota è anche l'interpretazione estensiva che la Corte europea dei diritti dell'uomo ha dato all'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), pervenendo a una più ampia nozione di "libertà di ricevere informazioni" e al riconoscimento di un diritto di accesso all'informazione[315].

Peraltro, al riguardo, il Consiglio d'Europa ha approvato la Convenzione sull'accesso ai documenti ufficiali, aperta alla firma il 18 giugno 2009, il primo strumento giuridico internazionale vincolante per le parti che riconosce il diritto

---

313 D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss.: il concetto di trasparenza/apertura è richiamato, altresì, negli artt. 10, comma 3, e 11, commi 2 e 3, TUE e nell'art. 298, comma 1, TFUE.

314 L'art. 42 della Carta è contiguo all'art. 41 relativo al diritto a una buona amministrazione con le due ricadute del principio di trasparenza/apertura, che consistono nel diritto di ogni persona ad essere ascoltata prima dell'adozione di un provvedimento che le rechi pregiudizio e nell'obbligo di motivazione per le amministrazioni; cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., che parla di un «doppio statuto: quello di diritto fondamentale (*ex* art. 42 CDUE) e quello di principio generale dei Trattati (*ex* art. 15 TFUE)».

315 M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit. Per un'analisi del diritto di accesso nell'Unione europea cfr., *inter alia*, C. ALBERTI, *La disciplina del diritto di accesso nel post Amsterdam tra consacrazione e limitazione*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 1, 2003, p. 55 ss.

generale di accesso ai documenti pubblici detenuti dalle autorità, anche se in pochi lo hanno ratificato e ciò preclude la sua entrata in vigore.

In Europa diversi Stati hanno approvato norme che regolano la *freedom of information*[316]: molti hanno preso esempio dal caso della Francia, che già nel 1978 adotta la legge n. 78-753 sul diritto di accesso ai documenti[317].

La normativa francese prevede la libertà di accesso ai documenti amministrativi detenuti dalle pubbliche autorità come diritto di ogni persona all'informazione. La richiesta di accesso è prevista, senza obbligo di motivazione, per i documenti amministrativi (e non le mere informazioni), qualunque sia la forma e il supporto[318]; sono previste una serie di esclusioni a protezione di altri interessi pubblici e privati, quali segreto, difesa nazionale, sicurezza dello Stato, pubblica sicurezza e sicurezza delle persone. A presidio delle norme, è prevista un'autorità amministrativa indipendente, la *Commission d'accès aux documents administratifs* (CADA)[319], che ha la funzione di promuovere e vigilare sul rispetto della normativa, formulare raccomandazioni ed esaminare i ricorsi in caso di diniego di accesso[320].

In tale contesto internazionale, l'ordinamento italiano si allinea oggi agli altri Paesi che tutelano il *right to know* prevedendo una disciplina del diritto a conoscere, condizione giuridica indispensabile per un effettivo *open government*[321]: il nostro

---

316 Fra questi Austria (1987), Portogallo (1993), Estonia (2000), Polonia (2001), Slovenia (2003), Svizzera (2004), Germania (2005); cfr. E. CARLONI, *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, cit. Per una comparazione tra le diverse legislazioni J.M. ACKERMAN - I.E. SANDOVAL-BALLESTEROS, *op. cit.*, 2006, p. 85 ss. e T. MENDEL, *op. cit.*

317 Si tratta della legge n. 78-753 del 17 luglio 1978.

318 I documenti devono essere identificati nella richiesta e l'amministrazione ha, di norma, un mese per la risposta. L'amministrazione non è tenuta a comunicare documenti che sono già oggetto di una diffusione pubblica.

319 Cfr. *www.cada.fr*.

320 Secondo A. BONOMO, *op. cit.* l'impostazione dell'ordinamento francese per quanto riguarda la *freedom of information* è ancora distante dai Paesi anglosassoni e tutela ancora molto il potere pubblico.

321 Cfr. M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «il FOIA è la premessa giuridica necessaria per creare le condizioni di *open government* e, più in generale, per promuovere una concezione democratica matura, che non si limiti a esaltare le elezioni come momento privilegiato di verifica sull'operato dei rappresentanti, ma postuli, altresì, una partecipazione consapevole alle decisioni pubbliche e un controllo informato sull'attività delle

ordinamento statuisce oggi un ampio principio di trasparenza, che si traduce nei volti della trasparenza proattiva, garantita dalla pubblicazione, e della trasparenza reattiva, tutelata da diversi strumenti di accesso.

2.4. Principi e strumenti nella disciplina vigente

2.4.1. Il diritto alla conoscibilità, all'accessibilità e alla qualità dei dati

Il principio di trasparenza, seppur privo di esplicito riconoscimento nella Carta costituzionale, è denominato significativamente "principio generale" dalla rubrica dell'art. 1 del d.lgs. 33/2013 e viene fornito di un solido fondamento costituzionale implicito quale canone interpretativo e di orientamento, dotato di chiara forza espansiva: viene conferita esplicita e diretta derivazione costituzionale ed è posto in posizione servente, quale sorta di meta-principio, verso una serie di principi costituzionali.

Il principio di trasparenza è funzionale a realizzare il principio democratico, pietra miliare dell'intero sistema costituzionale, che poggia anche sulla consapevole partecipazione dei cittadini resa possibile dalla trasparenza, e i principi di buon andamento e imparzialità dell'amministrazione, ponendosi concretamente come parametro dell'*agere* pubblico[322].

---

amministrazioni. […] Il FOIA può dare un contributo effettivo alla lotta della corruzione: che la trasparenza "reattiva" abbia, sotto questo profilo, potenzialità maggiori rispetto alla trasparenza "proattiva", sulla quale il nostro legislatore ha a lungo insisto in passato, è un dato intuitivo».

322 Il disegno di legge di riforma costituzionale del 2016, pubblicato nella Gazzetta Ufficiale n. 88 del 15 aprile 2016 e bocciato dal referendum del 4 dicembre 2016, aveva previsto nell'art. 97, tra i principi-guida nella definizione dell'organizzazione dei pubblici uffici, accanto al buon andamento e all'imparzialità, anche la trasparenza. Analogamente, il secondo comma dell'art. 118 prevedeva un esercizio delle funzioni amministrative volto ad assicurare "la semplificazione e la trasparenza dell'azione amministrativa". Cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., che sottolinea come l'art. 21 C. non sia il solo referente del diritto ad essere informati, ma la dottrina abbia affiancato anche gli artt. 97 e 98 C., intendendo la trasparenza come parametro dell'azione pubblica, che si aggiunge a buon andamento e imparzialità. F.G. ANGELINI, *Pubblica amministrazione digitale, diritto di accesso e privacy*, in L. BOLOGNINI - D. FULCO - P. PAGANINI (a cura di), *Next privacy. Il futuro dei nostri dati nell'era digitale*, Etas, Milano, p. 249 ss.

Alla luce di tali considerazioni, ai sensi del primo articolo del d.lgs. 33/2013, la trasparenza, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio, di segreto statistico e di protezione dei dati personali, concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione; nel decreto viene esplicitato che la trasparenza è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto a una buona amministrazione e concorre alla realizzazione di un'amministrazione aperta al servizio del cittadino, pilastro quindi dell'implementazione di un modello di *open government*[323].

Le disposizioni del decreto Trasparenza vengono dotate di particolare *vis* normativa, in quanto integrano l'individuazione del livello essenziale delle prestazioni erogate dalle amministrazioni pubbliche a fini di trasparenza, prevenzione, contrasto della corruzione e della cattiva amministrazione, a norma dell'art. 117, secondo comma, lettera m), della Costituzione e costituiscono esercizio della funzione di coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale, di cui all'art. 117, secondo comma, lettera r), della Costituzione[324]; tale collegamento mostra il saldo legame, già più volte evidenziato, tra trasparenza e digitalizzazione pubblica[325].

Come rilevato in dottrina, tali disposizioni mostrano le diverse dimensioni costitutive del principio di trasparenza: la dimensione di "sviluppo" di alcuni principi costituzionali (i principi che "concorre ad attuare"), la dimensione di garanzia di diritti e

---

evidenzia che un dovere dei pubblici poteri di informare si ricava a partire dal principio di sovranità popolare e dal principio democratico, cui si affianca il principio di imparzialità (art. 97 C.). Un dovere di informazione pubblica è presente anche negli artt. 9, 24 e 73. Cfr., altresì, V. PAGNANELLI, *Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, in *Giornale di storia costituzionale*, fasc. 31, 2016, p. 205 ss.

323 Art. 1, comma 2, d.lgs. 33/2013.

324 Art. 1, comma 3, d.lgs. 33/2013 e in tal senso anche art. 1, comma 36, legge 190/2012. Le disposizioni rientrano, pertanto, nelle materie di competenza legislativa esclusiva dello Stato, previste dal comma secondo dell'art. 117 C.

325 Cfr. F. CARDARELLI, *op. cit.*, p. 227 ss., che sottolinea come le possibilità legate alle tecnologie informatiche accrescono la domanda di conoscenza e trasparenza.

libertà e una dimensione in cui si sostanzia la tensione verso un nuovo modello di amministrazione pubblica, l'*open government*[326]. La tutela dei diritti e i principi dell'amministrazione aperta sono esplicitati anche dalla riforma recata dal d.lgs. 97/2016, come visto: la trasparenza, quale accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, è finalizzata a «*tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*»[327].

La riforma recata dalla legge delega 124/2015 e dal relativo d.lgs. 97/2016 rafforza ulteriormente il principio di trasparenza e riconosce esplicitamente la «libertà di accesso», che viene «*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*»[328]. Rispetto alla configurazione originaria del d.lgs. 33/2013 si passa da una trasparenza intesa come obbligo di pubblicazione a un'accezione come libertà di accesso,

---

326 In tal senso E. CARLONI, *I principi del codice della trasparenza (artt. 1, commi 1 e 2, 2, 6)*, cit., p. 38 ss., che sottolinea come gli articoli costituzionali di riferimento della disposizione siano individuabili negli artt. 1 (principio democratico), 28 (principio di responsabilità dei funzionari e dipendenti pubblici), 54 (diligenza e lealtà nel servizio alla nazione) e 97 (principi di imparzialità, legalità e buon andamento delle pubbliche amministrazioni); l'Autore rileva la significativa assenza fra i principi costituzionali richiamati dell'art. 21 C., in coerenza con il fatto che il decreto Trasparenza, prima della riforma del d.lgs. 97/2016, non configurava ancora un *Freedom of Information Act* (FOIA). Alla base del diritto all'informazione si pongono anche gli artt. 2 e 3 della Costituzione; *supra*, più ampiamente, cap. 1, § 3.

327 Art. 1, comma 1, d.lgs. 33/2013.

328 Art. 2, comma 1, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016. Anche la legge delega pone esplicitamente tale principio direttivo: «*fermi restando gli obblighi di pubblicazione, riconoscimento della libertà di informazione attraverso il diritto di accesso, anche per via telematica, di chiunque, indipendentemente dalla titolarità di situazioni giuridicamente rilevanti, ai dati e ai documenti detenuti dalle pubbliche amministrazioni, salvi i casi di segreto o di divieto di divulgazione previsti dall'ordinamento e nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati, al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*» (art. 7, comma 1, lett. h), legge 124/2015).

maggiormente conforme agli altri Paesi[329]. In tal modo, grazie al d.lgs. 97/2016, assume consistenza la significativa rubrica dell'art. 3 del d.lgs. 33/2013, "diritto alla conoscibilità", che prima della riforma rischiava di essere eccedente rispetto a quanto effettivamente garantito dalle disposizioni.

La stessa Dichiarazione dei diritti in Internet, atto privo di valore giuridico, ma dotato di valore culturale e di una significativa funzione di *moral suasion*, prevede che la gestione della Rete debba assicurare, tra gli altri, i principi di trasparenza e accessibilità alle informazioni pubbliche[330].

Il principio di trasparenza per potersi compiutamente realizzare, senza rimanere mera tecnica finalizzata al diritto a conoscere, ma incapace concretamente di raggiungerlo, necessita di alcuni presupposti, primo fra tutti il rispetto del principio costituzionale di uguaglianza sostanziale, che permetta a chiunque l'accesso ai siti istituzionali[331]: ciò richiama la problematica del *digital divide* che può tradursi in una potenziale discriminazione nel *right to know*.

Sotto tale profilo, oggetto di particolare attenzione deve essere il concetto di

---

329 Cfr. D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., secondo la quale la libertà di accesso è garantita in prima battuta dall'accesso civico (citato per primo), autonomo diritto e strumento principe della disciplina, e, in subordine, dalla pubblicazione. Secondo l'Autrice la modifica è da accogliere con favore dal momento che una trasparenza intesa essenzialmente come pubblicazione rischia di far conoscere a tutti cose che non interessano a nessuno e di cadere sotto l'obiezione di "voyerismo amministrativo". Al riguardo D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *federalismi.it*, fasc. 5, 2016, p. 17 sottolinea l'assenza di un rapporto di equivalenza diretta tra la quantità di informazioni rese disponibili in rete e la trasparenza quale conoscenza a causa di possibili fenomeni di c.d. "opacità per confusione". Cfr. E. FURIOSI, *op. cit.*, p. 1 ss. e A. MONEA, *La nuova trasparenza amministrativa alla luce del d.lgs. 97/2016. L'accesso civico*, in *Azienditalia*, fasc. 11, 2016, p. 1040 ss., secondo cui tra i difetti della disciplina prima della riforma spiccava la gravosità eccessiva degli obblighi di pubblicazione per le singole amministrazioni accompagnata da un circoscritto innalzamento del livello qualitativo di conoscenza, a causa della limitata utilità di quanto pubblicato per il cittadino, impossibilitato a conoscere quanto di proprio interesse.

330 Tali principi sono previsti nell'art. 14, comma 5, accanto ai principi di responsabilità delle decisioni e rappresentanza dei soggetti interessati.

331 Cfr. G. GARDINI, *op. cit.*, p. 875 ss.: «la trasparenza è una *tecnica* che serve a garantire il diritto di essere informati: i due concetti stanno, tra loro, in un rapporto di mezzo a fine».

accessibilità, definito dall'art. 2 della legge 4/2004 come «*la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari*». Anche l'art. 53 del Codice dell'amministrazione digitale, d.lgs. 82/2005, dedicato alle caratteristiche che i siti web istituzionali devono rispettare, pone prioritariamente «*i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili*» oltre a «*completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54*».

L'accesso e l'accessibilità ai dati messi a disposizione non sono sufficienti da soli a garantire un'effettiva *disclosure*. La trasparenza, per incarnare pienamente il principio previsto dalla normativa, deve garantire qualità alle informazioni pubblicate, *condicio sine qua non* e presupposto stesso della *disclosure* e del *right to know*; il controllo diffuso proprio del modello di *open government* non può che fondarsi su dati certi e attuali[332].

È consapevole di questo aspetto il legislatore, che nell'art. 6 del d.lgs. 33/2013 impone alle amministrazioni di garantire la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti, che si declina nell'assicurare «*l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, nonché la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità*»; come esaminato l'art. 53 del d.lgs. 82/2005 prevede aspetti analoghi quali caratteristiche da rispettare nei siti web istituzionali. A ben vedere si tratta di caratteristiche di cui si compone un'autentica trasparenza e il cui rispetto non può essere eluso, tanto che «*l'esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l'omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti*»[333].

Dal quadro normativo emerge un concetto di trasparenza, costituzionalmente

---

332 Cfr. F. PATRONI GRIFFI, *op. cit.*, p. 8.

333 Art. 6, comma 2, d.lgs. 33/2013.

orientato, basato sull'accesso, sull'accessibilità e sulla qualità, capace di dare forma e sostanza alla libertà di informazione e al diritto alla conoscenza di chiunque nei confronti delle pubbliche amministrazioni.

2.4.2. I diritti di accesso: documentale, civico semplice, civico generalizzato

Nell'ordinamento giuridico italiano, come già esaminato, sono diversi i volti della trasparenza e gli strumenti di conoscenza: accanto alla "trasparenza proattiva" (*proactive disclosure*), che si realizza con la pubblicazione di documenti, informazioni e dati, la "trasparenza reattiva" (*reactive disclosure*) si ottiene in risposta alle istanze di conoscenza avanzate dagli interessati[334]. Sotto questo profilo il d.lgs. 97/2016, cosiddetto *Freedom of Information Act* italiano, approvato in virtù della delega di cui all'art. 7 della legge 124/2015 (c.d. legge Madia)[335], come esaminato, ha portato significative novità ampliando il "diritto a conoscere" della collettività nei confronti delle istituzioni[336], grazie all'introduzione dell'accesso civico generalizzato, disciplinato dal d.lgs. 33/2013, come modificato dal d.lgs. 97/2016.

Di conseguenza, l'odierno ordinamento italiano si caratterizza per la convivenza di distinti strumenti di accesso, con funzioni e caratteristiche diverse: l'accesso documentale, l'accesso civico semplice e l'accesso civico generalizzato.

Il diritto di accesso documentale, disciplinato dalla legge 241/1990, prevede un diritto a conoscere condizionato, dal momento che sono necessari alcuni requisiti per poterlo esercitare: la legittimazione soggettiva, giacché il diritto di accesso spetta a tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente

---

334 Si esprime in tal senso il Consiglio di Stato nel parere sullo schema di decreto legislativo di quello che è diventato il d.lgs. 97/2016, reso nell'adunanza di sezione 18/02/2016 (n. 515/2016 del 24/02/2016).

335 Art. 7, comma 1, lett. h), legge 124/2015.

336 Il d.lgs. 97/2016 nel suo iter di approvazione ha recepito molte osservazioni sollevate sia dagli organi preposti al rilascio di pareri (quali il Consiglio di Stato, l'Autorità Nazionale Anticorruzione - Anac, il Garante per la protezione dei dati personali e le Commissioni Affari costituzionali di Camera e Senato), sia dalla stessa società civile.

tutelata e collegata al documento al quale è chiesto l'accesso (art. 22) e la motivazione, in quanto la richiesta di accesso deve essere motivata (art. 25)[337]. Oltre a questi requisiti, la distanza dalla *freedom of information* si coglie anche nel limite al controllo generalizzato, dal momento che «*non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni*» (art. 24, legge 241/1990)[338]. Si tratta, pertanto, di un accesso "qualificato" e strumentale alla tutela di una posizione sostanziale individuale, che non può tradursi in una forma di controllo diffuso dell'attività amministrativa[339].

Il diritto di accesso documentale si esercita con la visione e l'estrazione di copia dei documenti amministrativi (e non di qualsiasi dato o informazione): la richiesta deve essere rivolta all'amministrazione che ha formato il documento e che lo detiene stabilmente, che ha un termine di 30 giorni per rispondere, altrimenti si intende respinta; vige di conseguenza il cosiddetto silenzio diniego[340]. Sono previste ampie esclusioni e

---

337 C. BIANCO - F. RADICETTI, *Profili normativi e problematici dell'Accesso civico (nota a Cons. Stato, sez. IV, 12 agosto 2016, n. 3631)*, in *Rassegna dell'avvocatura dello Stato*, fasc. 4, 2016, p. 133 parlano di una prospettiva di natura pre-processualistica nel caso della legge 241/1990.

338 Secondo D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, cit., p. 2 ss. il diritto di accesso documentale si atteggia come una forma di garanzia riconosciuta a titolo particolare a determinati soggetti, che ha un collegamento debole con l'idea di trasparenza; la finalità dell'accesso documentale consiste nel porre i soggetti interessati «in grado di esercitare al meglio le facoltà - partecipative e/o oppositive - che l'ordinamento attribuisce loro a tutela della posizione giuridica qualificata di cui questi sono titolari, attraverso una più completa rappresentazione della situazione di fatto e di diritto che più direttamente li interessa».

339 F. PATRONI GRIFFI, *op. cit.* Sulla natura giuridica del diritto di accesso quale mero interesse legittimo o vero e proprio diritto soggettivo cfr. M.A. SANDULLI, *Il diritto di accesso ai documenti amministrativi: l'attualità di un istituto a vent'anni dalla legge n. 241/1990*, in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale Scientifica, Napoli, 2012, p. 39 ss.

340 Le modalità di esercizio del diritto di accesso ai documenti amministrativi ai sensi del capo V della legge 241/1990 sono disciplinate dal d.p.r. 12 aprile 2006, n. 184, «*Regolamento recante disciplina in materia di accesso ai documenti amministrativi*». L'accesso all'informazione ambientale è regolato da una disciplina speciale, a seguito della ratifica da parte dell'Unione europea della Convenzione di Aarhus con decisione 2005/370/CE del 17 febbraio 2005: la disciplina italiana è costituita dal d.lgs. 19 agosto

limitazioni nell'art. 24, relative alla difesa di interessi pubblici e privati, quali il segreto di Stato, il segreto statistico, il segreto industriale e la protezione dei dati personali.

In merito al diritto di accesso documentale è significativa la sentenza del TAR Lazio-Roma, Sezione III bis, del 22 marzo 2017, n. 3769, che ha riconosciuto il diritto di accesso documentale all'algoritmo del software che gestisce il procedimento amministrativo, configurandolo quale atto amministrativo informatico[341].

Innanzitutto il TAR ritiene la nozione di atto amministrativo informatico particolarmente estesa, dal momento che tiene conto della sostanziale valenza amministrativa del documento piuttosto che della sua provenienza. Secondo il TAR, poi, l'atto amministrativo ad elaborazione informatica «è giuridicamente ammissibile e legittimo quanto all'attività vincolata dell'amministrazione, atteso che l'attività vincolata è compatibile con la logica propria dell'elaboratore elettronico in quanto il software traduce gli elementi di fatto e i dati giuridici in linguaggio matematico dando vita a un ragionamento logico formalizzato che porta a una conclusione che, sulla base dei dati iniziali, è immutabile». Di conseguenza, con il software si concretizza la volontà finale dell'amministrazione procedente che, in definitiva, costituisce, modifica o estingue le situazioni giuridiche individuali, anche se lo stesso non produce effetti in via diretta all'esterno; il software finisce per identificarsi e concretizzare lo stesso

---

2005, n. 195, attuazione della direttiva 2003/4/CE (che ha abrogato la previgente disciplina del d.lgs. 24 febbraio 1997, n. 39).

341 Nella fattispecie concreta oggetto della sentenza, il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) aveva negato l'accesso all'algoritmo di calcolo che gestisce il software relativo ai trasferimenti interprovinciali del personale docente, limitandosi a consegnare un documento contenente la descrizione dell'algoritmo e del suo concreto funzionamento, ritenendo peraltro che il codice sorgente dei programmi non possa essere assimilato a un documento amministrativo; il TAR ha ordinato al MIUR il rilascio alla parte ricorrente di copia dei codici sorgente del software dell'algoritmo di gestione della procedura della mobilità dei docenti. Il TAR evidenzia che, nella fattispecie, l'algoritmo finisce per sostanziare esso stesso il procedimento, dal momento che la concreta sede spettante al singolo docente nell'ambito della mobilità è individuata esclusivamente dall'algoritmo: la mera descrizione dell'algoritmo e del suo funzionamento non assolve alla medesima funzione conoscitiva data dall'acquisizione diretta del linguaggio informatico sorgente. Secondo il TAR «le valutazioni in ordine alla funzionalità concreta del predetto algoritmo o anche a monte all'esistenza di eventuali errori nella programmazione possono, pertanto, essere effettuate esclusivamente alla luce della piena conoscenza del medesimo che può essere assicurata in modo completo soltanto con il richiesto penetrante accesso ai relativi codici sorgenti».

procedimento. Solo con l'accesso all'algoritmo è possibile avere conoscenza della funzionalità concreta dell'algoritmo stesso o anche dell'esistenza di eventuali errori nella programmazione. Peraltro, secondo il TAR, la scelta di uno strumento innovativo per la gestione amministrativa non può tradursi in una limitazione dell'ampiezza del potere di accesso di cui gode l'interessato.

Il TAR si mostra consapevole che tale tipologia di accesso si presenta particolarmente penetrante in quanto indirizzata proprio ai codici sorgente del software dell'algoritmo, ma, tuttavia, ritiene che l'interesse sotteso alla richiesta non possa ritenersi adeguatamente soddisfatto da un documento di descrizione dell'algoritmo e del suo funzionamento, «in quanto, evidentemente e intuitivamente, la descrizione della modalità di funzionamento dell'algoritmo assicura una conoscenza assolutamente non paragonabile a quella che deriverebbe dall'acquisizione del richiesto linguaggio sorgente, atteso che, se non altro, la predetta descrizione è, comunque, atto di parte».

La sentenza sicuramente apre scenari di indubbio interesse, anche in considerazione della configurazione stessa della società contemporanea, dominata da *big data*, algoritmi e soluzioni di intelligenza artificiale.

Rispetto al diritto di accesso documentale, si atteggia in modo diverso il diritto di accesso civico generalizzato, che si somma all'accesso civico semplice, già previsto prima della riforma.

L'accesso civico semplice non realizza una vera e propria forma di accesso, ma una sorta di misura sanzionatoria in caso di inadempimento dell'amministrazione ai previsti obblighi di pubblicazione; il suo esercizio non è sottoposto a legittimazione soggettiva, non deve essere motivato ed è gratuito, ma è limitato nell'oggetto della richiesta, che può riguardare solo dati, informazioni e documenti sui quali esiste un obbligo di pubblicazione violato dall'amministrazione[342]. In tal caso, l'istanza deve

[342] Cfr. G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit., p. 1 ss., che sottolinea come nell'accesso civico si sovrapponga al dovere di pubblicazione il diritto del privato di accedere a documenti, dati e informazioni interessati dall'inadempienza dell'amministrazione; D.U. GALETTA, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, cit., p. 5, secondo la quale tale forma di accesso non si configura come un diritto autonomo, ma come sanzione relativa al mancato rispetto degli obblighi di pubblicazione; S. VILLAMENA, *op. cit.*, p. 5 ss., secondo cui l'accesso civico semplice si pone come un rimedio nelle mani del privato, uno strumento funzionale all'emersione di inadempimenti

essere presentata al responsabile della prevenzione della corruzione e della trasparenza[343].

Oltre al diritto di accesso civico semplice, ossia il diritto di chiunque di richiedere documenti, informazioni o dati di cui sia stata omessa la pubblicazione obbligatoria (art. 5, comma 1, d.lgs. 33/2013), la riforma ha previsto il diritto di accesso civico generalizzato, ossia il diritto di accedere ai dati e ai documenti, detenuti dalle amministrazioni, diversi e ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria (art. 5, comma 2, d.lgs. 33/2013)[344].

Il diritto di accesso civico cosiddetto generalizzato non è sottoposto a condizioni come quello documentale di cui alla legge 241/1990 e garantisce un autentico *right to know*; l'esercizio del diritto, infatti, non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente, non richiede motivazione e non prevede il limite del controllo generalizzato[345].

In merito è necessaria una precisazione: l'accesso documentale, limitato e meno ampio, è però più profondo (i limiti dell'accesso civico generalizzato sono più ampi e dettagliati, come si esaminerà in seguito)[346], dal momento che è diversa la *ratio* che lo

---

amministrativi con una sorta di "effetto minaccia" per l'amministrazione; E. FURIOSI, *op. cit.*, p. 1 ss., secondo la quale «proprio queste limitazioni, relative sia al fine che ai documenti che potevano esserne oggetto, hanno fatto sì che l'accesso civico del 2013 sia rimasto pressoché lettera morta».

343 Art. 5, comma 3, lett. d), d.lgs. 33/2013.

344 L'«*obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione*» (art. 5, comma 1, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016); a questo si aggiunge che «*chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione*», nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti previsti dall'art. 5-bis (art. 5, comma 2, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016).

345 Art. 5, comma 3, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016.

346 In tal senso la stessa relazione illustrativa di accompagnamento allo schema di decreto legislativo 97/2016. Cfr. E. FURIOSI, *op. cit.*, p. 1 ss.: «il bilanciamento di interessi nel caso dell'accesso documentale ex l. 241/1990 può, infatti, consentire un accesso più approfondito, seppur limitato ai soli documenti collegati alla situazione giuridica tutelata. Vi potranno cioè essere dei casi, seppur residuali, in cui dei soggetti titolari di una posizione giuridica qualificata, per il tramite dell'accesso documentale, potranno avere accesso a documenti per i quali non sarebbe concesso l'accesso generalizzato». L'Autrice muove critiche alla compatibilità e al coordinamento del diniego tra accesso documentale e civico generalizzato,

anima, legata a posizioni giuridiche qualificate protette dall'ordinamento: la diversa finalità dei due strumenti è anche il motivo della loro convivenza nell'ordinamento[347], anche se al riguardo si può ragionevolmente prevedere che, proprio per le caratteristiche che lo connotano, l'accesso civico generalizzato finirà per prevalere nell'utilizzo come "lo" strumento di conoscenza[348].

Le finalità dell'accesso civico generalizzato sono ben diverse da quello documentale: consistono nel «*favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e nell'utilizzo delle risorse pubbliche*» e nel *«promuovere la partecipazione al dibattito pubblico*»[349]; nella partecipazione e nel controllo si coglie pienamente come la trasparenza sia elemento imprescindibile del modello di governo aperto e di una relazione collaborativa tra governanti e governati.

Nel caso dell'accesso civico generalizzato, l'istanza deve identificare i dati, le informazioni o i documenti richiesti[350], può essere trasmessa in via telematica e

---

anche alla luce delle linee guida dell'Anac, che avrebbero reso preferibile l'abrogazione delle parti dell'accesso documentale confliggenti con la nuova disciplina, data l'accentuata sovrapponibilità e inclusione dell'oggetto dell'accesso documentale in quello civico generalizzato.

347 In tal senso anche le linee guida dell'Anac, adottate con delibera n. 1309 del 28 dicembre 2016, che saranno oggetto di successiva analisi.

348 Cfr. E. FURIOSI, *op. cit.*, p. 1 ss. e M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «Il *right to know*, prima prigioniero dei confini dalla legge assegnati all'area della pubblicazione obbligatoria, travalica ora quei confini. Di questo nuovo diritto si detta una disciplina essenziale, che lascia in vita le altre forme di accesso procedimentale (1990) e civico (2013) destinate, tuttavia, col tempo, a divenire superflue».

349 Cfr. E. FURIOSI, *op. cit.*, p. 1 ss.: il diritto di accesso civico generalizzato è «strumento finalizzato a consentire forme diffuse di controllo e non è volto alla tutela di posizioni giuridiche soggettive, quanto piuttosto a consentire un controllo democratico sul perseguimento delle funzioni istituzionali e sull'utilizzo di risorse pubbliche».

350 Le linee guida dell'Anac del 28 dicembre 2016, trattate più avanti nel testo, chiariscono l'ambito oggettivo: i dati sono espressione di «un concetto informativo più ampio, da riferire al dato conoscitivo come tale, indipendentemente dal supporto fisico sui cui è incorporato e a prescindere dai vincoli derivanti dalle sue modalità di organizzazione e conservazione», i documenti sono «i supporti contenenti dati e/o informazioni» e le informazioni sono «le rielaborazioni di dati detenuti dalle amministrazioni effettuate per propri fini contenuti in distinti documenti». Per tale motivo la norma parla di dati e documenti e in caso di informazioni l'accesso è possibile solo per quelle già detenute e gestite dall'amministrazione stessa. Al riguardo cfr. E. FURIOSI, *op. cit.*, p. 1 ss.

presentata alternativamente a una pluralità di uffici dell'amministrazione, previsti dalla norma[351]; il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali[352].

Il principio di trasparenza emerge anche nella risposta a seguito dell'istanza: il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni e non è ammesso il silenzio diniego; il rifiuto, il differimento e la limitazione dell'accesso devono essere motivati con riferimento ai casi e ai limiti stabiliti[353]: grava, di conseguenza, sull'amministrazione dover provare l'esistenza di motivazioni che impediscono di soddisfare l'istanza[354].

La normativa dispone il diniego dell'istanza di accesso civico generalizzato in caso di "pregiudizio concreto" alla tutela degli interessi pubblici e privati tutelati dall'ordinamento e previsti dalla norma[355]. Al riguardo, sono state approvate con delibera n. 1309 del 28 dicembre 2016 le linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti dell'accesso civico, adottate dall'Anac,

---

351 Art. 5, comma 3, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016; gli uffici previsti cui può essere alternativamente presentata l'istanza sono l'ufficio che detiene i dati, le informazioni o i documenti, l'Ufficio relazioni con il pubblico o altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale.

352 Art. 5, comma 4, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016.

353 Art. 5, comma 6, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016.

354 Si configura, quindi, un ribaltamento dell'onere di motivazione rispetto al diritto di accesso documentale ai sensi della legge 241/1990, dove invece è il cittadino che deve motivare la propria richiesta di accesso; inoltre in tal caso non è prevista la possibilità del silenzio diniego. In caso di diniego, totale o parziale, di mancata risposta o di differimento sono previsti il ricorso al tribunale amministrativo regionale ai sensi dell'art. 116 del Codice del processo amministrativo, d.lgs. 2 luglio 2010, n. 104 (esperibile entro trenta giorni), ma anche la possibilità di strumenti di tutela amministrativa, ossia la richiesta di riesame al responsabile della prevenzione e della trasparenza dell'amministrazione (il provvedimento motivato del quale è reso entro venti giorni ed è impugnabile davanti al giudice amministrativo) e, qualora si tratti di atti delle amministrazioni delle regioni o degli enti locali, il rimedio stragiudiziale del ricorso al difensore civico competente, che si pronuncia entro 30 giorni (art. 5, commi 7 e 8, d.lgs. 33/2013).

355 Le linee guida dell'Anac, di cui alla delibera n. 1309 del 28 dicembre 2016, hanno chiarito che per configurarsi un pregiudizio concreto deve sussistere un preciso nesso di causalità tra l'accesso e il pregiudizio.

d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza Unificata, come previsto dall'art. 5-bis, d.lgs. 33/2013[356].

Accanto a quelle che l'Anac ha definito eccezioni assolute, ossia eccezioni tassative, previste dalla legge, nelle quali l'amministrazione è tenuta a rifiutare l'accesso (il segreto di Stato e i divieti di accesso e divulgazione)[357], sono previste eccezioni relative o qualificate, per le quali è necessario un pregiudizio concreto alla tutela di uno degli interessi pubblici o privati previsti, ossia un preciso nesso di causalità fra l'accesso e il pregiudizio, valutato in base al contesto temporale di riferimento; nel caso delle eccezioni relative è necessaria una valutazione caso per caso da parte dell'amministrazione con la tecnica del bilanciamento tra l'interesse pubblico alla *disclosure* generalizzata e la tutela di altrettanto validi interessi protetti dall'ordinamento[358]. In modo significativo, le linee guida dell'Anac precisano che l'amministrazione è tenuta «a privilegiare la scelta che, pur non oltrepassando i limiti di ciò che può essere ragionevolmente richiesto, sia la più favorevole al diritto di accesso del richiedente».

Gli interessi pubblici previsti sono:

a) la sicurezza pubblica e l'ordine pubblico;

---

356 Le amministrazioni pubbliche e gli altri soggetti previsti devono adeguarsi alle modifiche introdotte e assicurare l'effettivo esercizio del nuovo diritto di accesso civico, entro sei mesi dalla data di entrata in vigore, avvenuta il 23 giugno 2016 (art. 42, comma 1, d.lgs. 97/2016). M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «Nell'applicare le eccezioni previste dall'art. 5 *bis*, le amministrazioni italiane sono, dunque, chiamate ad aggiornare le tecniche di bilanciamento già impiegate per l'accesso procedimentale. Decisivi saranno gli orientamenti giurisprudenziali e le linee guida dell'Anac: l'auspicio è che gli uni e le altre forniscano indicazioni convergenti, utilizzando la giurisprudenza comunitaria come punto di riferimento comune». Sulle linee guida D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss. fa riferimento alla discussione sulla natura giuridica dell'atto, ma anche sull'opportunità dell'emanazione da parte dell'Anac, che ha allo stesso tempo funzioni di regolazione, indirizzo e controllo a scopo sia preventivo che sanzionatorio.

357 Tra le eccezioni assolute rientrano anche i casi già previsti dall'art. 24, comma 1, legge 241/1990 in materia di accesso documentale.

358 E. FURIOSI, *op. cit.*, p. 1 ss.: il diritto di accesso civico generalizzato subisce «una battuta d'arresto quando confligge con una posizione giuridicamente tutelata dell'individuo o con la necessità di tutelare interessi pubblici».

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.

Gli interessi privati ineriscono, invece, a:

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[359].

Proprio sui limiti posti al diritto di accesso civico generalizzato si sono incentrate le maggiori perplessità circa l'effettività del diritto a conoscere: le eccezioni sono state interpretate da parte della dottrina come numerose, ampie e talvolta eccessivamente indeterminate[360].

---

[359] Art. 5-bis, d.lgs. 33/2013, come modificato dal d.lgs. 97/2016. Nel caso di controinteressati (soggetti che potrebbero subire un pregiudizio concreto alla tutela di interessi privati), è previsto che l'amministrazione debba attivare uno specifico procedimento di comunicazione, che consenta ai controinteressati di presentare eventuale motivata opposizione. Al riguardo M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss. sottolinea come la normativa delinei due gruppi di interessi-limite: gli interessi pubblici riconducibili a funzioni sovrane dello Stato o funzioni che, per l'imparzialità che le caratterizza, richiedono un certo grado di riservatezza durante il loro svolgimento e gli interessi privati di rango costituzionale. Secondo E. FURIOSI, *op. cit.*, p. 1 ss. è «attraverso la previsione di limiti, che la trasparenza, e la sua incidenza, vengono graduate, limitandone più o meno l'estensione e la pervasività».

[360] Cfr., *inter alia*, E. CARLONI, *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, cit., p. 9 ss. (il cui commento avviene prima dell'approvazione definitiva), secondo cui se quello italiano è un FOIA, non è un buon FOIA: «i limiti appaiono non solo numerosi, ampi ed estesi, ma anche pericolosamente indeterminati, con il duplice effetto di ridurre sensibilmente l'estensione del diritto e della trasparenza che attraverso questa è assicurata e di costringere l'amministrazione di fronte ad un lavoro di bilanciamento complesso»; C. CUDIA, *op. cit.*, p. 1 ss., che porta come esempio di interessi particolarmente generici quelli "economici" di una persona fisica o giuridica e il riferimento alla "politica" dello Stato; D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss., che ritiene le limitazioni molto ampie e troppo poco puntuali, seppur in

Nelle linee guida, l'Anac precisa che sono possibili richieste massive, ma non per un numero manifestamente irragionevole di documenti, tale da paralizzare il buon funzionamento della pubblica amministrazione, a causa del carico di lavoro[361], e non devono essere presentate richieste meramente esplorative o generiche. L'amministrazione, inoltre, non è tenuta a formare, raccogliere o altrimenti procurarsi informazioni che non possieda già, ma deve solo basarsi su documenti e dati in suo possesso[362].

Peraltro, seppur sia prevista una responsabilità a carico di coloro che non rispettino le disposizioni dell'art. 5-bis, non sono previste sanzioni per i casi di illegittimo diniego di accesso, contrariamente a quanto previsto nella legge delega[363];

---

parte mitigate dalla possibilità di accesso parziale (esclusione dell'accesso non integrale) e di differimento dell'accesso in luogo del diniego; S. VILLAMENA, *op. cit.*, p. 1 ss. Lo stesso Consiglio di Stato, nel parere n. 515 del 24 febbraio 2016, reso sullo schema di decreto legislativo, aveva sottolineato che i limiti troppo ampi lasciano eccessiva discrezionalità alle amministrazioni nell'attuazione della normativa, con il rischio di comprimere la libertà di accesso. *Contra* M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «il numero e la formulazione degli interessi-limite indicati dal legislatore delegato sono in linea con lo standard prevalente. I dieci interessi pubblici e privati indicati dall'art. 5 *bis* corrispondono all'elencazione che compare nella maggior parte dei FOIA europei, rispetto ai quali, anzi, il nostro legislatore è stato più parco. Occorre, poi, considerare che gli interessi indicati coincidono con differenze marginali con quelli del FOIA dell'Unione europea. Questa scelta, non casuale, presenta un vantaggio importante: offrire alle amministrazioni e ai giudici italiani un prezioso ausilio interpretativo, rappresentato dalla ricca giurisprudenza comunitaria formatasi in relazione a ciascun interesse-limite».

[361] In tal caso è necessaria una ponderazione da parte dell'amministrazione tra l'interesse all'accesso e il carico di lavoro, al fine di salvaguardare l'interesse al buon andamento dell'amministrazione.

[362] Ai fini dell'applicazione della normativa, le linee guida forniscono suggerimenti alle amministrazioni in relazione all'adozione di una disciplina, un regolamento interno, sugli aspetti procedimentali dell'accesso (le varie tipologie), la realizzazione di adeguamenti organizzativi (in specifico la previsione di un unico ufficio competente sull'accesso) e la previsione del cosiddetto registro degli accessi, ossia un registro delle istanze di accesso presentate per tutte le diverse tipologie istituito presso ogni amministrazione, funzionale al monitoraggio dell'Anac. Le linee guida forniscono indicazioni in relazione alle diverse eccezioni e prevedono nell'allegato una guida operativa.

[363] L'art. 7, comma 1, lett. h), legge 124/2015 dispone, tra i principi e i criteri della delega, la «*previsione di sanzioni a carico delle amministrazioni che non ottemperano alle disposizioni normative in materia di accesso* […]». L'art. 46 del d.lgs. 33/2013 prevede una responsabilità a carico di coloro che violano le disposizioni dell'accesso civico generalizzato: «[…] *il rifiuto, il differimento e la limitazione*

tale aspetto, insieme all'ampiezza delle esclusioni[364], all'onerosità dell'applicazione della disciplina per le amministrazioni[365] e alla mancanza di un'autorità indipendente cui sia attribuita la guida del processo di applicazione[366], possono costituire possibili *vulnus* all'effettività del diritto a conoscere[367].

Al netto delle perplessità in merito ad alcuni aspetti inerenti l'applicazione e la connessa effettività dello strumento, l'introduzione del diritto di accesso civico

---

dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis, costituiscono elemento di valutazione della responsabilità dirigenziale, eventuale causa di responsabilità per danno all'immagine dell'amministrazione e sono comunque valutati ai fini della corresponsione della retribuzione di risultato e del trattamento accessorio collegato alla performance individuale dei responsabili». Ai sensi dell'art. 43, comma 4, d.lgs. 33/2013, «*i dirigenti responsabili dell'amministrazione e il responsabile per la trasparenza controllano e assicurano la regolare attuazione dell'accesso civico*» sulla base di quanto stabilito dal decreto.

364 Il Consiglio di Stato, nella sentenza n. 3631 del 12 agosto 2016, seppur relativa a una fattispecie di diritto di accesso documentale, tratta l'istituto dell'accesso civico generalizzato precisando che l'amministrazione deve in concreto valutare la sussistenza di limiti nel rispetto dei canoni di proporzionalità e ragionevolezza e in questa valutazione non potrà non tenere conto della «peculiarità della posizione legittimante del richiedente», che in realtà non rileva per la normativa.

365 Tra le criticità D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione*, cit., p. 1019 ss. segnala la gratuità quasi assoluta dell'accesso, in considerazione dei costi che graveranno sull'amministrazione e che rischiano di essere insostenibili, inficiando l'effettività stessa delle disposizioni normative; peraltro la previsione non è contenuta in termini analoghi né nel modello statunitense né nel diritto dell'Unione europea. Anche P. FALLETTA, *op. cit.*, p. 6 ss. sottolinea i problemi di aggravio di tempo e costi e di inevitabile disorganizzazione delle amministrazioni.

366 In tal senso cfr. M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «sarebbe stato preferibile come accade in altri sistemi FOIA assegnare la guida unitaria del processo di applicazione a un'apposita autorità indipendente, attribuendole il compito di decisore di ultima istanza sui ricorsi amministrativi». Peraltro, al riguardo, è opportuno richiamare l'art. 7, comma 1, lett. h), legge 124/2015, che dispone, tra i principi e i criteri della delega, la previsione «[…] *di procedure di ricorso all'Autorità nazionale anticorruzione in materia di accesso civico e in materia di accesso ai sensi della presente lettera*».

367 M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss. individua i principali limiti della riforma nei seguenti: «l'assenza di un sistema accentrato di ricorsi amministrativi, la sopravvalutazione dell'interesse alla *privacy* rispetto agli altri interessi-limite e la consueta clausola di invarianza della spesa». Cfr. E. FURIOSI, *op. cit.*, p. 1 ss., secondo la quale «sono proprio le limitazioni a delineare e delimitare l'efficacia dello strumento, e quindi indirettamente anche il peso dell'intera riforma da cui è scaturito».

generalizzato ha fatto parlare del riconoscimento della *freedom of information* anche in Italia, come in molti altri Paesi nel mondo, che già da tempo hanno previsto normativamente il diritto a conoscere nei confronti delle istituzioni[368]: adesso il *right to know* è tutelato nel nostro ordinamento alla stregua di un diritto fondamentale[369].

Il principio di trasparenza si è evoluto anche a seguito dello sviluppo della società di riferimento e dei suoi paradigmi sotto la spinta delle nuove tecnologie: *disclosure* e *openness* si sono integrate a definire una società aperta e un nuovo modello di *open government*.

Il collegamento fra trasparenza e apertura si coglie anche a livello normativo nell'art. 3 del d.lgs. 33/2013, da ultimo modificato dal d.lgs. 97/2016: tutti i documenti, le informazioni e i dati oggetto di accesso civico, compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa, sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, di utilizzarli e riutilizzarli ai sensi dell'art. 7: la disposizione, significativamente rubricata "*dati aperti e riutilizzo*", pone non solo il diritto a conoscere, ma anche il diritto all'apertura e al riutilizzo di documenti, informazioni e dati[370].

---

[368] Il Consiglio di Stato, nel citato parere 515/2016, esplicitamente parla del riconoscimento al cittadino di «un vero e proprio diritto alla richiesta di atti inerenti alle pubbliche amministrazioni, a qualunque fine e senza necessità di motivazioni: dunque, la *disclosure* non è più limitata a quelle informazioni riguardo alle quali egli sia titolare di un interesse specifico e qualificato ("*diretto, concreto e attuale*") idoneo a "motivare" la sua istanza di accesso, come disposto dalla legge sul procedimento amministrativo (l. 241/90)» e configura la previsione di una «trasparenza di tipo "reattivo", cioè in risposta alle istanze di conoscenza avanzate dagli interessati. Il passaggio dal bisogno di conoscere al diritto di conoscere (*from need to right to know*, nella definizione inglese *F.O.I.A*) rappresenta per l'ordinamento nazionale una sorta di rivoluzione copernicana, potendosi davvero evocare la nota immagine, cara a Filippo Turati, della Pubblica Amministrazione trasparente come una "casa di vetro"».

[369] M. SAVINO, *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento*, cit., p. 593 ss.: «L'area del conoscibile non termina più laddove finiscono gli obblighi di pubblicazione. […] Il principio di pubblicità non si fonda più sulla logica deontica e dirigista degli obblighi di legge, ma sul pieno riconoscimento della libertà del singolo di attingere alle informazioni amministrative. Tale libertà, in attesa di una esplicita copertura costituzionale, è ormai tutelata alla stregua di un diritto fondamentale».

[370] La disposizione, in linea con il modello di governo aperto, determina alcune riflessioni sulle modalità di applicazione concreta anche in considerazione del bilanciamento tra interessi in gioco. Cfr. G. D'URGOLO, *Trasparenza e prevenzione della corruzione nella P.A.*, cit., p. 1 ss. e B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso*

Questo conduce ad esaminare il volto contemporaneo della trasparenza, che non è solo di tipo proattivo e reattivo, ma altresì attivo, realizzato con lo strumento degli *open data*.

---

civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53), in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33. Analisi della normativa, impatti organizzativi ed indicazioni operative*, Maggioli, Rimini, 2013, p. 112 ss., secondo cui il diritto è assistito da una misura di tutela specifica, l'accesso civico. P. FALLETTA, *op. cit.*, p. 10 ss. mette in guardia circa i rischi del modello di trasparenza digitale e *open government*, che deve fare i conti con i rischi della rete relativi alla polarizzazione e alla deformazione, con conseguenti conflitti virtuali che spesso prendono di mira proprio l'azione dei pubblici poteri e l'apparato burocratico; di conseguenza «occorre rimediare a che l'interesse pubblico all'acquisizione di dati e documenti – così radicalmente potenziato dalle recenti riforme – non diventi meramente strumentale a una diffusione selettiva e deviante delle conoscenze, con effetti intuitivamente deleteri per l'informazione e la partecipazione dei cittadini, nonché per le garanzie di imparzialità e buon andamento della P.A.». Il rafforzamento della trasparenza in senso democratico e come tutela delle libertà e dei diritti passa dalla partecipazione, dalla condivisione dei processi e dalla collaborazione.

Capitolo 3

La società dei dati e degli algoritmi. *Open data* e *big data*

SOMMARIO: 3.1. *Open data*: principi e caratteristiche. – 3.1.1. La dimensione giuridica. – 3.1.2. La dimensione tecnica ed economica. – 3.2. Ecosistema *open data*: i profili sociali. – 3.3. I dati aperti nel quadro normativo vigente. – 3.4. Strategie e iniziative di *openness*. – 3.4.1. Iniziative a livello internazionale. – 3.4.2. Iniziative a livello nazionale e regionale. – 3.5. *Big data*: caratteristiche e aspetti tecnici. – 3.6. Finalità e valore dei *big data*. – 3.7. I profili relativi alla *digital economy*, i rischi e le implicazioni etico-sociali dei "grandi dati". – 3.8. Le problematiche giuridiche poste dai *big data*. – 3.9. Iniziative e progetti a livello nazionale e internazionale.

3.1. *Open data*: principi e caratteristiche

Sotto l'egida dell'*open government*, basato su un nuovo modello di partecipazione e collaborazione tra universo pubblico e privato, l'evoluzione normativa italiana è giunta a un significativo collegamento tra *disclosure* e apertura, dando vita ad una maturazione del concetto stesso di trasparenza che può essere definita "attiva" e viene realizzata con gli *open data*[371].

Gli *open data*, elemento cardine dei modelli di governo aperto, pongono attenzione al *quomodo* della trasparenza, al suo aspetto dinamico e attivo: la finalità è restituire i dati alla collettività e lasciare che l'intelligenza collettiva ne faccia uso,

[371] Sugli *open data*, oltre ai contributi richiamati nel corso dell'analisi, cfr., *inter alia*, B. WESSELS - R. FINN - T. SVEINSDOTTIR - K. WADHWA, *Open Data and the Knowledge Society*, Amsterdam University Press, Amsterdam, 2017; D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici,* in *Informatica e diritto*, nn. 1-2, 2011; F. DI DONATO, *op. cit.*; M. PALMIRANI - M. MARTONI - D. GIRARDI, *Open Government Data Beyond Transparency*, in A. KŐ - E. FRANCESCONI (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2014*, LNCS 8650, Springer, Cham, 2014, pp. 275-291; V. PAGNANELLI, *op. cit.*, p. 205 ss. Più ampiamente sui dati R. KITCHIN, *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, Sage, Los Angeles, 2014.

potendoli trasformare in leve di nuove e inedite potenzialità economiche e sociali[372]. La trasparenza abbraccia una nuova dimensione, dove la conoscenza è prodotta non solo dalle amministrazioni pubbliche, ma può essere generata da soggetti terzi sulla base di dati, informazioni e documenti resi disponibili dalle amministrazioni[373].

Secondo la *Open Definition* della *Open Knowledge Foundation* un contenuto o un dato si definisce aperto se chiunque è in grado di utilizzarlo, riutilizzarlo e ridistribuirlo, con la limitazione, al massimo, della richiesta di attribuzione e condivisione allo stesso modo[374]. Una definizione è presente anche nell'*International Open Data Charter*[375], secondo cui i dati aperti sono i dati digitali resi disponibili con le caratteristiche tecniche e legali necessarie per essere liberamente utilizzati, riutilizzati e ridistribuiti da chiunque, in qualsiasi momento e ovunque.

Come emerge dalle definizioni, gli *open data* possono essere prodotti da soggetti privati o pubblici; la presente analisi si concentrerà su questi ultimi, definibili più specificamente quali *open government data*, per i quali, però, per mera semplicità, sarà utilizzato il generico termine *open data*[376].

L'ordinamento giuridico italiano fornisce una definizione normativa degli *open*

---

372 Cfr. B. COCCAGNA - G. ZICCARDI, *op. cit.*, p. 395 ss. Alla base dell'approccio *open data* B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo*, cit., p. 114 richiama i presupposti di carattere filosofico: «si contesta che le informazioni gestite dalle amministrazioni in ragione della loro missione istituzionale possano essere trattate alla stregua di beni di proprietà delle PA da porre in commercio al fine di trarne un utile economico, in base alla considerazione del fatto che tali beni, per le loro caratteristiche intrinseche (le informazioni come beni *non rivali*), e per le modalità di raccolta e gestione (con risorse pubbliche, da parte di soggetti pubblici), meritano piuttosto di essere trattati alla stregua dei *commons*».

373 In tal senso B. PONTI, *Il codice della trasparenza amministrativa: non solo riordino, ma ridefinizione complessiva del regime della trasparenza on line*, in *neldiritto.it*, 2013.

374 L'*Open Knowledge Foundation* è un'organizzazione globale non-profit, nata nel 2004 per promuovere la cultura dell'*openness* e della conoscenza aperta. Cfr. *opendefinition.org* e *okfn.org*.

375 *Infra*, § 4.

376 Al riguardo, secondo G. MANCOSU, *op. cit.*, p. 9, nota 35 il procedimento amministrativo «può essere considerato un piccolo giacimento di dati in formato digitale, i quali, se opportunamente classificati, resi fruibili e riutilizzabili, possono sprigionare il loro valore informativo ben oltre il singolo episodio di vita amministrativa, con gli accorgimenti necessari alla tutela degli altri interessi giuridicamente rilevanti, in particolare quello alla riservatezza».

data nell'art. 1, comma 1, lett. l-ter), d.lgs. 82/2005[377], che individua i dati di tipo aperto nelle dimensioni giuridica, tecnologica ed economica.

Sono *open data* i dati che presentano le seguenti caratteristiche:

1. «*sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato*» (dimensione giuridica)[378];
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 lett. l-bis), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati*» (dimensione tecnologica);
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 quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36*» (dimensione economica)[379].

La normativa si preoccupa di definire anche il riutilizzo, ossia «*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*» (art. 1, comma 1, lett. n-bis), d.lgs. 82/2005 e art. 2, comma 1, lett. e), d.lgs. 36/2006).

---

377 La definizione di *open data*, contenuta originariamente nell'art. 68, è stata introdotta dal cosiddetto decreto Crescita 2.0 (d.l. 179/2012, convertito con modificazioni dalla legge 221/2012) ed è stata modificata dal d.lgs. 18 maggio 2015, n. 102, dal d.lgs. 179/2016 e dal d.lgs. 217/2017, che ne ha previsto l'opportuno spostamento nell'art. 1, comma 1, dedicato alle definizioni, in particolare nella lett. l-ter).

378 Il d.lgs. 217/2017 ha affiancato alla licenza, già prevista dalla disposizione, anche il fondamento giuridico della previsione normativa.

379 F. MINAZZI, *Il principio dell'*open data by default *nel Codice dell'Amministrazione Digitale: profili interpretativi e questioni metodologiche*, in *federalismi.it*, fasc. 23, 2013, p. 5 sottolinea i tre requisiti su cui posa la nozione di *open data*, ossia l'adozione di una licenza che consenta ampio riutilizzo, la pubblicazione in un formato aperto e la gratuità o, al più, la marginalità del costo di accesso; la disponibilità in formato aperto non incide sull'integrità delle informazioni e non implica arbitraria manipolabilità.

Gli *open data*, per mezzo del riutilizzo, permettono di generare valore sociale ed economico e, nel farlo, consentono di raggiungere obiettivi diversi: proprio le molteplici finalità che li caratterizzano hanno determinato l'attenzione al fenomeno[380].

Innanzitutto i dati aperti costituiscono strumento di trasparenza e controllo democratico; da tale punto di vista, contribuiscono a garantire maggiore efficienza della macchina pubblica, che è sollecitata a organizzare il patrimonio informativo e i propri processi[381]. Nella loro strumentalità rispetto alla trasparenza, gli *open data* costituiscono efficace mezzo di prevenzione e lotta alla corruzione; ciò permette di generare una maggiore fiducia nelle istituzioni da parte dei cittadini, garantendo altresì agli stessi maggiore partecipazione e coinvolgimento nell'azione pubblica: gli *open data* si pongono come tassello irrinunciabile di una società partecipativa basata su processi di co-produzione tra governanti e governati[382].

I dati aperti contribuiscono, poi, al miglioramento della qualità di vita delle persone che possono utilizzarli, condividerli, incrociarli; allo stesso tempo, concorrono al miglioramento delle politiche pubbliche, costituendo un potenziale supporto alle decisioni, permettendo valutazioni di impatto, analisi e misurazioni e, di conseguenza, potendosi tradurre in un vantaggio competitivo per i territori.

La finalità più significativa che gli *open data* permettono di raggiungere è costituita dal sostegno allo sviluppo economico, dato il grande valore dei dati detenuti dalle istituzioni e la possibilità di essere riutilizzati per nuovi prodotti e servizi: il valore dei dati è tanto maggiore quanto più possono essere impiegati in nuova conoscenza e in soluzioni inedite. I dati formano la "miniera" del patrimonio informativo pubblico e l'attenzione si concentra, quindi, sulla possibilità di restituirli alla collettività, per impiegarli in nuove analisi, servizi e soluzioni in grado di generare crescita economica e

---

380 Cfr. G. MANCOSU, *op. cit.*, p. 4, secondo cui «il dato costituisce, in sostanza, la "valuta" della società della conoscenza, il cui grado di ricchezza è misurabile in funzione dell'ampiezza e della velocità con cui sempre più numerosi *dataset* sono scambiati e riutilizzati, divenendo la base per la produzione di nuovo valore sociale ed economico».

381 Cfr. G. MANCOSU, *op. cit.*, p. 4.

382 Cfr. F. MARZANO, *La trasparenza nella P.A. passa dall'*Open Data *o l'*Open Data *passa dalla trasparenza?*, in *Informatica e diritto*, nn. 1-2, 2011, p. 298 ss.

sociale[383]. In specifico, gli *open data* possono essere valorizzati creando prodotti, *app* e servizi che impattano sulla pubblica amministrazione, sui cittadini, sulle imprese, sul territorio e sullo sviluppo economico[384].

In considerazione delle diverse finalità che permettono di realizzare e dell'eterogeneità dei dati trattati dalle amministrazioni, i dati "da aprire" sono innumerevoli e costituiscono un elenco necessariamente non definibile, perché non ne sono predeterminabili i riutilizzi: tutti i dati possono risultare preziosi e interessanti, basta pensare ai dati geografici, ambientali, sanitari, sociali, turistici, sui trasporti pubblici, sui bilanci, sull'azione amministrativa, sulle attività economiche, sulla criminalità etc.[385].

---

383 Cfr. B. COCCAGNA - G. ZICCARDI, *op. cit.*, pp. 403-404: «La suggestiva metafora del governo piattaforma, sia pure senza trascurare le differenze fra il settore pubblico e quello privato, consente di tratteggiare un nuovo e potente concetto di *trasparenza collaborativa* che si va affermando in rete e che fa leva sull'apertura per promuovere la creazione di valore. L'*open data*, allora, ben lungi dal ridursi a una statica pubblicazione di dati, acquista valore proprio nel suo dinamismo, rappresentando la prima tappa di un cammino che gli utenti proseguono autonomamente per creare impresa, operare un controllo diffuso sulle attività politiche, esprimere opinioni e *feedback*, collaborare nell'espletamento dei compiti istituzionali del governo e nel miglioramento dei servizi pubblici».

384 Cfr. F. CARDARELLI, *op. cit.*, secondo cui la declinazione dei dati aperti «non riguarda il principio di trasparenza (che risponde a finalità di prevenzione della corruzione, di controllo sociale sull'operato dell'amministrazione, e di partecipazione democratica all'attività amministrativa), ma quello della valorizzazione del patrimonio informativo pubblico per finalità connesse allo sviluppo economico (non attiene quindi all'esercizio di libertà politiche, o a posizioni giuridiche soggettive strumentali rispetto all'amministrazione – autorità, ma a quello di libertà economiche)». T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 582 rileva come la dottrina discuta circa l'ambiguità del concetto di *open government data* e proponga una caratterizzazione secondo l'accezione di trasparenza e *accountability* oppure secondo quella di fornitura di servizi legata al valore economico e sociale (*service delivery*). In realtà, anche se riguardano aspetti diversi della relazione tra istituzioni e cittadini, entrambe le accezioni sono importanti e, peraltro, spesso la distinzione non è così netta.

385 Secondo M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, cit., p. 241 ss. «ci sono diversi gruppi di persone ed organizzazioni che possono beneficiare della disponibilità di dati, incluso lo stesso governo. Allo stesso tempo è impossibile prevedere esattamente dove e come il valore sarà creato».

3.1.1. La dimensione giuridica

Al fine di comprendere la tutela che ricevono i *dataset* di *open data* delle amministrazioni pubbliche, è necessaria una premessa circa la protezione giuridica offerta dall'ordinamento agli insiemi strutturati di dati.

Le informazioni strutturate[386], i *dataset*[387] e le banche dati (*database*), quali insiemi organizzati di dati, ricevono la protezione giuridica del diritto d'autore e dei

---

386 I dati, particelle elementari dell'informazione, sono in grado di generare informazioni strutturate; cfr. G. MANCOSU, *op. cit.*, p. 3 ss. Secondo C. SAPPA, *Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano*, in *Informatica e diritto*, nn. 1-2, 2011, p. 186 ss. le informazioni strutturate sono oggetto di tutela, mentre restano fuori solo le informazioni semplici. Cfr. S. ALIPRANDI, Open licensing *e banche dati*, in *Informatica e diritto*, nn. 1-2, 2011, p. 26: dal punto di vista del linguaggio giuridico «"dati" ha una portata semantica più ristretta e si riferisce appunto solo alle singole e isolate informazioni, non organizzate e non elaborate dall'ingegno umano. Queste, in quanto singole informazioni deducibili dalla natura delle cose, non sono sottoposte ad alcuna tutela e privativa diretta»; di conseguenza «i "dati" sono oggetto di regolamentazione e tutela da parte del diritto della proprietà intellettuale solo quando si presentano come sistemi organizzati». A.M. ROVATI, *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, p. 155 descrive l'informazione come «un messaggio comunicabile ad altri attraverso un mezzo qualsiasi», che può essere oggetto di rapporti giuridici e contrattuali; le informazioni hanno valore economico, non esiste un diritto di proprietà o un diritto esclusivo sulle stesse ed il loro uso è teoricamente non rivale, salve le misure giuridiche che ne limitano l'uso. Secondo l'Autore le informazioni strutturate sono tutelate come opera dell'ingegno: di conseguenza, sono protette dalla disciplina sul diritto d'autore «banche dati tutelate da diritto d'autore, banche dati tutelate dal diritto sui generis, ed informazioni strutturate (che secondo parte della dottrina sono autonomamente proteggibili come opere dell'ingegno)» (pp. 169-170); poi ci sono le semplici informazioni, per così dire "grezze", che sono tutelate eventualmente in altre forme o che non ricevono alcuna protezione: «tuttavia anche le semplici informazioni, al pari del diritto patrimoniale d'autore sono beni immateriali ed in senso economico "beni pubblici"» (p. 170) e, di conseguenza, le forme di utilizzazione e circolazione sono molto simili in concreto. Laddove non sia applicabile la normativa sul diritto d'autore, la tutela è definita dallo strumento giuridico con cui le informazioni circolano, che può essere un contratto o un atto unilaterale.

387 Si può intendere per *dataset* un insieme, una collezione, un archivio di dati oggetto di gestione, erogazione e pubblicazione unitaria.

diritti connessi, a seguito, in particolare, delle modifiche alla legge 633/1941 da parte del d.lgs. 6 maggio 1999, n. 169, in attuazione della direttiva 96/9/CE[388].

In particolare, sono oggetto di protezione le opere dell'ingegno di carattere creativo, qualunque ne sia il modo o la forma di espressione[389], i programmi per elaboratore e le banche dati (raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti e individualmente accessibili mediante mezzi elettronici o in altro modo), «*che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore*»[390]; si parla di banche dati selettive (i contenuti sono selezionati in modo originale) e dispositive (è originale la disposizione del materiale) e il titolare del diritto vanta i relativi diritti morali e patrimoniali.

Le banche dati possono anche risultare prive di qualsiasi originalità nella scelta o nella disposizione del materiale, ma possono caratterizzarsi per lo sforzo necessario a reperire e predisporre i contenuti e per l'investimento economico e professionale: per tale motivo è tutelato, altresì, il c.d. diritto *sui generis* o diritto del costitutore[391], diritto cosiddetto connesso, che è autonomo rispetto al diritto d'autore e, a prescindere dall'esistenza di qualunque requisito di creatività e originalità, tutela il costitutore, assegnandogli il diritto di vietare le operazioni di estrazione o reimpiego della totalità o di parti sostanziali della banca dati (art. 102-bis, legge 633/1941)[392].

Alle amministrazioni pubbliche spetta il diritto di autore sulle opere create e pubblicate sotto il loro nome e a loro conto e spese, diritto che dura venti anni a partire dalla prima pubblicazione, qualunque sia la forma nella quale la pubblicazione è stata effettuata[393]; di conseguenza alle amministrazioni è applicabile il diritto d'autore in

---

388 Sulla tutela del diritto d'autore, più ampiamente, *infra*, cap. 4, § 4: in questo paragrafo sarà presente un accenno alla disciplina, strumentale a illustrare la dimensione giuridica degli *open data*.

389 Art. 2575 c.c. e art. 1, comma 1, legge 633/1941.

390 La tutela delle banche dati non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto (art. 1, comma 2, e art. 2, comma 1, n. 9, legge 633/1941).

391 La direttiva 96/9/CE e il relativo d.lgs. 169/1999 di attuazione si occupano di tale esigenza.

392 Il diritto del costitutore è indipendente dalla tutelabilità della banca dati a norma del diritto d'autore o di altri diritti e non pregiudica diritti sul contenuto o su parti di esso.

393 Artt. 11 e 29, legge 633/1941; le disposizioni della legge, ai sensi dell'art. 5, non si applicano ai testi degli atti ufficiali dello Stato e delle amministrazioni pubbliche, sia italiane che straniere, che dunque risultano in pubblico dominio.

relazione alle banche dati creative ed è altresì applicabile il diritto *sui generis* in relazione alle banche dati non creative[394].

Da ciò consegue che alle amministrazioni pubbliche spettano i diritti previsti dalla normativa in capo al titolare del diritto d'autore e, in specifico, i diritti morali, irrinunciabili, inalienabili e imprescrittibili, quale il diritto alla paternità[395], e i diritti patrimoniali o di utilizzazione economica, che si sostanziano in una serie di facoltà di utilizzazione economica esclusive e indipendenti[396]. Il titolare del diritto d'autore ha il diritto esclusivo di pubblicare quanto protetto e di utilizzarlo economicamente in ogni forma e modo, originale o derivato, nei limiti e per gli effetti fissati dalla legge.

La tutela offerta dalla normativa sul diritto d'autore non crea ostacoli al riutilizzo, ma impone che il titolare del diritto disciplini condizioni di utilizzo ed eventuali limitazioni con una licenza[397]. In tal senso si esprime anche la direttiva 2003/98/CE, secondo cui gli enti pubblici devono esercitare il proprio diritto d'autore in maniera tale da agevolare il riutilizzo dei documenti[398].

I diritti spettano all'amministrazione pubblica titolare dei dati: i dati, infatti, hanno un titolare, definito normativamente come uno dei soggetti cui si applica il Codice

---

394 In tal senso il considerando 22 della direttiva 2003/98/CE parla di diritti di proprietà intellettuale, indicando il diritto d'autore e i diritti connessi, compreso il diritto *sui generis*. Secondo C. SAPPA, *op. cit.*, p. 190 ss. l'art. 102-bis della legge 633/1941 va interpretato nel senso di offrire tutela anche alle raccolte di dati pubbliche. In merito cfr. A.M. ROVATI, *op. cit.*, p. 159 ss., secondo cui le informazioni possono essere protette anche come informazioni segrete ai sensi degli artt. 98 e 99 del Codice della proprietà industriale, d.lgs. 10 febbraio 2005, n. 30 (seppur altra dottrina ritenga di no) e come tali sono escluse dal riutilizzo. Si applica altresì la disciplina della concorrenza sleale alle amministrazioni solo in caso di attività economica dell'amministrazione (e non se si tratta solo di attività amministrativa nell'esercizio del potere pubblicistico, dello *ius imperii*); in ogni caso il riutilizzo non deve ledere diritti dei terzi relativi alla proprietà intellettuale e industriale.

395 Artt. 20-24, legge 633/1941.

396 Artt. 12-19, legge 633/1941.

397 Cfr. D. SOLDA KUTZMANN, *La circolazione dell'informazione del settore pubblico*, in *Digesto delle Discipline Privatistiche,* Utet, Torino, 2007.

398 Considerando 22 della direttiva 2003/98/CE: «*La direttiva lascia impregiudicate l'esistenza o la titolarità di diritti di proprietà intellettuale da parte degli enti pubblici e non limita in alcun modo l'esercizio dei diritti al di là di quanto da essa stabilito*»; la direttiva chiarisce che con l'espressione "diritti di proprietà intellettuale" «*si indicano esclusivamente il diritto d'autore e i diritti connessi (comprese le forme di protezione sui generis)*».

dell'amministrazione digitale che «*ha originariamente formato per uso proprio o commissionato ad altro soggetto il documento che rappresenta il dato, o che ne ha la disponibilità*» (art. 1, comma 1, lett. cc), d.lgs. 82/2005, inserita dal d.lgs. 179/2016)[399]. Sotto tale profilo «*il trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del dato*», ai sensi dell'art. 50, comma 3-bis, del d.lgs. 82/2005[400]. Di conseguenza, l'uso legittimo del dato avviene per mezzo di apposita licenza da parte del titolare: si intende per licenza standard per il riutilizzo «*il contratto, o altro strumento negoziale, redatto ove possibile in forma elettronica, nel quale sono definite le modalità di riutilizzo dei documenti delle pubbliche amministrazioni o degli organismi di diritto pubblico*» (art. 2, comma 1, lett. h), d.lgs. 36/2006)[401].

L'esaminata nozione normativa di *open data* chiarisce la tipologia di licenza, che deve permettere l'utilizzo dei dati «*da parte di chiunque, anche per finalità commerciali, in formato disaggregato*»[402]; la disposizione fa riferimento alle licenze cosiddette aperte e pare escludere l'imposizione di particolari vincoli e condizioni di rilascio.

Pertanto è necessario esaminare le licenze aperte, per capire quali tipologie tra queste, alla luce della definizione normativa, sono adatte per il rilascio di *open data*.

Per quanto riguarda le banche dati, utilizzando le categorie delle licenze dei software, si distingue tra sistemi di tutela tradizionali, con le relative licenze "proprietarie", e sistemi con licenze "aperte", in relazione ai diversi diritti concessi a chi ne fruisce, seppur entrambe fondate sulla disciplina normativa delle esclusive della proprietà intellettuale[403].

---

399 F. MINAZZI, *op. cit.*, p. 4 ritiene che la definizione di titolare non dia adito a confusione con la normativa in materia di protezione dei dati personali: la definizione di titolare di cui all'art. 4, comma 1, lett. f) del d.lgs. 196/2003 si riferisce, infatti, solo ai dati personali.

400 La disposizione prima dell'intervento del d.lgs. 179/2016 era allocata nell'art. 58 del d.lgs. 82/2005, ora abrogato.

401 Cfr. A.M. ROVATI, *op. cit.*, p. 172 ss., secondo cui le licenze sono qualificabili come atti unilaterali (se gratuite) o come contratti (se è richiesto un corrispettivo): la qualifica non cambia il regime, dal momento che ai sensi dell'art. 1324 c.c. le norme che regolano i contratti si osservano, in quanto compatibili, per gli atti unilaterali tra vivi aventi contenuto patrimoniale.

402 Art. 1, comma 1, lett. l-ter), d.lgs. 82/2005.

403 Cfr. B. CUNEGATTI, *Le licenze* creative commons, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, p. 641 ss.

La tutela tradizionale consiste nel riservare tutti i diritti al titolare; nella prassi si usa l'espressione "*all rights reserved* - tutti i diritti riservati" e in tali casi l'utente potrà limitarsi a fruire dei dati nei limiti previsti, ma senza il consenso di colui che detiene i relativi diritti non potrà copiare, pubblicare o modificare i dati protetti. Diverso è il caso delle licenze di tipo *open*, proprie di una cultura aperta, che al fine di agevolare la libera circolazione, seppur basate sulla disciplina della proprietà intellettuale, invece di stabilire i limiti di utilizzabilità, tendono a garantire una serie di diritti a chi entra in possesso dei dati. La caratteristica principale è la possibilità, poste alcune condizioni, di riutilizzare secondo il modello "*some rights reserved* - alcuni diritti riservati": al riguardo si parla di *copyleft* (in contrapposizione al concetto di *copyright*) e di permesso d'autore; l'unico vincolo sempre presente, anche in questi casi, è l'attribuzione di paternità, il diritto morale.

Sono licenze di tipo aperto le *Creative Commons* (CC) (*www.creativecommons.it*), le *Italian Open Data Licences* (IODL) (*www.dati.gov.it/iodl/2.0*), create allo scopo specifico della diffusione e del riutilizzo dei dati pubblici, e le *Open Data Commons Licenses,* in specifico le *Open Database Licenses* (*opendatacommons.org*), che sono state elaborate dall'*Open Knowledge Foundation*.

Per comprendere le caratteristiche di tali licenze, è opportuno soffermarsi sulle *Creative Commons*, che sono tra le licenze maggiormente utilizzate.

Le *Creative Commons* indicano quali sono le libertà che il titolare vuole concedere e, di conseguenza, a quali condizioni è possibile utilizzare quanto protetto dalle licenze; questo sistema giuridico "standard" semplice, modulare e flessibile consente al titolare, interessato a rendere liberamente accessibili proprie risorse digitali, di scegliere tra i diversi tipi di licenza standard e di specificare così a quali esclusive intenda rinunciare, permettendogli maggiore flessibilità nella modulazione del diritto d'autore[404]. Le licenze standard sono sei, gratuite e valide senza limitazioni di tempo e

[404] Tali licenze nascono negli Stati Uniti nel 2001, sono state rilasciate per la prima volta nel 2002 e poi diffuse in tutto il mondo per agevolare la libera circolazione delle opere dell'ingegno e della cultura, aumentare i contenuti liberamente disponibili in rete e facilitare la diffusione di opere digitali. *Creative Commons* è un'organizzazione non-profit statunitense (*creativecommons.org*); di tali licenze è considerato padre Lawrence Lessig, parte del gruppo di studiosi da cui è nata l'idea, in linea con quanto fatto da Richard Stallman per i software. Le *Creative Commons* italiane (*www.creativecommons.it*) sono

territorio (per la durata del diritto applicabile), frutto della combinazione tra quattro diverse clausole, identificate da una sigla e da un'icona relativa:

- Attribuzione (*Attribution - BY*), ossia il riconoscimento della paternità: tale clausola risponde al diritto morale d'autore, componente essenziale, inalienabile e non rinunciabile della licenza[405];
- Non commerciale (*NonCommercial - NC*), clausola che non autorizza utilizzi a scopi commerciali;
- Non opere derivate (*NoDerivatives - ND*), clausola che non autorizza la creazione di opere derivate, ossia la possibilità di modificare, elaborare, alterare o trasformare i *dataset* originali e crearne altri (si possono solo utilizzare nella versione originaria);
- Condividi allo stesso modo (*ShareAlike - SA*), secondo tale clausola se viene modificato, alterato o trasformato il *dataset* o ne viene creato un altro, quello risultante deve essere distribuito sotto lo stesso regime giuridico "aperto", ossia con la stessa licenza o una equivalente.

Le sei licenze che ne derivano, da quella che lascia maggiori libertà a quella più restrittiva, sono le seguenti, note con le diverse sigle che le caratterizzano: CC BY ("attribuzione"), CC BY-SA ("attribuzione - condividi allo stesso modo"), CC BY-ND ("attribuzione - non opere derivate"), CC BY-NC ("attribuzione - non commerciale"), CC BY-NC-SA ("attribuzione - non commerciale - condividi allo stesso modo"), CC BY-NC-ND ("attribuzione - non commerciale - non opere derivate")[406]. A livello

---

presentate, tradotte e adeguate al nostro ordinamento grazie a un gruppo di lavoro, fondato nel 2003, che fa capo all'Università e al CNR di Torino ed è coordinato dal *Nexa Center for Internet & Society* (le licenze sono state presentate nel 2004). Secondo G.A. CAVALIERE, *Open Data*, in M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014, p. 45 ss. le *Creative Commons* costituiscono «il massimo punto di equilibrio tra le istanze di protezione dei creatori e quelle di accesso della comunità degli utenti»; tali strumenti creano un ponte tra il mondo della cultura libera e quello dell'industria culturale, secondo le intenzioni di Lessig. Sulle *Creative Commons* cfr., *inter alia*, L. LESSIG, *Cultura libera: un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale,* trad. it., Apogeo, Milano, 2005.

405 Tale clausola è presente in tutte le licenze, mentre le altre sono presenti alternativamente o cumulativamente.

406 Tutte le licenze prevedono l'autorizzazione all'utilizzo dell'opera a fini non commerciali, ossia senza scopo di lucro, e tutte richiedono il riconoscimento della paternità (attribuzione). Le licenze

internazionale esiste anche la *Creative Commons zero* (CC0) per attribuire un'opera al pubblico dominio.

Le licenze sono espresse in diverse forme: il *legal code*, ossia la vera e propria licenza da un punto di vista giuridico[407], il *commons deed*[408] e il *digital code* o *machine readable code*, ossia il formato digitale, l'insieme di metadati[409]. Le licenze, redatte sulla base del diritto statunitense o su modelli neutri (internazionali), sono tradotte e adattate ai diversi ordinamenti dai gruppi di lavoro nazionali (c.d. *porting*); l'ultima versione è la 4.0[410].

Alla luce della tutela giuridica offerta agli insiemi strutturati di dati e in considerazione delle diverse tipologie di licenze aperte previste, la definizione normativa dell'art. 1, comma 1, lett. l-ter), d.lgs. 82/2005, che prevede l'utilizzo dei dati da parte di chiunque, anche per finalità commerciali, in formato disaggregato, rende adatta agli *open data* la licenza con la sola clausola di attribuzione di paternità, ossia la licenza *Creative Commons BY* e i corrispettivi della stessa, la IODL 2.0 e l'*Open Data Commons Attribution License*[411].

Creative Commons prevedono il divieto di apposizione di misure tecnologiche di protezione dei diritti concessi, in coerenza con gli obiettivi di condivisione che si prefiggono.

407 Il testo legale che ne esprime l'intero contenuto.

408 Il contenuto essenziale della licenza reso in forma semplificata, di facile comprensione, e identificato con la sigla e l'icona relativa alla licenza.

409 Il *digital code* permette di interfacciare la licenza con i sistemi informatici, di rintracciarla nella rete e di facilitarne la circolazione; cfr. M. TRAVOSTINO, *Le licenze creative commons*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, p. 204 ss.

410 Le licenze sono costantemente adattate, modificate, revisionate e aggiornate sia per adattarsi alle evoluzioni, sia per sanare questioni relative all'efficacia e alla validità: ciò si traduce nelle diverse "versioni", ad oggi 4.0 nella versione internazionale e italiana. Esistono anche versioni internazionali *unported,* basate sui trattati internazionali sul *copyright* e non adattate ad alcun ordinamento nazionale. Le licenze CC prevedono espressamente la necessità di accettazione da parte dell'utente, in conformità alla loro natura contrattuale, ma tale accettazione è ricondotta al mero comportamento dotato di sufficienti elementi per avere valore contrattuale, per essere "concludente" ai fini della stipula; cfr. B. CUNEGATTI, *op. cit.*, p. 650 ss.

411 Cfr. A.M. ROVATI, *op. cit.*, p. 172 ss., secondo cui «è comunque bene che la P.A. non rinunci in modo completo e definitivo alla titolarità su eventuali diritti d'autore o connessi relativi alle informazioni, con una cessione totale, ma semplicemente ne attribuisca la possibilità di utilizzazione (ovviamente senza

Limitazioni ulteriori, come l'apposizione della clausola "condividi allo stesso modo" (*ShareAlike*), possono risultare particolarmente limitanti per la circolazione a livello commerciale, per la creatività e per l'attività economica dei potenziali licenziatari[412] e non trovano fondamento e giustificazione normativa nella nozione di *open data* del nostro ordinamento. In tal senso si esprimono anche le linee guida nazionali per la valorizzazione del patrimonio informativo pubblico adottate dall'AgID per l'anno 2017, che suggeriscono la licenza CC-BY nella sua versione 4.0, presupponendo altresì l'attribuzione automatica di tale licenza nel caso di applicazione del principio o*pen data by default*, espresso nelle disposizioni contenute nell'art. 52 del d.lgs. 82/2005, che più avanti sarà oggetto di analisi[413]. Al riguardo, è opportuno ricordare che, accanto allo strumento della licenza, l'art. 1, comma 1, lett. l-ter), d.lgs. 82/2005 prevede esplicitamente la possibilità che sia una previsione normativa a rendere disponibili i dati, permettendone l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato.

La previsione circa l'irrinunciabilità, l'inalienabilità e l'imprescrittibilità del diritto morale d'autore[414] e la possibilità per l'amministrazione di esercitare i relativi rimedi previsti dalla normativa[415] rendono preferibile nel nostro ordinamento e più conforme alla normativa la scelta della licenza con la sola clausola di attribuzione rispetto a soluzioni di pubblico dominio; una significativa conferma in tal senso la offre anche l'art. 7 del d.lgs. 33/2013, che prevede il riutilizzo dei dati in formato aperto, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne

---

esclusiva salvo i casi previsti nell'art. 11, dir. 2003/98/CE), secondo lo schema del contratto di licenza (propriamente inteso)» (p. 177).

412 In tal senso anche la comunicazione della Commissione europea «*Comunicazione della Commissione — Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti*», 2014/C 240/01, pubblicata nella Gazzetta ufficiale dell'Unione europea il 24/07/2014: «è opportuno che la licenza copra unicamente le condizioni di attribuzione, perché qualsiasi altro obbligo rischia di limitare la creatività o l'attività economica del licenziatario e, quindi, di inibire le potenzialità di riutilizzo del documento».

413 Art. 52, comma 2, d.lgs. 82/2005; *infra*, § 3.

414 Artt. 20-24, legge 633/1941.

415 A.M. ROVATI, *op. cit.*, p. 172 ss.

l'integrità[416]. Inoltre in tale direzione devono essere considerati i principi di indisponibilità dei beni del demanio culturale, previsti negli artt. 10 e 53 del d.lgs. 22 gennaio 2004, n. 42 (Codice dei beni culturali)[417].

3.1.2. La dimensione tecnica ed economica

La dimensione tecnologica si traduce nel fatto che, per essere *open*, i dati devono essere «*accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera l-bis)*», «*adatti all'utilizzo automatico da parte di programmi per elaboratori*», ossia *machine readable*[418], e «*provvisti dei relativi metadati*».

Pertanto i dati devono essere rilasciati in formato aperto, ossia «*un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi*» (art. 1, comma 1, lett. l-bis), d.lgs. 82/2005)[419].

La norma prescrive, inoltre, la necessità che tali dati siano adatti all'utilizzo automatico da parte dei software e siano accompagnati da metadati, intendendosi per tali le informazioni e i dati che descrivono altri dati. Sono metadati il titolo del *dataset*, la data di ultimo aggiornamento, il soggetto che detiene e gestisce i diritti sui dati, la licenza utilizzata e la descrizione del *dataset*. La presenza dei metadati è particolarmente significativa per la ricerca, la localizzazione, l'interoperabilità e la correlazione di dati e per traghettare così anche l'amministrazione pubblica verso il *web*

---

416 Cfr. B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo*, cit., p. 118 ss., secondo cui mentre la disposizione del d.lgs. 82/2005, originariamente l'art. 68 e oggi l'art. 1, comma 1, lett. l-ter), indica in positivo il contenuto della licenza, l'art. 7 del d.lgs. 33/2013 la indica in negativo, ponendo le clausole restrittive da osservare (rispettare l'integrità e citare la fonte); sostanzialmente i due articoli si integrano a definire le condizioni giuridiche che regolano la disponibilità dei dati a fini di riutilizzo.

417 In tal senso le citate linee guida dell'AgID per l'anno 2017.

418 G. MODESTI, *op. cit.*, p. 31.

419 Come per la definizione di *open data*, anche nel caso della definizione di formato aperto il d.lgs. 217/2017 ha previsto l'opportuno spostamento dall'originario art. 68, dove era collocata, all'art. 1, comma 1, dedicato alle definizioni.

semantico o *web of data*[420].

Per quanto riguarda il profilo tecnologico e il grado di "apertura" è comunemente richiamata la classificazione "*5 stars*" di Tim Berners-Lee[421]:

1 stella, il dato è disponibile sul web in qualunque formato, ma con una licenza aperta (si parla anche di dato grezzo, *data raw*), es. pdf[422];

2 stelle, formato strutturato processabile in modo automatico da software, di tipo proprietario, accompagnato da licenza aperta, es. excel;

3 stelle, condivide le caratteristiche delle 2 stelle, ma in tal caso il formato è aperto, non proprietario, es. csv[423];

4 stelle, formati strutturati in formato aperto con licenza *open*, che seguono gli standard aperti proposti da W3C, dotati di URI (*Uniform Resource Identifier*) e quindi indirizzabili in rete e utilizzabili online, es. RDF (*Resource Description Framework*)[424];

---

420 I metadati richiamati nel testo sono descrittivi, ma esistono altre tipologie come quelli amministrativi e gestionali e quelli strutturali; cfr. Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA. Secondo D. SOLDA KUTZMANN, *op. cit.*, i metadati «hanno l'obiettivo di agevolare l'individuazione di un'informazione esistente, permettere la sua localizzazione, rintracciare una particolare occorrenza del dato, semplificarne la sua selezione, e, attraverso tecniche di analisi e valutazione, garantire la cosiddetta interoperabilità semantica, per permettere la ricerca in ambiti disciplinari diversi grazie a una serie di equivalenze fra descrittori. È questo il motivo, peraltro, per cui, nei progetti di digitalizzazione e nelle attività di gestione degli archivi di oggetti digitali, i metadati rivestono un'importanza tanto determinante, da essere considerati parte costituente dell'informazione stessa, e numerose politiche comunitarie siano dirette in tal senso verso la creazione di principi comuni per l'archiviazione e la descrizione dei dati». Cfr. F. MINAZZI, *op. cit.*, p. 10, secondo cui grazie ai metadati e alla pubblicazione dei dati tramite ontologie (sistemi di metadati strutturati in modo gerarchico) è possibile favorire la transizione verso il *web semantico*.

421 Si tratta di un modello di classificazione in cui ogni livello successivo ha i requisiti di quello precedente e alcune caratteristiche ulteriori che rendono i dati maggiormente aperti.

422 In tal caso i dati sono semplicemente resi disponibili in rete e sono *open* da un punto di vista giuridico, grazie al fatto che sono accompagnati da una licenza aperta. Dal dato grezzo, grazie a operazioni di *data scraping*, è possibile estrarre i dati e convertirli in un formato aperto.

423 Il livello 3 *stars* consente di rimuovere le barriere tecnologiche di accesso che vincolano all'uso di determinate piattaforme, promuovendo neutralità e interoperabilità; cfr. T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 585.

424 In tal modo i dati si svincolano in modo permanente dalla locazione fisica della risorsa e possono collegarsi tra loro: grazie a RDF due risorse, soggetto e oggetto, sono in relazione grazie a un predicato

5 stelle, i *linked open data* (LOD), dove i dati di livello 4 stelle contengono anche link ad altri dati e quindi, fornendo un contesto e un collegamento dinamico, acquisiscono maggior valore[425]. I *dataset* sono messi a disposizione come servizi (*data as a service*) per l'utilizzo e la correlazione con altri *dataset*[426].

Viene comunemente utilizzato un "catalogo" standard di principi e caratteristiche che i dati aperti devono possedere per essere autenticamente tali: completi; primari[427]; tempestivi; accessibili; processabili da computer[428]; non discriminatori[429]; non proprietari[430]; liberi da licenze che ne limitino l'uso[431]; riutilizzabili; ricercabili[432]; permanenti[433].

(tripla, in cui ogni elemento è identificato da URI); T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 585 ss.

425 Cfr. *5stardata.info*. I *linked open data* si situano nel passaggio da una rete che connette documenti con *html* e *hyperlink* al web basato su un'interconnessione di dati o risorse digitali univocamente identificate tramite URI e linkate con RDF. I requisiti base per pubblicare *linked open data* consistono, quindi, nell'utilizzo di URI per l'identificazione, nell'esposizione dei dati per l'accesso tramite protocollo http e nell'uso, per descrivere i contenuti e collegarli, del modello di dati RDF, che codifica le relazioni tra dati in base ad asserzioni costituite da triple (soggetto, predicato, oggetto). Le triple linkate creano grafi sempre più complessi; SPARQL, *Simple protocol and RDF Query Language*, è lo standard per interrogare archivi conformi a RDF. Cfr. T. AGNOLONI, Linked Open Data *nel dominio giuridico*, cit., p. 411 ss., secondo cui il vantaggio dei *linked open data* sta nell'interoperabilità: «il valore dei dati si accresce significativamente quando *dataset* diversi creati e pubblicati indipendentemente da soggetti diversi, possono essere riutilizzati liberamente e messi in correlazione da terze parti senza barriere tecniche» (p. 414). Secondo G. RIZZO - F. MORANDO - J.C. DE MARTIN, *op. cit.*, p. 493 ss. «il web è lo spazio di tutte le cose (*web of Things*), le quali sono rappresentate mediante dei dati (*web of Data*)» (p. 503) e «il sottosuolo è il luogo ove i dati vengono inseriti, *Open Data*, mentre la pianta nasce dall'unione delle radici, *Linked Data*. L'incontro tra le radici crea nuove piante, dalle quali nasce un nuovo dato. Ma il dato più fertile è il dato *raw*» (p. 510).

426 T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 586 ss.

427 I dati sono prelevati dalla fonte e possiedono il massimo grado di granularità.

428 I dati sono strutturati in modo da consentire un'elaborazione automatica da parte delle macchine.

429 Disponibili per chiunque, senza requisiti di autenticazione.

430 Dati in formato non proprietario.

431 Sono ammesse ragionevoli restrizioni di privacy, sicurezza e privilegi di accesso.

432 Facilmente identificabili in rete, grazie a cataloghi indicizzabili dai motori di ricerca.

433 In tal senso il manifesto di attivisti e sostenitori del movimento *open government* del 2007 (che prevede i primi otto principi indicati), noto come "*8 principles of Government Data*", elaborato in un

Alla dimensione giuridica e tecnica si sposa quella economica: per essere *open* i dati «*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 quanto previsto dall'articolo 7 del decreto legislativo 24 gennaio 2006, n. 36*».

Le linee guida dell'AgID per l'anno 2017 suggeriscono espressamente azioni volte a rendere gli *open data* disponibili esclusivamente a titolo gratuito. La possibilità di richiedere un corrispettivo specifico per il riutilizzo dei dati è limitata ai costi sostenuti effettivamente per la riproduzione, messa a disposizione e divulgazione dei dati, in base a tariffe standard determinate, su proposta motivata del titolare del dato, dall'AgID sulla base dei costi marginali, corrispondenti ai costi effettivi e pubblicate sul proprio sito istituzionale[434].

L'art. 7 del d.lgs. 36/2006 prevede casi specifici per i quali non si applicano tali previsioni e per i quali, di conseguenza, è possibile determinare tariffe superiori ai costi marginali in deroga al principio generale: è il caso delle biblioteche, comprese quelle universitarie, dei musei e degli archivi; delle pubbliche amministrazioni e degli organismi di diritto pubblico, che devono generare utili per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico; dei casi eccezionali relativi a documenti per i quali le pubbliche amministrazioni e gli organismi di diritto pubblico sono tenuti a generare utili sufficienti per coprire una parte sostanziale dei costi di raccolta, produzione, riproduzione e diffusione. In queste ipotesi, i Ministeri competenti, di concerto con il Ministero dell'economia e delle finanze, sentita l'AgID, determinano, con appositi decreti, i criteri generali per le tariffe e le relative modalità di versamento, mantenendo aggiornate le stesse ogni due anni.

---

meeting negli Stati Uniti guidato da Tim O' Reilly e Carl Malamud e divenuto standard per valutare gli *open data*, e il Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA e realizzato nell'ambito delle attività finalizzate all'elaborazione delle linee guida per i siti web delle pubbliche amministrazioni (previste dalla direttiva n. 8 del 26 novembre 2009 del Ministro per la pubblica amministrazione e l'innovazione).

[434] Art. 7, d.lgs. 36/2006.

3.2. Ecosistema *open data*: i profili sociali

La gestione dei dati è un aspetto imprescindibile e fisiologico delle attività svolte dalle amministrazioni; le informazioni pubbliche, in considerazione della loro qualità, completezza e affidabilità, assumono particolare valore e il loro utilizzo è appetibile per i cittadini, per le imprese e per l'industria dei contenuti digitali[435]. La valorizzazione e la circolazione dei dati pubblici è possibile per mezzo della loro messa a disposizione e del successivo uso[436]: passa quindi dall'uscita "dalle mani" del titolare verso nuovi soggetti grazie al riutilizzo[437].

Sotto tale profilo la genesi degli *open data* si colloca all'interno di una più ampia filosofia che può essere descritta con il concetto di *openness* che pervade la società, le relazioni e il cambio di paradigma nel rapporto tra mondo pubblico e privato[438]. In coerenza con il principio di apertura di cui si fanno latori, gli *open data* devono la loro nascita a un insieme di "spinte" che arrivano sia a livello istituzionale sia a livello di

---

435 Cfr. M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, cit., p. 239 ss.: i benefici sono limitati «sia da preoccupazioni inerenti la riservatezza, la sicurezza, la fiducia sia dalla mancanza (o carenza) di accesso a Internet, usabilità, capacità adeguate o accessibilità per tutti».

436 Cfr. T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 581, secondo cui la trasparenza non riguarda solo l'accesso, ma anche la condivisione e il riuso dei dati. «Spesso per capire i dati è necessario analizzarli, combinarli con altri, processarli e visualizzarli in modi e contesti diversi da quelli della loro originale pubblicazione e questo richiede che i dati siano "aperti" e possano essere liberamente riusati».

437 Cfr. D. SOLDA KUTZMANN, *op. cit.*: le amministrazioni per alcune tipologie di dati possono essere gli unici produttori e gestori e quindi occupare una posizione di monopolio naturale; laddove i formati non siano standard o ci siano tariffazioni per ottenere ritorni economici ciò si pone in contrasto con le norme e può risultare lesivo delle regole poste a tutela della concorrenza sul mercato.

438 F. MARZANO, *op. cit.*, p. 288: «l'*openness* sottende una filosofia di base: il fatto che l'apertura in tutte le sue forme e concretizzazioni sia fondamentale per rendere l'uomo più libero dai vincoli impostigli dalle strutture della società». Sotto tale profilo T. AGNOLONI, *Dall'informazione giuridica agli* open data *giuridici*, cit., p. 583 sottolinea che la filosofia dell'*openness* si è originariamente sviluppata nell'ambito dei software *open source* e poi si è estesa a tutte le risorse digitali.

società civile, grazie a movimenti di associazioni e cittadini[439], sollecitazioni che, pertanto, giungono contemporaneamente dall'alto e dal basso, ma risultano sinergiche nella direzione cui sono dirette e rispondono all'evoluzione stessa della società di riferimento in senso aperto, acentrico e acefalo.

La premessa etica e filosofica implicita del fenomeno *open data* si annida nell'idea che i dati pubblici appartengono alla collettività e con la loro "liberazione" tornano alla collettività, come valore per la stessa da poter impiegare[440]. Il presupposto necessario perché questo si verifichi consiste in una forte fiducia da parte dei diversi attori del processo *open data* nella tecnologia, che si ottiene con il rispetto dei limiti giuridici, quali la protezione dei dati personali e la tutela della proprietà intellettuale, ma anche con l'impegno, la responsabilità e la trasparenza nel condurre la relazione con la collettività[441]. Da questo punto di vista sono importanti gli atti della singola amministrazione relativi alla propria strategia *open data*, in cui è opportuno chiarire gli obiettivi in modo esplicito, pianificare le azioni e prevedere forme di monitoraggio dell'uso dei dati[442].

Il processo relativo agli *open data*, composto da identificazione e mappatura dei dati, analisi, pubblicazione e diffusione deve essere reso trasparente e chiaro anche

---

439 Nel caso italiano, per limitarsi a qualche esempio, Spaghetti open data (SOD) (*www.spaghettiopendata.org*), gruppo che dal 2010 promuove l'apertura e il riutilizzo dei dati e OpenPolis (*www.openpolis.it*), associazione che dal 2006 promuove l'*openness* nelle sue diverse forme (*open source*, *open data*, *open government*).

440 I dati prodotti dalle amministrazioni sono finanziati dalle tasse dei contribuenti. Cfr. G. DE MINICO, *Gli open data: una politica "costituzionalmente necessaria"?*, in *forumcostituzionale.it*, 2014, p. 2: «Se il dato detenuto dall'amministrazione appartiene al patrimonio indiviso di una collettività, su di esso il soggetto pubblico non può vantare un titolo proprietario esclusivo perché il dato è della collettività, mentre l'amministrazione ne è semplicemente il custode, peraltro temporaneo. E allora la p.a. non è facoltata, ma obbligata a diffonderlo perché non fa altro che restituire al suo legittimo proprietario quanto già gli appartiene».

441 Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA. In tal senso, altresì, M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, cit, p. 251 ss.: «sicurezza, fiducia, trasparenza, accessibilità e *privacy* diventano gli anelli di una catena unica».

442 Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA.

all'esterno dell'amministrazione. Il *trust* necessario per lo sviluppo dell'"ecosistema *open data*" significa anche fiducia riposta nei dati messi a disposizione, che non devono essere parziali o fuorvianti e idonei a manipolare gli utenti. Si collega a questo la necessità di accessibilità, da intendersi sia come facilità di fruizione, ma altresì come possibilità di integrazione[443].

Il paradigma *open data* su cui si fonda, anche se non esclusivamente, il modello di *open government* chiama governanti e governati ad assumere un ruolo proattivo gli uni verso gli altri: gli *open data* si pongono come mezzo per realizzare il governo aperto e, quindi, per ottenere anche una diffusa partecipazione attiva e una costante collaborazione dei cittadini alle scelte e all'azione amministrativa[444].

In questo percorso di apertura i diversi soggetti che compongono la società sono coinvolti in un nuovo processo di *empowerment*.

Nel caso delle amministrazioni pubbliche, questo atteggiamento proattivo si traduce in una riorganizzazione dei processi relativi ai dati e in un'attività di programmazione e pianificazione finalizzata a rendere disponibili i dati come *open data*[445]. Gli *open data* permettono maggiore trasparenza dell'azione pubblica e portano le istituzioni a comportarsi più come "gestori" che come "proprietari" o, peggio, "monopolisti" dei dati, potendo fruire peraltro delle elaborazioni fatte da terzi sui propri e su altri dati[446].

Per quanto riguarda cittadini, associazioni e imprese, gli *open data* esigono una cittadinanza più matura e consapevole, in grado di essere proattiva in modo autonomo nei confronti dell'amministrazione e di coadiuvarla nello svolgimento di attività di interesse generale grazie ad analisi, combinazioni, servizi realizzati con i dati messi a disposizione: una cittadinanza autenticamente "attiva"[447]. Ciò non significa

---

443 Cfr. M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, cit., p. 251 ss., secondo i quali si tratta di un'accessibilità rivolta «sia alle persone sia alle tecnologie. L'accessibilità può far riferimento sia alla libertà di fruizione sia alla libertà dei dati stessi» (p. 258).

444 Cfr. F. PATRONI GRIFFI, *op. cit.*, p. 3 ss.

445 Cfr. G. MANCOSU, *op. cit.*, p. 4 e F. MARZANO, *op. cit.*, p. 295 ss.

446 F. MARZANO, *op. cit.*, p. 295 ss.

447 F. MARZANO, *op. cit.*, p. 292 ss. al riguardo richiama il concetto di *citizensourcing*, ossia un nuovo rapporto tra istituzioni e cittadini che si basa sulla motivazione, partecipazione e integrazione, finendo per

deresponsabilizzare le amministrazioni, ma sprigionare il loro ruolo a servizio della collettività: si traduce in un nuovo modo di operare e in un'inedita forma di interazione e controllo[448].

Gli *open data* aiutano i cittadini nelle loro scelte, accrescendo la loro conoscenza e la loro consapevolezza, e li spingono, altresì, ad essere maggiormente attivi nei confronti delle istituzioni, potendo essere riutilizzatori o, quantomeno, beneficiari di servizi a valore aggiunto basati sul riutilizzo[449]. Questo è ancora più vero se si pensa alle imprese, che dal riutilizzo sono favorite nello sviluppo di nuovi servizi e prodotti e nella creazione correlata di posti di lavoro; le associazioni e le imprese possono porsi nell'ecosistema *open data* anche come intermediari tra governanti e governati, capaci di creare sui dati applicazioni fruite poi dai cittadini[450].

Pertanto quello che possiamo chiamare "ecosistema *open data*" vive grazie all'interazione e alla sinergia tra i ruoli agiti dai diversi attori della società e permette ad ognuno di loro di ricavare vantaggi: trasparenza e apertura si nutrono e, al tempo stesso, valorizzano il contributo della società civile alla formazione delle politiche pubbliche e all'azione amministrativa. È consapevole di questo anche l'Unione europea quando nel considerando 4 della direttiva 2013/37/UE espressamente prevede che «*la possibilità di riutilizzare i documenti detenuti da un ente pubblico conferisce un valore aggiunto per i riutilizzatori, gli utenti finali e la società in generale e, in molti casi, per lo stesso ente pubblico, grazie alla promozione della trasparenza e della responsabilizzazione e al ritorno di informazione fornito dai riutilizzatori e dagli utenti finali che permette all'ente pubblico in questione di migliorare la qualità dei dati che raccoglie*»[451].

«esternalizzare un compito tradizionalmente svolto da un funzionario pubblico presso un largo e indefinito gruppo di cittadini sfruttando la forma dell'*open call*».

448 Cfr. R. CAZZANTI, *op. cit.*, p. 71 ss.

449 M.C. DE VIVO - A. POLZONETTI - P. TAPANELLI, Open Data, Business Intelligence *e* Governance *nella Pubblica Amministrazione*, cit., p. 242: «L'obiettivo dell'*Open Government Data* consiste sostanzialmente nell'aiutare il cittadino a prendere decisioni migliori, o almeno più efficienti, nella vita di tutti i giorni, oppure a rendere più abile e più attivo nella vita di tutti i giorni il suo operato».

450 G. RIZZO - F. MORANDO - J.C. DE MARTIN, *op. cit.*, p. 496 ss.

451 Cfr. B. COCCAGNA - G. ZICCARDI, *op. cit.*, p. 414 ss., che considerano «i grandi "giacimenti informativi" di cui sono detentori gli enti pubblici una miniera la cui importanza va ben oltre l'intrinseco valore economico della mole dei dati *liberati*: non solo aumenta in misura esponenziale con il suo

In tale contesto disponibilità e riutilizzo sono biunivocamente collegati, dal momento che il riutilizzo avviene su dati resi disponibili in modo aperto, ma allo stesso tempo alimenta ulteriori richieste di messa a disposizione di *open data* utili o necessari. Il dato si "anima", "prende vita" consentendo non solo la fruizione, ma divenendo base per nuova conoscenza, nuovi servizi, nuove applicazioni.

Per rendere efficace e realmente operativo l'ecosistema *open data* sono necessari una serie di presupposti imprescindibili.

Prima fra tutti si pone l'esigenza improcrastinabile di una cultura sull'apertura dei dati e dei governi capace di mutare la fisionomia delle amministrazioni e di pervadere la società. Alla cultura si lega in modo stretto la consapevolezza, indispensabile per agire pienamente i ruoli che i diversi attori hanno nel funzionamento di questo peculiare ecosistema. In specifico ciò si traduce in consapevolezza del valore dei dati e della necessità della loro qualità da parte delle amministrazioni e consapevolezza della disponibilità e del possibile uso dei dati stessi da parte della collettività.

Cultura e consapevolezza, a loro volta, necessitano di alcuni profili organizzativi, in specifico di un cambiamento dei processi, di una maturazione della relazione con l'utenza e del conseguente instaurarsi di un modello orizzontale e bidirezionale, capace *ex ante*, durante ed *ex post*, ossia in modo costante durante tutto il processo di produzione e pubblicazione degli *open data*, di avvalersi dell'apporto esterno di altre istituzioni, imprese, cittadini, associazioni[452]. Ciò si traduce nel confrontarsi con la collettività per identificare i dati da aprire (*ex ante*), monitorare, raccogliere suggerimenti e *feedback* sul processo di apertura e conoscere quanto realizzato con il riutilizzo dei dati (durante ed *ex post*).

Nel percorso di apertura dei dati e dei governi evolve parallelamente il ruolo stesso degli attori protagonisti, muta il volto delle amministrazioni che diventano aperte

---

riutilizzo, ma innesca, grazie alle autonome iniziative dei cittadini, meccanismi virtuosi e imprevedibili. E sviluppi inattesi».

[452] Cfr. E. BELISARIO - G. COGO - R. SCANO, *I siti web delle pubbliche amministrazioni. Norme tecniche e giuridiche dopo le Linee Guida Brunetta*, Maggioli, Rimini, 2011, p. 163 ss., secondo cui l'amministrazione aperta, «che era già auspicabile per un'Amministrazione tradizionale (analogica), diventa oggi possibile grazie all'uso delle tecnologie info-telematiche; soltanto adesso, con il progresso tecnologico rappresentato dal *Web 2.0*, ciò può essere realizzato efficacemente e con costi sostenibili».

e matura la capacità di incidere della collettività, che diventa più consapevole, attiva, proattiva.

3.3. I dati aperti nel quadro normativo vigente

Dalla configurazione del principio di trasparenza quale meta-principio servente a un insieme di significativi principi costituzionali discende il diritto dei cittadini di accedere ai dati pubblici, che di conseguenza devono essere resi disponibili.

Il Codice dell'amministrazione digitale, d.lgs. 82/2005, è particolarmente attento al principio di disponibilità dei dati pubblici in formato digitale[453]. Già nell'enunciazione iniziale delle finalità il d.lgs. 82/2005 chiarisce questo aspetto: Stato, Regioni e autonomie locali devono assicurare «*la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate e nel modo più adeguato al soddisfacimento degli interessi degli utenti le tecnologie dell'informazione e della comunicazione*»[454].

Il principio viene poi declinato nell'esplicita previsione dell'art. 50 del d.lgs. 82/2005, ai sensi del quale i dati delle pubbliche amministrazioni devono essere formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie informatiche che ne consentano fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e da parte dei privati; vengono fatti salvi

---

453 L'art. 2, comma 1, lett. d), d.lgs. 36/2006 definisce il dato pubblico come «*il dato conoscibile da chiunque*»; in merito, secondo C. SAPPA, *op. cit.*, p. 186 ss., in base alla definizione normativa, «viene da pensare che i dati pubblici siano quelli pubblicati, distribuiti o messi a disposizione di un numero non determinato di soggetti, che possono dunque accedervi anche individualmente in tempi e luoghi da essi prescelti». Al riguardo D. SOLDA KUTZMANN, *op. cit.*, in merito alla nozione di dati pubblici, precisa che «gli obblighi dettati in materia di accesso e riuso si applicano compatibilmente con la disciplina sulla protezione del diritto d'autore e con le disposizioni di accordi internazionali sulla protezione dei diritti di proprietà intellettuale, e lasciano impregiudicati i diritti di proprietà intellettuale ovvero diritti di proprietà industriale facenti capo a terzi».

454 Art. 2, d.lgs. 82/2005. Secondo G. MANCOSU, *op. cit.*, p. 8 ss. la norma indica all'amministrazione sia il compito da svolgere (accesso all'informazione), sia i mezzi per attuarlo (le tecnologie ICT).

dalla norma i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali e il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico[455].

Negli ultimi anni, la normativa italiana ha rafforzato questo principio e ha promosso esplicitamente gli *open data*, sotto lo stimolo "dall'alto" del panorama internazionale e dell'Unione europea, che ha dedicato direttive e strategie alla valorizzazione e al riutilizzo dell'informazione nel settore pubblico, ma anche in conseguenza alla pressione "dal basso" sia da parte dei soggetti pubblici, in particolare tramite le norme e le strategie regionali e locali, sia da parte dei soggetti privati, riuniti in movimenti a favore e sostegno dei dati aperti.

La maturazione del concetto di trasparenza verso l'apertura ben si giustifica e può ritenersi favorita dalla Costituzione italiana, dal momento che le strategie di *open data* sono strumentali al principio democratico e all'esercizio della sovranità popolare, ai principi di eguaglianza e sviluppo della persona, al buon andamento e all'imparzialità dell'azione pubblica e alla sussidiarietà orizzontale, che auspica una nuova relazione tra governanti e governati[456]. La maturazione del principio di trasparenza coincide con l'evoluzione dalla concezione di "proprietà" del dato a quella di "accesso" e "apertura" del dato, in coerenza con il parallelo passaggio dal paradigma della proprietà a quello dell'accesso che connota la società della conoscenza[457].

Nell'evoluzione normativa europea e nazionale, inizialmente le politiche e le strategie relative agli *open data* si affacciano sulla scena come inviti e incoraggiamenti alla pubblica amministrazione, per poi assurgere a veri e propri doveri cui la pubblica

---

455 F. MINAZZI, *op. cit.*, p. 2 sottolinea che l'art. 50 costituisce norma generale in tema di disponibilità dei dati pubblici, siano essi aperti o meno, mentre l'art. 52 ne costituisce una specificazione.

456 In tal senso cfr. G. MANCOSU, *op. cit.*, p. 3, che evidenzia l'assonanza tra il modello di *open government* e il paradigma di sussidiarietà e la capacità delle politiche di apertura dei dati di influire direttamente sulle modalità di esercizio della sovranità popolare. Secondo l'Autore alla pubblicazione deve quindi accompagnarsi la "liberazione" dei dati.

457 Cfr. G. MANCOSU, *op. cit.*, p. 15: «si passa da una concezione "proprietaria" del dato pubblico, utilizzato dalla sola pubblica amministrazione per l'assolvimento di compiti istituzionali e per l'(eventuale) elaborazione di "prodotti informativi" predeterminati *ex lege*, ad una concezione *open* del dato, nella consapevolezza che solo attraverso la sua "disseminazione" esso è in grado di sprigionare tutto il proprio potenziale informativo».

amministrazione è chiamata, mostrando una progressiva crescente consapevolezza circa il valore degli *open data*.

Sotto tale profilo, a livello normativo, rileva particolarmente la direttiva 2003/98/CE del 17 novembre 2003, dedicata al riutilizzo dell'informazione del settore pubblico, modificata dalla direttiva 2013/37/UE del 26 giugno 2013[458].

Seppur consapevole del valore delle informazioni pubbliche e del loro riutilizzo per assicurare il diritto alla conoscenza, la direttiva 2003/98/CE sul «*re-use of public sector information*» (cosiddetta direttiva PSI) si limita ad avviare un'armonizzazione delle normative e delle prassi nazionali relative al riutilizzo dei documenti nel settore pubblico, ma senza prescrivere nessun obbligo al riguardo[459]; la direttiva 2013/37/UE modifica e fortifica le previsioni della direttiva 2003/98/CE con l'esplicita e netta previsione di un obbligo di consentire il riutilizzo di tutti i documenti da parte degli Stati, a meno che l'accesso sia limitato o escluso ai sensi delle disposizioni nazionali sull'accesso ai documenti[460]. Quest'ultimo aspetto, che costituiva un possibile ostacolo

---

458 Fin dal 1998 la Commissione europea si interessa al tema con la presentazione del Libro verde sull'informazione del settore pubblico nella società dell'informazione, «*L'informazione del settore pubblico: una risorsa fondamentale per l'Europa*» - COM(1998)585, che richiamava l'esigenza di sinergie tra mondo pubblico e privato nel mercato delle informazioni; il Libro verde ha ispirato la direttiva 2003/98/CE. Per completezza deve essere richiamata, altresì, la direttiva 2007/2/CE del 14 marzo 2007 che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea (INSPIRE), attuata in Italia con il d.lgs. 27 gennaio 2010, n. 32.

459 Il considerando 16 della direttiva 2003/98/CE, prima della riforma del 2013, denota la consapevolezza del valore economico e sociopolitico del riutilizzo e della sua strumentalità per rendere effettivo il diritto a conoscere, a sua volta principio di democrazia: «*Rendere pubblici tutti i documenti generalmente disponibili in possesso del settore pubblico — concernenti non solo il processo politico ma anche quello giudiziario e amministrativo — rappresenta uno strumento fondamentale per ampliare il diritto alla conoscenza, che è principio basilare della democrazia*». Oltre alla mancanza dell'obbligo, il valore della direttiva era ridotto, in quanto l'accesso era subordinato ad apposita istanza e al versamento di un corrispettivo (artt. 4 e 6); cfr. G. MANCOSU, *op. cit.*, p. 5 ss.

460 La direttiva 2013/37/UE è consapevole che le politiche di apertura dei dati svolgono «*un ruolo importante nel dar vita allo sviluppo di nuovi servizi basati su modi innovativi di combinare tali informazioni tra loro e di usarle, nonché stimolare la crescita economica e promuovere l'impegno sociale. Questo però presuppone che le decisioni in merito all'autorizzazione o al divieto di riutilizzo di determinati documenti siano adottate secondo condizioni uniformi a livello unionale, che non possono essere garantite se tali condizioni sono lasciate alle diverse norme e pratiche degli Stati membri o degli*

e un potenziale freno a livello italiano, prima della riforma del d.lgs. 97/2016[461], in una situazione che, accanto alla pubblicità obbligatoria, vedeva una forma di accesso limitata alle condizioni della legge 241/1990, con l'introduzione dell'accesso civico generalizzato e il riconoscimento della *freedom of information* nel Paese, ha cessato di costituire fonte di preoccupazione per l'ordinamento interno.

A livello strategico europeo, la *Digital Agenda for Europe* prevede l'importanza del ruolo dei governi nel mettere a disposizione e consentire il riutilizzo delle informazioni relative al settore pubblico in modo trasparente, efficace e non discriminatorio, per incentivare i mercati e contribuire alla crescita potenziale di servizi online innovativi e più efficaci, assicurando così un miglioramento nella vita dei cittadini. Particolarmente significativa è anche la comunicazione della Commissione europea dedicata agli *open data*, «*Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*», COM(2011) 882 def. del 12 dicembre 2011, finalizzata a valorizzare gli *open data* tra i Paesi europei, in considerazione del grande valore, anche economico, che rivestono: la strategia è composta da una serie di misure dirette

---

enti pubblici interessati» (considerando 3). Significativo al riguardo il considerando 5 della direttiva 2013/37/UE: «*Da quando è stato adottato il primo insieme di norme sul riutilizzo dell'informazione del settore pubblico nel 2003, si è assistito a una crescita esponenziale della quantità di dati nel mondo, compresi i dati pubblici, e alla comparsa e raccolta di nuovi tipi di dati. Parallelamente, si assiste a un'evoluzione costante delle tecnologie per l'analisi, lo sfruttamento e l'elaborazione dei dati. Questa rapida evoluzione tecnologica permette di creare nuovi servizi e nuove applicazioni basate sull'uso, sull'aggregazione o sulla combinazione di dati. Le norme adottate nel 2003 non rispecchiano più questi rapidi mutamenti e di conseguenza si rischia di non poter cogliere le opportunità economiche e sociali offerte dal riutilizzo di dati pubblici*». La direttiva 2013/37/UE è tesa all'armonizzazione delle normative e delle prassi seguite negli Stati membri in relazione allo sfruttamento delle informazioni del settore pubblico, idonea a contribuire all'istituzione di un regime inteso a garantire l'assenza di distorsioni della concorrenza sul mercato interno (considerando 6). La direttiva prevede tariffe limitate ai costi marginali ed estende l'applicazione anche al settore culturale, in particolare alle biblioteche, comprese le biblioteche universitarie, ai musei e agli archivi.

[461] G. MANCOSU, *op. cit.*, p. 22 ss. parla prima della riforma del d.lgs. 97/2016 di «incolmabile distanza tra il regime dell'accesso (ex l. 241/1990) e quello del riutilizzo dei documenti pubblici»: la direttiva europea fa salvo il regime di accesso di ciascuno Stato e questo poteva portare a un cortocircuito tra la disciplina comunitaria sul riutilizzo e quella interna, traducendosi in una attuazione "monca" della direttiva oppure in una piena affermazione della stessa e in uno "svuotamento" del diritto di accesso interno.

allo scopo, quali l'adeguamento del quadro giuridico (che ha portato alla direttiva 2013/37/UE), la previsione di investimenti finanziari dedicati, la realizzazione di un portale europeo e di un portale paneuropeo[462].

A livello nazionale, in attuazione della direttiva 2003/98/CE, già il d.lgs. 36/2006 interpretava i dati pubblici come importante "materia prima" per prodotti e servizi digitali, da riutilizzare per contribuire alla crescita economica e sociale, ma, in coerenza con la direttiva che recepiva, non imponeva l'obbligo di consentire il riutilizzo dei documenti, lasciando al riguardo libere le amministrazioni nella scelta di consentirlo o meno[463]. Il d.lgs. 102/2015 ha dato attuazione alla direttiva 2013/37/UE sugli *open data*, modificando il d.lgs. 36/2006, e ha rafforzato gli obblighi delle istituzioni in materia di dati aperti, prevedendo che le amministrazioni provvedano affinché i documenti siano riutilizzabili a fini commerciali o non commerciali secondo le modalità previste.

Il d.lgs. 36/2006 si rivolge in modo più ampio al riutilizzo dei documenti, quale rappresentazione di atti, fatti o dati giuridicamente rilevanti, a prescindere dal supporto, nella disponibilità della pubblica amministrazione o dell'organismo di diritto

---

462 In materia di *open data* cfr., altresì, la comunicazione della Commissione europea «*Comunicazione della Commissione — Orientamenti sulle licenze standard raccomandate, i dataset e la tariffazione del riutilizzo dei documenti*», 2014/C 240/01, pubblicata nella Gazzetta ufficiale dell'Unione europea il 24 luglio 2014.

463 In conformità alla direttiva europea, il d.lgs. 36/2006 fa salva la disciplina in materia di accesso, oltre a quelle in materia di proprietà intellettuale e industriale. Come nella direttiva, anche nella disciplina italiana è necessaria un'istanza, soggetta a tariffazione (limitata ai soli costi effettivi sostenuti dall'amministrazione in caso di riutilizzo non commerciale). Successivamente al d.lgs. 36/2006, l'art. 47 del c.d. decreto Semplificazioni inserisce la «*promozione del paradigma dei dati aperti (open data)*» fra gli obiettivi per l'attuazione dell'Agenda digitale italiana «*quale modello di valorizzazione del patrimonio informativo pubblico, al fine di creare strumenti e servizi innovativi*» (art. 47, comma 2-bis, lett. b), d.l. 5/2012, convertito con modificazioni dalla legge 35/2012, comma abrogato dal d.lgs. 179/2016). Poi l'art. 18 del d.l. 83/2012, convertito con modificazioni dalla legge 134/2012, rubricato significativamente "Amministrazione aperta" (ora abrogato e confluito nei suoi contenuti nel d.lgs. 33/2013), ha disposto, corredandola di specifiche responsabilità e sanzioni, la pubblicazione in formato aperto di determinate tipologie di informazioni, particolarmente rilevanti; per la prima volta, seppur in modo parziale e non organico, si pone un dovere in capo alla pubblica amministrazione in materia di *open data* e si integrano trasparenza e apertura in una disposizione.

pubblico[464], mentre parla specificamente di riutilizzo dei dati il Codice dell'amministrazione digitale, come scaturente dalle modifiche e integrazioni avute nel corso degli anni che hanno seguito l'evoluzione del principio di trasparenza in senso attivo[465].

Il d.lgs. 82/2005, negli artt. 1, 52 e 53, modificati e integrati dal c.d. decreto Crescita 2.0 (d.l. 179/2012, convertito con modificazioni dalla legge 221/2012), dal d.lgs. 102/2015, dal d.lgs. 179/2016 e dal d.lgs. 217/2017, introduce l'esaminata definizione di *open data* e prevede disposizioni generali con la finalità di razionalizzare il processo di valorizzazione del patrimonio informativo pubblico nazionale.

È interessante rilevare che l'introduzione degli *open data* nel Codice dell'amministrazione digitale avviene nel 2012, quando, contemporaneamente, viene approvata la legge 190/2012 che delega all'adozione del d.lgs. 33/2013: anche a livello normativo la maturazione del concetto di trasparenza avviene nella sua integrazione con l'apertura[466].

L'attenzione verso il binomio trasparenza-apertura e accesso-riutilizzo è centrale, del resto, nella stessa riforma Madia, legge 124/2015, che tra i criteri direttivi pone espressamente l'obiettivo di «*garantire l'accesso e il riuso gratuiti di tutte le informazioni prodotte e detenute dalle amministrazioni pubbliche in formato aperto*»[467]. Nel quadro normativo vigente, quindi, la trasparenza è attiva, si coniuga con il concetto di apertura per esprimere pienamente le proprie potenzialità, permettendo il riutilizzo dei dati e agevolando, così, la conoscenza stessa.

Secondo le disposizioni della normativa che regola oggi i dati aperti, le pubbliche

---

464 Art. 2, comma 1, lett. c), d.lgs. 36/2006; la definizione di documento non comprende i programmi informatici.

465 Cfr. D. SOLDA KUTZMANN, *op. cit.*, secondo cui il documento si pone «quale rappresentazione codificata di un fenomeno osservabile, tale da essere memorizzata ed elaborabile. L'oggetto del riutilizzo è quindi il documento, quale rappresentazione di atti, fatti e dati, benché il riferimento al supporto sia solo strumentale e in relazione al suo ruolo di medium che incorpora il dato» e F. MINAZZI, *op. cit.*, p. 3 ss., secondo cui è configurabile un rapporto tra *genus* (il d.lgs. 36/2006) e *species* (d.lgs. 82/2005), dal momento che il d.lgs. 36/2006 è finalizzato a rendere maggiormente accessibili i documenti rappresentativi di dati e non solo i dati e prescinde, altresì, dal supporto documentale (il d.lgs. 82/2005 tratta dati comunque elettronici).

466 Cfr. V. PAGNANELLI, *op. cit.*, p. 205 ss.

467 Art. 1, comma 1, lett. c), legge 124/2015.

amministrazioni sono tenute a pubblicare, ai sensi dell'art. 9 del d.lgs. 33/2013, il catalogo dei dati e dei metadati, nonché delle relative banche dati in loro possesso e i regolamenti che disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo di tali dati e metadati[468]. Inoltre, nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la formazione, la raccolta e la gestione di dati, i soggetti cui si applica il Codice dell'amministrazione digitale sono tenuti a prevedere clausole idonee a consentirne l'utilizzazione in conformità a quanto previsto dall'articolo 50[469].

Il *favor* verso gli *open data* è evidente nel significativo principio *open data by default*: i dati e i documenti pubblicati dai soggetti cui si applica il Codice dell'amministrazione digitale con qualsiasi modalità, senza l'espressa adozione di una licenza standard per il riutilizzo, si intendono rilasciati come dati di tipo aperto, ad eccezione dei casi in cui la pubblicazione riguardi dati personali (art. 52, comma 2, d.lgs. 82/2005). Di conseguenza, nei casi di applicazione del principio *open data by default* si presuppone l'attribuzione automatica della licenza con la sola clausola di attribuzione della paternità, quale la CC-BY nella versione 4.0, come precisato anche nelle linee guida per l'anno 2017 adottate dall'AgID[470].

L'art. 52 del CAD si preoccupa di assicurare effettività a quanto previsto e, a tal fine, collega espressamente le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni ai parametri di valutazione della performance dirigenziale[471].

Da un punto di vista di *governance*, per la valorizzazione del patrimonio

---

468 Art. 53, comma 1-bis, d.lgs. 82/2005: sono fatti salvi i dati presenti in Anagrafe tributaria.

469 Art. 52, comma 3, d.lgs. 82/2005, come modificato dal d.lgs. 217/2017.

470 Peraltro, a seguito delle modifiche del d.lgs. 217/2017, oggi la definizione di dati di tipo aperto, contenuta nell'art. 1, comma 1, lett. l-ter), d.lgs. 82/2005, prevede esplicitamente che i dati debbano essere resi disponibili, da un punto di vista giuridico, secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato.

471 Art. 52, comma 4, d.lgs. 82/2005. Sull'art. 52 del d.lgs. 82/2005, F. MINAZZI, *op. cit.*, p. 12 ritiene che amministrazioni e utenti ne abbiano sottovalutato la portata, «le prime non intuendo che esso le libera dalla responsabilità e dall'impegno di licenziare appositamente i dati, i secondi non richiedendo in maniera efficace la loro liberazione, nonostante il nuovo ed importante istituto dell'accesso civico».

informativo pubblico, riveste un ruolo significativo a livello nazionale l'Agenzia per l'Italia Digitale, organismo cui sono attribuite funzioni strategiche e tecniche al fine di "traghettare" e accompagnare le amministrazioni italiane verso la digitalizzazione e l'apertura, assicurando la corretta attuazione delle norme[472].

La stessa Dichiarazione dei diritti in Internet prevede che la gestione della Rete debba assicurare non solo i principi di trasparenza e accessibilità alle informazioni pubbliche, ma anche l'accesso e il riutilizzo dei dati generati e detenuti dal settore pubblico: *disclosure* e *openness* sono principi saldamente collegati[473].

Da un punto di vista politico e strategico, il Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, elaborato dall'AgID e approvato dal Presidente del Consiglio dei ministri, ai sensi dell'art. 14-bis, comma 2, lett. b), d.lgs. 82/2005[474], nella sezione dedicata ai dati delle pubbliche amministrazioni, prevede una visione sistemica, in cui il dato è inteso come bene comune, condiviso, di norma, gratuitamente e utilizzabile dalla società civile; a tal fine sono previsti, in relazione agli *open data*, obiettivi, corredati da una serie di azioni, che consistono nella definizione e applicazione di standard, nella previsione di un piano di rilascio, nell'apertura dei dati di forte impatto sulla società e nel monitoraggio costante circa una serie di parametri, quali l'adozione delle linee guida, il raggiungimento degli obiettivi, il soddisfacimento di istanze della società civile, la qualità dei dati e la presenza di API[475].

---

472 Il d.lgs. 217/2017 ha abrogato i commi 5, 6 e 7 dell'art. 52, d.lgs. 82/2005, che prevedevano specifici compiti strategici e tecnici dell'AgID, tenuta a definire e aggiornare annualmente le linee guida nazionali che individuano gli standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati, le procedure e le modalità di attuazione delle disposizioni, con l'obiettivo di rendere il processo omogeneo a livello nazionale, efficiente ed efficace. Dopo la riforma del d.lgs. 82/2005 da parte del d.lgs. 217/2017, il riferimento alle linee guida è contenuto in via generale nell'art. 14-bis, comma 2, lett. a), sul ruolo dell'AgID e, in relazione all'analisi dei dati, in un nuovo comma 2-bis dell'art. 50. Le linee guida per l'anno 2017 sono disponibili al link *www.dati.gov.it/content/linee-guida-nazionali-valorizzazione-patrimonio-informativo-pubblico.* V. PAGNANELLI, *op. cit.*, p. 208: «la normativa italiana non offre molti altri elementi di chiarezza o punti saldi che si pongano come pietre angolari di una struttura organica, razionale e quindi riconoscibile».

473 Art. 14, commi 5 e 6, Dichiarazione dei diritti in Internet.

474 Il piano è disponibile al link *pianotriennale-ict.italia.it*.

475 Le API (*Application Programming Interface*) sono istruzioni standard che permettono a terzi di poter sviluppare *tools* alimentati dai flussi informativi di una piattaforma o di un portale.

In questo percorso normativo si è inserito il d.lgs. 33/2013, da ultimo modificato dal d.lgs. 97/2016[476], che collega trasparenza e apertura negli artt. 3 e 7. Tutti i documenti, le informazioni e i dati oggetto di accesso civico, compresi quelli oggetto di pubblicazione obbligatoria, sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, utilizzarli e riutilizzarli ai sensi dell'art. 7 del d.lgs. 33/2013[477]: secondo la disposizione[478] devono essere pubblicati in formato aperto e devono essere riutilizzabili ai sensi dei d.lgs. 36/2006, d.lgs. 82/2005 e d.lgs. 196/2003, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità[479]. Tali norme costituiscono il fondamento non solo del diritto a conoscere, ma anche del diritto all'apertura e al riutilizzo di documenti, informazioni e dati[480].

Nel delineare la trasparenza "attiva" è significativa la collocazione delle norme dedicate agli *open data*, che non si limita al Codice dell'amministrazione digitale, d.lgs. 82/2005, ma è presente in modo esplicito nella normativa dedicata alla trasparenza, d.lgs. 33/2013, creando così un ponte e un legame tra le diverse anime del diritto alla conoscenza, che è oggi allo stesso tempo *transparent, digital* e *open*[481].

---

476 *Infra*, cap. 2, § 3 e § 4.

477 Art. 3, comma 1, d.lgs. 33/2013.

478 L'art. 7 è significativamente rubricato «*dati aperti e riutilizzo*».

479 Cfr. F. MINAZZI, *op. cit.*, p. 8 ss., secondo cui, nel porre l'inciso «*senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità*», la norma richiama le caratteristiche imprescindibili degli *open data*; di conseguenza il rispetto dell'integrità va inteso come «divieto di effettuare sui dati mutilazioni, mutazioni, manipolazioni o correzioni sleali: ossia volte a "falsificare" l'affidabilità del dato, così come pubblicato dalla PA titolare, ovvero ad indurre in errore i terzi, dichiarando falsamente che il dato modificato faccia fede come l'originale (senza contare le eventuali responsabilità civili, penali od amministrative conseguenti)».

480 Cfr. B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo*, cit., p. 112 ss., che parla di «pretesa giuridicamente protetta di acquisire la disponibilità dei dati di cui fruire e da destinare al riutilizzo», che è soddisfatta, al pari del diritto a conoscere, sia dalla pubblicazione obbligatoria sia dall'esercizio dell'accesso civico.

481 *Contra* V. PAGNANELLI, *op. cit.*, p. 209, secondo la quale la portata innovativa delle norme è ridimensionata dalla collocazione, in quanto «l'articolo 7, che disciplina il riutilizzo dei dati, appare collocato erroneamente all'interno del Decreto Trasparenza, risultando invece concettualmente più vicino al contenuto e alla *ratio* del CAD. L'Open Data italiano appare dunque essere una conseguenza della

Da un punto di vista giuridico l'apertura del patrimonio informativo pubblico deve necessariamente fare i conti con esclusioni e limiti normativamente previsti a tutela di altri interessi protetti dall'ordinamento, quali il segreto di Stato, il segreto statistico, il diritto d'autore, la sicurezza pubblica e la protezione dei dati personali[482]. L'apertura, infatti, non significa condividere automaticamente e rendere disponibile al riutilizzo ogni dato indiscriminatamente, ma solo quelli consentiti dalle norme, rispettando i limiti giuridici a tutela di altri interessi: il rispetto di altri diritti è essenziale anche per ottenere la fiducia della società nell'apertura, elemento necessario per un effettivo *open government*[483].

Da tale punto di vista risulta particolarmente complesso il bilanciamento tra *open data* e protezione dei dati personali[484].

Il profilo è oggetto di norme specifiche nel d.lgs. 33/2013[485] e la difficoltà dell'equilibrio emerge chiaramente anche nelle linee guida del Garante privacy del 2014[486], secondo cui i dati pubblicati online non sono liberamente utilizzabili da chiunque per qualunque finalità e i dati personali sono riutilizzabili solo in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto delle norme sulla *data protection*. In caso di dati personali è necessario rispettare, infatti, i principi che ne informano il trattamento, ossia i principi di necessità, finalità, pertinenza e non eccedenza. Secondo il Garante, di conseguenza, l'obbligo di pubblicare i dati in "formato aperto" non comporta che tali dati siano anche "dati aperti", cioè liberamente

---

trasparenza come lotta alla corruzione e non il frutto di una scelta ponderata del legislatore e rivolta alla "apertura dei dati"».

482 Cfr. C. SAPPA, *op. cit.*, p. 185 ss.: «il riutilizzo è chiaramente subordinato al rispetto di situazioni giuridiche soggettive (possesso, misure tecniche di protezione), di privative di derivazione privatistica (diritti di proprietà, di proprietà intellettuale, ma anche diritti contrattuali) o pubblicistica (diritti generali e speciali sui beni culturali)». D. SOLDA KUTZMANN, *op. cit.*: la circolazione delle informazioni «subisce delle limitazioni nel caso risulti in contrasto con la tutela di interessi ritenuti preminenti».

483 In tal senso anche Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA.

484 In questo paragrafo si troverà solo un accenno alla problematica, che sarà trattata nel capitolo 5 di questo lavoro.

485 In particolare l'art. 7-bis del d.lgs. 33/2013 cerca di tracciare l'equilibrio tra apertura e *data protection*.

486 Provvedimento 15 maggio 2014, n. 243 (in *G.U.* 12 giugno 2014, n. 134), doc. web 3134436.

utilizzabili da chiunque per qualunque scopo, dal momento che non deve essere pregiudicato il livello di tutela con riguardo alla protezione dei dati personali; sono esclusi dal riutilizzo i dati sensibili e giudiziari[487].

3.4. Strategie e iniziative di *openness*

3.4.1. Iniziative a livello internazionale

Al *favor* delle norme l'Italia ha accompagnato specifici impegni a livello internazionale in materia di *open data*: oltre all'esaminata adesione all'*Open Government Partnership* (OGP)[488], nel 2013 ha aderito all'iniziativa del G8 *Open Data Charter* e nel 2015 all'*International Open Data Charter*.

L'*Open Data Charter* ha lo scopo di rendere disponibili online e in formato aperto i dati delle pubbliche amministrazioni nazionali e di favorirne l'utilizzo da parte di cittadini e imprese. A tal fine, sono previsti 5 principi strategici per rendere aperto il patrimonio informativo pubblico: 1) *Open Data by Default*; 2) *Quality and Quantity*; 3) *Usable by All*; 4) *Releasing Data for Improved Governance*; 5) *Releasing Data for Innovation*[489].

La *International Open Data Charter*, finalizzata alla diffusione dell'accesso e del riutilizzo dei dati, è stata sottoscritta nel *summit* dell'OGP e mostra consapevolezza circa la strumentalità degli *open data* per contribuire allo sviluppo della conoscenza in senso ampio e comprensivo sia della crescita economica sia del progresso sociale,

---

487 Art. 7-bis, commi 1, 3 e 4, d.lgs. 33/2013 e provvedimento del Garante n. 243 del 15 maggio 2014, secondo cui le pubbliche amministrazioni devono inserire nella sezione "Amministrazione trasparente" un *alert* con cui informare il pubblico che i dati personali sono riutilizzabili solo in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto delle norme sulla privacy. Al riguardo cfr. E. CARLONI, *Le Linee guida del Garante: protezione dei dati e protezione dell'opacità (commento a provv. Autorità garante protezione dati personali 15 maggio 2014)*, in *Giornale di diritto amministrativo*, fasc. 11, 2014, p. 1113 ss. e sia consentito il rinvio a F. FAINI, *Quale equilibrio fra trasparenza, apertura e privacy nello scenario del d.lgs. 33/2013?*, in *Diritto, Economia e Tecnologie della Privacy*, 2014, pp. 57-103.

488 *Supra*, cap. 1, § 2.

489 Cfr. *www.gov.uk/government/publications/open-data-charter*.

culturale e scientifico[490]. La Carta stabilisce 6 principi: 1) *Open by Default*; 2) *Timely and Comprehensive*; 3) *Accessible and Usable*; 4) *Comparable and Interoperable*; 5) *For Improved Governance and Citizen Engagement*; 6) *For Inclusive Development and Innovation*[491].

Sono molteplici le iniziative relative agli *open data* in diversi Paesi del mondo.

La spinta a "liberare" i dati arriva dagli Stati Uniti, dove nasce il modello di *open government*, si afferma il paradigma degli *open data* e viene realizzato il portale apripista *data.gov*[492]. Nella strategia statunitense la conoscenza pubblica è gestita traendo ispirazione dai modelli di *knowledge management* cosiddetto a *bazar*, tipici degli ambienti di sviluppo di software *open source*[493]. Nella gestione degli *open data* tramite *data.gov* prendono forma i tre pilastri del governo aperto: la trasparenza grazie all'accessibilità e alla riutilizzabilità dei dati, la partecipazione alla gestione degli stessi e la collaborazione tramite l'apertura a commenti, suggerimenti e feedback degli utenti[494]. Gli Stati Uniti dedicano figure specifiche al processo *open data* quali il *Chief Data Officer* e il *Chief Data Scientist*.

A livello di Unione europea, a seguito delle politiche e delle strategie dedicate ai dati aperti, sono stati realizzati il portale *European Union Open Data Portal*, che

---

490 Cfr. B. CAROTTI, *L'amministrazione digitale. Le sfide culturali e politiche del nuovo Codice*, cit., p. 12 ss.

491 Cfr. *opendatacharter.net*.

492 Cfr. *www.data.gov*. Il portale *data.gov* funziona come un *index* che raccoglie link e permette di verificare l'esistenza dei *dataset* di interesse, che poi possono essere utilizzati e scaricati appoggiandosi al sito dell'Agenzia che ha prodotto il *dataset*. In *data.gov* è possibile ricorrere alle API (*application programming interface*). Cfr. V. LUBELLO, *op. cit.*, p. 383 ss.

493 V. LUBELLO, *op. cit.*, p. 371 ss.: «La possibilità che i cittadini, forti di una mutata nozione di comunicazione stato-cittadino, possano applicare la legge di Linus ai "codici" delle proprie democrazie ha scatenato una corsa all'*Open Government* in pressoché tutte le democrazie avanzate». Ogni Agenzia è tenuta a pubblicare su *data.gov*, dotarsi di una pagina web quale *gateway* per adempiere a quanto previsto e a pubblicare un *Open Government Plan*, in cui esplicitare le iniziative per migliorare la trasparenza, la partecipazione e la collaborazione.

494 Cfr. V. LUBELLO, *op. cit.*, p. 383 ss., che rileva l'assenza di sanzioni a carico delle Agenzie inadempienti e l'eterogeneità delle diverse piattaforme delle Agenzie dovuta all'autonomia nello sviluppo delle strategie di *open government*.

riguarda le istituzioni e gli organismi europei[495], e il portale *European Data Portal*, che collega i portali *open data* dei diversi Stati, nazionali, regionali, locali o afferenti a settori specifici[496].

Molti Stati europei hanno avviato strategie in materia di *open data* e, tra questi, anche l'Italia; si pensi al Regno Unito con il portale *data.gov.uk*[497], alla Francia con *data.gouv.fr*, alla Germania con *govdata.de* e alla Spagna con *datos.gob.es*.

In particolare, il Regno Unito ha accompagnato il *Freedom of Information Act*, approvato nel 2000, con l'*Open Data White Paper* pubblicato nel 2012, che pone il paradigma di utilizzo e riutilizzo dei dati aperti per il miglioramento dei servizi e lo sviluppo sociale ed economico[498]. Il governo inglese ha predisposto una licenza, la *Open Government Licence* specifica per le *public sector information*; nella realtà inglese trova ampia implementazione il paradigma dei *linked open data*.

La Francia recepisce la direttiva 2003/98/CE integrando la legge sull'accesso, *loi* n. 78-753 del 17 luglio 1978, mostrando così di optare per un collegamento tra trasparenza e apertura, tra accesso e riutilizzo; la stessa autorità *Commission d'accès aux document administratifs* (CADA) è chiamata a vigilare, accanto al rispetto della libertà di accesso, sull'applicazione della normativa sul riutilizzo delle informazioni pubbliche[499]. Successivamente la legge n. 2015-1179 del 28 dicembre 2015 ha recepito la direttiva 2013/37/UE. Sotto il profilo giuridico la Francia si è dotata di apposita licenza, la *Licence Information Publique* e nel 2014 si è dotata di uno *State Chief Data Officer*[500].

In merito all'apertura dei Paesi nel mondo, l'*Open Knowledge Network* ha predisposto il *Global Open Data Index*, strumento atto a misurare il grado di apertura e la qualità della "liberazione" dei dati pubblici dei diversi Paesi, in base ad una serie di

---

495 Cfr. *data.europa.eu/euodp/en/data*.

496 Cfr. *www.europeandataportal.eu*.

497 Si basa sull'infrastruttura *ckan.org*, soluzione *open source* sviluppata dall'*Open Knowledge Foundation*.

498 V. PAGNANELLI, *op. cit.*, p. 211 ss. sottolinea come, in relazione al recepimento della direttiva 2013/37/UE, a differenza dell'Italia, il Regno Unito si sia avvalso del coinvolgimento e della collaborazione della collettività, tramite consultazione online.

499 Cfr. G. MANCOSU, *op. cit.*, p. 6.

500 La predisposizione di licenze da parte dei governi è finalizzata ad avere licenze comuni e standard.

parametri: la Gran Bretagna risulta seconda, la Francia quarta e l'Italia si ferma al trentaduesimo posto[501].

Le iniziative in materia di *open data*, proprio in considerazione della nuova dimensione partecipativa e collaborativa che realizzano tra il mondo pubblico e privato, non originano solo dai poteri pubblici, ma anche da cittadini, associazioni, imprese. Sotto tale punto di vista sono moltissime le iniziative sia istituzionali sia civiche in ogni parte del mondo, fra le quali esemplificativamente si possono ricordare: "*USAspending.gov*", piattaforma istituzionale americana in cui sono raccolti i dati afferenti alle spese effettuate dalle istituzioni ai diversi livelli di governo, come contratti, finanziamenti, prestiti, stipendi; "*Where does my money go?*", iniziativa civica inglese, che servendosi di *open data* del Governo, fornisce informazioni e analisi sulla spesa pubblica, mostrando come il denaro dei contribuenti viene impiegato dal governo; "*Open Street Map*", progetto che utilizza dati cartografici aperti e genera mappe a contenuto libero; *DBpedia*, iniziativa che crea link verso contenuti aperti generati dagli utenti di Wikipedia, li rappresenta in RDF e li mette a disposizione.

3.4.2. Iniziative a livello nazionale e regionale

L'Italia è particolarmente attiva in materia di *open data*, grazie all'impulso normativo e alle strategie governative, ma anche alla dinamicità delle amministrazioni nazionali e territoriali e all'attivismo civile.

Nel 2011 il Governo italiano ha lanciato il portale nazionale di *open data* (*www.dati.gov.it*), che ospita il catalogo dei dati aperti pubblicati dalle amministrazioni italiane ed è stato aggiornato nel tempo per favorire qualità e uniformità. Nel corso degli anni sono stati realizzati portali tematici di *open data*; tra questi SoldiPubblici (*soldipubblici.gov.it*), OpenExpo (*dati.openexpo2015.it*), OpenDemanio (*dati.agenziademanio.it*), OpenCantieri (*opencantieri.mit.gov.it*), ItaliaSicura (*mappa.italiasicura.gov.it*), OpenCup (*opencup.gov.it*).

Il ruolo rivestito dall'Agenzia per l'Italia Digitale fa sì che ci sia una regia

[501] Cfr. *index.okfn.org*. In particolare risultano per l'Italia problematici gli aspetti relativi alla qualità dell'acqua, alla spesa pubblica, alle coordinate spaziali e ai relativi codici postali e mappe catastali.

nazionale nell'evoluzione e nell'implementazione omogenea delle strategie relative agli *open data* nel Paese.

In materia di dati aperti, le Regioni italiane sono state particolarmente attive nel promuovere strategie di apertura del patrimonio informativo pubblico e, in molti casi, hanno dedicato norme specifiche agli *open data*. Anzi, al riguardo, mentre cresceva la consapevolezza a livello nazionale ed evolveva la relativa normativa, le esperienze regionali si sono poste come "pioniere" del fenomeno e all'avanguardia anche a livello legislativo, basandosi su metodi di partecipazione e collaborazione e riuscendo a ispirare anche l'azione di molte altre amministrazioni locali[502].

La Regione Piemonte è stata la prima nel 2010 a rilasciare le sue informazioni pubbliche in *open data*, a creare un portale dedicato (*www.dati.piemonte.it*) e ad emanare la legge regionale 23 dicembre 2011, n. 24: la Regione ha dettato disposizioni anticipando lo Stato, che ha cominciato a legiferare in materia nel 2012. L'Emilia Romagna segue l'esempio del Piemonte nel 2011 con un proprio portale (*dati.emilia-romagna.it*). Nel corso degli anni successivi, molte altre Regioni hanno seguito l'esempio piemontese, dedicando portali ai dati aperti e approvando norme dedicate, come il Lazio[503], la Provincia autonoma di Trento[504], il Friuli Venezia Giulia[505] e la Toscana[506]; hanno dedicato specifiche strategie agli *open data* anche altre Regioni, come Lombardia[507], Puglia[508], Campania[509], Umbria[510], Marche[511], Veneto[512], Liguria[513], Basilicata[514] e Sardegna[515]. Anche Comuni ed enti locali hanno realizzato

---

502 Cfr. G. MANCOSU, *op. cit.*, p. 19 ss.

503 Portale *dati.lazio.it* e legge regionale 18 giugno 2012, n. 7.

504 Portale *dati.trentino.it* e legge provinciale 27 luglio 2012, n. 16.

505 Portale *www.dati.friuliveneziagiulia.it* e legge regionale 17 aprile 2014, n. 7.

506 Portale *open.toscana.it* (sezione dati) e legge regionale 18 febbraio 2015, n. 19.

507 Portale *www.dati.lombardia.it* e legge regionale 18 aprile 2012, n. 7.

508 Portale *www.dati.puglia.it* e legge regionale 24 luglio 2012, 20.

509 Portale *dati.regione.campania.it* e legge regionale 13 settembre 2013, n. 14.

510 Portale *dati.umbria.it* e legge regionale 29 aprile 2014, n. 9.

511 Portale *goodpa.regione.marche.it* e legge regionale 16 febbraio 2015, n. 3.

512 Portale *dati.veneto.it* e legge regionale 24 febbraio 2015, n. 2.

513 Portale *www.regione.liguria.it/opendata.html.*

514 Portale *dati.regione.basilicata.it*

significative strategie in materia di *open data*, come a titolo di esempio il Comune di Firenze (*opendata.comune.fi.it*) e il Comune di Lecce (*dati.comune.lecce.it*).

L'ecosistema *open data* si nutre dell'apertura ai diversi livelli di governo: il portale nazionale e i portali territoriali, regionali e locali, collaborano per lo scambio di dati per mezzo di API che ne garantiscono l'aggiornamento permanente[516].

A livello regionale le strategie si sono tradotte, come evidenziato, oltre che in portali dedicati, anche in vere e proprie leggi. La Costituzione, infatti, in materia di *e-government* permette un ruolo legislativo delle Regioni, che, salvo il coordinamento informatico dei dati di competenza esclusiva statale, hanno un ampio margine entro cui legiferare[517].

In particolare, in materia di *open data*, viene declinato quel ruolo di guida attribuito dal legislatore nel d.lgs. 82/2005 alle Regioni, che si prevede promuovano sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali[518]. Per questo motivo le leggi e le strategie territoriali, accanto alle caratteristiche degli *open data* sotto il profilo giuridico, tecnico ed economico, si soffermano sugli interventi di carattere organizzativo e attuativo rivolti all'interno e all'esterno delle amministrazioni. Questo dimostra la consapevolezza e la maturità nell'affrontare gli *open data* da parte dei

---

515 Portale *opendata.regione.sardegna.it*. Secondo G. MANCOSU, *op. cit.*, p. 20 l'aspetto più debole delle normative regionali sta nel meccanismo di reclamo, cui viene affidata l'effettività del diritto al riutilizzo. Per l'analisi puntuale delle strategie nazionali e regionali in materia di *open data* sia consentito il rinvio a F. FAINI, *Italian Open Government Strategy in National and Regional Regulation* in A. KÖ - E. FRANCESCONI (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2015*, LNCS 9265, Springer, Cham, 2015, pp. 271-286.

516 Come già chiarito, le API (*application programming interface*) consistono in istruzioni standard che permettono a programmi e servizi di poter interagire ed essere alimentati dai flussi informativi di altre piattaforme. Cfr. Vademecum "O*pen data*. Come rendere aperti i dati delle pubbliche amministrazioni" (2011), curato da Formez PA.

517 Al riguardo il riferimento normativo è costituito dell'art. 117, comma 2, lett. r), della Costituzione italiana, che conferisce alla competenza legislativa esclusiva dello Stato il «*coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale*»; su quanto non rientra in tale coordinamento la potestà legislativa è esclusiva (residuale) delle Regioni, ai sensi dell'art. 117, comma 4, Cost. In tal senso, altresì, art. 14, comma 1, d.lgs. 82/2005.

518 Art. 14, comma 2-bis, d.lgs. 82/2005.

territori, dal momento che le strategie di apertura per essere efficacemente realizzate hanno bisogno di un forte investimento organizzativo, sia per conformare i processi interni e responsabilizzare le strutture e gli uffici, sia per creare una cultura digitale negli utenti e spingerli a svolgere un ruolo propulsivo e a creare un rapporto costante di dialogo con le amministrazioni pubbliche. Ciò è quanto mai importante in considerazione del fatto che cittadini e imprese sono i riutilizzatori dei dati: è determinante comprendere quali dati vorrebbero aperti, esaminare le loro segnalazioni e sollecitazioni e avere conoscenza di ciò che riescono a creare in termini di prodotti e servizi per mezzo dei dati aperti.

Sotto il profilo degli enti locali e degli altri soggetti pubblici del territorio il ruolo delle Regioni risulta fondamentale per stimolare, dare indicazioni e offrire strumenti per avviare strategie di apertura: costituiscono l'ente territoriale intermedio che può efficacemente svolgere questa funzione.

In materia di *open data* e di *open government* le norme nazionali e regionali generano un virtuoso equilibrio, senza confliggere, ma integrandosi e permettendo allo Stato di delineare le regole univoche ed omogenee necessarie a realizzare il coordinamento informatico dei dati previsto dalla Costituzione e alle Regioni di svolgere un ruolo di guida necessario ad una digitalizzazione dell'azione amministrativa coordinata e condivisa tra gli enti locali dei diversi territori.

Anche gli utenti italiani (cittadini, associazioni, *startup* e imprese) si sono dimostrati particolarmente sensibili al tema e hanno realizzato progetti di grande utilità, generando proficue sinergie con le istituzioni, quali, a mero titolo di esempio, "Monithon", piattaforma di monitoraggio civico *bottom-up* dei progetti finanziati dalle politiche di coesione, che si basa sui dati del portale "Open Coesione"[519], "OpenParlamento", iniziativa che, attraverso l'elaborazione dei dati di Camera e Senato, permette di monitorare l'attività politica, le proposte parlamentari e l'iter della produzione normativa[520] e la piattaforma "ConfiscatiBene", progetto partecipativo per la raccolta, l'analisi dei dati e il monitoraggio dei beni confiscati alla criminalità organizzata[521].

---

519 Cfr. *www.monithon.it* e *www.opencoesione.gov.it.*

520 Cfr. *parlamento17.openpolis.it.*

521 Cfr. *www.confiscatibene.it*.

In un quadro di vivace attenzione verso gli *open data*, analizzando le iniziative italiane emergono, però, le criticità costituite dalla differente qualità e dalla mancanza di uniformità, standardizzazione e omogeneità nell'apertura del patrimonio informativo pubblico: non tutti i dati potenzialmente utili sono rilasciati in modo aperto o non lo sono in modo uniforme su tutto il territorio nazionale, a causa di differenze di formato, licenza e metadati, traducendosi in un potenziale danno per chi vi faccia affidamento e riutilizzi i dati anche per finalità commerciali[522]. Questi aspetti critici sono aggravati da una corrispondente scarsa consapevolezza della disponibilità di questi dati e del loro possibile riutilizzo[523].

A tali criticità si accompagna un elemento più generale che consiste nell'erronea equivalenza tra il modello *open government* e lo strumento *open data*, che rischia di appiattire i due concetti senza permettere loro di realizzarsi compiutamente: i due elementi hanno bisogno l'uno dell'altro per dar vita ai pilastri di trasparenza, partecipazione e collaborazione; le strategie relative all'apertura dei dati devono quindi essere integrate dalla partecipazione e dalla collaborazione all'interno del sistema pubblico, ma anche all'esterno da ulteriori meccanismi idonei a coinvolgere la collettività nell'azione amministrativa e nelle scelte decisionali delle istituzioni, creando nuove interazioni tra mondo pubblico e privato[524].

---

522 G. MANCOSU, *op. cit.*, p. 26 ss., in considerazione di tali aspetti auspica la previsione di un'autorità nazionale indipendente, deputata a farsi promotrice e garante dell'effettività della disciplina, affiancata dall'AgID per le questioni di carattere tecnico-informatico. Cfr. E. CARLONI, *I principi del codice della trasparenza (artt. 1, commi 1 e 2, 2, 6)*, cit., p. 53 ss., che intende la qualità anche come standardizzazione e omogeneità, dal momento che permette la confrontabilità e l'integrazione delle basi di dati.

523 Cfr. B. CAROTTI, *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa*, cit., secondo cui «il tema dell'*open data* è ancora un tasto dolente: molto rimane da fare, soprattutto in termini di intellegibilità delle informazioni, nonché di consapevolezza della loro disponibilità»; in tal senso anche D. SOLDA KUTZMANN, *op. cit.*

524 Sulla criticità consistente nella scorciatoia di scambiare gli *open data* con l'*open government* cfr. L. SARTORI, *op. cit.*, p. 774 ss. Secondo B. CAROTTI, *L'amministrazione digitale. Le sfide culturali e politiche del nuovo Codice*, cit., p. 12 ss. i dati messi a disposizione non mancano, ma manca il proficuo uso e il correlato sfruttamento del loro valore aggiunto; a tale aspetto si collega la dispersione delle banche dati, che crea inefficienze, incertezze e duplicazioni. G. RIZZO - F. MORANDO - J.C. DE MARTIN, *op. cit.*, p. 509 ss. segnalano quali questioni aperte il ruolo degli enti certificatori dei dati e l'uso di dizionari e ontologie standard.

Seppur i limiti e le problematiche non siano assenti, gli *open data* costituiscono un tassello fondamentale nella costruzione di amministrazioni aperte e capaci di creare inedite sinergie con il mondo privato. Sono efficaci a questo proposito le parole di Tim Berners-Lee «*data drives a huge amount of what happens in our lives and it happens because somebody takes that data and does something with it*».

Proprio da tale punto di vista, è degno di particolare attenzione un fenomeno che riguarda la conoscenza e si basa sull'utilizzo dei dati: i *big data.*

3.5. *Big Data*: caratteristiche e aspetti tecnici

Nell'ordinamento giuridico europeo e in quello nazionale non sono presenti una definizione normativa e una regolazione esplicita dei *big data*, a differenza degli *open data*, tranne per alcuni aspetti afferenti specificamente ai *big data* pubblici, a seguito dell'introduzione di disposizioni dedicate nel Codice dell'amministrazione digitale, d.lgs. 82/2005, da parte della riforma recata dal d.lgs. 217/2017, oggetto di successiva analisi[525].

Questo non significa che il fenomeno non sia sotto i riflettori mondiali per la sua rilevanza cruciale nell'evoluzione tecnologica e nel progresso umano[526].

Nel Report «*Big Data: Seizing Opportunities, Preserving Values*» pubblicato nel maggio 2014 dall'*Executive Office* del Presidente degli Stati Uniti si precisa che «*most*

---

525 Neanche in letteratura c'è una definizione condivisa del fenomeno. I *big data* sono citati a livello europeo nel reg. (UE) 2015/2003 del 10 novembre 2015 e nel reg. (UE) 2017/1515/UE del 31 agosto 2017, relativi alle statistiche comunitarie sulla società dell'informazione. I *big data* sono menzionati in alcuni interventi normativi nazionali, come l'allegato 1 del d.m. 15 ottobre 2014, *Intervento del Fondo per la crescita sostenibile in favore di grandi progetti di ricerca e sviluppo nel settore delle tecnologie dell'informazione e della comunicazione elettroniche e per l'attuazione dell'Agenda digitale italiana*, e l'allegato 1 del d.m. 1° giugno 2016 dall'oggetto affine e, a livello regionale, nell'art. 1 della legge regionale dell'Umbria n. 9 del 29 aprile 2014 e negli artt. 1, 2 e 7 della legge regionale della Lombardia n. 29 del 23 novembre 2016. A seguito delle modifiche e integrazioni apportate dal d.lgs. 217/2017, rilevano oggi l'art. 50, comma 2-bis, e l'art. 50-ter del d.lgs. 82/2005, oggetto di analisi nel prossimo paragrafo.

526 M. OREFICE, *op. cit.*, p. 702 ss. riporta come anno convenzionale di nascita dei *big data* il 2010, anno di pubblicazione del *paper* di Google cosiddetto *Dremel*, che spiega come compiere ricerche su milioni di *gigabytes* di dati in frazioni di secondo.

definitions [of big data] reflect the growing technological ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data»[527].

L'Europa si è occupata di *big data* in diversi atti[528]; in particolare, nella comunicazione «*Verso una florida economia basata sui dati*» del 2 luglio 2014 con il termine *big data* si fa riferimento a «grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti. La gestione di questi *dataset* ad elevata variabilità e in tempo reale impone il ricorso a nuovi strumenti e metodi, quali ad esempio potenti processori, *software* e algoritmi»[529].

Nelle «*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*», adottate il 23 gennaio 2017 dal Comitato della Convenzione del Consiglio d'Europa per la protezione dei dati (nota anche come "Convenzione 108") si constata l'esistenza di molte definizioni di *big data* che differiscono in base alla specifica disciplina di riferimento, ma che nella maggior parte si concentrano «*on the growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data*» e, di conseguenza, «*usually identifies extremely large data sets that may be analysed computationally to extract inferences about data patterns, trends, and correlations*»[530].

---

527 Negli Stati Uniti, in relazione ai *big data*, è, altresì, particolarmente interessante il «*The Federal big data research and development strategic plan*», pubblicato dall'*Executive Office of the President, National Science and Technology Council* nel maggio 2016.

528 Sui dati si pensi alle Comunicazioni della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014 e «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017. In materia di *big data* sono interessanti e significative le pubblicazioni dell'*Organisation for Economic Co-operation and Development* (OECD), quale in particolare «*Data-Driven Innovation: Big Data for Growth and Well-Being*», OECD Publishing, Paris, 2015.

529 Al riguardo E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, n. 6, 2017, p. 2: «Il valore delle informazioni non è dunque intrinseco ma dato dalla capacità di organizzarle, analizzarle, misurarle e conseguentemente ricavarne fattori e decisioni. Ciò significa che le attività di analisi dei Big Data riposano su due piani: software e algoritmi per l'analisi, da un lato, e l'insieme dei dati raccolti e aggregati, dall'altro».

530 Le *Guidelines* riportano anche la definizione di *big data* dell'*International Telecommunication Union* (recommendation Y.3600 del 2015: *Big data – Cloud computing based requirements and*

Di conseguenza, i *big data* possono essere definiti come enormi volumi di dati detenuti da grandi organizzazioni, come governi e multinazionali, provenienti da diverse fonti e analizzati per mezzo di algoritmi informatici, tecniche di *data mining*[531] e tecnologie specifiche[532].

Dalla definizione del fenomeno emerge, accanto alla grandezza, una caratteristica fondamentale dei *big data*: l'eterogeneità dei dati.

I *big data*, infatti, sono formati dalle eterogenee "tracce digitali" derivanti dalle interazioni in rete: dati forniti su base volontaria nei *social* e nelle svariate piattaforme online (Facebook, Twitter, Google, Amazon), dati "scambiati" a fronte di utilità conseguibili (raccolte punti, tessere fedeltà), dati forniti in modo più o meno consapevole (GPS del telefono, rilevatori biometrici), dati registrati automaticamente (*cookies*) o ricavati da altri dati, dati raccolti dai poteri pubblici, anche talvolta condivisi come *open data*, che si porranno quindi come sottoinsieme dei *big data*[533].

---

capabilities): «*a paradigm for enabling the collection, storage, management, analysis and visualization, potentially under realtime constraints, of extensive datasets with heterogeneous characteristics*». Secondo G. COLANGELO, Big data*, piattaforme e antitrust*, in *Mercato Concorrenza Regole*, fasc. 3, 2016, pp. 425-426 con il termine *big data* si intende «l'ammontare impressionante di informazioni, spesso di carattere personale (*personal data* o *user data*), prodotta da numerose fonti, gestita in modo automatico o semiautomatico tramite processori ed algoritmi (c.d. *machine learning*) e filtrata mediante un processo di estrazione (c.d. *knowledge discovery in database*) che si avvale di appositi software (*data mining* e *text mining* o *knowledge discovery in texts*)».

[531] Con il cosiddetto *data mining* si intende «l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un sapere o di una conoscenza, a partire da grandi quantità di dati (attraverso metodi automatici o semi-automatici), e l'utilizzo scientifico, industriale o operativo di questo sapere»; cfr. R. MORO VISCONTI, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, in *Il Diritto industriale*, fasc. 1, 2016, p. 46. Secondo M.F. DE TULLIO, *La* privacy *e i* big data *verso una dimensione costituzionale collettiva*, in *Politica del diritto*, fasc. 4, 2016, pp. 637 ss. il *data mining* si caratterizza per essere un procedimento decisionale poco trasparente, che serve a scoprire modelli e relazioni tra i dati e dedurre regole che permettono di predire futuri risultati; in alcuni casi è impossibile comprendere logicamente tali decisioni, che non sono interpretabili.

[532] Tale definizione è conforme a quanto espresso anche nella *Opinion* 03/2013 *on purpose limitation*, adottata il 2 aprile 2013 dall'*Article 29 Data Protection Working Party*.

[533] Cfr. S. FARO - N. LETTIERI, Big Data*: una lettura informatico-giuridica*, in L. LOMBARDI VALLAURI (a cura di), *Scritti per Luigi Lombardi Vallauri*, vol. I, Cedam, Padova, 2016, p. 503 ss. Sul fenomeno *big data* cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*

Come le briciole di pane di Pollicino, ognuno di noi lascia tracce dei suoi percorsi digitali, con il medesimo rischio di perdersi del protagonista della fiaba, ma con la significativa differenza che non ci saranno in tal caso uccelli a far sparire le "briciole digitali", che resteranno "incastrate" nei *byte* e saranno raccolte da mani che ne faranno prevedibilmente uso per profilarci, per impiegarle in servizi, anche commerciali, per crearne di nuovi o per migliorare quelli esistenti[534]. Significativo a tale proposito il "*data exhaust*" o i cosiddetti dati residui, ossia la scia digitale di dati sottoprodotto delle azioni e dei comportamenti in rete dei soggetti, che possono essere reimpiegati per altri servizi; è il caso degli errori di digitazione nel motore di ricerca, utilizzati da Google con sistemi di *deep learning* per migliorare il correttore ortografico e quindi impiegati come prezioso vantaggio competitivo[535].

I *big data* sono dislocati ovunque intorno a noi.

Sono *big data* i dati prodotti dall'*Internet of Things* (IoT)[536], ossia dalle "case intelligenti", dai dispositivi indossabili che monitorano la condizione fisica, dalle

---

534 «Le informazioni richieste con dati personali, spesso legate alla possibilità di fruire gratuitamente di *app* (ad es. *antivirus*, prenotazioni *on-line*, etc.), sono raccolte e veicolate su database con finalità commerciali, per poi essere rivendute a utilizzatori terzi (di norma all'insaputa dell'utente e non sempre nel rispetto della protezione dei suoi dati personali, anche sfruttando l'extraterritorialità di molti *server*, che ostacola l'imposizione e osservanza di norme a tutela della *privacy*)»; cfr. R. MORO VISCONTI, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, cit., p. 47. M. OREFICE, *op. cit.*, p. 717 ss. sottolinea che, nel momento in cui sono generati e approdano sulle piattaforme *cloud*, i dati sfuggono dalle mani dei legittimi proprietari per finire in quelle del soggetto che li riceve e che li utilizza direttamente, estraendone il valore, o li dà in licenza a terzi affinché ne estraggano il valore. Sotto tale profilo Google occupa le diverse posizioni, dal momento che raccoglie i dati, mette a disposizione le API per consentire il riutilizzo (di cui beneficerà soprattutto Google) e ne estrae il valore innovativo: i suoi servizi apparentemente gratuiti sono pagati con i dati utili per vendere profili accurati e integrati, cui gli inserzionisti possono rivolgere le pubblicità.

535 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 152 ss.

536 L'espressione è stata coniata da Kevin Ashton nel 1999 in una presentazione presso la Procter & Gamble (al riguardo K. ASHTON, *That "Internet of Things" Thing*, in *RFID Journal*, 22 giugno 2009) e identifica una rete di oggetti dotati di tecnologie di identificazione e sensori, connessi fra loro, in grado di comunicare sia reciprocamente sia verso punti nodali del sistema e, altresì, di essere rintracciabili per nome e in riferimento alla posizione; spesso si parla di IoT anche in relazione al *web semantico*. In relazione all'IoT è significativa la comunicazione della Commissione europea «*L'internet degli oggetti – Un piano d'azione per l'Europa*» - COM(2009) 278 definitivo del 18 giugno 2009: «si tratta di oggetti

automobili autonome e da tutti gli "oggetti" che semplificano la nostra vita e si basano sull'utilizzo di dati[537].

Nelle premesse alla deliberazione del 26 marzo 2015 del Garante per la protezione dei dati personali recante l'avvio della consultazione pubblica sull'Internet delle cose (*Internet of Things*) viene precisato il fenomeno: «L'*Internet of Things* (IoT) fa riferimento ad infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es. RFID, *bluetooth* etc.), sia tramite una rete di comunicazione elettronica. I dispositivi interessati non sono soltanto i tradizionali computer o *smartphone*, ma anche quelli integrati in oggetti di uso quotidiano ("*things*"), come dispositivi indossabili (c.d. *wearable*), di automazione domestica (c.d. domotica) e di georeferenziazione e navigazione assistita; ciò comporta la raccolta e la gestione di dati relativi a comportamenti, abitudini, preferenze e stato di salute degli utenti spesso inconsapevoli, con l'effetto di consentirne l'identificazione, diretta o indiretta, mediante la creazione di profili anche dettagliati».

Al riguardo, in conformità al pensiero di Cardon, si può distinguere tra i sensori che monitorano gli esseri umani stessi e ne registrano le tracce comportamentali,

---

che talora disporranno del proprio indirizzo IP (Internet Protocol), saranno inseriti in sistemi complessi e utilizzeranno sensori per ottenere informazioni dal proprio ambiente (ad esempio, prodotti alimentari che registrano la temperatura in ogni fase della catena dell'approvvigionamento) e/o dispositivi di comando per interagire con lo stesso (ad esempio, valvole dell'aria condizionata che reagiscono alla presenza di persone)». Il piano d'azione individua 14 linee di azione: *governance*; monitoraggio permanente degli aspetti relativi alla vita privata e alla protezione dei dati personali; il "silenzio dei chip"; identificazione dei rischi emergenti; l'Internet degli oggetti quale risorsa fondamentale per l'economia e la società; mandato di normalizzazione; ricerca e sviluppo; partenariato pubblico-privato; innovazione e progetti pilota; sensibilizzazione delle istituzioni; dialogo internazionale; la RFID negli impianti di riciclaggio; misurare l'accettazione; valutazione degli sviluppi.

[537] Si tratta del doc. web n. 3898704. Sul fenomeno IoT, che si collega strettamente ai *big data*, cfr., altresì, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, adottata dall'*Article 29 Data Protection Working Party* il 16 settembre 2014 e la *Mauritius Declaration on the Internet of Things*, adottata il 14 ottobre 2014 nel corso della 36ma Conferenza internazionale delle Autorità di protezione dei dati personali. Su IoT e *big data* cfr. M. SOFFIENTINI, *Il futuro della privacy: dall'Internet of Things ai Big Data*, in *Diritto e Pratica del Lavoro*, n. 13, 2015, p. 809 ss.

misurando le loro attività sportive, i loro spostamenti, i segnali corporei, e i rilevatori inseriti nell'ambiente che misurano il nostro ecosistema, come auto, contatori elettrici, rivelatori di inquinamento[538]. In entrambi i casi l'*Internet of Things* si basa sui *big data*[539].

I *big data* sono, dunque, davvero *everywhere* e si caratterizzano come strumento cruciale delle evoluzioni tecnologiche presenti e future: la stessa intelligenza artificiale si basa su enormi quantità di dati e su algoritmi capaci di risolvere problemi per mezzo di approcci deduttivi che traggono benefici dai dati a disposizione[540].

Dunque, l'estrema varietà di fonti da cui derivano mostra l'estrema eterogeneità dei *big data*: convergono dati strutturati e non strutturati, dati generati dagli utenti, dati personali.

La "grandezza" è sicuramente il termine che caratterizza le diverse dimensioni che costituiscono il fenomeno. In specifico, i *big data* si connotano per peculiari caratteristiche cui è possibile associare l'aggettivo "*big*" e idonee a rendere a loro volta i dati "grandi", così individuabili:

- la varietà: l'esaminata eterogeneità della tipologia e dei formati dei dati,

---

538 Cfr. D. CARDON, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Mondadori Università, Milano, 2016, p. 63 ss., secondo cui il soggetto tende oggi a misurarsi e a perfezionarsi servendosi di questi sensori, mentre «gli oggetti che ci circondano tendono sempre più a schiudere il recinto del loro spazio digitale per infilarsi nelle attività quotidiane» (p. 64).

539 R. MORO VISCONTI, *Internet delle cose, Networks e plusvalore della connettività*, in *Il Diritto industriale*, fasc. 6, 2016, p. 536: «L'Internet delle cose (Internet of Things, IoT) è fondato su una famiglia di tecnologie innovative (*chips*, sensori *wired* e *wireless*, *tags*, codici qr e *barcodes*, identificazioni Rfid a radio frequenza, GPS, etc.), che collegano oggetti (*gadgets*...) - in sé e per sé "inanimati" - in dispositivi *smart* sempre connessi al *web* (come i cellulari), per raccogliere, scambiare e processare dati in tempo reale. L'IoT è l'estensione di *internet* al mondo degli oggetti e dei luoghi fisici […]». L'Autore segnala tra i principali settori interessati da IoT: domotica, robotica, avionica, industria automobilistica, biomedicale, monitoraggio in ambito industriale, sorveglianza, rilevazione di eventi avversi, *smart home*, *smart grid*, *smart metering* e *cyber-security*, *smart city*, etc.

540 L. AGRÒ, *op. cit.*, p. 73: rispetto all'intelligenza umana «l'intelligenza di una macchina, per quanto evoluta, parte da presupposti diversi e si basa su grandi quantità di dati e molteplici algoritmi che concorrono per ottenere un risultato sulla base di questi dati, o per generare nuovi algoritmi pur di raggiungere il risultato richiesto».

provenienti da fonti diverse (strutturate e non strutturate)[541];

- il volume: la capacità di acquisire, memorizzare, accedere ed elaborare enormi quantità di dati[542];
- la velocità: la capacità di acquisizione e analisi in tempo reale o ad "alta velocità". Questa caratteristica ne sottende altre due particolarmente significative: la dinamicità, che connota questi dati, e il tempo, dimensione fondamentale per assicurarne il valore, dal momento che in tempi brevi il dato diventa obsoleto[543].

I *big data* si connotano quindi per "grande" volume, "grande" velocità e "grande" varietà. Ma non solo. Frequentemente vengono considerate caratteristiche anche due aspetti ulteriori che, a parere di chi scrive, sono meno legati agli aspetti necessari e imprescindibili del fenomeno (che ricorrono sempre anche nelle diverse definizioni dello stesso) e sono, invece, maggiormente connessi a circoscriverlo in modo più puntuale e a descriverne effetti derivanti dalle caratteristiche principali e dall'elaborazione dei *big data* stessi: il valore, ossia quanto i *big data* valgono come insieme, dal momento che la somma supera le singole parti, e la veracità, da intendersi come veridicità, ossia la qualità e l'accuratezza dell'analisi[544].

---

541 Cfr. G. D'ACQUISTO - M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, Torino, 2017, p. 5 ss., che sottolineano come la varietà riguardi fonti e formati.

542 Nel caso dei *big data* i volumi sono sull'ordine di *zettabyte* e *yottabyte*, ossia miliardi di *terabyte*, destinati a crescere e ad arrivare nel tempo a numeri sempre più grandi, sull'ordine di *brontobyte* e *gegobyte*. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 47: «Quando parliamo di big data, intendiamo il "big" più in termini relativi – rispetto all'intero set di dati – che in termini assoluti». Tale caratteristica consente di analizzare i fenomeni non più parzialmente per mezzo di campioni, ma globalmente considerando tendenzialmente tutti i dati di riferimento; cfr. G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 5 ss.

543 G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 6 ss.

544 L'eterogeneità rende più complessa la correttezza dei dati, aumentando peraltro l'incertezza degli stessi; secondo G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 7 è necessario che il dato sia accompagnato da un elevato numero di descrittori e attributi, che rendono più facili i collegamenti tra dati e le relative connessioni tra fenomeni.

Da questo insieme di caratteristiche deriva il paradigma, piuttosto consolidato, delle 3, 4 o 5 "V" (a seconda degli aspetti presi in considerazione), su cui si basano i dati: volume, velocità, varietà, valore e veracità[545].

I *big data* si caratterizzano, inoltre, come già evidenziato, per la loro ubiquità, la reperibilità a basso costo (ossia la facilità e l'economicità della loro raccolta), la non esclusività e la intrinseca non-rivalità, caratteristiche tipiche dei dati stessi[546], che sono in genere limitate surrettiziamente dalle concentrazioni di mercato e dai correlati interessi economici. La non-rivalità implica che l'utilizzo dell'uno non esaurisca, non impedisca e non limiti quello degli altri; i *big data* possono essere sottoposti a illimitate elaborazioni contemporanee da parte di soggetti diversi senza usura o perdita di valore dei dati[547]. Queste caratteristiche hanno fatto parlare per i *big data* di *commons*, ossia beni immateriali condivisi, che dovrebbero essere controllati e gestiti dalle comunità di riferimento per tradursi in strumento di democrazia economica[548].

---

545 Sulla grandezza F. DI PORTO, *La rivoluzione* Big Data. *Un'introduzione*, in *Concorrenza e mercato*, 2016, p. 5: «Ciò che è grande atterrisce e affascina l'uomo sin dai tempi del fuoco dei vulcani. […] L'informazione da sempre costituisce il motore dell'economia […]. Ciò che è cresciuto esponenzialmente nell'ultimo decennio è il Volume, la Varietà, la Velocità, la Veracità e, dunque, il Valore economico dell'informazione».

546 G. COLANGELO, *op. cit.*, p. 429 ss. riporta che proprio questo insieme di caratteristiche, secondo parte della dottrina, rende inconsistente un significativo rischio antitrust legato ai *big data* non determinando barriere all'entrata e *foreclosure*, mentre altri contestano le caratteristiche stesse mettendo in rilievo impedimenti legali o contrattuali alla condivisione dei dati, strategie di *lock-in* degli utenti, economie di scala ed effetti di rete diretti e indiretti, che contribuiscono ad erigere barriere all'ingresso e a portare all'affermazione di piattaforme dominanti.

547 F. DI PORTO, *La rivoluzione* Big Data. *Un'introduzione*, cit., p. 8 ss. I riutilizzi potenziali determinano il "valore opzionale" del dato, da poter sfruttare sia con il riutilizzo sia mediante la fusione di *dataset* e l'identificazione della possibilità di estensione; un esempio può essere Street View che acquisisce dati non solo per Google maps, ma anche per scopi diversi e futuri; cfr. M. OREFICE, *op. cit.*, p. 704.

548 Secondo M. OREFICE, *op. cit.*, p. 712 ss. i *big data*, per essere *commons* anche soggettivamente, oltre che oggettivamente, devono essere effettivamente gestiti e riconosciuti dalle comunità di riferimento. Per tale motivo alle comunità andrebbero affidati i diritti di proprietà dei *big data*, ossia i diritti relativi al loro controllo e alla loro gestione. M.F. DE TULLIO, *op. cit.*, p. 641 ss. parla per l'utilizzo dei dati di bene-mezzo che si presta a diversi scopi e, di conseguenza, deriva rango e natura dagli scopi a cui di volta in volta è funzionalizzato, che possono essere libertà economiche come diritti fondamentali e

Per comprendere pienamente la rivoluzione innescata dai *big data* e poterne successivamente valutare gli aspetti giuridici maggiormente problematici è necessario rivolgere l'attenzione più ampiamente all'attuale società degli algoritmi[549].

Proprio grazie agli algoritmi i dati che fanno parte dei *big data* perdono staticità e diventano dinamica materia prima capace di generare valore grazie all'utilizzo insieme ad altri dati: attraverso analisi ed elaborazioni tecniche i dati possono "parlare", essere fonte di innovazione e generare nuovi servizi[550]. «I dati sono per la società dell'informazione quello che era il petrolio per l'economia industriale: la risorsa critica che alimenta le innovazioni su cui fa affidamento la gente»[551].

Il valore deriva dall'uso combinato di enormi volumi di dati per scopi diversi da quelli primari; si conosce, si apprende e comprende dall'analisi e dal riutilizzo costante dei dati. «Il cambiamento di dimensione ha prodotto un cambiamento di stato. Il cambiamento quantitativo ha prodotto un cambiamento qualitativo»[552].

La trasformazione è epocale e deriva dalla convergenza di diversi fattori di cambiamento: la possibilità di analizzare enormi quantità di dati (tendenzialmente tutti quelli disponibili) e non soltanto campioni limitati e ristretti; la possibilità di rinunciare a un po' di esattezza e accettare un po' di confusione a livello micro, che viene recuperata nella conoscenza e comprensione a livello macro[553]; la possibilità di smettere

---

l'esercizio della sovranità popolare: «la disciplina dello strumento è assorbita da quella del fine cui è rivolto, perché solo la disponibilità del primo permette di godere in modo effettivo del secondo» (p. 642).

549 L'algoritmo è un procedimento di calcolo, in specifico una serie di istruzioni che permettono di risolvere un problema e ottenere un risultato.

550 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 9 ss.

551 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 246.

552 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 15.

553 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 47 ss., secondo i quali l'incremento dei volumi apre la porta all'inesattezza: mentre in un mondo di *small data* misurare e ridurre gli errori erano impulsi connaturali al contesto di riferimento, in un mondo di *big data* si accettano imprecisione e confusione, capaci peraltro di apportare anche benefici qualitativi, che si annidano nella probabilità più che nella precisione. Il quantitativo enorme dei dati compensa questo profilo di congenita inesattezza e conseguente confusione, che non sono propriamente caratteristiche intrinseche dei *big data*, ma degli strumenti utilizzati per analizzare i dati. Esempio di tale aspetto sono le traduzioni di Google, migliorate con l'aumento dei dati e con la tolleranza della confusione. Precisa M. OREFICE, *op. cit.*, p. 707 che la confusione può derivare da errori nella misurazione oppure dall'incongruenza della formattazione del

di chiedersi *il perché* cercando affannosamente la causalità nei fenomeni, ma accertare soltanto *il cosa*, prendendo atto di semplici correlazioni e senza bisogno di conoscere le cause sottostanti[554]. Le correlazioni sono rapide, prescindono da ipotesi preventive e permettono di indicare la direzione per successive indagini causali: di conseguenza si inverte il rapporto e si parte dalle conseguenze per risalire alla valutazione delle probabili cause[555]. Muta, allo stesso tempo, il modo di pensare umano abituato all'esattezza, alla precisione e alla ricerca dei *perché* di tutto ciò che accade, soppiantato da un modello che si trova ad agio con incertezza e disordine e si accontenta del *cosa* accade[556].

Le decisioni sono state prese storicamente su informazioni limitate, esatte e causali, servendosi spesso di campionamenti[557]: questo aspetto muta drasticamente nel mondo dei *big data*, dove la decisione è assunta dalle elaborazioni dei dati basate non su nessi causali, ma su preziose correlazioni, che permettono analisi più profonde e previsioni migliori e portano ad accettare una dose di confusione e imprecisione, a fronte di grandi e inattesi risultati conseguibili[558].

---

dato o dalla combinazione di dati da diverse fonti; in ogni caso «*dataset* più numerosi offrono un valore così alto che la quantità compensa abbondantemente la confusione».

554 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 15 ss. e D. CARDON, *op. cit.*, p. 41 ss.: «Questa maniera invertita di fabbricare il sociale testimonia il rovesciamento della causalità operato dal calcolo statistico per far fronte all'individualizzazione delle nostre società e alla sempre maggiore indeterminazione di ciò che determina le nostre azioni» (p. 44).

555 D. CARDON, *op. cit.*, p. 31 ss.; M. OREFICE, *op. cit.*, p. 707: «le correlazioni possono favorire la ricerca della relazione causale, indicando la direzione da seguire in futuro. Per cui una ricerca *funditus* della relazione causale (analisi del perché) potrà avvenire solo dopo che i *Big Data* ci avranno rivelato il fenomeno».

556 Al riguardo R. MORO VISCONTI, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, cit., p. 52: «La correlazione è in realtà una condizione necessaria ma non sufficiente e l'interpretazione interdisciplinare della causalità (sotto il profilo scientifico-tecnologico, sociologico, economico, giuridico, etc.) rappresenta un imprescindibile passaggio per un utilizzo consapevole dei dati».

557 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 42: «Il campionamento è il prodotto di un'era caratterizzata da forti vincoli alla processazione delle informazioni, in cui le persone misuravano il mondo ma non avevano gli strumenti per analizzare i dati raccolti».

558 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 92: «Così come il campionamento era una scorciatoia che usavamo perché non eravamo in grado di processare i dati, la percezione della causalità è

In questa evoluzione emerge anche una caratteristica della società contemporanea, che consiste nella rivendicazione della singolarità e nella conseguente difficoltà di utilizzare classificazioni statistiche per rappresentare individui che rifuggono le tradizionali categorizzazioni aprioristiche e tendono sempre più ad autorappresentarsi[559].

Alla luce di tali considerazioni, ruolo da protagonista in tale configurazione è detenuto dagli algoritmi, che strutturano e organizzano le informazioni, automatizzano processi che abitualmente erano controllati dagli uomini e danno supporto agli uomini stessi nelle decisioni[560]; «gli algoritmi codificano il mondo, lo classificano e predicono il nostro futuro»[561] e, nelle selezioni che operano, finiscono progressivamente per gerarchizzare i valori e dare forma all'ossatura cognitiva e culturale della società[562].

Si delinea un futuro, in cui cambia il modo di interpretare il mondo, guidato dai dati e dalla loro analisi[563], che si basa sulla "datizzazione" della realtà, ossia sulla conversione in dati dei fenomeni, al fine di analizzarli[564]: sotto tale profilo una spinta

---

una scorciatoia che utilizza il cervello per evitare un ragionamento lungo e faticoso»; peraltro gli Autori sottolineano come la causalità non si possa provare quasi mai, ma solo dimostrare con alta probabilità.

559 D. CARDON, *op. cit.*, p. 31 ss.: «Mentre il web ha aperto a tutti il diritto di prendere la parola in pubblico, il monopolio esercitato dai rappresentanti sulla descrizione della società è stato minato e, con esso, le categorie che le servivano a far parlare gli altri. Lo spazio pubblico digitale ha liberato le soggettività, permettendo agli individui di autorappresentarsi» (p. 38).

560 M. OREFICE, *op. cit.*, cit., p. 703: «Il valore dei dati è generato dal calcolo automatizzato, basato su logiche algoritmiche, per cui senza *software* che siano in grado di estrapolare, gestire e processare le informazioni che racchiudono i dati, entro un tempo ragionevole, il loro valore sarebbe nullo».

561 D. CARDON, *op. cit.*, p. 5.

562 D. CARDON, *op. cit.*, p. 5 ss.: «I calcolatori fabbricano la nostra realtà, la organizzano e la orientano» (p. 7).

563 In tale evoluzione, diversamente da ciò che può sembrare, non sono soppiantate teorie e saperi, dal momento che i dati si basano su fondamenti teorici e sono analizzati applicando teorie; V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 99 ss.

564 La "datizzazione" si riferisce al processo di conversione dei fenomeni in dati, ossia in forme analizzabili di informazione. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 130: «La datizzazione consiste nel convertire in forma analizzabile non solo atteggiamenti e sentimenti, ma anche il comportamento umano, assai difficile da rilevare in altri modi, specie nel contesto della comunità sociale e dei sottogruppi che esistono al suo interno»; Google, Facebook, Twitter, LinkedIn «siedono letteralmente su una montagna di informazioni datizzate che, una volta analizzate, faranno luce sulle

cruciale è arrivata dalla digitalizzazione e dall'*Internet of Things*, che a sua volta permette di datizzare tutto ciò che ci circonda, inserendo sensori e chip negli oggetti della nostra vita. La datizzazione è capace di arricchire la comprensione umana[565].

Nei *big data* si sostanzia la promessa della società dell'informazione e della conoscenza, che mette al centro in modo pervasivo e ubiquo i dati[566]. In questi mutamenti il potere si sposta, dal momento che processare vastissime quantità di dati non è più appannaggio solo dei poteri pubblici, ma anche dei soggetti privati, è una possibilità che si diffonde nelle grandi aziende.

In queste evoluzioni che riguardano i dati, ma investono il modo di pensare, misurare, vivere e relazionarsi al nostro mondo, i *big data* permettono «una percezione più completa della realtà», configurandosi come «l'equivalente di un dipinto impressionista in cui ogni pennellata è imprecisa se lo guardiamo da vicino, ma l'immagine complessiva diventa meravigliosamente dinamica se ci allontaniamo un po'»[567].

L'affidamento esteso ai dati e a quel che riescono a dire rischia, però, al tempo stesso di contrarre le caratteristiche umane di intuito, ingegno e creatività, potendo incidere in vario modo anche sullo stesso progresso; si tratta di uno strumento che a

---

dinamiche sociali a tutti i livelli, dall'individuo alla società nel suo complesso». Cfr. M. OREFICE, *op. cit.*, p. 702 ss., che sottolinea come i *big data* abbiano reso «gli esseri umani misurabili e controllabili» (p. 702): «tutto può essere convertito in dati, cioè in forme analizzabili di informazioni: da semplici atteggiamenti e sentimenti all'intero agire umano» (p. 703).

565 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 103 ss.: «la digitalizzazione mette le ali alla datizzazione. Ma non la sostituisce. La mera digitalizzazione – ossia la conversione di informazioni digitali in un formato leggibile – di per sé non datizza» (p. 115). Il mutamento è tale che saranno trasformati interi settori intorno ai *big data* (come i servizi finanziari e le industrie farmaceutiche) e si affermeranno nuove figure professionali strategiche, come i *data scientist*, esperti di analisi di dati, che «vedono ciò che è possibile anziché farsi limitare da ciò che ritengono fattibile» (p. 175). R. MORO VISCONTI, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, cit., p. 46: il *data scientist* è «colui che analizza i dati per fornire informazioni utili al *management*, al fine del *decision making* e delle strategie da intraprendere».

566 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 257 ss.

567 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, pp. 71-72. In merito alle tecnologie, secondo D. CARDON, *op. cit.*, p. 1 «sarebbe ingenuo credere che non abbiano trasformato profondamente ciò che siamo, ciò che sappiamo, le nostre maniere di pensare e le rappresentazioni che abbiamo di noi stessi».

seconda del suo utilizzo può aumentare la conoscenza come portare a fraintendimenti, aumentare le possibilità dell'uomo o appiattirne le potenzialità, rendendoci meno "umani".

L'Europa è consapevole che è in atto «una nuova rivoluzione industriale trainata dai dati digitali, dall'informatica e dall'automazione. Le attività umane, i processi industriali e la ricerca generano un livello senza precedenti di raccolta ed elaborazione di dati, le quali favoriscono la comparsa di nuovi prodotti, servizi, processi commerciali e metodologie scientifiche»[568].

Sotto tali profili emerge una caratteristica di affinità con gli *open data*: *open data* e *big data* esprimono il loro valore nella dinamicità e nel riutilizzo; il valore non diminuisce, ma aumenta con il riutilizzo in modi diversi dall'uso originario. In questo profilo emerge il nuovo volto contemporaneo dei dati, un volto attivo, seppur con una decisiva differenza: nel caso dei dati aperti chiunque può utilizzarli, mentre questo non è detto avvenga con i *big data*. E proprio in questo aspetto si disvelano valore e rischi dei "grandi" dati.

3.6. Finalità e valore dei *big data*

Sono "grandi", eterogenei e molteplici non solo i dati, frutto in larga parte delle nostre attività nella realtà digitale, ma anche gli obiettivi che i *big data* contribuiscono a raggiungere, causa della significativa attenzione rivolta al fenomeno.

I *big data* possiedono, infatti, un enorme valore economico[569], che emerge già dalle loro caratteristiche e dai molteplici utilizzi cui possono essere destinati[570].

---

568 Comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014.

569 Cfr. M. BOGNI - A. DEFANT, *Big data: diritti IP e problemi della privacy*, in *Il Diritto industriale*, fasc. 2, 2015, pp. 117-126.

570 Secondo R. MORO VISCONTI, *Valutazione dei* Big data *e impatto su innovazione e* digital branding, cit., p. 47 ss. le opportunità dell'analisi dei *big data* sono «molteplici e variano dall'aumento della produttività, alla riduzione dei costi, dal miglioramento della comunicazione con i consumatori, alla maggiore accuratezza delle previsioni».

Al riguardo, come emerge anche dagli aspetti che connotano il fenomeno, è necessario premettere che, nelle strategie relative ai *big data*, non è necessariamente predefinito a priori l'oggetto di indagine e non sono prevedibili al momento della raccolta dei dati le molteplici finalità raggiungibili, dal momento che le analisi e le elaborazioni sui *big data* sono capaci di condurre a interessanti risultati inattesi[571]. «Un'indagine effettuata sui *big data* assomiglia un po' a una battuta di pesca: all'inizio non si sa se si prenderà qualcosa, e tantomeno *che cosa*»[572]; le domande da porre per lo più non sono note *ex ante*, ma emergono nella raccolta e nell'analisi dei dati. In un certo senso, l'elaborazione dei *big data* fornisce risposte a domande che non abbiamo ancora posto o che non sapevamo di dover porre; l'approccio non si basa più su ipotesi, ma su dati e in tal modo è meno condizionato anche dai pregiudizi, dalle convinzioni e dalle intuizioni umane che possono essere fallaci[573]. Questo aspetto, come si vedrà, è particolarmente critico quando i dati sono personali e si configura l'applicazione della relativa normativa.

Una prima e intuitiva finalità si colloca nell'informazione aggiuntiva che i *big data* permettono di generare e nella conseguente conoscenza che consentono. In collegamento a tale aspetto, i *big data* permettono di interpretare bisogni ed esigenze, profilare gli utenti, monitorare consumi e *performance*, ottimizzare la produzione, agevolare la pianificazione strategica, supportare istituzioni e aziende nelle scelte e nelle decisioni.

Tale conoscenza ulteriore, laddove i *big data* siano opportunamente analizzati con strumenti appropriati, può assumere anche il volto di una vera e propria capacità predittiva, che si traduce nella possibilità di effettuare previsioni politiche, predizioni

---

571 Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2012, pp. 135-144 e G. SARTOR - M. VIOLA DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/EU*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 657-680.

572 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 46.

573 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 73 ss.: «Nel mondo degli *small data*, sia le indagini sul rapporto di causalità sia le analisi di correlazione partivano da un'ipotesi, che veniva poi messa alla prova per essere confermata o confutata» (p. 88); in tal modo erano soggette a pregiudizi e intuizioni fuorvianti. Oltre a ciò, prima dei *big data*, ci si limitava a cercare relazioni lineari.

sugli andamenti di mercato[574] e sulle problematiche relative agli ambiti presi come oggetto di osservazione. La capacità di previsione è insita nell'esaminata caratteristica dei *big data*, che consiste nel loro fondarsi su correlazioni e non su causalità: se una correlazione è elevata è alta la probabilità di un collegamento e ciò permette non solo di comprendere il presente, ma di fare previsioni sul futuro[575]. Questo aspetto, che trova fondamento nel desiderio costante dell'uomo di riuscire a conoscere il futuro, riveste una notevole rilevanza sociopolitica, costituendo un significativo potenziale supporto alle decisioni dei poteri pubblici e traducendosi in un grande vantaggio competitivo per le imprese[576].

A questo proposito, un caso interessante è stato fornito nel 2009 da *Google Flu Trends*, che ha pubblicato uno studio sulla rivista scientifica *Nature* nel quale dimostrava di poter prevedere la diffusione del virus influenzale H1N1 negli Stati Uniti, basandosi sull'analisi di *big data*, in particolare sulle *queries* degli utenti: il sistema previsionale di Google si è dimostrato più efficace delle statistiche governative e ha fornito preziose indicazioni alle autorità sanitarie[577]. Ha valorizzato le possibilità di previsione del futuro dei *big data* anche la ricerca che, per mezzo di tecniche di *machine learning* (apprendimento automatico dai dati), ha definito un modello per la predizione delle decisioni della Corte Suprema degli Stati Uniti: basandosi solo su dati disponibili prima della data della decisione è stato capace di prevedere correttamente più del 70%

---

574 D. DE PASQUALE, *La linea sottile tra manipolazione della rete e pubblicità*, in *Il Diritto industriale*, fasc. 6, 2012, p. 552 ss. porta l'esempio delle tecniche predittive utilizzate da Amazon per intuire i gusti degli utenti e prevedere il comportamento dei consumatori. Secondo D. CARDON, *op. cit.*, p. 58 gli algoritmi sono predittivi «perché si basano costantemente sull'ipotesi che il nostro futuro sarà una riproduzione del nostro passato».

575 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 73 ss., i quali avvertono anche che la crescita esponenziale dei dati fa emergere anche più correlazioni false, interconnessioni apparenti fra fenomeni. «Le vecchie certezze vengono messe in discussione. I big data ci obbligano a riesaminare da zero la natura del processo decisionale, del destino e della giustizia. Una visione del mondo che si fondava sulla ricerca delle cause viene messa in dubbio dalla preponderanza delle correlazioni. Il sapere, che un tempo si identificava con la conoscenza del passato, viene a identificarsi con la capacità di prevedere il futuro» (p. 257).

576 Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., pp. 138-139 e D. DE PASQUALE, *op. cit.*, p. 552 ss.

577 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 9 ss.

dei voti dei singoli giudici[578]. O, ancora, degno di attenzione è il caso della catena discount americana Target che, basandosi su correlazioni di dati personali e dati relativi agli acquisti, è riuscita a stimare in modo piuttosto attendibile lo stato di gravidanza delle clienti e, di conseguenza, ha potuto inviare buoni sconto su misura[579].

L'analitica previsionale dei *big data* può dare significative indicazioni sull'usura di strumenti e infrastrutture, come macchine e ponti, può prevenire disastri, migliorare le diagnosi e le relative cure, può rendere più *smart* e vivibili le città (es. gestione del traffico e dell'inquinamento), fino ad essere usata in politica per le scelte, le decisioni e le elezioni (il caso di Obama e poi di Trump, che si sono affermati anche grazie ai *big data*)[580].

A vedere bene gli esempi di "predizione" sono quotidiani: quando Amazon consiglia il libro che davvero vorremmo o la ricerca su Google seleziona il sito che cercavamo, i *big data* hanno centrato il loro obiettivo e con loro, ancor più, le aziende private che se ne servono.

Già questi pochi esempi mostrano i molteplici impieghi dei *big data* e come le analisi e le predizioni possano rispondere parimenti sia ad esigenze di tutela di interessi generali, sia alla realizzazione di vantaggi economici per i soggetti privati[581]. Di conseguenza, l'analisi degli obiettivi cui sono diretti fa emergere quanto le finalità dei *big data* siano appetibili sia per il mondo pubblico che per il mondo privato; i *big data* hanno valore in entrambi i contesti, con differenze significative dovute al diverso ruolo svolto da tali soggetti nella società.

Le amministrazioni pubbliche hanno nella propria disponibilità enormi volumi di dati e relative banche dati, strumentali all'esercizio dei propri compiti. In specifico, i *big data* possono essere usati per svariate funzioni e scopi che caratterizzano l'*agere* pubblico: funzioni di controllo, come la rilevazione di irregolarità amministrative, ad esempio quelle fiscali; funzioni di regolazione, che rendono i *big data* utili per conoscere i fenomeni, monitorarli e valutare l'impatto di eventuali scelte;

---

578 Il caso è analizzato in D.M. KATZ - M.J. BOMMARITO - J. BLACKMAN, *Predicting the Behavior of the Supreme Court of the United States: A General Approach*, 2014 - *ssrn.com/abstract=2463244*. Al riguardo, cfr. S. FARO - N. LETTIERI, *op. cit.*, p. 516.

579 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 73 ss.

580 M. OREFICE, *op. cit.*, p. 706 ss.

581 M. OREFICE, *op. cit.*, p. 706 ss.

miglioramento dell'efficienza e dell'efficacia dei servizi pubblici, come esemplificativamente rendere *smart* i territori[582]. L'elaborazione di *big data* in ambito pubblico incide fortemente sull'attività conoscitiva delle amministrazioni, permettendo di "oggettivarla", di rafforzare la capacità istruttoria e, di conseguenza, verosimilmente quella decisoria; un altro effetto significativo più ampio consiste nel poter raggiungere una conoscenza autonoma e adeguata dei fenomeni, potendo così evitare di dipendere da organismi tecnici o da soggetti privati. Più profondamente i *big data* sono capaci di mutare l'approccio delle amministrazioni verso i dati e la loro organizzazione, finendo per evolvere la dinamica dell'agire pubblico.

Da tale punto di vista, l'utilizzo dei *big data* in ambito pubblico deve essere attentamente valutato e deve fare i conti con gli elementi di incertezza e con la natura inferenziale e probabilistica delle elaborazioni basate sui *big data*, profili ancora più problematici nel contesto pubblico che ontologicamente deve garantire certezza del diritto e dell'attività amministrativa espletata nello svolgimento delle pubbliche funzioni, oltre ad assicurare la trasparenza delle fasi del procedimento e la qualità dei dati pubblici. La logica dei *big data*, attenta alla quantità e alle correlazioni, rischia di mettere in crisi la disciplina sulla qualità dei dati pubblici, necessaria per garantire certezza e assicurare affidabilità e fiducia[583]. In considerazione di tali aspetti, le istituzioni devono valutare se lo strumento dei *big data* conduca a una verità oggettiva e materiale, che rafforza la certezza dell'agire pubblico e rende le decisioni prese ottimali, o rischi di incrinarla in modo preoccupante[584].

Sicuramente i soggetti pubblici, in quanto retti dal principio di legalità amministrativa, devono attenersi scrupolosamente alla normativa in materia di dati, che risulta composta da un insieme di norme afferenti all'amministrazione digitale e alla normativa sulla trasparenza, alle quali si sommano le disposizioni da osservare a tutela

---

582 Cfr. M. FALCONE, *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista Trimestrale di Diritto Pubblico*, fasc. 3, 2017, pp. 601-639.

583 Cfr. M. FALCONE, *op. cit.*, p. 601 ss.

584 Cfr. M. FALCONE, *op. cit.*, p. 601 ss., che peraltro rileva come il principio di verità materiale incontra limiti in altri principi del procedimento amministrativo, come il principio di economicità e non aggravamento e negli istituti di semplificazione o di certificazione. In proposito, l'Autore rileva come le amministrazioni abbiano ancora difficoltà a raccogliere e conservare i dati e utilizzarli in modo organizzato.

dei diritti, in particolare in materia di proprietà intellettuale e di protezione dei dati personali; in larga parte tali norme sono esaminate in capitoli e paragrafi precedenti del presente lavoro, dedicati alla trasparenza e agli *open data*, e in capitoli successivi, dedicati ai diritti nell'era digitale[585].

Proprio l'apertura dei dati può permettere di utilizzare in modo conforme alla normativa il patrimonio dei *big data* pubblici riducendo il rischio di incorrere nelle problematiche e nei pericoli congeniti allo strumento[586].

Il legislatore, sotto tale profilo, infatti, mostra grande interesse per la razionalizzazione delle basi di dati e la valorizzazione del patrimonio informativo pubblico, al fine di agevolare un proficuo utilizzo da parte dei poteri pubblici, ma altresì da parte della collettività con il riutilizzo[587]. In tale direzione vanno lette le disposizioni introdotte dal d.lgs. 217/2017, che ha modificato il Codice dell'amministrazione digitale, prendendo esplicitamente in considerazione il fenomeno dei *big data* pubblici; in particolare rilevano l'articolo 50, comma 2-bis, e l'articolo 50-ter del d.lgs. 82/2005.

Ai sensi dell'art. 50, comma 2-bis, d.lgs. 82/2005, le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti cui si applica il Codice, fermi restando i limiti previsti dalla normativa, e sono tenute a svolgere tale attività secondo le modalità individuate dall'Agenzia per l'Italia Digitale con le linee guida. Nella disposizione emerge l'aspetto precedentemente messo in evidenza, ossia la necessità in ambito pubblico della finalizzazione dell'analisi dei *big data* alle funzioni istituzionali che caratterizzano l'azione pubblica; i *big data* si pongono come strumento utile a raggiungere gli obiettivi e a svolgere le funzioni istituzionali, in modo più efficace.

In tal senso e a tale scopo particolarmente significativa è la Piattaforma Digitale Nazionale Dati (PDND) o *Data & Analytics Framework* (DAF), prevista dall'art. 50-ter del d.lgs. 82/2005, introdotto dal d.lgs. 217/2017, e già precedentemente individuata

---

585 *Supra*, cap. 2 e i primi paragrafi di questo capitolo; *infra*, cap. 4, § 4, e cap. 5.

586 Su tale aspetto, più ampiamente, *infra*, cap. 6, § 2.2.

587 Il Piano triennale per l'informatica nella pubblica amministrazione 2017-2019, nel richiamare le basi di dati di interesse nazionale, di cui all'art. 60 del d.lgs. 82/2005, parla espressamente dell'utilizzo di metodologie *big data*.

quale progetto strategico della trasformazione digitale del Paese dal Piano triennale per l'informatica nella pubblica amministrazione 2017-2019.

In specifico, la Presidenza del Consiglio dei ministri è tenuta a promuovere la progettazione, lo sviluppo e la sperimentazione di una Piattaforma Digitale Nazionale Dati finalizzata a favorire la conoscenza e l'utilizzo del patrimonio informativo detenuto, per finalità istituzionali, dalle pubbliche amministrazioni[588], nonché la condivisione dei dati tra i soggetti che hanno diritto ad accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese, in conformità alla disciplina vigente[589].

In sede di prima applicazione, la sperimentazione della Piattaforma Digitale Nazionale Dati viene affidata al Commissario straordinario per l'attuazione dell'Agenda digitale non oltre il 31 dicembre 2018[590], che, a tali fini, provvede, nel rispetto dei limiti, delle condizioni e delle modalità stabilite dal Garante per la protezione dei dati personali e dal decreto previsto dalla norma, ad acquisire i dati detenuti dalle pubbliche amministrazioni, organizzarli e conservarli, nel rispetto delle norme tecniche e delle metodologie idonee a garantire la condivisione dei dati tra le pubbliche amministrazioni stabilite dall'Agenzia per l'Italia Digitale nelle linee guida[591].

Accanto al ruolo svolto dal Commissario, la normativa prevede in modo speculare un obbligo in capo ai soggetti detentori dei dati, identificati nel decreto previsto, che devono riscontrare la richiesta del Commissario, rendendo disponibili i dati richiesti senza nuovi o maggiori oneri per la finanza pubblica[592].

La normativa affida a un decreto del Presidente del Consiglio dei ministri, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e le Amministrazioni titolari dei dati, di stabilire le modalità di attuazione della disposizione, al fine di favorire la condivisione dei dati fra le pubbliche amministrazioni, di semplificare l'accesso ai dati stessi da parte dei

---

588 La disposizione fa riferimento ai soggetti di cui all'art. 2, comma 2, lett a), escludendo esplicitamente le autorità amministrative indipendenti di garanzia, vigilanza e regolazione, ivi previste accanto alle pubbliche amministrazioni.

589 Art. 50-ter, comma 1, d.lgs. 82/2005.

590 Art. 50-ter, comma 2, d.lgs. 82/2005.

591 Art. 50-ter, comma 3, d.lgs. 82/2005.

592 Art. 50-ter, comma 3, d.lgs. 82/2005.

soggetti che hanno diritto ad accedervi e di semplificare gli adempimenti e gli oneri amministrativi per i cittadini e le imprese; al d.p.c.m. previsto spetta, altresì, identificare l'elenco dei dati che le pubbliche amministrazioni sono tenute a rendere disponibili per le finalità previste dalla norma[593] e stabilire i limiti e le modalità di acquisizione, organizzazione e conservazione dei dati. La disposizione ribadisce, in coerenza con la normativa di riferimento e l'art. 50, comma 3-bis, che il trasferimento dei dati nella Piattaforma non modifica la titolarità del dato.

Il *Data & Analytics Framework*, precipuamente finalizzato alla conoscenza e all'utilizzo dei dati detenuti dalle amministrazioni, si pone come strumento strategico al fine di valorizzare il patrimonio informativo pubblico, autentica miniera di conoscenza, impiegando i *big data* pubblici attraverso analisi ed estrazione di soluzioni orientate a realizzare in modo più efficiente ed efficace le finalità istituzionali. Al raggiungimento di tale obiettivo, a sua volta finalizzato a soddisfare in modo migliore le esigenze di cittadini e imprese, la disposizione affianca esplicitamente la condivisione dei dati e l'accesso agli stessi da parte dei soggetti che ne hanno diritto e la correlata semplificazione degli adempimenti e degli oneri amministrativi per i cittadini e le imprese; emerge un impiego dei *big data* pubblici, oltre che per il miglioramento nello svolgimento delle funzioni delle amministrazioni, anche a diretto vantaggio della collettività di riferimento, nella logica orizzontale che caratterizza l'*open government*, interpretando in un'ottica sinergica i *big data* e gli *open data* in ambito pubblico. In tal modo viene offerto all'utilizzo dei *big data* pubblici un fondamento normativo e una regolamentazione, che sarà contenuta in modo precipuo nel previsto decreto.

In questo contesto, proprio anche alla luce di tali recenti disposizioni introdotte dal d.lgs. 217/2017, vale evidenziare l'importanza strategica che rivestono l'interconnessione e la cooperazione tra le banche dati pubbliche, cui portano i principi di disponibilità e fruibilità, previsti nella normativa, e alle quali si somma il concetto di riutilizzo che emerge negli ultimi anni prepotentemente, promettendo di far utilizzare i

[593] Art. 50-ter, comma 4, d.lgs. 82/2005; l'elenco è aggiornato periodicamente con decreto del Presidente del Consiglio dei ministri, sentito il Garante per la protezione dei dati personali e le Amministrazioni titolari dei dati.

dati pubblici anche a soggetti privati[594]. In tal modo i *big data* pubblici finiscono per connettersi a quelli privati in sinergie inedite foriere di risultati inattesi e utili alla collettività, prendendo i connotati di un sottoinsieme "*big*" dei *big data* latamente intesi.

Se l'interesse pubblico muove le istituzioni e ciò ha portato a strategie di *open data* al fine di reimmettere il grandissimo valore dei dati nella collettività con finalità di trasparenza, efficienza e miglioramento della vita della collettività, perché questa possa farne uso a fini di sviluppo sociale, economico e scientifico[595], ben diverso è il caso delle grandi aziende che utilizzeranno verosimilmente quel valore a fini di profitto economico e non avranno certo interesse ad aprirlo e a condividerlo, ma al contrario tenderanno a proteggerlo e a "chiuderlo".

A ciò va aggiunta la considerazione che i soggetti pubblici non sono solo fonti e produttori di *big data*, ma anche potenziali utilizzatori degli stessi servendosi di quelli prodotti dal sistema privato: tale possibilità apre la porta a rischi e implicazioni etiche e sociali che devono essere attentamente esaminate[596].

---

[594] I riferimenti normativi sono principalmente contenuti nel Codice dell'amministrazione digitale e, in particolare, oltre all'art. 50-ter, negli artt. 50 (principio di disponibilità, fruizione e riutilizzazione da parte delle altre pubbliche amministrazioni e dei privati) e 52 (*open data*) del d.lgs. 82/2005, cui va sommata la disciplina sul riutilizzo delle informazioni del settore pubblico, in particolare il d.lgs. 36/2006 e il d.lgs. 102/2015, che ha modificato il primo. Sull'interconnessione tra banche dati pubbliche cfr. G. CARULLO, *Big data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e mercato*, 2016, pp. 181-204, che sottolinea «il saldo collegamento tra dati e funzione pubblica svolta. Collegamento che, naturalmente, deve sussistere poi anche nella fase di effettiva fruizione dei dati», dal momento che deve essere consentita esclusivamente per il raggiungimento delle finalità istituzionali delle altre amministrazioni che ne chiedono la fruizione (p. 200); la fruizione deve essere strumentale a un preciso interesse pubblico del soggetto terzo rispetto al titolare dei dati, che resta tale anche in caso di trasferimento del dato (art. 50, comma 3-bis, d.lgs. 82/2005).

[595] Sono svariati i settori di impiego dei *big data* pubblici: sicurezza, sanità, trasporti, energia, meteo, istruzione. Secondo V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *Ten legal perspectives on the "Big data revolution"*, in *Concorrenza e mercato*, 2016, p. 36 ss. non si può prevedere un diritto generale di accesso ai dati di un terzo, a meno che non esista una legittimazione da parte delle disposizioni.

[596] Cfr. D. CARDON, *op. cit.*, p. 47: «I data base più funzionali appartengono alle amministrazioni, alle imprese e, soprattutto, alle grandi piattaforme del web (Google, Facebook, Amazon). La maggior parte di queste ha chiuso il rubinetto dei dati, allo scopo di riservarsene l'uso o di commercializzarne l'accesso».

3.7. I profili relativi alla *digital economy*, i rischi e le implicazioni etico-sociali dei "grandi dati"

La dimensione economica è centrale nel contesto dei *big data*, dal momento che la conoscenza prodotta è un valore che può essere impiegato per ottenere profitti. La stessa Europa, quando si occupa di dati e di *big data*, lo fa con un approccio prevalentemente economico e non a caso parla di *data-driven innovation* o *data-driven economy*, economia "guidata dai dati". Anche nella connessione con la problematica giuridica forse più significativa, ossia la protezione dei dati personali, emerge il profilo dello sfruttamento economico dei dati nonostante le garanzie giuridiche a tutela di quelli personali, ma anche lo sfruttamento economico dei dati personali stessi, la loro "monetizzazione" e la capacità di essere scambiati e commercializzati[597].

Ma, come risulta evidente già dall'analisi del fenomeno, l'impatto dei *big data* non è soltanto economico, dal momento che si pone la necessità di bilanciare il valore e le opportunità offerte dai "grandi dati" con le questioni etiche e sociali che sono in grado di sollevare nella società contemporanea[598].

«Le nostre percezioni e le nostre istituzioni sono state costruite per un mondo caratterizzato dalla scarsità, e non dalla sovrabbondanza, di informazioni»[599]; il valore insito nei *big data* è capace di cambiare le geometrie del potere, indebolire il vantaggio competitivo delle istituzioni pubbliche, detentrici tradizionali delle informazioni, della loro misurazione e del sapere correlato, e consegnare questo potere anche in mano a grandi aziende detentrici di dati o capaci di estrarne il valore.

---

[597] Cfr. C. FOCARELLI, *op. cit.*, p. 45 ss. e E. NUNZIANTE, *op. cit.*, p. 10, che evidenzia «la questione della progressiva reificazione del dato personale e della configurabilità di quest'ultimo come bene giuridico». G. COLANGELO, *op. cit.*, p. 426 riporta i modelli di business legati ai dati anche di carattere personale, come le imprese che offrono riduzioni del corrispettivo per i servizi offerti a fronte dell'autorizzazione a usare e condividere dati personali ("*pay-for-pricing*") o il *market of data*, che vede *broker* acquisire dati personali da varie fonti per poi rivenderli.

[598] Tali aspetti sono oggetto di attenta considerazione nel Report del maggio 2014 dell'*Executive Office* del Presidente degli Stati Uniti «*Big Data: Seizing Opportunities, Preserving Values*».

[599] V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 201.

Lo scenario aperto dai *big data* vede realizzarsi una contrapposizione significativa tra i "signori dei dati" [600] e tutti gli altri.

Gli Stati conoscono ingenti quantità di dati necessari per svolgere le attività pubbliche ed erogare servizi, Google traccia i nostri percorsi in rete e misura i *clic*, Amazon monitora, predice e condiziona gli acquisti, Twitter e Facebook sanno cosa ci interessa, conoscono le nostre relazioni e modellano la nostra reputazione.

In questo contesto l'individuo perde sostanzialmente la propria libertà, in quanto viene "guidato", grazie ai dati che lui stesso ha fornito, nelle strade digitali di preferenze, relazioni e decisioni che finiscono per non essere autonome[601]; «le infrastrutture dei *big data* cercano di guidare senza veicolare, di indirizzare senza obbligare»[602].

La dittatura degli algoritmi mostra così il proprio lato oscuro e rischia di guidare i comportamenti e confinare le volontà individuali costringendo l'individuo apparentemente libero a rinchiudersi in una *filter bubble*[603]: tutto ciò palesa l'esigenza di nuovi principi a tutela della libertà, della dignità e della persona[604].

---

600 Li definisce così A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 135 ss.

601 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 203 ss. Secondo D. CARDON, *op. cit.*, p. 76 esistono diverse forme e tecniche di calcolo usate per riorganizzare la società a partire dagli individui: «i clic degli internauti producono popolarità, le citazioni ipertestuali autorità, gli scambi tra cerchie affini reputazione, le tracce dei comportamenti predizioni personalizzate ed efficaci». Secondo l'Autore esistono, infatti, quattro famiglie di calcolo digitale sulla base della posizione assunta rispetto al mondo digitale: *accanto*, che misura i *clic* e la *popolarità* (*Google Analytics*); *al disopra*, che si fonda sui *link* e valuta l'*autorevolezza* (*PageRank* di Google); *dentro*, che si basa sui *like* e misura la *reputazione* (*social network*); *al disotto*, che si basa sulle *tracce* e permette la *predizione* (le raccomandazioni di Amazon, che utilizza il *machine learning*, l'apprendimento automatico dai dati). Tali famiglie sono emerse una dopo l'altra e oggi convivono e si mescolano nella rete.

602 D. CARDON, *op. cit.*, p. 86: «gli algoritmi sognano di alleggerire gli umani di quanto c'è di più meccanico nelle loro attività, asserendo che lo fanno per lasciar loro la libertà di dedicarsi a funzioni cognitive più elevate, più complesse o più ambiziose». Il rischio sta nel fatto che le infrastrutture di calcolo predispongono le scelte degli individui canalizzandole in processi irreversibili e, di conseguenza, la sfida sta nella capacità di disinnestarle e «imparare a non disimparare» (p. 87).

603 D. CARDON, *op. cit.*, p. 54 ss.: nelle piattaforme e nei *social* l'algoritmo, basandosi sulle affinità dell'individuo, finisce per rinchiuderlo in una "bolla" limitando il "paesaggio" alle scelte sue e dei suoi amici; gli individui seguendo le consuetudini comportamentali del *social* o della piattaforma finiscono da

Tale configurazione, frutto della società degli algoritmi, è foriera di un'implicazione di rilevante impatto etico e sociale: l'asimmetria di potere informativo che i *big data* possono generare tra i loro detentori e la collettività, costituita da cittadini e piccole e medie imprese, apre un pericoloso *big data divide*[605]. In concreto pochi soggetti, pochi grandi *player* detengono *big data* e questo provoca una forbice nel potere informativo, permettendo, di fatto, ai detentori dei *big data* di essere dominanti sul mercato con il rischio di violazione delle norme antitrust, delle regole a protezione dei consumatori e delle regole a tutela dei dati personali[606].

L'asimmetria di potere acquisisce ampia connotazione, dal momento che si cerca di predire e indirizzare l'internauta grazie ai calcoli sulle sue tracce digitali e su quelle di coloro che gli somigliano[607], facendo scomparire la persona nella sua unicità tra navigazioni, *like* e *cookie*, grazie a tecniche di calcolo volutamente sconosciute al grande pubblico per non suscitarne l'ostilità e nascoste accuratamente dietro burocratiche richieste di consenso e di accettazione di condizioni generali: i dati sono forniti senza attenzione da soggetti per lo più inconsapevoli e in ogni caso imprigionati in una trattativa iniqua con l'imprenditore[608].

---

soli per rinchiudersi nella *filter bubble*, continuando ad essere «prevedibili, topolini meccanici nelle grinfie dei calcolatori» (p. 57).

604 Cfr. D. CARDON, *op. cit.*, p. 45 ss., secondo cui «un algoritmo "funziona" davvero quando riesce ad armonizzarsi a tal punto con l'ambito nel quale opera, da portare gli attori a regolare le azioni sui suoi verdetti, da nutrirne gli immaginari secondo i principi da lui stabiliti. Lo si può dire per PageRank di Google, del sistema di raccomandazione di Amazon, dei voti attribuiti agli alberghi da TripAdvisor o dal GPS integrato nelle automobili» (p. 51).

605 M. ANDREJEVIC, *The Big Data Divide*, in *International Journal of Communication*, n. 8, 2014, pp. 1673-1689.

606 *Preliminary Opinion* dell'EDPS *«Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*», marzo 2014. *Infra*, cap. 5, § 6.

607 Cfr. D. CARDON, *op. cit.*, p. 31 ss.: «L'algoritmo incolla l'internauta alle proprie tracce e non gli consente di distanziarsene» (p. 41).

608 Cfr. M.F. DE TULLIO, *op. cit.*, p. 651 ss. Secondo D. CARDON, *op. cit.*, p. 25 ss. le tecniche di calcolo partono dalle tracce e dai comportamenti degli individui nella realtà digitale; «gli architetti dei nuovi algoritmi dei *big data* assicurano che bisogna dare fiducia soltanto ai comportamenti reali degli individui, e non a ciò che sostengono di fare quando raccontano se stessi sulle espressive piattaforme del social web» (pp. 26-27).

Tali dinamiche messe in atto dagli algoritmi finiscono per riprodurre nel contesto digitale la struttura della società con le sue asimmetrie, disparità e discriminazioni, finendo per non distanziarsi troppo dall'ordine sociale; profilazioni incontrollate e commercializzazioni predatorie, discriminazioni di prezzo e disuguaglianze economiche, disparità di trattamento e distorsioni del mercato sono tra i principali danni che gli utenti ricavano dalle asimmetrie di potere[609]. Come sottolinea significativamente Cardon, si crea il paradosso per cui si amplificano le coordinazioni e le gerarchizzazioni, ma gli individui si sentono più liberi nelle loro scelte[610]: «i calcolatori danno alla società i mezzi per riprodurre da sé le disparità e le gerarchie che le sono connaturali» e questo mina la libertà individuale e il principio di uguaglianza, aprendo la strada a vecchie e nuove discriminazioni[611].

Di conseguenza, questo squilibrio può tradursi anche in forme di controllo sociale: al fine di realizzare previsioni politiche e avere supporto nelle decisioni intraprese, anche in connessione con i propri *big data*, i soggetti pubblici possono decidere di servirsi delle grandi banche dati dei privati, che detengono informazioni acquisite su base contrattuale, e così possono arrivare a monitorare la collettività di riferimento tramite rapporti negoziali con le grandi aziende. Per tale strada si realizza un controllo sociale indiretto, che utilizza e sfrutta i grandi raccoglitori di dati privati: questo può tradursi in una forma di sorveglianza e persino di repressione capace di allontanare

---

609 M. OREFICE, *op. cit.*, p. 733 ss., secondo la quale «i dati possono divenire uno strumento di dominio […], la *privacy* rischia così di diventare un privilegio» (p. 735).

610 Secondo D. CARDON, *op. cit.*, p. 89 ss. gli algoritmi «non ci impongono la meta. Non scelgono ciò che ci interessa. Siamo noi a dire loro la meta ed essi ci chiedono di seguire la "loro" strada»; nascono da un desiderio di libertà e autonomia, ma «contribuiscono anche ad assoggettare l'internauta a quella strada calcolata, efficace, automatica, che si adatta ai nostri desideri regolandosi, in segreto, sul traffico altrui».

611 Cfr. D. CARDON, *op. cit.*, p. 70 ss., secondo cui «in maniera assai conservatrice, il calcolo algoritmico riproduce l'ordine sociale aggiungendo i propri verdetti alle disparità e alle discriminazioni della società: quelli giudicati male saranno serviti male e così il giudizio su di loro diventerà ancora più negativo» (p. 72). Del resto «l'individuo calcolato non è altro che un flusso. Esso è trasparente, e viene estrapolato dalle sue stesse tracce» (p. 73) e, così, «il probabile si arroga il diritto di prelazione sul possibile» (p. 74). Certo non mancano anche gli aspetti positivi, quale in particolare la ricomposizione della società a partire dagli investimenti espressivi degli individui.

governanti e governati, in direzione opposta rispetto alla filosofia di *open government*[612].

Il rischio è concreto ed è diventato già reale: è davanti ai nostri occhi il *Datagate* e quanto ha rivelato Edward Snowden sulle operazioni di intercettazione, raccolta e analisi da parte delle agenzie di *intelligence* statunitensi, grazie a rapporti con i colossi della rete, che hanno dato vita a una sorveglianza di massa sui dati personali di cittadini di tutto il mondo, inclusi capi di Stato e di governo europei[613].

Nell'utilizzo dei *big data* si affaccia anche il rischio ancora più temibile che aziende e governi possano utilizzare i dati contro di noi, ossia possano basarsi sui dati per presumere di conoscerci fino a poter impiegare in vario modo le previsioni, fornite dai *big data*, per finalità diverse da quelle originarie con potenziali effetti discriminatori, come esemplificativamente nell'ambito assicurativo o in quello lavorativo, fino ad arrivare anche a "predire" possibili crimini in uno scenario che ricorda quello di *Minority Report*[614]. Nel film i soggetti vengono dichiarati colpevoli e sono arrestati

---

612 La relazione 2013 del Garante privacy è dedicata a «*La protezione dei dati nel cambiamento. Big data; Trasparenza; Sorveglianza*». M.F. DE TULLIO, *op. cit.*, pp. 648 ss.: «*Élite* statali e commerciali delle informazioni possono infine fondersi tra loro: lo Stato lavora a stretto contatto con le *corporation*, in quanto esternalizza la raccolta e analisi di dati o attinge direttamente dagli archivi dei fornitori di servizi di comunicazione»; peraltro in questo scenario raccoglitori su larga scala sono anche i servizi di *intelligence*.

613 Nel 2013 Edward Joseph Snowden, ex tecnico della CIA (*Central Intelligence Agency*) e collaboratore di una società di servizi informatici fornitrice della NSA (*National Security Agency*) ha rivelato al quotidiano The Guardian le attività di sorveglianza dei servizi di intelligence statunitensi connesse in particolare al programma governativo segreto di sorveglianza di massa, denominato PRISM (da prisma ottico). Il programma PRISM permetteva l'accesso e la raccolta ad opera dell'NSA di dati quali email, profili, chat, conversazioni, video e foto da aziende come Google, Microsoft, Facebook, Apple e Yahoo, che hanno negato di conoscere il programma e di fornire accesso ai propri flussi di dati; sulla vicenda cfr. G. GREENWALD, *Sotto controllo. Edward Snowden e la sorveglianza di massa*, trad. it., Rizzoli, Milano, 2014. È consapevole dei rischi di sorveglianza l'Europa nella comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014: «le notizie sull'utilizzo di tecnologie simili a fini di sorveglianza da parte di soggetti pubblici o privati possono alimentare preoccupazioni e ridurre la fiducia nell'economia digitale di individui e organizzazioni. […] Un elevato livello di fiducia è indispensabile per l'economia basata sui dati».

614 In merito alla previsione di possibili crimini, tra i software si possono ricordare PredPol negli Stati Uniti (*www.predpol.com*) e Keycrime in Italia.

prima di aver commesso il fatto, dal momento che i "Precog", esseri dotati della capacità di precognizione, riescono a prevedere i crimini che avverranno.

Se non sono i Precog a prevedere il futuro, ci pensano i *big data* e l'analisi previsionale a poter minare la libertà individuale e il diritto di autodeterminazione: in tale profilo emerge uno dei molti aspetti problematici per il diritto, cui va sommata la complessa questione giuridica relativa all'attribuzione delle responsabilità in caso di previsioni erronee o dannose e il potenziale utilizzo discriminatorio delle previsioni[615].

3.8. Le problematiche giuridiche poste dai *big data*

«*"Big Data" are not simply a bigger phenomenon to which one can simply apply well know rules. "Big data" are ontologically different from "small data" because of the use which is made of them and their potentialities for human decisions, cooperation, and commerce*»[616]. Non solo i volumi, le finalità e le implicazioni sociali sono "grandi", ma altresì le problematiche che il diritto si trova ad affrontare nell'utilizzo dei *big data*[617].

---

615 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 203 ss., che riportano progetti di ricerca e programmi sperimentali che in America vanno in tal senso, cercando ad esempio di identificare potenziali terroristi; M. OREFICE, *op. cit.*, p. 711 ss.; V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 53 ss., che per far emergere il potenziale discriminatorio delle analisi predittive portano l'esempio di dati di *screening* medico usati in contesti diversi dalla medicina preventiva, come quello lavorativo (per selezionare i lavoratori) o assicurativo (per emettere o meno la polizza o impostare il premio); gli Autori sottolineano la difficoltà di trovare un equilibrio tra principio di discriminazione e abbassamento del livello di rischiosità, anche in considerazione della forte asimmetria informativa tra le parti.

616 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 57; nel contributo gli Autori esaminano il fenomeno *big data* al cospetto di dieci categorie giuridiche tipiche: *ownership*; *personal data*; *access to data*; *data transactions*; *consumer transactions*; *liability in data driven innovation contexts*; *competition issues*; *choice of law and jurisdiction*; *sovereignty*; *philosophical and ethical issues in big data*.

617 M. FALCONE, *op. cit.*, p. 601 ss.: «Il fenomeno dei *big data*, quindi, sta avendo un rilievo giuridico sempre più marcato: sta modificando aspetti cardine della disciplina antitrust; sta indebolendo la tutela dei consumatori e la disciplina sul diritto d'autore; sta paralizzando la disciplina sulla protezione della

L'attenzione ai profili giuridici è essenziale al fine di garantire certezza del diritto e fiducia nelle tecnologie utilizzate: l'Europa è consapevole, da questo punto di vista, di dover «fare in modo che i pertinenti quadri giuridici e le politiche, ad esempio in materia di interoperabilità, protezione dei dati, sicurezza e diritti di proprietà intellettuale, favoriscano l'uso dei dati, al fine di rafforzare la certezza giuridica per le imprese e infondere nei consumatori la fiducia nei confronti delle tecnologie per i dati»[618].

Trattandosi di dati, anche in tal caso come per gli *open data*, i profili maggiormente problematici si individuano nella relazione con la normativa in materia di protezione dei dati personali, problematica particolarmente evidente se si pensa ad esempio all'*Internet of Things*.

Al riguardo, il quadro normativo non è allineato con il nuovo contesto tecnologico: neanche il regolamento europeo (UE) 2016/679 del 27 aprile 2016 tratta esplicitamente i *big data*, anche se alcune disposizioni e alcuni strumenti sembrano sottintenderne l'esistenza, in particolare gli strumenti che mirano a un approccio sistematico, a un atteggiamento proattivo e a una ponderazione *ex ante* dell'impatto e dei rischi sulla *data protection*, come i principi *privacy by default* e *privacy by design* o il c.d. *Data Protection Impact Assessment*[619].

In specifico, a causa delle esaminate caratteristiche che connotano il fenomeno, l'utilizzo dei *big data*, laddove siano presenti dati personali, rende particolarmente problematico il rispetto del principio di finalità previsto dalla normativa[620], dal momento che spesso nelle strategie *big data* al momento della raccolta non si conosce il risultato atteso, essendo capaci di condurre a risultati imprevisti di indubbio interesse.

---

riservatezza dei dati e sta facendo sorgere in modo evidente un profilo collettivo della *privacy*, prima non ancora così evidente»; tali problematiche saranno oggetto del presente paragrafo.

618 Comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014.

619 Si tratta del regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (cosiddetto regolamento generale sulla protezione dei dati): si applica dal 25 maggio 2018. Tali strumenti saranno trattati nel capitolo 5.

620 Art. 5, paragrafo 1, reg. (UE) 2016/679, in particolare lett. b) e lett. c), e art. 11, d.lgs. 196/2003, in specifico, comma 1, lett. b).

Di conseguenza è difficile garantire l'informativa[621] e il consenso[622], elementi fondamentali su cui ruota la disciplina a livello europeo e nazionale, che rischiano di vanificarsi dal momento che non si conoscono gli scopi: tutto questo, di conseguenza, può inficiare la stessa liceità del trattamento.

Proprio a causa dei limiti che sconta l'odierna disciplina nei confronti del fenomeno oggetto di regolazione, è opportuno immaginare nuovi modelli più flessibili e maggiormente incentrati sull'uso dei dati e sulla responsabilità, al fine di poter arginare con efficacia le nuove problematiche che vengono a porsi[623].

Peraltro lo stesso trasferimento di dati e la conseguente applicazione di disposizioni normative afferenti a ordinamenti giuridici diversi fanno emergere problemi di tutela dei dati personali; al riguardo il celebre caso *Schrems versus Facebook*[624], oggetto della sentenza della Corte di Giustizia dell'Unione europea nel 2015 e conseguenza delle rivelazioni di Snowden, ha portato a dichiarare invalida, perché incompatibile con il diritto dell'Unione, la decisione della Commissione europea 2000/520 e, di conseguenza, l'accordo "*Safe Harbour*" ("approdo sicuro")[625], che sostanzialmente permetteva il trasferimento dei dati dall'Unione europea agli Stati Uniti: la motivazione afferisce al fatto che gli Stati Uniti non garantiscono una tutela

---

621 Artt. 13-14, reg. (UE) 2016/679 e art. 13, d.lgs. 196/2003.

622 Art. 7, reg. (UE) 2016/679 e art. 23, d.lgs. 196/2003. I profili relativi al rapporto tra *big data* e privacy saranno approfonditi nel capitolo 5, § 6.

623 Cfr. *Report* del *President's Council of Advisors on Science and Technology* (PCAST), «*Big data and privacy: a technological perspective*», maggio 2014 e C. FOCARELLI, *op. cit.*, p. 55 ss.

624 Sentenza della Corte di Giustizia dell'Unione europea del 6 ottobre 2015 nella causa C-362/14 *Maximillian Schrems versus Data Protection Commissioner*, in cui Schrems, a seguito delle rivelazioni di Snowden, chiedeva di esercitare i propri poteri e, in specifico, di vietare il trasferimento dei suoi dati da parte di Facebook verso gli Stati Uniti, in considerazione del fatto che il programma PRISM permetteva di accedere liberamente ai dati dei *server* ubicati negli USA. Al riguardo, cfr. R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, fasc. 1, 2016, pp. 289-307; G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4, 2015, p. 697 ss.; V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2015, p. 683 ss.

625 Nella decisione 2000/520 del 26 luglio 2000 la Commissione europea ha ritenuto che nel contesto del cosiddetto regime di "approdo sicuro" (*Safe Harbour*) gli Stati Uniti garantissero un livello adeguato di protezione dei dati personali trasferiti.

equivalente dei dati personali degli utenti europei[626]. Il caso ha portato al più garantista "*EU-US Privacy Shield*" del 2 febbraio 2016, che, seppur sempre basato su un sistema di autocertificazione, esclude la possibilità di svolgere attività indiscriminate di sorveglianza di massa sui dati personali trasferiti negli Stati Uniti e sottopone a limitazioni, garanzie, vigilanza e meccanismi di controllo l'accesso delle autorità pubbliche ai dati, che avviene in applicazione della legge o per scopi di sicurezza nazionale.

Del resto, anche laddove i dati non siano personali il problema non è completamente superato, dal momento che il *data mining* e le analisi tecniche dei *big data* sono capaci di intaccare anonimato e anonimizzazioni e, altresì, di produrre fenomeni di re-identificazione, de-anonimizzazione[627] e cosiddetto "effetto mosaico", che consentono di rivelare l'identità di una persona o di piccoli gruppi e i comportamenti collegati, riproponendo le esigenze di tutela della normativa in materia di *data protection*[628]; è dunque necessario verificare che l'anonimizzazione non sia facilmente reversibile.

Più ampiamente, in considerazione dell'assenza di una regolamentazione esplicita del fenomeno da parte della normativa anche sotto il profilo della protezione dei dati personali, l'analisi e l'utilizzo dei *big data* implicano la definizione esplicita degli

---

626 I principi di *Safe Harbour* sono applicabili esclusivamente alle organizzazioni americane private che li sottoscrivono, mentre le autorità pubbliche non sono tenute alla loro osservanza e, quindi, possono accedere in maniera generalizzata al contenuto di comunicazioni elettroniche con conseguente lesione del diritto fondamentale al rispetto della vita privata. Inoltre, le esigenze afferenti alla sicurezza nazionale, al pubblico interesse e all'osservanza delle leggi statunitensi prevalgono sul *Safe Harbour*, cosicché le imprese private nordamericane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime laddove queste ultime entrino con esse in conflitto, con conseguente ed inevitabile ingerenza nei diritti e nelle libertà fondamentali delle persone i cui dati vengono trasferiti dall'Unione europea verso gli Stati Uniti. Cfr. V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 51 ss. e F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Rivista di diritto internazionale*, fasc. 3, 2016, pp. 690-724.

627 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 210: «In presenza di un quantitativo sufficiente di dati, la totale anonimizzazione è assolutamente impossibile».

628 Cfr. V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 33 ss., che sottolineano, di conseguenza, come nessun dato sia totalmente anonimo.

obiettivi, l'emanazione di *policy* e di linee guida dedicate e la previsione di una specifica regolamentazione di accompagnamento. Ciò è necessario anche al fine di garantire la qualità dell'informazione e la sicurezza, che si ottiene non solo sotto il profilo tecnologico, ma ponendo attenzione, altresì, all'aspetto umano e organizzativo, per mezzo di protocolli specifici, delineando puntuali responsabilità e potendo anche immaginare autorità sovranazionali di controllo. Da questo punto di vista la possibilità di regolamentazione sconta, peraltro, criticità geopolitiche per la differenza tra le normative applicabili e la conseguente diversità nella tutela, si pensi alle differenze fra gli Stati Uniti e i Paesi europei[629].

Inoltre, l'analisi tecnica dei *big data*, consistendo in un processo di approssimazione, genera il rischio di trarre conclusioni imprecise e discriminatorie. Un rilevante profilo problematico è costituito proprio dall'illusione della capacità descrittiva dei *big data*: l'overdose informativa generata dalla quantità dei dati non si traduce necessariamente in conoscenza; perché questo avvenga c'è necessità di contestualizzazione, analisi e interpretazione dei dati[630]. In sintesi, è necessario «controllare i *big data*, per evitare che siano loro a controllare noi»[631]. Dal dato alla conoscenza, infatti, possono intercorrere elementi che minano questo percorso, come la scarsa qualità dei dati usati[632] o il loro utilizzo improprio o manipolatorio[633]. Si

---

629 Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 140 ss.: «la creazione di autorità di controllo sovranazionali dovrebbe da un lato incidere sulla standardizzazione dei servizi in termini soprattutto di sicurezza, ma dovrebbe anche servire come strumento per sorvegliare ed eventualmente contenere sia le pretese invasive dei governi, sia gli eventuali abusi dei detentori/gestori dei *big data*» (p. 141).

630 Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 135 ss.: l'overdose informativa porta al risultato inverso di una diminuzione della conoscenza, con il rischio di confusione e di attribuzione di valore a fonti scarsamente attendibili. Cfr. D. CARDON, *op. cit.*, p. 45 ss., secondo cui «i dati parlano solo in funzione di come vengono interrogati e degli interessi di coloro che li interrogano» (p. 46).

631 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 229.

632 I dati sono fortemente condizionati dalla tempestività e dall'accuratezza; cfr. G. COLANGELO, *op. cit.*, p. 430.

633 Cfr. D. CARDON, *op. cit.*, p. 32 ss.: «La competenza dei calcolatori soppianta l'autorità professionale. Il fatto che le misure siano false non è più considerato un problema. Quello che importa, invece, è impiantare un ciclo riflessivo che porti gli attori a sapersi osservati da un sistema metrico e a

affiancano quindi a problematiche di incapacità tecnica o errori nell'analisi e nell'interpretazione dei dati anche i rischi ben più gravi di manipolazioni e deformazioni volute della realtà. Per dirla con Cardon «non è solo l'algoritmo a destare sospetti, ma anche coloro che cercano di manipolarlo»[634].

Un altro aspetto problematico da un punto di vista giuridico è quello relativo alla "proprietà" dei dati che formano i volumi dei *big data*. Chi è proprietario dei *big data* e dei dati prodotti dall'*Internet of Things*?

A tale proposito all'approccio della proprietà tradizionale è preferito quello della proprietà intellettuale, ma anche in tal caso si pongono problemi di applicazione della normativa.

Sotto tale profilo le grandi aziende si atteggiano a "proprietari" dei nuovi dati prodotti dalla combinazione di dati di cui sono titolari soggetti terzi. Da tale punto di vista, infatti, accanto alla protezione delle creazioni intellettuali, delle informazioni strutturate e delle banche dati "creative" per mezzo del diritto d'autore[635], l'ordinamento giuridico fornisce tutela alle banche dati "non creative" e prevede la correlata protezione del cosiddetto diritto *sui generis*. Generalmente le raccolte di *big data* possono essere ricondotte a banche dati "non creative", anche a causa dell'estrema varietà dei dati inclusi, ma evidentemente questo si traduce nella tutela del diritto *sui generis*, meno intensa del diritto d'autore[636]. Per questo si può ragionevolmente dubitare che si tratti di una tutela in grado di fornire una protezione sufficiente e adeguata.

Talvolta, ritenendo che il valore economico non sia nei dati, ma nelle elaborazioni, nei calcoli e negli algoritmi, la tutela giuridica si sposta dalla proprietà al contratto di fornitura di servizi[637].

---

orientare le loro azioni secondo gli effetti che esse avranno sulla misura. Le misurazioni servono a fabbricare il futuro» (p. 34).

634 D. CARDON, *op. cit.*, p. 67.

635 L'informazione allo stato puro è esclusa dalla protezione; cfr. E. NUNZIANTE, *op. cit.*, p. 4.

636 Secondo M. FALCONE, *op. cit.*, p. 601 ss. l'attuale disciplina non è in grado di comprendere il fenomeno dei *big data* in cui ad essere "originale" non è la banca dati o la sua organizzazione, ma le modalità di interrogazione e analisi dei dati.

637 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 30 ss. chiariscono come le tre prospettive (proprietà tradizionale, proprietà intellettuale, contratto) non sono reciprocamente esclusive, ma sono utilizzate in base ai diversi contesti e alla situazione prevalente: «*e.g. the first one in a*

La questione è poi particolarmente complessa nel caso dell'*Internet of Things*, dal momento che non si tratta di un singolo bene immateriale, ma di un processo che spesso vede titolarità diverse tra chi possiede lo strumento e chi il servizio e pone connessi problemi di responsabilità[638]. Anche in tal caso emergono, peraltro, le conseguenti relative problematiche di divergenza tra discipline europee e statunitensi.

Nel contesto dei *big data* possono venire in rilievo le norme in materia di segreto industriale, in particolare gli articoli 98 e 99 del Codice di proprietà industriale, in specifico per proteggere gli algoritmi, ma con la difficoltà di dover provare l'applicazione di misure efficaci a garantire la segretezza e l'impossibilità di proteggersi da atti indipendenti di terzi o da pratiche di *reverse engineering*[639].

Laddove la tutela della proprietà intellettuale e la protezione del *trade secret* non soccorrano nel fornire una protezione efficace, si può pensare di ricorrere all'autonomia contrattuale per tutelare i *database* e individuare puntualmente i profili di responsabilità reciproca[640]. La disciplina contrattualistica viene poi in gioco in caso di *sale of data*, cessione dei *database*, dove in ogni caso si porranno problemi di rispetto dei dati, anche personali, contenuti nel *database* stesso, e nei casi di *data-services*, concessione di diritti di utilizzo temporaneo con licenze, che si alloca nel contesto della prestazione di servizi[641].

Una relazione contrattuale è anche quella che lega i collettori di dati e i consumatori: in specifico si è di fronte a contratti con i consumatori, in cui dovrebbero essere chiari i vincoli, le responsabilità e l'uso che verrà fatto dei dati e dei contenuti, che sostanzialmente sono "la moneta" con la quale sono pagati servizi sedicenti

---

bankruptcy procedure; the second one when contrasting unfair competition; the third one in the ordinary business of the big data holder with third parties».

638 In via esemplificativa il proprietario di un sensore non lo è necessariamente dei *server* che processano il segnale o dei classificatori e interpreti dei *big data*; così R. MORO VISCONTI, *Internet delle cose, Networks e plusvalore della connettività*, cit., p. 539, che sottolinea come i singoli elementi del *network* della filiera IoT abbiano un valore atomistico, cui si associa un plusvalore olistico.

639 Cfr. E. NUNZIANTE, *op. cit.*, p. 4; M. BOGNI - A. DEFANT, *op. cit*., che rilevano come per i *big data* possa venire in gioco anche la protezione del diritto di proprietà industriale sulle informazioni riservate.

640 Cfr. E. NUNZIANTE, *op. cit.*, p. 6, che in merito alla protezione dei *database* grazie all'autonomia contrattuale richiama la sentenza della Corte di Giustizia dell'Unione europea *Ryanair Ltd. versus PR Aviation Bp* (ECJ C-30/14).

641 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 38 ss.

gratuiti[642]. Ma nella realtà rischia di risultare inefficace la disciplina a tutela del consumatore, vittima di una visione opaca e di dinamiche di mercato discriminatorie[643].

I *big data*, inoltre, sollevano questioni e problematiche di concorrenza inedite, che non si limitano ai mercati digitali, ma involgono i mercati tradizionali, i mercati dei prodotti e i mercati ancora non configurabili, rendendo di difficile declinazione gli istituti tipici e consolidati quali mercato rilevante, potere di mercato, prezzi discriminatori[644] e abuso di posizione dominante[645]; le problematiche, laddove siano individuabili abusi, mostrano la necessità di soluzioni atte a riequilibrare il mercato come l'interoperabilità, la condivisione e la concessione in licenza dell'accesso ai dati[646].

In dottrina, per quanto riguarda *big data* e *antitrust* si contrappongono le posizioni di chi evidenzia il ruolo strategico dei *big data*, capaci di conferire vantaggi competitivi e di erigere barriere all'ingresso, portando all'affermazione di posizioni dominanti, grazie a impedimenti legali o contrattuali alla condivisione dei dati, strategie di *lock-in* degli utenti, economie di scala ed effetti di rete diretti e indiretti, e di coloro che invece non ravvisano barriere all'entrata e che attribuiscono valore strategico ai risultati scaturenti dall'analisi dei dati e non ai dati in sé, che, di conseguenza, non potrebbero portare a penalizzazioni dei soggetti[647].

---

642 In merito cfr. V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 40 ss.

643 Cfr. M. FALCONE, *op. cit.*, p. 601 ss.

644 In dottrina c'è chi mostra maggiore preoccupazione per le discriminazioni comportamentali che possono derivare dai *big data* e dalle loro analisi, capaci di influenzare e ingabbiare le scelte dei singoli; cfr. G. COLANGELO, *op. cit.*, p. 448 ss.

645 Al riguardo cfr. M. OREFICE, *op. cit.*, p. 722 ss., che sottolinea come Google abbia molti più dati di chiunque altro e assuma una posizione di vantaggio nella "*data collection*", potendo configurare abuso di posizione dominante con natura escludente in caso di rifiuto di dare accesso ai propri diritti di esclusiva sui dati.

646 In particolare viene in gioco la legge 10 ottobre 1990, n. 287 sulla tutela della concorrenza e del mercato. Cfr. F. DI PORTO, *La rivoluzione* Big Data. *Un'introduzione*, cit., p. 5 ss. e M. OREFICE, *op. cit.*, p. 711 ss. Per le problematiche generate dai *big data* sui temi di diritto della concorrenza, più ampiamente, cfr. il numero speciale di F. DI PORTO (a cura di), *Big Data e Concorrenza*, in *Concorrenza e mercato*, parte I, 2016.

647 Cfr. G. COLANGELO, *op. cit.*, p. 429 ss.

Al riguardo la casistica *antitrust* relativa ai *big data* è limitata e concerne prevalentemente fattispecie concentrative: in via esemplificativa, la Commissione europea nel caso COMP/M.6281, con decisione del 7 ottobre 2011, ha approvato la concentrazione *Microsoft/Skype*, ponendo attenzione alla qualità dei servizi e alla loro diversificazione, e nel caso M.7217 *Facebook/WhatsApp*, con decisione del 3 ottobre 2014, nel valutare la concentrazione tra Facebook e WhatsApp l'ha approvata senza condizioni, evidenziando la natura dinamica del mercato, le limitate barriere all'ingresso e una concorrenza sufficiente[648].

L'analisi condotta mostra che molte ed eterogenee problematiche giuridiche si intersecano nei *big data* metaforicamente proprio come le complesse correlazioni e interazioni tra i dati che li compongono; non a caso *l'European Data Protection Supervisor* (EDPS), nell'*Opinion* 8/2016 del 23 settembre 2016 «*on coherent enforcement of fundamental rights in the age of big data*» afferma la necessità di porre particolare attenzione alle connessioni tra protezione dei dati personali, tutela della concorrenza e tutela dei consumatori, incentivando anche la relativa cooperazione tra le rispettive autorità competenti, in coerenza con quanto espresso nel 2014 con la *Preliminary Opinion «Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy»*[649].

Le questioni di responsabilità giuridica si fanno, poi, particolarmente spinose in caso di *Internet of Things* o di intelligenza artificiale, dove a seconda dei casi può cambiare la partecipazione umana all'azione e alla decisione che conduce a eventuali danni, è necessaria e complessa l'imputazione delle responsabilità e si aprono scenari circa la personalità giuridica di nuovi soggetti[650].

---

[648] Cfr. G. COLANGELO, *op. cit.*, p. 458 ss. Per quanto riguarda la messa a disposizione di API (*Application Programming Interfaces*), queste in astratto permettono di sviluppare programmi e servizi collegandosi con il servizio base, ma restano i vantaggi in capo a chi di fatto ha assunto una posizione di *big player* nel mercato.

[649] L'EDPS nell'*Opinion* del 2016 raccomanda l'istituzione di una *Digital Clearing House*, una struttura di coordinamento digitale, quale rete di partecipazione volontaria tra organismi di regolamentazione per permettere una collaborazione finalizzata alla tutela dei diritti e al contrasto degli abusi.

[650] V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 43 ss.

La raccolta e l'utilizzo dei *big data* ha carattere sovranazionale e non si limita ai confini territoriali: questo provoca anche una serie di problematiche giuridiche relative alla scelta della legge applicabile e della giurisdizione competente nel momento patologico del conflitto tra le parti. Generalmente, nelle controversie con i consumatori i *big player* prevedono l'applicazione della legge statunitense e la competenza dei tribunali della California, ma in realtà in ambito europeo tali clausole sono da considerare nulle e si applicano le norme europee: in particolare, i contratti sono sottoposti alla legge del Paese nel quale il consumatore ha la sua residenza abituale[651]; la competenza è del giudice del luogo di domicilio del consumatore, se l'azione è proposta dall'altra parte, mentre se l'azione è proposta dal consumatore questo può scegliere il giudice del luogo in cui è domiciliato o il giudice dello Stato in cui è domiciliata l'altra parte[652]. Naturalmente la questione cambia laddove la relazione non

---

[651] Art. 6, reg. (CE) 593/2008 (Roma 1), a condizione che questo sia anche il Paese nel quale il professionista svolge le sue attività o verso il quale dirige le sue attività e il contratto rientri in tale attività; in deroga le parti possono scegliere la legge applicabile, ma ciò non può avere il risultato di privare il consumatore della protezione garantita dalle disposizioni non derogabili del Paese in cui risiede abitualmente. In merito l'art. 36, comma 5, d.lgs. 206/2005 dispone la nullità di ogni clausola contrattuale che, prevedendo l'applicabilità al contratto di una legislazione di un Paese extracomunitario, abbia l'effetto di privare il consumatore della protezione assicurata dalle disposizioni del Codice, laddove il contratto presenti un collegamento più stretto con il territorio di uno Stato membro dell'Unione europea. In caso di responsabilità extracontrattuale, secondo il reg. (CE) 2007/864 (Roma II), di norma, ai sensi dell'art. 4, si applica la legge dello Stato in cui il danno è avvenuto, a prescindere dallo Stato in cui si è verificato l'evento che ha determinato il danno e a prescindere dallo Stato o dagli Stati in cui si verificano le conseguenze indirette di tale fatto.

[652] Sulla competenza giurisdizionale si applica l'art. 18, commi 1 e 2, reg. (CE) 1215/2012: «*L'azione del consumatore contro l'altra parte del contratto può essere proposta davanti alle autorità giurisdizionali dello Stato membro in cui è domiciliata tale parte o, indipendentemente dal domicilio dell'altra parte, davanti alle autorità giurisdizionali del luogo in cui è domiciliato il consumatore. L'azione dell'altra parte del contratto contro il consumatore può essere proposta solo davanti alle autorità giurisdizionali dello Stato membro nel cui territorio è domiciliato il consumatore*». Ai sensi dell'art. 66-bis, d.lgs. 206/2005 la competenza è del giudice del luogo di residenza o domicilio del consumatore, se ubicati nel territorio dello Stato. In caso di responsabilità extracontrattuale, cui si applica il reg. (CE) 2007/864 (Roma II), l'autorità giurisdizionale è quella del luogo in cui l'evento dannoso è avvenuto o può avvenire; il danno su Internet è considerato ubiquo e, di conseguenza, c'è una preferenza generale per il giudice del Paese in cui l'attore subisce la parte più importante del danno.

intercorra con un consumatore: in tal caso tendenzialmente si applicherà il contratto con i relativi termini e condizioni, a meno che non si configurino motivi di ordine pubblico o la mancanza di requisiti formali[653].

Le problematiche giuridiche mostrano con evidenza la costante tensione tra apertura e chiusura, tra accesso ed esclusione che caratterizza i *big data* e, più ampiamente, il concetto di dato e informazione[654].

I *big data* e la rilevanza attribuita ai numeri e ai calcoli mettono più profondamente in questione il diritto stesso, che riguarda valori (e non numeri) e che è prescrittivo (e non descrittivo), sfidando epistemologicamente il modo in cui il giurista vede la realtà[655]. Pertanto il contrasto è profondo e si configura tra teorie che poggiano sulla libera volontà e sulla scelta individuale e teorie deterministiche, che si basano su eventi passati, su circostanze "oggettive" e su probabilità[656].

In questo scenario complesso non bisogna indulgere nel vedere nei *big data* gli intrecci del nostro fato o, addirittura, affidarsi alle analisi predittive come a nuovi oracoli digitali capaci di determinare il nostro destino: emerge in modo incontrovertibile il ruolo fondamentale che devono giocare l'uomo e il diritto per governare la complessità di un mondo nuovo, fatto di algoritmi e di dati.

---

653 In caso di responsabilità extracontrattuale, come esaminato, si può applicare il reg. (CE) 2007/864 (Roma II). Sulla legge applicabile e sulla competenza giurisdizionale cfr. V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 49 ss.

654 Cfr. E. NUNZIANTE, *op. cit.*, p. 12, secondo la quale «nell'ambito dei Big Data, dunque, si palesano le contraddizioni intrinseche dell'informazione. Il flusso dei dati, infatti, è connotato da una costante tensione tra accesso ed esclusione. Ambedue i poli devono essere valutati da due prospettive, portatrici di interessi contrapposti: le imprese e i soggetti».

655 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 49 ss.

656 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 53 ss.

3.9. Iniziative e progetti a livello nazionale e internazionale

In considerazione del valore che rivestono, sono stati realizzati progetti a livello internazionale e nazionale che riguardano l'utilizzo e la promozione dei *big data*[657].

Al riguardo è molto significativo il progetto *GlobalPulse*, avviato dal Segretariato delle Nazioni Unite, che servendosi di *big data* monitora l'andamento del benessere della popolazione mondiale[658]. Nel progetto i *big data* sono valorizzati e interpretati come bene pubblico da utilizzare in modo sicuro e responsabile per lo sviluppo sostenibile e il benessere dell'umanità.

Rilevante è anche il progetto europeo *Big Data Europe*, di cui fa parte anche l'Italia, finalizzato a costruire una società della conoscenza basata sull'innovazione e sul rafforzamento della competitività dell'economia europea, permettendo alle imprese di realizzare prodotti e servizi innovativi grazie a una piattaforma tesa a tali fini[659]. Gli strumenti della piattaforma sono stati realizzati in considerazione delle maggiori sfide sociali del nostro tempo, individuate dalla Commissione europea nelle seguenti: sanità, alimentazione, energia, trasporti, clima, scienze sociali, sicurezza.

L'Italia è capofila del progetto europeo *SoBigData*, avviato nel 2015, con la *mission* di creare un *Social Mining & Big Data Ecosystem*, ossia un ecosistema integrato di dati, strumenti e competenze che renda possibili scoperte scientifiche e nuove applicazioni su tutte le dimensioni della vita sociale ed economica, partendo dai *big data* disseminati nella vita quotidiana e consentendo di eseguire avanzate ricerche e analisi sulle sfide emergenti poste dai *big data*[660]. «*The mission of the European Laboratory on Big Data Analytics and Social Mining is to perform advanced research and analyses on the emerging challenges posed by big data, namely the digital breadcrumbs of human activities continually sensed by the ICT systems that people use.*

---

657 Quelli citati nel paragrafo sono solo alcuni dei progetti in materia di *big data*, cui se ne affiancano altri come il progetto europeo BYTE (*The Big data roadmap and cross-disciplinarY community for addressing socieTal Externalities*).

658 Cfr. *www.unglobalpulse.org.*

659 Cfr. *www.big-data-europe.eu*.

660 Il sito del progetto è *www.sobigdata.eu*.

The extreme detail of these data is surprising and, ultimately, they are at the heart of the very idea of a knowledge society».

Basandosi su diverse infrastrutture nazionali consolidate, *SoBigData* apre nuovi percorsi di ricerca in diversi settori, tra cui matematica, ICT e scienze umane, sociali ed economiche, consentendo un facile confronto, riutilizzo e integrazione di *big data*, metodi e servizi, in nuove ricerche. Non solo rafforza gli esistenti *cluster* di eccellenza nel *social data mining*, ma crea anche una comunità paneuropea e interdisciplinare di *social data scientist*, promossa da una vasta formazione, da attività di *networking* e innovazione; come infrastruttura di ricerca aperta, promuove l'*open science*. Sebbene *SoBigData* sia rivolto principalmente ai bisogni dei ricercatori, i set di dati aperti e metodi e servizi *open source* forniti dall'infrastruttura di ricerca sono capaci di influenzare anche chi opera nell'industria e gli altri soggetti interessati (ad esempio organismi governativi, organizzazioni non-profit, finanziatori, *policy makers*). Il consorzio *SoBigData* è composto da 12 partner provenienti da 6 Paesi membri dell'Unione Europea (Italia, Regno Unito, Germania, Estonia, Finlandia, Paesi Bassi) e dalla Svizzera. Il progetto vede come capofila il CNR di Pisa ed è finanziato a livello europeo dal programma Horizon.

Un altro progetto italiano di estremo interesse è quello del Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Firenze, Km4city[661]: si tratta di una piattaforma che aggrega dati aperti e dati privati, statici e dinamici, aggiornati anche in tempo reale, che riguardano la Toscana, la Provincia e in particolare l'area di alcune città, quali Firenze, Empoli, etc.: il progetto è finalizzato a consentire l'interconnessione e la successiva interrogazione di dati da molte fonti diverse, come i vari portali della Regione Toscana e gli *open data* dei Comuni. Per le sue caratteristiche di interoperabilità, di interrogazione "smart" dei dati e di supporto per applicazioni ad uso pubblico e privato, Km4City costituisce un sistema di riferimento unitario per lo sviluppo di un "modello di conoscenza" della città e del territorio, per orientare le decisioni, ottimizzare i servizi e sostenere la crescita economica e sociale della comunità, oltre che per lo sviluppo di applicazioni[662]. Utilizzando i servizi e le API di

---

661 Cfr. *www.disit.org/km4city*.

662 I dati aggregati includono il grafo delle strade regionali, i dati meteo provenienti dal LAMMA (Consorzio tra Regione Toscana e CNR specializzato in meteorologia, climatologia, sistemi informativi

Km4City, è stata sviluppata l'applicazione "Km4city. Firenze dove, cosa", che mostra tutti i servizi vicini alla posizione dell'utente e permette di navigare nella città, trovando ristoranti, bagni, free WiFi, piste ciclabili, parchi, parcheggi, farmacie, bancomat, orari ed eventuali ritardi di alcune linee bus, etc.[663].

Il modello Km4City, che si avvale di tecniche di *big data* e *semantic computing*, viene ulteriormente sviluppato nel progetto Smart City nazionale Sii-Mobility e nel progetto europeo RESOLUTE H2020.

Sii-Mobility[664] è un progetto strategico nell'ambito *smart city* a livello nazionale, cofinanziato dal MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca), sviluppato in modo congiunto e coordinato da centri di ricerca e industrie con il supporto della pubblica amministrazione per la sperimentazione sul campo, svolta in Toscana e in altre Regioni italiane: si basa anche su *big data* ed è stato avviato il 1° gennaio 2016. Sii-Mobility prevede l'implementazione delle nuove tecnologie e l'utilizzo di piattaforme *social* per migliorare la mobilità urbana, ottimizzando i servizi; a tal fine, il progetto sviluppa soluzioni per gestire i sistemi di trasporto e di mobilità e fornire informazioni e servizi a cittadini, imprese e pubbliche amministrazioni.

RESOLUTE H2020[665], che vede come capofila il Dipartimento di Ingegneria dell'Informazione dell'Università degli Studi di Firenze, ha l'obiettivo di migliorare la gestione del sistema di trasporto urbano nelle città europee in situazioni di crisi, di calamità naturali e di altre emergenze, definire linee guida al riguardo e applicarle in fase sperimentale nei centri di Firenze e Atene: è stato avviato nel giugno 2015 ed è finanziato nell'ambito del programma europeo Horizon 2020. Il progetto prevede lo studio, l'analisi e la valutazione dello stato dell'arte in materia di resilienza, come base da cui poter ricavare dei modelli e delle simulazioni che possano prevenire e rendere più

---

geografici e geologia - *www.lamma.rete.toscana.it*), gli *open data* del Comune di Firenze e della Regione, i dati del gestore del traffico (posizione dei mezzi del trasporto pubblico locale, parcheggi, flussi), gli eventi in città, le *digital location* di Firenze, i servizi a livello regionale, accessibili tramite *servicemap.disit.org*.

663 I dati accessibili sono elencati in *www.disit.org/6726*.

664 Supporto all'interoperabilità integrata per i servizi ai cittadini e alla pubblica amministrazione; cfr. *www.sii-mobility.org*.

665 *RESilience management guidelines and Operationalization appLied to Urban Transport Environment*; cfr. *www.resolute-eu.org*.

preparati di fronte alle condizioni critiche, accrescere l'efficienza operativa delle operazioni dei soccorsi, ottimizzare l'assegnazione e l'utilizzazione delle risorse disponibili, riducendo al minimo incidenti, infortuni e danni ecologici.

In ambito pubblico, Istat, in considerazione della rilevanza per la statistica ufficiale dell'utilizzo di fonti di grandi dimensioni variamente strutturate, quali i *big data*, ha costituito nel 2013[666] una Commissione di Studio e nel 2016 il *Big Data Committee* con il compito, entro il 2020, di definire *policy* a supporto dell'uso dei *big data* per la statistica ufficiale e per monitorare e orientare le scelte sul tema[667]. In merito, è interessante il Parere sul PSN (Programma Statistico Nazionale) 2014-2016, aggiornamento 2015-2016 del Garante per la protezione dei dati personali (provvedimento n. 411 del 18 settembre 2014, doc. web n. 3458502), con cui è stato dato parere favorevole allo schema di PSN che prevedeva per la prima volta la possibilità di fare uso di *big data* di telefonia mobile, in via sperimentale, a fini statistici.

In merito all'importanza strategica dei *big data*, è opportuno richiamare anche la Task Force sull'Intelligenza Artificiale, promossa dall'Agenzia per l'Italia Digitale e dalla Presidenza del Consiglio dei ministri, formata da un coordinamento di 30 profili multidisciplinari e da una *community*, con il compito di analizzare le modalità di utilizzo di soluzioni e tecnologie di intelligenza artificiale nell'evoluzione dei servizi pubblici per migliorare il rapporto tra pubblica amministrazione e cittadini[668]. La Task Force, i cui lavori sono stati avviati nel settembre 2017, ha elaborato un Libro bianco sull'intelligenza artificiale al servizio del cittadino, dedicato ad esaminare gli ambiti di applicazione, le potenzialità e le opportunità dell'intelligenza artificiale nella pubblica amministrazione[669]. Il Libro bianco si compone di sfide e di raccomandazioni al Governo e alla pubblica amministrazione; in considerazione della centralità dei *big data* nelle soluzioni di intelligenza artificiale, è interessante osservare che una sfida è dedicata proprio al ruolo dei dati ed è centrata sulla creazione di condizioni che

---

666 Delibera Istat n. 20/PRES, 14 febbraio 2013.

667 Delibera Istat n. 4/PRES, 26 gennaio 2016.

668 Cfr. *ia.italia.it*.

669 La prima versione del Libro bianco è stata messa in consultazione tra febbraio e marzo 2018. Cfr. *libro-bianco-ia.readthedocs.io/it/latest*.

consentano all'intelligenza artificiale di utilizzare basi di dati costituite in maniera corretta e nelle quali siano assicurate consistenza, qualità e intelligibilità.

A livello di istituzioni italiane merita rilevare anche l'esperimento di analisi previsionale basata sui *big data* condotto da Inps per stimare il ricorso alla cassa integrazione guadagni da parte delle aziende, che ha fornito un risultato esatto al 93,1%.

Le iniziative e i progetti in materia di *big data* mostrano l'interesse verso il fenomeno da parte di soggetti pubblici e privati e le possibili sinergie tra i due mondi nell'utilizzo dei *big data* a fini di evoluzione e progresso non solo tecnologico, ma umano.

Capitolo 4

Tutela e bilanciamento dei diritti nel governo dei dati

SOMMARIO: 4.1. Il diritto all'esistenza digitale e al governo dei dati. – 4.2. Il diritto alla conoscenza. – 4.3. Il diritto all'identità e il diritto all'oblio. – 4.3.1. Il diritto all'identità: identità personale e identità digitale. – 4.3.2. Il *right to be forgotten*. – 4.3.3. Bilanciamento tra diritti: *right to know*, identità, oblio. – 4.4. Il diritto d'autore nella *digital age*. – 4.4.1. La disciplina italiana del diritto d'autore online. – 4.4.2. Il contesto internazionale. – 4.4.3. La proprietà intellettuale nel governo dei dati. – 4.4.4. Diritto d'autore e *right to know*: alla ricerca dell'equilibrio.

4.1. Il diritto all'esistenza digitale e al governo dei dati

Dal momento che l'esistenza digitale si basa sui dati, la tutela e il bilanciamento dei diritti nel governo dei dati stessi è un aspetto imprescindibile di cui deve occuparsi il diritto per riuscire a proteggere la persona nella regolazione delle tecnologie informatiche. Peraltro, come viene rilevato in dottrina, il processo di creazione della conoscenza pubblica, che si genera attraverso la produzione e la circolazione di dati e informazioni, è capace di potenziare i presupposti su cui si basa l'esercizio della cittadinanza digitale e il soddisfacimento delle istanze collegate[670].

L'impatto delle tecnologie informatiche, come già evidenziato, è tale da superare il limite ontologico di mero "strumento" per porsi quale inedito mezzo poliedrico, che non consente soltanto l'esercizio di uno o più diritti collegati a un aspetto specifico dell'esistenza, ma permette più ampiamente di svolgere la propria esistenza stessa, quella digitale. Non si tratta solo del diritto di accesso alla rete, prodromico a tutti gli altri e su cui si sono concentrati studi e riflessioni dottrinarie nonché i progetti di

[670] P. MARSOCCI, *op. cit.*, p. 16.

revisione costituzionale[671], ma sempre più emergono anche i diritti e le libertà "nella rete", ossia l'uso effettivo che si può fare dell'accesso a Internet e più ampiamente delle tecnologie informatiche[672], che si traduce nella tutela di diversi diritti individuali, espansione delle classiche libertà costituzionali o frutto inedito della nuova realtà[673]. Di conseguenza lo stesso diritto di accesso si traduce più propriamente, come suggerisce Rodotà, nell'«espressione di un diverso modo d'essere della persona nel mondo» e, in tal modo, configura una «sintesi tra una situazione strumentale e l'indicazione di una serie tendenzialmente aperta di poteri che la persona può esercitare in rete»[674].

Allora si può arrivare a parlare metaforicamente di un diritto più ampio e pervasivo, "il diritto all'esistenza digitale", che è parte integrante e sostanziale, difficilmente separabile e distinguibile dell'esistenza *tout court* e poggia sui principi

---

671 *Supra*, cap. 1, § 3. A. MASERA - G. SCORZA, *op. cit.*, p. 12: «Non disporre effettivamente del diritto di accedere a Internet, nell'era dell'accesso – come Jeremy Rifkin ha definito l'età che stiamo vivendo –, significa essere individui, persone, cittadini in una condizione permanente di semilibertà, di inferiorità sociale, culturale, politica ed economica, impossibilitati a partecipare alla vita della propria comunità, eremiti analogici in un mondo digitale».

672 Cfr. L. CUOCOLO, *op. cit.*, p. 276 ss., secondo cui le qualificazioni come diritto umano dell'accesso a Internet «rischiano di produrre l'effetto-paradosso di un ottimismo della volontà non supportato da alcuna garanzia concreta» (p. 282); tale diritto, in mancanza di un riconoscimento positivo da parte dell'ordinamento, non è giustiziabile, come invece devono essere i diritti per essere tali. Per tali ragioni secondo l'Autore è preferibile inquadrare il diritto di accesso a Internet come diritto sociale a prestazione, strumentale alla realizzazione di altri diritti fondamentali, che determina la pretesa del cittadino-utente nei confronti dei poteri pubblici di ottenere le infrastrutture necessarie, in condizioni non discriminatorie e con un livello qualitativo adeguato; secondo l'Autore tale diritto trova fondamento nella clausola aperta dell'art. 3, comma 2, e nell'art. 117, comma 2, lett. m) della Costituzione.

673 G. AZZARITI, *op. cit.*; P. PASSAGLIA, *Diritto di accesso a Internet e giustizia costituzionale. Una (preliminare) indagine comparata*, cit., p. 82 parla di tutela a "geometria variabile", dal momento che «se l'accesso ad Internet è un diritto strumentale all'esercizio di altri, la sua natura e il suo rango, e, quindi, il grado di tutela ad esso approntata non è determinabile a priori ed in astratto, ma deve essere commisurato al tipo di situazione specifica che l'accesso medesimo è volto a tutelare: al crescere del rilievo del diritto (o del dovere) al cui esercizio è funzionale, la protezione del diritto di accesso si rafforza»; nello stesso senso, L. NANNIPIERI, *op. cit.*, p. 23 secondo cui dall'analisi dell'accesso ad Internet, in relazione alla possibilità di esercitare un particolare diritto (come il diritto alla salute, nel caso del fascicolo sanitario elettronico, o il diritto al voto, in caso di voto elettronico), appare evidente che il rango ad esso attribuito debba corrispondere a quello della specifica situazione giuridica rispetto a cui è strumentale.

674 S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 384.

fondamentali della dignità e dello sviluppo della persona[675]. Nelle attuali democrazie, a ben vedere, il diritto all'esistenza digitale altro non è che il diritto all'esistenza nell'era contemporanea, che non ammette di essere offline se non per propria scelta e si riassume in un attuale *navigo ergo sum*[676].

Il diritto all'esistenza digitale si pone come ombrello sotto il quale dare ospitalità ai diversi diritti nei quali si traducono la libertà informatica e l'*habeas data*, che involgono la dimensione individuale, ma anche quella sociale e collettiva della partecipazione alla società democratica.

In questo scenario si pone una chiara responsabilità pubblica nel garantire ciò che è componente della cittadinanza e, di conseguenza, precondizione della stessa democrazia[677].

I diritti afferenti alla realtà e all'esistenza digitale, come esaminato, trovano tutela in interpretazioni evolutive della nostra Carta costituzionale, talvolta in disposizioni di rango primario e in una Dichiarazione dal valore culturale e politico, seppur certo non giuridico[678]. Sono diritti spesso "senza legge", basta pensare al diritto di accesso a Internet, dal momento che è insufficiente l'eventuale normazione nazionale presente e si pongono complesse problematiche nell'individuare l'adeguato potere costituente transnazionale[679].

Di conseguenza, i diritti digitali finiscono per incontrare una tutela nel momento patologico del conflitto, grazie alle interpretazioni e al ruolo supplente svolto dai giudici

---

675 T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 688, secondo cui il principio fondamentale della dignità «costituisce il fondamento costituzionale di tutti i diritti strettamente connessi allo sviluppo della persona».

676 Il brocardo è diversamente declinabile in formule analoghe: T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 60 parla di *digito ergo sum* e G. SCORZA, *op. cit.* utilizza *accedo ergo sum*, dal momento che nella società dell'informazione accedere significa esistere.

677 S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 387 ss.: «Si colgono così non le peculiarietà di una cittadinanza digitale separata, ma l'intima attitudine di questa a contribuire incessantemente alla definizione/costruzione di quel complessivo patrimonio di diritti che si proietta al di là d'ogni luogo, e che appunto chiamiamo cittadinanza, senza aggettivi» (p. 388).

678 *Supra*, cap. 1, § 3. Cfr. A. MORELLI, *I diritti senza leggi*, in *Consulta online*, fasc. 1, 2015, pp. 1-25.

679 Cfr. D. POLETTI, *Il c.d. diritto alla disconnessione nel contesto dei "diritti digitali"*, in *Responsabilità civile e previdenza*, fasc. 1, 2017, pp. 8-26.

delle Corti sovranazionali, dimensionalmente più adeguati alla connotazione globale che caratterizza l'esercizio degli stessi, ma ontologicamente confinati nella fattispecie da esaminare e infungibili rispetto al ruolo del legislatore nell'offrire un riconoscimento "generale e astratto"[680]. Le Corti permettono di far emergere istanze ed esigenze della società prive di riconoscimento e tutela, agevolando evoluzioni giuridiche: questi diritti che emergono a livello giurisdizionale esigono, però, per il loro concreto ed effettivo esercizio, interventi e prestazioni da parte dei poteri pubblici[681], come peraltro sembra indicare l'art. 117, comma 2, lett. m), Cost., e dunque necessitano del diritto positivo; è proprio dello Stato costituzionale e degli ordinamenti democratici riconoscere e tutelare i diritti fondamentali e colmare le eventuali lacune normative dell'ordinamento[682].

Alla luce delle evoluzioni esaminate che configurano la nostra contemporaneità come società della conoscenza e degli algoritmi, come *data society*, il diritto all'esistenza digitale significa necessariamente anche diritto al governo dei dati, da

---

680 Cfr. A. MORELLI, *I diritti senza leggi*, cit., p. 16 ss., che, nell'affidarsi al momento giurisdizionale, evidenzia il rischio di un abbassamento del livello di tutela dei diritti, ancor più per quelli "nuovi", dal momento che il giudice è confinato nei limiti posti dal principio della domanda, è condizionato necessariamente dal caso oggetto di giudizio e non può, come il legislatore, dare un riconoscimento generale e astratto, ma deve limitarsi ad applicare il diritto nei casi particolari e concreti. Del resto le figure del giudice e del legislatore non sono fungibili, ma entrambe necessarie alla democrazia costituzionale. Secondo l'Autore, «non si può trascurare la distorsione che l'ampliamento, di fatto, delle competenze degli organi giurisdizionali provoca rispetto al modello di Stato costituzionale» (p. 31), dal momento che la giurisdizione è parte dell'ordinamento giuridico statale e ha la valenza "negativa" degli organi di garanzia; ciò provoca anche una forma di disuguaglianza tra chi può permettersi l'accesso a tali strumenti e chi, invece, non ha i mezzi necessari e pone problemi relativi alla responsabilità degli stessi organi di garanzia.

681 Cfr. A. MORELLI, *I diritti senza leggi*, cit., p. 17 ss. che configura i nuovi diritti come «diritti a prestazione, aspirando ad una legislazione attuativa utile a consentirne l'esercizio» (p. 19).

682 Cfr. A. MORELLI, *I diritti senza leggi*, cit., p. 17 ss. L'art. 117, comma 2, lett. m), Cost. prevede l'esercizio della funzione legislativa esclusiva statale per la determinazione dei "livelli essenziali" delle prestazioni concernenti i diritti sociali e civili. Basta pensare al diritto di accesso a Internet, che nella sua veste di diritto sociale necessita di adeguati interventi atti ad eliminare problematiche come il *digital divide*. L'Autore richiama l'autorevole dottrina secondo cui il passaggio dalla "certezza del diritto" alla "certezza dei diritti" caratterizzerebbe il processo d'integrazione sovranazionale in corso, ma per l'Autore «all'ampliamento delle garanzie delle libertà non parrebbe seguire una proporzionale valorizzazione delle esigenze dell'eguaglianza» (p. 29).

intendersi come tutela delle libertà e dei diritti nelle diverse fasi di gestione dei dati; la gestione dei dati, merita ripeterlo, caratterizza ogni attività digitale e permea quindi la realtà digitale stessa[683].

Nel governo dei dati, di conseguenza, garantire effettività ai diritti significa affrontare complessi bilanciamenti tra le dimensioni che si intrecciano e confliggono nella realtà digitale. Tensioni diverse, infatti, muovono il diritto a conoscere e il diritto a non essere (più) conosciuti (il diritto all'oblio), parte significativa del proprio diritto all'identità, il diritto all'informazione e alla condivisione da una parte e il diritto d'autore e al riconoscimento della proprietà intellettuale dall'altra, il *right to know* e il diritto al riutilizzo da un lato e il diritto alla protezione dei dati personali dall'altro.

Una connessione intricata di dati dà luogo a una speculare intricata connessione tra diritti indivisibili e difficilmente gerarchizzabili[684], cui è necessario rivolgere l'attenzione perché nell'era dei dati qui si gioca la sfida delle libertà.

In una realtà in cui ogni operazione si basa su dati e in cui i processi si fondano su calcoli e algoritmi, l'analisi della protezione da offrire ai diritti coinvolti nel governo dei dati è questione giuridica determinante per realizzare un'efficace tutela della persona.

Le problematiche da risolvere e gli equilibri da generare, peraltro, trovano diverse sfumature, gradazioni e intensità a seconda dei dati oggetto di considerazione: come esaminato, ci troviamo di fronte a *closed data* conoscibili grazie a strumenti di trasparenza proattiva (la pubblicazione) e reattiva (le diverse forme di accesso documentale, civico semplice e civico generalizzato), a *open data* con la consacrazione di un diritto al riutilizzo e la realizzazione di una trasparenza attiva a beneficio della

---

683 È consapevole della rilevanza dei dati la comunicazione della Commissione europea, «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017: «con la sempre maggior penetrazione delle trasformazioni basate sui dati nell'economia e nella società, crescenti quantità di dati sono generate da macchine o processi supportati da tecnologie emergenti, quali l'internet delle cose (IoT), le fabbriche del futuro e i sistemi autonomi connessi». Di conseguenza, «le questioni dell'accesso e della trasmissione in relazione ai dati generati dalle macchine o dai processi sono dunque al centro dell'emergere di un'economia basata sui dati e richiedono un'attenta valutazione».

684 S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 394 parla, accanto all'indivisibilità e alla non gerarchizzabilità dei diritti online, di una cittadinanza sempre più "orizzontale" promossa proprio dalla rete che rifiuta le gerarchie.

collettività e a *big data* caratterizzati attualmente da una congenita rischiosa asimmetria di informazione e del relativo potere tra i "signori dei dati" e tutti gli altri.

In queste correlazioni di dati e bilanciamenti di diritti emerge il ruolo dei diversi soggetti che si muovono nel governo dei dati: la persona a cui afferiscono i dati, che è al tempo stesso consumatore e parte debole del rapporto con i privati, ma anche cittadino e protagonista (almeno sulla carta) dell'attenzione e delle riforme delle amministrazioni pubbliche; le istituzioni digitali e aperte, che ontologicamente devono interessarsi del governo dei dati sia in quanto produttrici e titolari di dati, sia in quanto possibili fruitrici e riutilizzatrici dei *big data* dei privati; le grandi aziende private, i cui imperi si basano su *big data* sempre più grandi[685], potenti e invasivi, capaci di "dare anima" agli oggetti (*Internet of Things*), ma anche a nuovi soggetti (intelligenza artificiale) e idonei a incidere su utenti sempre più piccoli nel loro consenso inconsapevole fornito per "pagare" con i propri dati servizi ritenuti ormai irrinunciabili per l'esistenza digitale. In questo scenario il diritto si trova sorpreso e impreparato nel difficile compito di regolare un mondo senza confini, senza sovrani, senza limiti.

Il governo dei dati impone l'analisi dei diritti che sono maggiormente esposti e la ricerca dei bilanciamenti da compiere perché in questi si annida la possibilità di dare effettiva tutela ai diritti stessi, si gioca la dignità e lo sviluppo della persona nell'era digitale, si gioca più ampiamente la capacità dell'uomo di controllare i dati e gli algoritmi senza finire per esserne controllato e soggiogato.

4.2. Il diritto alla conoscenza

Il *right to know* è il diritto che forse più di ogni altro caratterizza l'attuale *data society*: i dati permettono di avere informazioni che, a loro volta, laddove correttamente analizzate e interpretate, consentono di generare conoscenza. Non a caso si parla anche di *knowledge society*, come si è già avuto modo di esaminare nei precedenti capitoli.

685 Al riguardo, però, cfr. G. AZZARITI, *op. cit.*, p. 3, secondo cui «proprio WikiLeaks – ma non solo – dimostra come le banche dati, su cui s'è costruito il potere di molti potenti, rischiano di rivoltarsi contro gli stessi detentori del potere informatico».

Il diritto alla conoscenza è mutato profondamente nel corso del tempo ed ha assunto nuovi volti.

Oggi, rispetto al passato, è un diritto "globale" che non incontra confini geografici e statuali, è capace di superare i tradizionali limiti della memoria grazie alle tecnologie digitali[686] ed è privo di condizionamenti temporali, dal momento che la fruizione è sostanzialmente immediata, può avvenire in ogni luogo e in ogni momento. È un diritto che ha la capacità di scardinare e spostare il potere: la conoscenza non è più solo appannaggio delle istituzioni pubbliche, ma diventa terreno di conquista dei giganti della rete, nuovi potenti detentori di dati e informazioni, imprevisti custodi del passato, del presente e, anche, del futuro (si pensi ai *big data* e alle loro predizioni). Del resto conoscere è potere: l'ampiezza e la profondità del diritto alla conoscenza determina la libertà individuale e il volto delle democrazie[687]. Sotto tale profilo, il mondo digitale è ontologicamente non adatto ai segreti e, al contrario, è fedele alleato della trasparenza e dell'apertura, ma, nonostante questo, può essere proprio l'intervento umano a creare nuove asimmetrie e forme di "segreto"[688].

Nell'era digitale, insieme al *right to know*, cambia anche la configurazione della correlata cultura, non più legata a oggetti fisici, ma all'accesso a servizi digitali in cui l'informazione, in grandi quantità, è sempre reperibile facilmente. Peraltro in rete molti

---

686 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 18 evidenzia «la diffusione capillare e su larga scala di supporti di memoria che possono contenere milioni d'informazioni in un piccolo spazio fisico e che possono relazionarsi con un tipo di rete, Internet, che garantisce la diffusione di documenti anche segreti in pochi istanti e li mantiene *per sempre* a disposizione di chiunque fosse interessato a consultarli».

687 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 18: «L'idea di segreto, con le teorie sociali e politiche ad essa strettamente correlate, è da sempre vista come lo strumento essenziale, caratteristico e irrinunciabile per ottenere il potere e per il suo mantenimento».

688 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 18 ss.; secondo l'Autore nell'era digitale, seppur sia uno dei fattori più difficili da mantenere, il segreto è comunque cercato con sempre maggiore intensità, ma rischia di diventare anche una possibile vulnerabilità dei centri di potere, potendo venire svelato grazie proprio all'utilizzo delle tecnologie. La trasparenza, d'altra parte, soprattutto laddove radicale, non ha solo i vantaggi del maggior controllo pubblico, della partecipazione e della democrazia, ma può prestarsi anche a usi distorti e fraintendimenti e può minare la sovranità e la sicurezza nazionale.

contenuti sono liberi e facilmente condivisibili e questo permette una democratizzazione dell'accesso alla cultura stessa, anche se non mancano nuove modalità per detenere il potere. Il sapere non è più orientato dalle *élites* intellettuali, ma dalla potenza degli algoritmi; il parere di ognuno vale quanto quello dell'altro, anche se esperto, con nuovi e inediti rischi di appiattimento[689].

Il più grande spazio pubblico dell'umanità, la rete, permette a tutti e ciascuno di vivere una libertà inedita di esprimersi, di informare e di informarsi e permette lo sviluppo della persona e il progresso della società; questo nuovo assetto ha inevitabilmennte i suoi punti di forza e le sue debolezze[690]. La conquistata libertà mostra, infatti, anche la faccia negativa, che si nutre delle *fake news*, delle bufale e delle manipolazioni, il volto oscuro che prende corpo nelle molestie, nelle discriminazioni, nel bullismo, nella violenza e nell'odio online[691].

In considerazione del ruolo che rivestono, spetta alle istituzioni il difficile compito di governare i dati e la correlata conoscenza, con la connessa responsabilità verso le generazioni presenti e future di sottrarre al mercato questi beni identificativi dell'uomo contemporaneo e dei suoi diritti. Per questo quando si parla di diritto a conoscere vengono in gioco i pubblici poteri e il rapporto tra governanti e governati: i poteri pubblici sono i detentori di una grande e significativa mole di dati e, in ogni caso, anche rispetto ai dati detenuti dai privati, sono i soggetti deputati al governo dei dati stessi, da esercitare per mezzo di regole idonee a tutelare e bilanciare i diritti e le libertà che vengono in gioco.

---

689 A. MASERA - G. SCORZA, *op. cit.*, p. 13 ss.

690 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 131: «In questo spazio tutti e ciascuno acquistano la possibilità di prendere la parola, acquisire conoscenze, creare idee e non solo informazioni, esercitare il diritto di critica, discutere, partecipare alla vita pubblica, costruendo così una società diversa, nella quale ciascuno può rivendicare il suo diritto ad essere ugualmente cittadino»; T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 683: «è cambiato il senso e il significato della libertà di manifestazione del pensiero nell'era di Internet. Perché ha consentito il recupero della nozione di manifestazione del pensiero come libertà individuale, cioè senza "filtri", ovvero senza mediazioni di sorta, un *open network*».

691 Tali tematiche non saranno oggetto del presente lavoro. Al riguardo si rinvia alla lettura di G. ZICCARDI, *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina, Milano, 2016; M. GRANDI, *Far web. Odio, bufale, bullismo. Il lato oscuro dei social*, Rizzoli, Milano, 2017; G. PITRUZZELLA - O. POLLICINO - S. QUINTARELLI, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, Milano, 2017.

In questo contesto, grazie alla costante e intensa evoluzione tecnologica, il diritto alla conoscenza ha vissuto l'evoluzione ampia e profonda esaminata nei precedenti capitoli, che ha permesso a questo diritto di essere "polimorfo", di assumere nuove connotazioni e potersi realizzare grazie a nuovi strumenti[692].

Il web diventa *web of data*, la trasparenza e la correlata conoscenza assumono volti diversi e si traducono in strumenti differenti, che attengono alle diverse configurazioni assunte dai dati nella contemporaneità. Di conseguenza, insieme alle nuove declinazioni dei dati evolve il diritto a conoscere: rispetto ai *closed data* il *right to know* si traduce negli strumenti della trasparenza proattiva (la pubblicazione) e reattiva (le varie forme di accesso) che permettono di conoscere dati, informazioni e documenti detenuti dalle istituzioni pubbliche[693]; in relazione agli *open data* e alla trasparenza attiva, il diritto a conoscere si sposa con il diritto "attivo" al riutilizzo dei dati, in linea con il "matrimonio" che lega trasparenza e apertura[694]; nei confronti dei *big data*, capaci di evolvere l'essenza stessa dei dati e dei loro usi, il *right to know* diventa anche "diritto a predire", a conoscere non solo il presente, ma anche il futuro e necessita di riequilibri per non essere appannaggio solo di *big player* e poteri pubblici, lasciando l'individuo in uno stato di mancata conoscenza e inconsapevolezza in merito a ciò che permettono di fare i dati che in vario modo lo riguardano[695].

Nella contemporanea *data society* il diritto alla conoscenza, quale libertà di espressione e libertà di informarsi, ossia quale «*libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere attraverso ogni mezzo e senza riguardo a frontiere*»[696], nelle sue declinazioni ed interpretazioni evolutive, trova fondamento

---

692 Al riguardo, M. BOMBARDELLI, *Fra sospetto e partecipazione: la duplice declinazione del principio di trasparenza*, in *Istituzioni del Federalismo*, fasc. 3-4, 2013, pp. 670-671 rileva nella normativa sulla trasparenza il rischio di una sorta di "voyeurismo" amministrativo da parte di chiunque acceda al web, con il conseguente pericolo di un eccesso di informazione disponibile che può diventare rumore e causare un generico sospetto nei confronti delle amministrazioni, invece di favorire la buona amministrazione.

693 *Supra*, capitolo 2.

694 *Supra*, capitolo 3.

695 *Supra*, capitolo 3.

696 Si esprime così l'art. 19 della Dichiarazione universale dei diritti dell'uomo del 1948 e, nello stesso senso, l'art. 19 del Patto internazionale sui diritti civili e politici del 1966.

nell'art. 19 della Dichiarazione universale dei diritti dell'uomo del 10 dicembre 1948 e nell'art. 19 del Patto internazionale sui diritti civili e politici del 16 dicembre 1966. Il diritto è previsto nell'art. 10 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) del 4 novembre 1950 e nell'art. 11 della Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000[697]. In tali atti sono tutelate ampiamente le due anime che connotano la libertà d'espressione: non solo la libertà d'opinione e di comunicare informazioni o idee, ma anche la libertà di ricevere informazioni o idee e, quindi, il *right to know*, senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Significativamente l'art. 10 della CEDU chiarisce il carattere relativo e non assoluto della tutela, che è soggetta a limitazioni, restrizioni e sanzioni, previste dalla legge e necessarie, in una società democratica, alla tutela di altri interessi, diritti e istanze parimenti oggetto di protezione[698].

Nel nostro ordinamento il diritto alla conoscenza risulta fondato indirettamente su base costituzionale: quale interesse del cittadino a "sapere", oltre che libertà di informare e di informarsi di cui all'interpretazione sistematica ed evolutiva dell'art. 21 C. [699], risulta necessario per la formazione di una corretta opinione pubblica e per l'attuazione dei principi di democrazia e sovranità popolare di cui all'art. 1 Cost.[700], per

---

697 La libertà d'espressione è prevista anche dall'art. 13 della Convenzione americana dei diritti umani del 22 novembre 1969.

698 L'art. 10 nel secondo comma precisa i limiti: «*L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario*». Cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, in *Diritti umani e diritto internazionale*, fasc. 3, 2016, p. 554 ss.

699 Sulla libertà di informare e di essere informati e l'art. 21 Cost. cfr., *inter alia*, A. M. GAMBINO - A. STAZI, *Diritto dell'informatica e della comunicazione*, II ed., Giappichelli, Torino, 2012, p. 17 ss. e R. RAZZANTE, *op. cit.*, p. 1 ss.

700 Tale accezione afferisce alla concezione della democrazia come *«governo del potere pubblico in pubblico*», come sosteneva N. BOBBIO, *Il futuro della democrazia*, Einaudi, Torino, 1995, p. 76. Secondo

lo sviluppo della persona di cui all'art. 2 Cost., per l'eguaglianza di cui all'art. 3 Cost. e per lo sviluppo della cultura di cui all'art. 9[701]: il *right to know* si fonda sulla lettura sistematica di un combinato disposto di norme costituzionali. Nei confronti dei poteri pubblici, il diritto si collega al principio di trasparenza, fondato su un insieme di principi costituzionali che caratterizzano l'agire delle amministrazioni pubbliche[702]: a livello normativo il diritto a conoscere, reso possibile dai principi di trasparenza e *openness*, viene disciplinato dalla normativa sulla trasparenza contenuta in larga parte nel d.lgs. 33/2013, come modificato dal d.lgs. 97/2016, e nel d.lgs. 82/2005[703].

In tale quadro il requisito della qualità della trasparenza, previsto nella normativa (art. 6, d.lgs. 33/2013) si collega strettamente al principio di sicurezza giuridica, che chiama le amministrazioni ad agire razionalmente e in modo univoco: il cittadino deve poter fare affidamento sulla sicurezza giuridica, corollario dello Stato di diritto[704].

Parla di «diritto alla conoscenza e all'educazione in rete» l'art. 3 della Dichiarazione dei diritti in Internet, che correla strettamente il diritto alla conoscenza, l'educazione in rete e la cultura digitale al diritto di accesso a Internet, considerandoli parimenti essenziali, dal momento che ne costituiscono anche parte ed evoluzione. A tale proposito viene evidenziato il ruolo dei poteri pubblici, esplicitando il dovere in capo alle istituzioni di «assicurare la creazione, l'uso e la diffusione della conoscenza in rete intesa come bene accessibile e fruibile da parte di ogni soggetto». La Dichiarazione è consapevole anche di dover garantire protezione ad altri interessi tutelati dall'ordinamento, che possono "scontrarsi" con questo, come il diritto d'autore, la

---

I. NICOTRA, *La dimensione della trasparenza tra diritto alla accessibilità totale e protezione dei dati personali: alla ricerca di un equilibrio costituzionale*, in *federalismi.it*, fasc. 11, 2015, p. 4 il principio di trasparenza «si pone quale presupposto retrostante alla disposizione contenuta nell'art. 1 della Costituzione, diretta conseguenza del principio di sovranità popolare. La spettanza della sovranità al popolo esige strumenti che rendono effettiva la partecipazione dei cittadini alle scelte politiche fondamentali che non possono esaurirsi nella selezione dei rappresentanti nei vari livelli di governo, ma consentire, altresì, un controllo sull'operato degli stessi».

701 M.F. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, in *Il diritto di famiglia e delle persone*, fasc. 2, 2015, pp. 740-758.

702 Art. 1, d.lgs. 33/2013; *supra*, cap. 2, § 4.

703 *Supra*, cap. 2 e cap. 3.

704 Cfr. I. NICOTRA, *op. cit.*, p. 5, che richiama la sentenza della Corte costituzionale, 26 luglio 1995, n. 390.

proprietà intellettuale e, quindi, i diritti derivanti dal riconoscimento degli interessi morali e materiali legati alla produzione di conoscenze.

Il diritto alla conoscenza si lega anche al diritto all'educazione e alla cultura digitale ed è per questo che la Dichiarazione dei diritti in Internet esplicita il diritto di ogni persona di essere posta in condizione di acquisire e aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei diritti e delle libertà fondamentali. A tale diritto corrisponde la prestazione sociale cui sono tenute le istituzioni pubbliche, che devono promuovere l'educazione in rete, in particolare attraverso il sistema dell'istruzione e della formazione, e rimuovere ogni forma di ritardo culturale. La cultura digitale è, infatti, letta come condizione necessaria e prodromica per il conseguimento dei principi e dei valori costituzionali, in particolare «per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla rete tra attori economici, Istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui».

Come emerge anche dalle norme e dagli atti che lo regolano, la maggiore *vis* e l'ampiezza che connota il diritto a conoscere nell'era digitale provocano conflitti e difficili bilanciamenti con un insieme di diritti e libertà che sono particolarmente coinvolti dal governo dei dati, come il diritto all'identità e il diritto all'oblio, il diritto d'autore e il diritto alla protezione dei dati personali, oggetto dell'analisi dei successivi paragrafi e del prossimo capitolo.

4.3. Il diritto all'identità e il diritto all'oblio

Il nostro "io" digitale è composto dai dati.

Di conseguenza il governo dei dati deve confrontarsi e garantire la tutela dell'identità digitale e il collegato diritto all'oblio, chiedendosi quali siano e quali dovrebbero essere le condizioni da rispettare nei processi di raccolta ed elaborazione dei dati da parte degli algoritmi[705].

[705] Cfr. M. MARTONI - M. PALMIRANI, *Internet e identità personale*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma,

Per poter analizzare tali aspetti è necessario comprendere il significato di identità e oblio, con le evoluzioni che hanno avuto con l'avvento delle tecnologie digitali e della rete, e come tali diritti siano protetti dall'ordinamento.

4.3.1. Il diritto all'identità: identità personale e identità digitale

La tutela dei dati significa protezione dell'identità dinamica e aggiornata della persona nella rete.

Per comprendere il concetto è necessario fare riferimento all'identità personale, da cui l'identità digitale promana, anche se è bene precisare subito che le due declinazioni (personale e digitale) finiscono oggi per sposarsi nel concetto unitario di identità, esattamente come la realtà analogica e quella digitale perdono i confini che le definiscono e collassano nel semplice concetto di realtà.

L'identità personale è «la formula che riassume ciò che rende una persona ciò che essa è»[706], ossia «il diritto che ha ciascuna persona di essere se stessa, cioè di distinguersi e di essere distinta»[707] e si concretizza, pertanto, nell'espressione di una "verità" attinente all'individuo, ossia il fatto non controvertibile che ognuno è simile, ma non uguale agli altri: ognuno ha una propria individualità e ha il relativo interesse alla reale rappresentazione della sua personalità e dei suoi comportamenti. Nel conoscere questa "verità" il diritto ha riguardo sia al soggetto in se stesso sia al modo d'essere del soggetto nella vita di relazione[708].

Il diritto all'identità personale conosce due accezioni giuridiche: un'accezione storica, di valenza essenzialmente pubblicistica, si riferisce ai "segni identificativi" di

---

2015, p. 295 ss., che ritengono questi interrogativi necessari per non incorrere in un vincolo deterministico moderno; «noi siamo i nostri dati (*habeas data*) che composti in rete definiscono le nostre identità digitali» (p. 301).

706 Così G. PINO, *L'identità personale*, in S. RODOTÀ - M. TALLACCHINI (a cura di), *Ambito e fonti del biodiritto*, vol. I del *Trattato di Biododiritto* diretto da S. RODOTÀ - P. ZATTI, Giuffrè, Milano, 2010, p. 297.

707 Così M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, in *Il diritto di famiglia e delle persone*, fasc. 3, 2016, pp. 949-968.

708 Cfr. M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, cit., pp. 949-968.

un soggetto, rilevabili in modo oggettivo, come i dati anagrafici che, in tal modo, permettono ai poteri pubblici una sicura identificazione dei consociati; l'altra, maggiormente moderna, fa riferimento non solo ai dati oggettivi di identificazione, ma alla corretta proiezione sociale della personalità dell'individuo, ossia all'immagine, socialmente mediata e oggettivata, del soggetto[709]. Ai fini della presente analisi si terrà in considerazione questa seconda accezione.

L'ordinamento giuridico è chiamato, pertanto, a garantire "il diritto ad essere se stessi", a tutelare e non veder travisare una corretta e reale rappresentazione della personalità dell'individuo e dei suoi comportamenti nel contesto sociale. Peraltro, anche gli altri consociati hanno interesse a considerare ciascuno nella sua peculiare individualità e non in una diversa. Una distorsione della personalità integra la violazione di quella "verità" protetta dal diritto ed è idonea a produrre un danno ingiusto[710].

Nella costruzione del diritto all'identità personale un ruolo significativo è stato giocato dalla giurisprudenza: è il caso della sentenza della Corte di Cassazione 22 giugno 1985, n. 3769, che parla dell'identità personale come di «una formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni (morali, sociali, politiche, intellettuali, professionali, ecc.)», che comporta la corretta rappresentazione della persona e l'interesse conseguente «a non vedersi all'esterno alterato, travisato, offuscato, contestato il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale». Particolarmente rilevanti, al riguardo, la sentenza della Corte costituzionale del 3 febbraio 1994, n. 13, che ha configurato l'identità personale quale diritto garantito dall'art. 2 Cost. e, in specifico, «il

---

709 V. RICCIUTO, *Diritto di rettifica, identità personale e danno patrimoniale all'uomo politico (nota a Trib. Roma, 7-11-1984)*, in *Il diritto dell'informazione e dell'informatica*, 1985, p. 225 ss.; G. BAVETTA, voce *Identità (diritto alla)*, in *Enciclopedia del diritto*, vol. XIX, Milano, 1970, pp. 953-957; G. RESTA, *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2007, pp. 511-531, che parla, in merito al concetto di identità personale, di sintesi ideale della "biografia".

710 M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, cit., p. 949 ss.: «L'identità implica una considerazione globale delle qualità e degli attributi della persona, tende a rappresentare quest'ultima nella molteplicità dei suoi caratteri distintivi, finendo, quindi, con l'essere espressione completa della personalità individuale».

diritto ad essere se stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo» e la sentenza della Corte di Cassazione del 7 febbraio 1996, n. 978, che parla di «bene-valore costituito dalla proiezione sociale della personalità dell'individuo, cui si correla un interesse del soggetto ad essere rappresentato, nella vita di relazione, con la sua vera identità, e non vedere, quindi, all'esterno modificato, offuscato o comunque alterato il proprio patrimonio intellettuale, ideologico, etico, religioso, professionale (ecc.) quale già estrinsecatosi o destinato, comunque, ad estrinsecarsi, nell'ambiente sociale, secondo indici di previsione costituiti da circostanze obiettive ed univoche».

L'identità personale vive una nuova e burrascosa vita con l'avvento delle tecnologie e della rete, dove le informazioni non sono strutturate e organizzate, non hanno limiti di spazio e di tempo e sono prive di filtri, di contestualizzazione, di qualità e dei criteri essenziali dell'archiviazione[711]: l'identità, unitaria nel mondo analogico, al contrario tende ad essere scomposta e frammentata nei *byte* delocalizzati nei *cloud*, si moltiplica nei diversi profili legati al soggetto, capaci di sopravvivere al soggetto stesso[712] e può essere a rischio di distorsioni, alterazioni e travisamenti[713].

---

711 Cfr. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2010, p. 393, secondo la quale in rete «non si svolge un discorso, con un filo e un suo autonomo senso, ma si raccolgono frammenti di discorsi. […] Oggi la memoria della rete non è un archivio: assomiglia molto di più a un deposito, nel quale ci sono degli archivi».

712 Sulle problematiche legate alla "morte digitale" si rinvia alla lettura di G. ZICCARDI, *Il libro digitale dei morti: memoria, lutto, eternità e oblio nell'era dei social network*, Utet, Milano, 2017.

713 A. MASERA - G. SCORZA, *op. cit.*, p. 50: «L'immagine digitale dell'identità di una persona è fallace, perché imprecisa, parziale, magari non aggiornata, oppure costruita sulla base di deduzioni algoritmiche condizionate dalle finalità di una raccolta». G. CASSANO - A. CONTALDO, *Diritti della persona, internet e responsabilità dei soggetti intermediari*, in *Il Corriere giuridico*, fasc. 8-allegato 1, 2010, pp. 5-38, nel rilevare che «la persona virtuale è proiettata dal contesto originario di elaborazione a quello più vasto e potenzialmente illimitato – si può dire globale – della interconnessione telematica», parlano di «pericolo di uno scollamento della rappresentazione dell'individuo stesso, quale egli è e ha il diritto di apparire in tutti i contesti sociali ove egli opera: una manipolazione assolutamente contrastante con l'affermazione del diritto al libero svolgimento dei diritti della persona, e con la loro funzione strumentale alla protezione della dignità umana». E. JANNUZZI - A. REGI, *Diritto all'oblio: finzione o realtà?*, in *Law and Media Working Paper Series*, n. 13, 2016, p. 2 sottolineano che «la diffusione

Al riguardo, di conseguenza, si parla di identità digitale, che si declina in due accezioni correlate come nel caso dell'identità personale: una prima accezione "ristretta" si collega a un valore anche qui di carattere pubblicistico e fa riferimento all'identificazione informatica del soggetto, ossia all'«insieme di caratteristiche essenziali e univoche in grado di identificare digitalmente un soggetto»[714] o, secondo la definizione del Codice dell'amministrazione digitale, alla «*rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale*» (è il caso di SPID - Sistema Pubblico per la gestione delle Identità Digitali di cittadini e imprese)[715]. L'accezione più "ampia", invece, fa riferimento all'identità personale in rete, al "corpo elettronico" ed è maggiormente legata ai diritti e alle libertà del soggetto; tale seconda accezione, come nel caso dell'identità personale, è quella che sarà tenuta in considerazione ai fini della presente analisi che si concentra sul governo dei dati.

L'elaborazione dei diritti di identità personale e di identità digitale ha matrice nelle riflessioni della dottrina e nelle ricostruzioni della giurisprudenza, trovando fondamento nella clausola aperta dell'art. 2 della Costituzione, in particolare nel collegamento al concetto di dignità, anima comune dei diversi diritti fondamentali della persona.

Da un punto di vista normativo, mentre l'identità personale viene semplicemente citata dall'art. 2, comma 1, del d.lgs. 196/2003, l'identità digitale nell'accezione ampia presa qui in considerazione non ha un preciso fondamento legislativo[716].

---

incontrollata di dati veicolati on line e la condivisione interattiva di numerose notizie lascia una traccia permanente dell'identità personale di ogni individuo».

[714] H. ABELSON - L. LESSIG (*et al.*), *Digital identity in cyberspace*. *White paper submitted for 6.805/ Law of Cyberspace: Social Protocols*, *6*, 1998.

[715] In tal senso art. 1, comma 1, lett. u-quater), d.lgs. 82/2005, che al riguardo richiama le modalità fissate nel decreto attuativo previsto dall'art. 64. In merito all'identificazione informatica, G. MAGLIO, *Identità digitale*, in M. MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Tangram edizioni scientifiche, Trento, 2017, p. 58: «È chiaro che non tutti i servizi *online* richiedono di stabilire con certezza l'identità dell'utilizzatore, ma per alcuni di essi, come per esempio l'invio di una richiesta alla Pubblica Amministrazione, l'apertura di un nuovo conto corrente o la partecipazione a una gara d'appalto, determinare con certezza l'identità del richiedente risulta essere fondamentale».

[716] L'accezione ristretta come identificazione informatica, invece, è normativamente prevista e disciplinata dal cosiddetto regolamento eIDAS 910/2014 del 23 luglio 2014 e dal CAD, d.lgs. 82/2005,

Nella Dichiarazione dei diritti in Internet, atto dal valore culturale e politico, ma privo di cogenza giuridica, il diritto all'identità *tout court* (personale e digitale) è presente e se ne dettagliano i principi nell'art. 9, che ribadisce il diritto di ogni persona alla «rappresentazione integrale e aggiornata delle proprie identità in rete» e alla «libera costruzione della personalità», che non può essere sottratta alla conoscenza e all'intervento dell'interessato. La disposizione è conscia del fatto che l'identità deve fare i conti con i *big data*: «l'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano»[717].

4.3.2. Il *right to be forgotten*

L'aggettivo "aggiornata", opportunamente utilizzato con riferimento all'identità dalla Dichiarazione dei diritti in Internet, richiama la dimensione peculiare della rete, un presente perenne, sostanzialmente incancellabile[718], capace peraltro di condizionare il futuro come è stato messo in luce con i *big data*: il profilo del tempo, a sua volta, chiama in causa un altro diritto che si collega strettamente all'identità, in particolare nella sua traduzione digitale, quello che viene definito diritto all'oblio[719].

Nella rete si pone, infatti, l'esigenza, prestando attenzione all'esatta diffusione dei dati, di tutelare la rappresentazione dell'identità, la proiezione sociale della stessa,

---

come successivamente riformato, in particolare negli art. 1, comma 1, lett. u-quater), e art. 64, oltre alla relativa normazione di rango secondario.

717 La norma, nel comma 5, contempla anche l'accezione più ristretta di identità digitale, richiamando l'attribuzione e la gestione dell'identità digitale da parte delle istituzioni pubbliche, che deve essere accompagnata da adeguate garanzie in particolare in termini di sicurezza.

718 M.F. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, cit., pp. 740-758. In proposito G. MAGLIO, *op. cit.*, p. 63 sottolinea che per il funzionamento stesso della rete la conservazione dei dati e delle informazioni può durare nel corso del tempo.

719 Sul diritto all'oblio cfr., *inter alia*, M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Edizioni Scientifiche Italiane, Napoli-Roma, 2009; G. RESTA - V.ZENO-ZENCOVICH, *Il diritto all'oblio su internet dopo la sentenza Google Spain*, RomaTre Press, Roma, 2015; S. MARTINELLI, *Diritto all'oblio e motori di ricerca: memoria e privacy nell'era digitale*, Giuffrè, Milano, 2017.

intendendo per tale quella che corrisponde all'identità attuale: questo può determinare l'esigenza che, col passare del tempo, il soggetto si riappropri di informazioni, sulle quali non c'è più il pubblico interesse[720].

Il diritto all'oblio ha avuto diverse accezioni nel corso del tempo[721]; quella tradizionale e più risalente, elaborata dalla dottrina e dalla giurisprudenza[722], lo individua nel diritto a non vedere rievocati fatti risalenti nel tempo[723], nel «diritto a che fatti, pure pubblici, attinenti al soggetto, col decorso del tempo cessino di avere tale qualità»[724]. In tale accezione il diritto all'oblio si riferisce a fatti di cronaca[725] o pubblicazioni lecite, rispetto alle quali si configura il diritto del soggetto a non vederle

---

720 M.C. DAGA, *Diritto all'oblio: tra diritto alla riservatezza e diritto all'identità personale (nota a Cass., sez. III civ., 26 giugno 2013, n. 16111)*, in *Danno e responsabilità*, fasc. 3, 2014, p. 274 ss.: «Ognuno di noi cambia, migliora, e ha il diritto di non vedere distrutta la nuova immagine all'interno della società».

721 Il concetto di "diritto all'oblio" nasce nella dottrina in Francia (*droit à l'oubli*) nel 1965 in occasione di un processo a carico del regista di un film sulla vita del serial killer Henri Landru (o Barbablù), che aveva ucciso molte donne per impadronirsi dei loro beni e che, per questo, venne condannato a morte: il film rievoca tra i protagonisti anche un'amante sopravvissuta, che si trovava così a dover rivivere fatti passati estremamente dolorosi e drammatici. Nel caso di specie il giudice non ha accolto l'istanza della donna a causa del suo comportamento contraddittorio, dal momento che la stessa aveva redatto e diffuso un libro in cui rievocava quei fatti.

722 Cfr. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 591-603.

723 M.F. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, cit., pp. 740-758 e M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, cit., p. 949 ss.

724 Cfr. V. ZENO-ZENCOVICH, *Una svolta giurisprudenziale nella tutela della riservatezza*, in *Il diritto dell'informazione e dell'informatica*, vol. 1, 1986, p. 934 ss., che porta come esempio l'illecito commesso molti anni prima.

725 In relazione al diritto di cronaca merita ricordare che la giurisprudenza ha elaborato i tre fondamentali parametri della verità dei fatti narrati, dell'interesse pubblico alla conoscenza della notizia (rilevanza sociale dell'informazione – pertinenza) e della continenza verbale con la quale è espressa (forma "civile" di esposizione); cfr. G.E. VIGEVANI, *Diritto all'informazione e privacy nell'ordinamento italiano: regole ed eccezioni*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2016, pp. 473-498, che interpreta il requisito dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico non quale condizione per l'esercizio del diritto di cronaca, ma quale elemento la cui sussistenza comporta la prevalenza di tale diritto nel bilanciamento con altri contrapposti, dato il collegamento tra informazione e democrazia che allarga i confini del diritto di cronaca e consente di prevalere sui diritti della personalità.

più nuovamente pubblicate trascorso un adeguato lasso di tempo e in assenza dell'utilità sociale della pubblicazione, a meno che non permanga o sorga un interesse pubblico all'informazione; il concetto quindi afferisce alla liceità di una nuova pubblicazione, in considerazione del tempo trascorso rispetto all'accadimento e al mutamento delle situazioni[726]. Il diritto all'oblio mira a tutelare il diritto all'identità, che, come esaminato, è dinamico in relazione a informazioni e dati veri e legittimamente pubblicati, ma che per il trascorrere del tempo non sono più conformi all'attuale identità personale del soggetto[727].

Come nel caso del diritto all'identità, anche il diritto all'oblio muta drasticamente con la rete, che, per le proprie caratteristiche di struttura e diffusione, non cancella le informazioni che restano disponibili e "appiattite" nel tempo e, di conseguenza, fa divenire regola la memoria ed eccezione l'oblio: in rete dimenticare diventa molto più difficile che ricordare[728].

---

[726] In giurisprudenza, *inter alia*, Corte di Cassazione civile, 18 ottobre 1984, n. 5259; Tribunale di Roma, 15 maggio 1995; Corte di Cassazione civile 9 aprile 1998, n. 3679. Cfr. G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Rivista di diritto civile*, fasc. 6, 1990, p. 808, secondo cui il diritto all'oblio appartiene alle "ragioni" e alle "regioni" del diritto alla riservatezza; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss., secondo la quale il tempo gioca un ruolo fondamentale anche quando non si tratti di eventi di cronaca, ma sia trascorso un significativo lasso di tempo e non ci sia contestualizzazione: in tal caso la violazione afferisce all'identità personale; G. CASSANO, *Il diritto all'oblio nell'era digitale*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, p. 46, secondo cui il diritto all'oblio «è la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca» e «sorge proprio nel momento in cui non vi è più alcuna necessità di informare o aggiornare il pubblico».

[727] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss. e M. RIZZUTI, *Il diritto e l'oblio*, in *Il Corriere giuridico*, fasc. 8-9, 2016, p. 1078.

[728] Cfr. V. MAYER-SCHÖNBERGER, *Delete*, trad. it., Egea, Milano, 2010, p. 2 ss., secondo cui sono stati il *web 2.0*, ma anche i *media* tradizionali, abbinati al potere di Internet, ad alimentare questo sviluppo; «con la tecnologia digitale la capacità di dimenticare della società è temporaneamente sospesa, sostituita da una memoria perfetta» (p. 3). G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 392: «La memoria sembra essere illimitata. Il mare di Internet in cui si naviga è anche un oceano di memoria. Dati, immagini, audio, frammenti di informazione vanno incontro al navigatore, in una dimensione spaziale avvertita come del tutto nuova che pare ignorare la dimensione temporale. Per la sua stessa struttura, difficilmente la Rete dimentica. […] Antropomorficamente, la percezione è che la Rete

Nel mutato contesto quello che cambia è proprio il tempo: non è più da considerare quello che intercorre tra la prima e la nuova pubblicazione, ma il tempo di permanenza della pubblicazione, ossia quello della pubblicazione iniziale che perdura. In rete la memoria storica è un presente sempre attuale[729]. Non solo: la rete è capace di cambiare la percezione dello scorrere degli eventi, dal momento che i motori di ricerca e l'indicizzazione compiuta dagli stessi possono far recuperare eventi più risalenti nel tempo tra i primi risultati; i risultati seguono infatti un criterio di rilevanza legato a un insieme complesso di fattori connessi agli algoritmi e non a un ordine cronologico[730].

Gli effetti sono ampi e profondi e riguardano non solo i singoli, ma l'intera società e i suoi assetti[731].

Nell'età contemporanea ricordare diventa semplice ed economico grazie alla digitalizzazione[732], alla memorizzazione a buon mercato[733], alla facilità di recupero[734] e

---

travalichi i confini dell'umano e sia una divinità o un mostro: un'entità unica dotata di memoria infinita e senza tempo. Questa sensazione è palesemente avvertita quando si utilizzano i motori di ricerca».

729 G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss. e G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 397: «Come il diritto all'identità personale, così il diritto all'oblio, che da quello è gemmato, è figlio della comunicazione. Il diritto all'identità personale è il diritto ad esercitare una forma di controllo sulla propria immagine sociale, che può giungere fino a pretendere che alcuni eventi siano dimenticati. Ma nato dalla cronaca, vive una nuova vita su Internet». Secondo l'Autrice «su Internet cambia non solo la quantità, ma anche la natura della comunicazione: le informazioni non solo sono moltissime, ma sono facilmente reperibili, sovente prive di contestualizzazione e spesso prive di fonte che consenta di attribuire ad esse un peso. Sono, per così dire, appiattite». Cfr. M. D'AMBROSIO, *Il c.d. principio dell'*openness *nelle procedure giudiziarie tra oblio e anonimato*, in *Rassegna di diritto civile*, fasc. 1, 2017, p. 37 ss.

730 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars Interpretandi*, fasc. 1, 2017, p. 69. S. RODOTÀ*, Il diritto di avere diritti,* cit., pp. 404-405: «Dalla cancellazione alla imposizione. Ieri la *damnatio memoriae*, oggi l'obbligo del ricordo. Che cosa diviene la vita nel tempo in cui "Google ricorda sempre"? L'implacabile memoria collettiva di Internet, dove l'accumularsi d'ogni nostra traccia ci rende prigionieri d'un passato destinato a non passare mai, sfida la costruzione della personalità libera dal peso d'ogni ricordo, impone un continuo scrutinio sociale da parte di una infinita schiera di persone che possono facilmente conoscere le informazioni sugli altri»; per l'Autore il cambiamento tecnologico ha portato a un mutamento antropologico e genera «un'espansione senza limiti della memoria sociale che condiziona la memoria individuale».

731 Per il ruolo del ricordo e dell'oblio nella storia dell'uomo cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 15 ss.

all'accesso universale[735] e, al contrario, è costoso ed estremamente difficile, se non impossibile, far dimenticare un'informazione che, una volta condivisa, esce dal controllo del suo titolare e rischia, peraltro, di sopravvivergli. Di conseguenza cambia la dimensione del tempo, cambiano le geometrie del potere non più appannaggio di chi tradizionalmente lo deteneva, cambiano gli interrogativi: «Vogliamo un futuro che non è in grado di perdonare perché non è in grado di dimenticare?», si chiede al riguardo Mayer-Schönberger[736].

La perdita di controllo sulle informazioni trasferisce il relativo potere ad altri soggetti, privati e pubblici, favoriti dalla facile accessibilità, dalla durevolezza e dall'universalità delle informazioni, ossia dall'accumulo e dal collegamento tra le stesse, capaci di dar vita a veri e propri dossier: con il controllo delle informazioni si sposta il potere correlato[737]. Sicuramente disporre di una "memoria perfetta" è allettante non solo per il settore privato, ma anche per quello pubblico con immaginabili pericoli di controllo di massa.

---

732 Grazie alla digitalizzazione le copie hanno la stessa qualità degli originali e gli strumenti digitali sono capaci di gestire e memorizzare qualsiasi tipo di informazione come segnale binario, senza avere necessità di ricorrere a diversi tipi di supporto. La standardizzazione dell'informazione digitale ha, peraltro, favorito condivisione e distribuzione. Cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 47 ss.

733 È diventato molto più costoso, anche in termini di tempo, dimenticare (si pensi alla cancellazione di *file* o foto). Cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 54 ss.: «I costi contenuti rendono spesso più economico tenere tutta l'informazione digitale che non investire del tempo a eliminare quella che non serve».

734 Cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 63 ss.: «La differenza con l'era analogica è sbalorditiva: grazie alla facilità di recupero, centinaia di gigabyte di informazioni non sono più frammenti dispersi in un mare sterminato in cui rischiamo di annegare ma un'estensione potente, versatile e veloce della memoria umana» (p. 67), anche se i risultati delle ricerche hanno il difetto di essere decontestualizzati.

735 L'accesso all'informazione non dipende più dalla presenza fisica e dall'ubicazione geografica; cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 45 ss.: «Per centinaia di anni, muoversi da una comunità all'altra ha permesso alle persone di ricominciare da capo, visto che le informazioni su di loro rimanevano nel luogo di origine» (p. 86).

736 V. MAYER-SCHÖNBERGER, *op. cit.*, p. 4.

737 Cfr. V. MAYER-SCHÖNBERGER, *op. cit.*, p. 1 ss. e p. 85 ss., secondo cui gli esseri umani non possono più sfuggire al loro passato. «Il passato li insegue, pronto a farsi catturare da chiunque abbia una connessione internet» (p. 90).

Il pericolo, peraltro, non è solo nel controllo esterno da parte dei colossi del web o dei poteri pubblici, ma anche nell'auto-controllo, ossia nei rischi relativi al comportamento degli individui, che possono essere inibiti nel presente per paura del ricordo di quel che faranno o diranno in futuro, condizionati nella propria capacità di esprimersi, di decidere e nelle relazioni[738]: in pericolo è la stessa capacità di pensare, giudicare e agire nel presente, con il conseguente effetto di ostacolare il cambiamento[739].

Sono evidenti anche i rischi di imprecisione e manipolazione di quella enorme memoria digitale esterna, con i danni correlati che questo può provocare alla persona.

Il nuovo scenario e le relative complesse problematiche chiamano in gioco la regolazione da parte degli ordinamenti giuridici. L'esigenza che si configura per il diritto è il rispetto della corretta rappresentazione del soggetto nel presente, ossia non vedere travisato o alterato all'esterno il patrimonio intellettuale, politico, sociale, religioso, ideologico, professionale e, di conseguenza, vedere garantita la verità dell'immagine del soggetto nel momento storico attuale[740].

Pertanto si pone un'esigenza di storicizzazione e contestualizzazione, attribuendo un peso all'informazione in un contesto complessivo, che vede l'identità come protagonista e bene giuridico oggetto di tutela: si profila, di conseguenza, un diritto a

---

738 V. MAYER-SCHÖNBERGER, *op. cit.*, p. 97 ss.: «l'oblio non è una lacuna fastidiosa, ma un vantaggio che salva la vita. Dimenticando, recuperiamo la libertà di generalizzare, concettualizzare e soprattutto agire» (p. 101). Secondo l'Autore «la memoria digitale ha un impatto negativo sulla storia, ostacolando la nostra capacità di giudizio e di agire nel presente. Ci nega la possibilità di evolvere, crescere e imparare, lasciandoci in balia di una situazione difficile: passato sempre presente e futuro ignorante» (pp. 108-109).

739 V. MAYER-SCHÖNBERGER, *op. cit.*, p. 107: «Se niente di ciò che facciamo può essere cancellato, allora non ha senso impegnarsi a cambiare. In un mondo in cui la storia non diventa mai passato, nessuno è incentivato a darsi da fare per sottrarsi al destino e uscire dalla situazione in cui si trova […]».

740 S. RODOTÀ*, Il diritto di avere diritti,* cit., pp. 405-406 parla di «persona "digitale", disincarnata, tutta risolta nelle informazioni che la riguardano, unica e "vera" proiezione nel mondo dell'essere di ciascuno»; in tale contesto «la folla non è più solitaria, ma "nuda", restituita a una realtà nella quale ogni individuo è scrutato, schedato, ricondotto a una misura che lo rende riconoscibile e riconosciuto».

contestualizzare più che a dimenticare[741] per proteggere l'identità del soggetto nel suo dinamismo e nella sua corretta rappresentazione online[742].

Per tale motivo la Corte di Cassazione, nel *landmark case* costituito dalla sentenza 5 aprile 2012, n. 5525, ha ritenuto di proteggere quello che definisce come diritto all'oblio per mezzo della contestualizzazione e dell'aggiornamento nel tempo dell'informazione, dato che «la notizia, originariamente *completa* e *vera* diviene *non aggiornata*, risultando quindi *parziale* e *non esatta*, e pertanto sostanzialmente *non vera*». La Corte di Cassazione ha quindi stabilito, nel caso di specie, che nell'archivio che rendeva accessibile la notizia originaria fosse segnalata (nel corpo o a margine) la sussistenza di un seguito e di un successivo sviluppo della notizia, consentendone il rapido e agevole accesso ai fini del relativo adeguato approfondimento: di conseguenza, i titolari di archivi online sono tenuti a predisporre sistemi di aggiornamento costante dei contenuti, al fine di evitare di risponderne giudizialmente, obbligo peraltro di difficile esigibilità tecnica[743].

Per la Corte di Cassazione, in merito ai dati, il soggetto ha «il diritto al relativo controllo a tutela della propria immagine sociale, che anche quando trattasi di notizia vera, e *a fortiori* se di cronaca, può tradursi nella pretesa alla contestualizzazione e

---

741 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 73: «l'unico risultato che sembra realistico raggiungere, allora, è quello di essere (non dimenticato, ma) correttamente ricordato. Ma in questo modo si chiede oblio e si ottiene memoria (seppur contestualizzata)».

742 In dottrina sono individuati come tratti distintivi del diritto all'oblio la vetustà dei fatti, il decorso del tempo e l'inutilità sociale dell'informazione; cfr. M. MEZZANOTTE, *Il diritto all'oblio. Contributo alla studio della privacy storica*, cit., p. 122, che parla del diritto all'oblio come diritto al controllo della diffusione delle scelte fatte in passato. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 395 sottolinea come in rete «ci troviamo spesso davanti a pagine isolate di libri custoditi in mille diverse biblioteche». Cfr., altresì, G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss. e M.F. COCUCCIO, *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, cit., p. 740 ss.

743 Nel caso di specie un esponente politico, indagato e arrestato per corruzione e poi prosciolto, chiedeva venisse aggiornato un vecchio articolo presente in un archivio online, dando conto dello sviluppo favorevole della vicenda. Cfr. E. STRADELLA, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare e, infine,* cui prodest*?*, in *Rivista AIC*, fasc. 4, 2016, p. 5 e S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 73.

aggiornamento dei medesimi e se, del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione»; dall'altra parte, il titolare del sito è tenuto a continuare a mantenere i «caratteri di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante il relativo aggiornamento e contestualizzazione», «a tutela del diritto del soggetto cui i dati pertengono alla propria identità personale o morale nella sua proiezione sociale, nonché a salvaguardia del diritto del cittadino utente di ricevere una completa e corretta informazione, non essendo al riguardo sufficiente la mera generica possibilità di rinvenire all'interno del "mare di Internet" ulteriori notizie concernenti il caso di specie»[744]. Di nuovo, come per l'identità, il diritto si preoccupa di ristabilire la verità nel momento storico attuale e in questa significativa sentenza lo fa imponendo al titolare dell'archivio l'aggiornamento della notizia, ponendo quindi l'accento sulla qualità delle informazioni[745].

A ben vedere, le due dimensioni dell'identità personale/digitale e del diritto all'oblio si fondono nel diritto dinamico all'identità su cui si costruisce la dignità e lo sviluppo della persona[746] e derivano dalla libertà informatica, quale diritto all'*habeas*

---

744 La Corte di Cassazione, al riguardo, afferma (diversamente da quel che verrà affermato nella celebre sentenza *Google Spain*, trattata più avanti nel testo) che è il titolare del sito (nel caso, la società Rcs Quotidiani s.p.a.), e non già il motore di ricerca (nel caso, Google), a dover provvedere al raggiungimento del suindicato obiettivo. Secondo Cass. Civile, sez. III, 26 giugno 2013, n. 16111, «i fattori decisivi dei quali il giudice di merito deve tenere conto nel delicato bilanciamento tra il diritto di cronaca e quello alla riservatezza sono costituiti dall'essenzialità dell'informazione e dall'interesse pubblico delle notizie divulgate» e, di conseguenza, «il diritto del soggetto a pretendere che proprie, passate vicende personali siano pubblicamente dimenticate (nella specie c.d. diritto all'oblio in relazione ad un'antica militanza in bande terroristiche) trova limite nel diritto di cronaca solo quando sussista un interesse effettivo e attuale alla loro diffusione, nel senso che quanto recentemente accaduto (nella specie, il ritrovamento di un arsenale di armi nella zona di residenza dell'ex terrorista) trovi diretto collegamento con quelle vicende e ne rinnovi l'attualità». Altrimenti viene a essere violato il diritto alla riservatezza, mancando la concreta proporzionalità tra la causa di giustificazione (il diritto di cronaca) e la lesione del diritto antagonista.

745 P. HÄBERLE, *Diritto e verità*, ed. it., Einaudi, Torino, 2000, p. 100 ss.: «lo stato costituzionale punta alla ricerca della verità, il tema della verità è un suo problema fondamentale».

746 T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 688: «È il principio fondamentale della dignità, infatti, che costituisce il fondamento costituzionale di tutti i diritti strettamente connessi allo sviluppo della persona. […] La tutela della dignità dell'uomo passa (anche) attraverso il diritto all'oblio, ovvero il diritto

data, nella sua connotazione negativa (la protezione della propria sfera e la pretesa ad essere lasciati soli - *right to be let alone*) e in quella positiva e dinamica (il diritto di controllo e l'autodeterminazione informativa sui propri dati e sulle proprie informazioni)[747]. Del resto il *right to be forgotten*, come il diritto all'identità da cui deriva, non è arbitrario, ma protegge la proiezione sociale dell'identità personale, che richiede dunque una mediazione sociale tra l'immagine che il soggetto ha di sé (la verità personale) e l'insieme di dati oggettivi riferibili al soggetto (verità storica), proteggendo quindi l'immagine, socialmente mediata e oggettivata, e dunque l'identità del soggetto[748].

Si tratta di «un diritto a governare la propria memoria»[749]; al singolo compete, infatti, la frazione di sovranità sulla propria sfera personale, sulla sua identità e sui suoi dati[750]. Si affaccia qui con evidenza l'altra anima e l'altra accezione del diritto all'oblio, legata alla protezione dei dati personali.

Da questo punto di vista, ponendosi in scia alla sentenza *Digital Rights Ireland* o *Data Retention*[751], è particolarmente significativa la sentenza *Google Spain*[752], in cui la

---

a cancellare, ovvero a contestualizzare, i dati personali per vietare […] un travisamento dell'immagine sociale di un soggetto, per evitare che la vita passata possa costituire un ostacolo per la vita presente e possa ledere la propria dignità umana».

747 M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, cit., p. 949 ss. *Supra*, cap. 1, § 3.

748 Cfr. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., pp. 398-399 e M.F. COCUCCIO, *Il diritto all'identità personale e all'identità "digitale"*, cit., p. 949 ss.

749 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 406: «Il diritto all'oblio si presenta come diritto a governare la propria memoria, per restituire a ciascuno la possibilità di reinventarsi, di costruire personalità e identità affrancandosi dalla tirannia di gabbie nelle quali una memoria onnipresente e totale vuole rinchiudere tutti». Cfr., altresì, T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 686.

750 M. RIZZUTI, *op. cit.*, p. 1078.

751 Caso *Digital Rights Ireland e Seitlinger e a.*, sentenza della Corte di Giustizia dell'Unione europea dell'8 aprile 2014, cause riunite C-293/12 e C-594/12. La Corte ha dichiarato invalida la direttiva 2006/24/CE del 15 marzo 2006 per incompatibilità con gli artt. 7, 8 e 52, comma 1, della Carta dei diritti fondamentali dell'Unione europea e, in specifico, per incompatibilità della conservazione di dati generati o trattati nell'ambito di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione per un periodo da 6 a 24 mesi al fine di renderli disponibili per il perseguimento di gravi reati (criminalità organizzata e terrorismo), dal momento che non prevedeva garanzie sufficienti ad assicurare una tutela efficace dei dati personali contro rischi di abusi e accesso o utilizzo illecito degli

Corte fa riferimento a una diversa accezione del diritto all'oblio, rispetto alle due esaminate[753], ossia quella che attribuisce all'interessato il diritto alla cancellazione dei

stessi; abbonati e utenti non erano informati al riguardo e questo poteva ingenerare in loro la sensazione di essere sottoposti a sorveglianza. Infatti, anche se la conservazione può servire a una eventuale trasmissione alle autorità nazionali per rispondere a un obiettivo di interesse generale, ossia la pubblica sicurezza, questo non può eccedere i limiti posti dal principio di proporzionalità e interferire eccessivamente con i diritti fondamentali. La direttiva 2006/24/CE non prevedeva il controllo di giudici o autorità amministrative indipendenti circa l'utilizzo da parte delle autorità nazionali dei dati personali limitato a fini di prevenzione, accertamento e perseguimento dei reati sufficientemente gravi da giustificare l'ingerenza nei diritti fondamentali, in specifico quelli tutelati dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Cfr. F. ROSSI DAL POZZO, *op. cit.*, pp. 690-724.

[752] Caso *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González*, sentenza della Corte di Giustizia dell'Unione europea del 13 maggio 2014, causa C-131/12. Nella fattispecie, le questioni pregiudiziali sollevate dall'*Audiencia Nacional* spagnola alla Corte di Giustizia riguardavano il caso del sign. Mario Costeja González, che aveva presentato reclamo all'*Agencia Española de Protección de Datos* (AEPD) fondato sul fatto che, introducendo il suo nome nel motore di ricerca del gruppo Google (*Google Search*), otteneva dei link verso due pagine del quotidiano La Vanguardia rispettivamente del 19 gennaio e del 9 marzo 1998, nelle quali figurava un annuncio, menzionante il nome del sig. Costeja González, per una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. In primo luogo, il reclamo era contro il quotidiano La Vanguardia, chiedendo di sopprimere o modificare le pagine o di ricorrere a strumenti di protezione dei suoi dati: la richiesta con riferimento all'editore è stata respinta ritenendo la pubblicazione legalmente giustificata, dato che aveva avuto luogo su ordine del Ministero del Lavoro e degli Affari sociali e aveva avuto lo scopo di conferire la massima pubblicità alla vendita pubblica, al fine di raccogliere il maggior numero di partecipanti all'asta. Ha avuto successo, invece, il reclamo rivolto a Google Spain e Google inc., con cui González chiedeva fosse ordinato loro di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca relativi al suo nome, in considerazione della distanza nel tempo che privava di rilevanza la notizia del pignoramento effettuato nei suoi confronti, ormai interamente definito da svariati anni. Google Spain e Google Inc. hanno proposto due ricorsi separati contro la decisione dinanzi all'*Audiencia Nacional*, dei quali quest'ultima ha disposto la riunione e sui quali ha deciso di sospendere il procedimento e di sottoporre alla Corte tre questioni pregiudiziali relative a: ambito territoriale di applicazione della direttiva 95/46 e, di conseguenza, della normativa spagnola sulla protezione dei dati; attività dei motori di ricerca quali fornitori di contenuti in relazione alla direttiva 95/46; portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio. La sentenza verrà trattata solo negli aspetti rilevanti ai fini di questa analisi.

[753] Le due accezioni si riferiscono al diritto a non vedere rievocati fatti risalenti nel tempo e al diritto alla contestualizzazione.

dati e il diritto all'opposizione al trattamento degli stessi e che si colloca nello spazio della normativa dedicata alla protezione dei dati personali[754].

La Corte, in modo innovativo, infatti, ha accolto il reclamo contro Google e ha ritenuto i gestori dei motori di ricerca soggetti alla normativa in materia di privacy, in qualità di responsabili del trattamento dei dati personali[755], dal momento che ne determinano le finalità e gli strumenti: configurano "trattamento", infatti, le operazioni con cui il gestore "raccoglie", "estrae", "registra" e "organizza" i dati nell'ambito dei suoi programmi di indicizzazione, per poi "conservarli", "comunicarli" e "metterli a disposizione" degli utenti. Il trattamento effettuato dai motori di ricerca, spiega la Corte, svolge un ruolo decisivo nella diffusione globale dei dati, in quanto facilita notevolmente l'accesso, rendendolo possibile anche solo effettuando una ricerca a partire dal nome, potendo incidere in modo significativo e moltiplicando l'ingerenza sui diritti fondamentali alla vita privata e alla protezione dei dati personali.

Di conseguenza, la Corte ha ritenuto che l'interessato ha diritto a richiedere direttamente al gestore del motore di ricerca la deindicizzazione e, quindi, la rimozione dell'indicizzazione, sopprimendo dall'elenco dei risultati, che appare a seguito di una

---

754 Tra i numerosissimi interventi sulla sentenza *Google Spain* cfr., *inter alia*, M. BASSINI, *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quaderni costituzionali*, fasc. 3, 2014, pp. 730-733; T.E. FROSINI, *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 563-567; A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella* digital economy, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 681-701; D. MINIUSSI, *Il diritto all'oblio: i paradossi del caso Google*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 1, 2015, pp. 209-234; S. PIETROPAOLI, *Chi deve essere il custode della rete? Considerazioni sul problema dell'esercizio del "diritto all'oblio"*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, p. 545 ss.; O. POLLICINO, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 569-589; G. RESTA - V.ZENO-ZENCOVICH, *op. cit.*; S. MARTINELLI, *Diritto all'oblio e motori di ricerca: memoria e privacy nell'era digitale*, cit.

755 La direttiva 95/46/CE, riferimento della causa, parla solo di responsabili del trattamento e non di titolari; il nuovo regolamento (UE) 2016/679 parla, invece, di titolari e responsabili, come già peraltro la normativa italiana. Il responsabile del trattamento, di cui all'art. 2, paragrafo 1, lett. d), direttiva 95/46/CE, corrisponde al titolare del trattamento nella nuova disciplina europea, definito nell'art. 4, paragrafo 1, n. 7, reg. (UE) 2016/679.

ricerca effettuata a partire dal nome di questa persona, link verso pagine web legittimamente pubblicate e contenenti informazioni veritiere, se la cancellazione è necessaria per tutelare il diritto all'oblio[756].

La riduzione della visibilità dell'informazione, infatti, permette di tutelare il soggetto: la sentenza afferma propriamente un diritto alla deindicizzazione, un diritto a non trovare (o a trovare più difficilmente) la notizia più che all'oblio, dato che l'informazione permane sul web. In considerazione dell'impossibilità sostanziale di cancellazione dalla rete e del fatto che storicizzare e contestualizzare in realtà significano il contrario rispetto all'oblio (l'informazione resta nella memoria della rete, seppur storicizzata e contestualizzata), per proteggere l'interesse a dimenticare una strada consiste proprio nel rendere difficile trovare in rete quelle informazioni, modificando i risultati dei processi di indicizzazione dei motori di ricerca[757].

Nella sentenza appare anche un altro principio di diritto fondamentale: nel valutare la domanda, occorre verificare in particolare se l'interessato abbia diritto a che l'informazione che riguarda la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di tale diritto presupponga che l'inclusione dell'informazione in tale elenco arrechi un pregiudizio e anche nel caso in cui la pubblicazione sia lecita e la pagina indicizzata contenente l'informazione non venga rimossa dal sito sorgente. Se ne ha diritto, i link verso pagine web contenenti tali informazioni devono essere cancellati dall'elenco di risultati, a meno che sussistano ragioni particolari, come il ruolo ricoperto dalla persona nella vita pubblica, giustificanti un interesse preminente del pubblico all'informazione[758].

---

[756] Secondo la Corte l'interessato può rivolgere le domande direttamente al gestore del motore di ricerca in qualità di responsabile del trattamento, che deve in tal caso procedere al debito esame della loro fondatezza e, eventualmente, porre fine al trattamento dei dati in questione. Qualora il gestore non dia seguito a tali domande, l'interessato può adire l'autorità di controllo o l'autorità giudiziaria affinché effettuino le verifiche necessarie e ordinino al responsabile l'adozione di precise misure conseguenti.

[757] S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 73.

[758] La sentenza afferma tre punti di diritto: due sono trattati nel testo (attività dei motori di ricerca quali responsabili del trattamento e portata del diritto all'opposizione/cancellazione in relazione al diritto all'oblio) e il terzo consiste nell'applicazione della legge nazionale del Paese nel quale il motore di ricerca opera, esercitando anche altre attività, come nel caso in cui il gestore apra una succursale o filiale

Per la Corte, infatti, i diritti fondamentali basati sugli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, tra cui il diritto all'oblio, in linea di principio prevalgono non solo sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico ad avere accesso all'informazione in occasione di una ricerca concernente il nome della persona, tranne «qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione, all'informazione di cui trattasi».

In tal modo, nonostante l'affermazione non particolarmente fortunata[759], la Corte non intende affermare un predominio assoluto del diritto all'oblio, dal momento che in realtà effettua il necessario bilanciamento tra i diritti contrapposti, oblio da una parte e libertà di informazione, libertà di espressione e libertà di impresa dall'altra e, nel farlo, applica esplicitamente i principi della normativa in materia di protezione dei dati personali: in particolare, la valutazione circa l'adeguatezza, la pertinenza e la non eccedenza rispetto alle finalità del trattamento, l'aggiornamento e la conservazione che consenta di identificare l'interessato per un arco di tempo non superiore a quello necessario, a meno che non si imponga per determinati motivi. In specifico, secondo la Corte, infatti, l'incompatibilità con la normativa europea in materia di protezione dei dati personali «può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici»: un trattamento inizialmente lecito può diventare, nel tempo, incompatibile con la normativa, «qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso».

---

destinata alla promozione e alla vendita di spazi pubblicitari proposti dal motore di ricerca. Cfr. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., pp. 591-603.

759 Per G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss. «questa affermazione appare apodittica e destinata a trovare molte correzioni e precisazioni».

Nel caso di specie, «tenuto conto del carattere sensibile delle informazioni contenute in tali annunci per la vita privata di detta persona, nonché del fatto che la loro pubblicazione iniziale era stata effettuata 16 anni prima, la persona interessata vanta un diritto a che tali informazioni non siano più collegate al suo nome attraverso un elenco siffatto. Pertanto, dal momento che nella fattispecie non sembrano sussistere ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso, nel contesto di una ricerca siffatta, a dette informazioni», la persona interessata può esigere la soppressione dei link suddetti da tale elenco di risultati.

La valutazione da compiere permette di accertare se un trattamento inizialmente lecito di dati esatti sia divenuto, con il tempo, incompatibile con la normativa: in tale valutazione viene in gioco, dunque, la qualità delle informazioni, ossia il rispetto dei principi e delle caratteristiche previste dalla relativa normativa, che devono essere osservate anche da parte dei gestori di motori di ricerca[760].

A seguito della sentenza, l'*Article 29 Data Protection Working Party* ha elaborato specifiche linee guida, pubblicate il 26 novembre 2014, tese a implementare i principi espressi nella decisione, offrendo un'interpretazione univoca della stessa e criteri comuni di attuazione per orientare l'attività dei Garanti nazionali, che hanno un compito significativo nell'equilibrio tra "memoria individuale" e "memoria sociale"[761].

Inoltre, a seguito della significativa pronuncia della Corte di Giustizia dell'Unione europea, Google, così come gli altri motori di ricerca, nel recepirne i principi, hanno messo a disposizione un servizio per consentire agli utenti di esercitare il diritto

---

760 A seguito e in linea con la sentenza *Google Spain*, il Tribunale di Roma con sentenza 3 dicembre 2015, n. 23771 ha configurato il diritto all'oblio «quale peculiare espressione del diritto alla riservatezza (privacy) e del legittimo interesse di ciascuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona […]». In questo caso si è trattato di un rigetto della domanda di deindicizzazione (a causa del ruolo pubblico del ricorrente e del fatto che erano notizie alquanto recenti) da parte del Tribunale, che ha mostrato equilibrio senza eccedere nel *favor* della privacy, rischio tangibile dopo *Google Spain*; cfr. G.E. VIGEVANI, *op. cit.*, pp. 473-498, che invece riporta la sentenza della Corte di Cassazione civile, sezione I, 24 giugno 2016, n. 13161, come caso in cui forse il diritto a informare è stato eccessivamente sacrificato in favore del diritto all'oblio.

761 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 407. Il Garante italiano per la protezione dei dati personali, in merito alle segnalazioni relative alla violazione del diritto all'oblio, ha effettuato questo bilanciamento applicando i principi previsti dalla normativa e dalle linee guida in materia di privacy.

all'oblio: nel caso di Google si tratta di una *form* per inoltrare la richiesta di rimozione di risultati di ricerca relativi a *query* che includono il nome dell'interessato, qualora tali risultati risultino illeciti, inesatti oppure obsoleti. Sarà Google a valutare «ogni singola richiesta» e a bilanciare «i diritti alla privacy della persona con il diritto di rendere accessibili le informazioni e con l'interesse del pubblico di trovarle». Google si esprime al riguardo in termini chiarissimi: «Durante la valutazione della richiesta stabiliremo se i risultati includono informazioni obsolete sull'utente e se le informazioni sono di interesse pubblico. Ad esempio, potremmo rifiutarci di rimuovere determinate informazioni se riguardano frodi finanziarie, negligenza professionale, condanne penali o la condotta pubblica di funzionari statali»[762].

Rispetto alla significativa sentenza *Google Spain*, si pone in continuità[763] il regolamento (UE) 2016/679, che nell'art. 17, rubricato significativamente «diritto alla cancellazione ("diritto all'oblio")», attribuisce all'interessato il diritto di chiedere la cancellazione dei dati personali in presenza di uno dei seguenti motivi:

«*a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

---

762 Si esprime così il modulo predisposto da Google, disponibile al link *support.google.com/legal/contact/lr_eudpa?product=websearch&hl=it*.

763 In tal senso G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss., che riporta come nei commenti in dottrina la disposizione, al contrario, sia stata evidenziata ed enfatizzata. A tal proposito O. POLLICINO, *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giurisprudenza costituzionale*, fasc. 3, 2014, pp. 2949-2958 ritiene che oggetto di attenzione e protezione della Corte nel caso *Google Spain* sia un nuovo *digital right to privacy* che adegua alle caratteristiche tecniche della rete un diritto alla privacy pensato per un mondo di atomi.

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1».

La finalità dell'oblio è raggiunta, pertanto, per mezzo della cancellazione dei dati. In proposito il regolamento reca un'innovazione nella disciplina europea nel comma 2 dell'art. 17[764], ai sensi del quale il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi della norma, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione deve adottare le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Il diritto alla cancellazione dei propri dati personali si configura in forma rafforzata e, oltre a questo aspetto, la disposizione mostra un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice italiano, d.lgs. 196/2003, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo la revoca del consenso al trattamento[765].

Lo stesso art. 17, al fine di bilanciare il diritto con altri diritti e interessi protetti, pone eccezioni nell'applicazione del diritto alla cancellazione «*nella misura in cui il trattamento sia necessario:*

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

---

764 G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 rileva che tale previsione era già presente nella normativa italiana.

765 In tal senso la Guida all'applicazione del regolamento europeo in materia di protezione dei dati personali predisposta dal Garante: *www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*.

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria».

A livello europeo, pertanto, il diritto all'oblio, si può dire "rafforzato", è ospitato nell'art. 17 del regolamento (UE) 2016/679 e chiarito nella sua portata dai relativi considerando 65 e 66[766]. Anche nella disciplina europea emerge la necessità del bilanciamento tra diritti e interessi diversi protetti dall'ordinamento giuridico; significativamente l'esercizio del diritto alla libertà di espressione e di informazione è posto come la prima eccezione all'applicazione del diritto alla cancellazione (diritto all'oblio).

L'attenzione al tempo e all'oblio è presente anche nei principi stessi del regolamento europeo, in specifico nell'art. 5, paragrafo 1, lett. e), reg. (UE) 2016/679: i dati personali devono essere «*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*».

Nella sua configurazione legata alla protezione dei dati, il diritto all'oblio, oltre al regolamento europeo, attualmente, in attesa di eventuali modifiche, trova collocazione nella disciplina nazionale nell'art. 11, comma 1, lett. e), del d.lgs. 196/2003, ai sensi del quale i dati personali oggetto di trattamento devono essere «*conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati*», in combinato disposto con l'art. 7, comma 3, lett. b), del d.lgs. 196/2003, ai sensi del quale l'interessato ha diritto di ottenere «*la cancellazione, la trasformazione in*

[766] Rileva anche il considerando 156.

forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati»[767].

Alla luce delle considerazioni svolte, il diritto all'oblio risulta quindi, più che un diritto autonomo, un diritto strumentale all'identità personale, in particolare nelle prime due accezioni (il diritto a non vedere rievocati fatti risalenti nel tempo e il diritto alla contestualizzazione), e alla protezione dei dati personali, nella terza accezione (il diritto alla cancellazione, alla deindicizzazione e all'opposizione al trattamento), finendo in tutti i casi per garantire la persona, che risulta centrale nelle diverse dimensioni in cui si esplica il diritto[768]. Sotto tale profilo, infatti, il diritto all'oblio, come il diritto all'identità personale e digitale, trova anch'esso fondamento nella clausola aperta dell'art. 2 della Costituzione, insieme all'art. 3 Cost.[769] e anche in tal caso, nella sua configurazione odierna, hanno giocato un ruolo determinante dottrina e giurisprudenza.

---

[767] Secondo G. CASSANO, *Il diritto all'oblio nell'era digitale*, cit., p. 45 ss. i concetti di oblio e riservatezza, seppur strettamente contigui, non coincidono e il fattore che distingue i due concetti è il tempo: il diritto all'oblio «non è rivolto a cancellare il passato, ma a proteggere il presente […]» (p. 48).

[768] Cfr. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss. e M.C. DAGA, *op. cit.*, p. 276, che ritiene il diritto all'oblio uno strumento a tutela del diritto all'identità personale; T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 686: «Diritto all'oblio e diritto alla *privacy* possono ben rappresentare due facce di una stessa medaglia, che affondano nella dignità della persona la loro rilevanza costituzionale […] la notizia non è un dato astratto alla *mercé* di tutti, perché riguarda la persona e la sua immagine in un dato momento storico; i dati personali, vale la pena ricordarlo, costituiscono una parte della espressione della personalità dell'individuo. Come ancora di recente, ha sostenuto la Corte di Giustizia UE nella decisione c.d. *Google Spain* (2014) e poi ha ribadito e confermato nella sentenza sul caso *Safe Harbour*, o altrimenti c.d. *Schrems* (2015)»; S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 70: «Sul piano della ricostruzione teorica il "diritto all'oblio" è connesso tanto al diritto alla riservatezza (e quindi alla *privacy*) quanto al diritto all'identità personale (e ai diritti della personalità in genere)»; secondo l'Autore, però, non è mera espressione del diritto alla riservatezza, ma «una proiezione, una variante, un riflesso».

[769] Cfr. T.E. FROSINI, *Liberté, Egalité, Internet*, cit., p. 118, che, come visto, qualifica il principio fondamentale della dignità umana quale fondamento costituzionale di tutti i diritti strettamente connessi allo sviluppo della persona, principio che apre nell'art. 1 la Carta dei diritti fondamentali dell'Unione europea; la protezione della dignità passa anche attraverso il diritto all'oblio. Secondo E. STRADELLA, *op. cit.*, pp. 24-25, accanto all'art. 2 Cost., la connessione tra diritto all'oblio e diritto all'identità personale giustifica anche «una differenziazione tra ipotesi di oblio costituzionalmente fondate *ex* art. 3, Cost., e

Il diritto all'oblio è previsto anche nella Dichiarazione dei diritti in Internet, che lo disciplina nell'art. 11: «Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica». La Dichiarazione tiene conto anche dei diritti e degli interessi confliggenti, nella consapevolezza che è necessario trovare un complesso equilibrio fra il diritto all'oblio del singolo e il diritto all'informazione e alla conoscenza della collettività nell'era della rete, dal momento che «il diritto all'oblio non può limitare la libertà di ricerca e il diritto dell'opinione pubblica a essere informata», «condizioni necessarie per il funzionamento di una società democratica». Nel caso di persone note o alle quali sono affidate funzioni pubbliche il diritto può essere esercitato solo se i dati che le riguardano non hanno alcun rilievo in relazione all'attività o alle funzioni esercitate. Peraltro, proprio in considerazione del suddetto bilanciamento, «se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all'autorità giudiziaria per garantire l'interesse pubblico all'informazione».

4.3.3. Bilanciamento tra diritti: *right to know*, identità, oblio

La persona con la sua identità come sintesi dinamica viene, quindi, tutelata nelle sue diverse molteplici espressioni, che afferiscono alla sua corretta rappresentazione contestualizzata e aggiornata, alla sua immagine fisica, sociale, digitale, alle sue informazioni e ai suoi dati personali e trova traduzione in una serie intricata e correlata di diritti, quali il diritto all'identità, il diritto all'oblio, il diritto alla protezione dei dati personali[770].

---

perciò meritevoli di una tutela specifica da parte dell'ordinamento, al di fuori e oltre i casi di cancellazione derivanti dalla tutela del diritto alla riservatezza nelle ipotesi di trattamento illecito dei dati personali e alle condizioni individuate dalla legislazione in materia di *privacy*, e generiche ipotesi di oblio»; l'Autrice porta l'esempio dell'evoluzione relativa alla sfera dell'identità sessuale rispetto a un'evoluzione di natura meramente comportamentale.

[770] Al riguardo è opportuno richiamare la sentenza della Corte di Giustizia dell'Unione europea *Wegrzybowski e Smolczewski vs. Polonia* del 16 luglio 2013, che delinea un diritto alla contestualizzazione, con integrazioni e precisazioni delle informazioni al fine di aggiornarle agli

In considerazione della sua ontologica configurazione, il diritto all'oblio, che si collega all'identità digitale oltre che alla protezione dei dati personali, si scontra inevitabilmente con il diritto all'informazione della collettività e pone la necessità di un bilanciamento tra il diritto a conoscere e il diritto a non essere più riconosciuti e quindi sostanzialmente ad essere conosciuti per la rappresentazione veritiera non del passato, ma qui e ora.

Entrambi i diritti si connettono strettamente ai dati e alle relative informazioni e, di conseguenza, chiamano in gioco il governo dei dati stessi; entrambi trovano fondamento ontologico nella persona che, da una parte, ha diritto a conoscere e, dall'altra, ha diritto ad essere conosciuta in modo veritiero: ciò fa emergere punti di convergenza nella disciplina dei due aspetti confliggenti, dal momento che in ambedue i casi è necessario dare piena centralità alla persona. E allora il contrasto si stempera perché il *right to know* e il *right to be forgotten*, almeno nella sua accezione legata all'identità, mirano entrambi alla tutela della persona e alla verità, rifuggendo la confusione incrementata dall'era degli algoritmi e dovendosi necessariamente affidare alle informazioni di qualità per ottenere tale risultato.

Diritto a conoscere e diritto all'oblio convergono anche in un comune dinamismo, che caratterizza altresì la protezione dei dati personali, di cui del resto il diritto all'oblio costituisce, altresì, un aspetto e una dimensione. Il fatto di mantenere contestualizzata e aggiornata l'immagine del soggetto, così come il diritto all'opposizione e alla cancellazione al ricorrere delle condizioni previste, richiamano, infatti, quella caratteristica di qualità, che è necessaria all'informazione nelle sue diverse declinazioni. L'aspetto fondamentale della qualità ricorre nelle diverse configurazioni attuali dei dati e delle informazioni: è imposta alla trasparenza amministrativa, è necessaria per gli *open data* ed è caratteristica intrinseca per avere reale valore dai *big data*, evitando manipolazioni o confusioni rispetto alla realtà e alle predizioni.

Esistono quindi punti di convergenza e si possono valorizzare le comuni istanze di qualità e verità, ma il bilanciamento resta comunque estremamente complesso, da svolgere caso per caso. Forse si può concordare, al riguardo, sul fatto che l'interesse di ogni individuo è sotteso a quello generale all'informazione e alla conoscenza, solo

---

avvenimenti successivi; la sentenza può ricordare, con differenze, il *leading case* della Corte di Cassazione italiana del 2012. Cfr., al riguardo, E. STRADELLA, *op. cit.*, p. 13 ss.

quando questa sia "inerente" alla finalità per la quale l'informazione è stata raccolta e risulti essere aggiornata e vera. In tal modo tutto sta in equilibrio.

Ma il problematico bilanciamento tra oblio e diritti della personalità da un lato e diritto all'informazione e diritto di cronaca dall'altro, tra art. 2 e art. 21 della Costituzione, si traduce anche in un sostanziale interrogativo di difficile risoluzione, ossia chi possa e chi debba effettuare questo bilanciamento[771].

In considerazione della natura globale della rete e del conseguente esercizio del diritto, tale soggetto non può essere lo Stato, costretto nel limite dei propri confini nazionali e caratterizzato da un conseguente atteggiamento rinunciatario rispetto alla dimensione globale di tali questioni[772], ma nemmeno si può ritenere soluzione perseguibile quella cui di fatto conduce la sentenza *Google Spain*, che con effetto perverso e contrario alle aspettative ha attribuito tale potere proprio nelle mani di quei privati, in specifico i motori di ricerca, ritenuti responsabili del trattamento e apparentemente sconfitti nella sentenza[773]. Al riguardo è dubbio che soggetti, mossi da finalità economiche e non dall'interesse della collettività, possano svolgere un ruolo para-costituzionale effettuando una valutazione circa la fondatezza delle richieste e operando un bilanciamento neutrale e indipendente; al contrario è probabile ritenere che soggetti non istituzionali antepongano il proprio interesse all'interesse della collettività alla conoscenza e siano propensi ad accogliere le richieste al fine di evitare altrimenti contenziosi, tranne nei casi in cui l'interesse generale coincida con il proprio, come laddove si profili il rischio di perdita di fiducia da parte degli utenti nel motore di ricerca[774].

Nonostante tali profonde e insanabili perplessità, di fatto i motori di ricerca si sono attivati a seguito della sentenza *Google Spain*, rendendo disponibili in rete moduli di richiesta per la cancellazione di dati, uscendo così vincitori nei fatti da una sentenza

---

771 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 70.

772 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 70.

773 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 75.

774 E. STRADELLA, *op. cit.*, pp. 12-13 e S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 70, secondo cui gli attori privati «invocando ora argomenti tecnocratici, ora il proprio carattere transnazionale, ora la libertà del commercio se non addirittura la libertà di pensiero, sfuggono senza difficoltà alle larghe maglie delle disposizioni nazionali o sovranazionali che tali diritti dovrebbero tutelare».

che li vedeva sconfitti e assumendo ancor più il ruolo di protagonisti e arbitri nel bilanciamento tra diritti nell'era contemporanea e nel governo dei dati; la procedura per la richiesta di cancellazione diventa allora "una questione privata" e ne è ben consapevole Google quando precisa «in quanto organizzazione privata, potremmo non essere nella posizione giusta per prendere decisioni in merito al tuo caso»[775]. È il caso di dire che la cura e i suoi effetti sono stati peggiori del male che si tentava di curare.

Ma sotto tale profilo una strategia interessante può consistere nell'affidarsi proprio a quel diritto contrapposto all'oblio, ossia al diritto alla conoscenza e in particolare ai processi di trasparenza e di apertura delle informazioni relative all'esercizio del potere di deindicizzazione e rimozione di contenuti da parte dei motori di ricerca: fornire in *open data* tali informazioni può essere una politica complementare proficuamente esperibile, nella quale il diritto all'informazione non confligge, ma permette di tutelare in modo più ampio il diritto all'oblio stesso, rendendo possibile un'adeguata valutazione dei processi decisionali adottati dai motori di ricerca al riguardo[776].

Tale strategia può essere attuata mediante diverse modalità concrete, con differenti potenzialità e diverse problematiche, che vanno da archivi *open data* con informazioni puntuali sui casi e sulle decisioni oppure *repository* con dati anonimizzati o pseudonimizzati senza possibilità di re-identificare i soggetti coinvolti o una banca dati contenente solo informazioni aggregate relative alle rimozioni (è la via scelta dal *Transparency Report* sul diritto all'oblio pubblicato da Google[777]) o, ancora, un archivio aperto solo a terzi qualificati quali sorta di revisori (ad esempio istituzioni accademiche) che possono rilasciare report periodici in merito: quest'ultima soluzione appare di maggior equilibrio tra le istanze di protezione dei dati dei soggetti coinvolti, da un lato,

---

775 S. PIETROPAOLI, *La rete non dimentica. Una riflessione sul diritto all'oblio*, cit., p. 77. Per supportare il proprio ruolo e le proprie valutazioni riguardo al diritto all'oblio, Google ha nominato un *Advisory Council* formato da esperti internazionali.

776 Cfr. A. MANTELERO, *The protection of the right to be forgotten: lessons and perspectives from open data*, in *Contratto e impresa – Europa*, fasc. 2, 2015, pp. 734-743.

777 Per esaminare le richieste arrivate a Google e gli esiti delle valutazioni cfr. *transparencyreport.google.com/eu-privacy/overview*. Come sottolinea A. MANTELERO, *The protection of the right to be forgotten: lessons and perspectives from open data*, cit., p. 740 tale scenario ha la debolezza di non fornire alcuna informazione sul contesto delle decisioni prese.

e l'interesse collettivo a conoscere come sono prese le decisioni, dall'altro; peraltro tale soluzione, basata sull'affidamento a istituzioni accademiche, non incontra ostacoli nell'art. 17 del regolamento europeo, che tra le eccezioni prevede il trattamento a fini di ricerca[778].

Nel pensiero della dottrina e anche nelle sentenze esaminate, il bilanciamento, per essere tale, non permette prevalenze apodittiche e assolute del diritto all'oblio a difesa della persona, che possono arrivare laddove estremizzate a far perdere il ricordo della stessa realtà, confliggendo con il diritto alla memoria e alla storia della collettività, di ogni consociato e, quindi, di ogni persona, arrivando a falsificare la verità e anche la democrazia[779]; non si possono quindi immaginare soluzioni di "oblio by default"[780], che

---

778 Sono i quattro scenari immaginati da A. MANTELERO, *The protection of the right to be forgotten: lessons and perspectives from open data*, cit., p. 737 ss., che di ognuno descrive punti di forza e di debolezza. Il quarto scenario è considerato condivisibilmente la soluzione migliore in termini di qualità della valutazione, indipendenza dei revisori terzi e riservatezza dei dati personali.

779 Cfr. S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 407, secondo cui «la via di una memoria sociale selettiva, legata al rispetto dei fondamentali diritti della persona, può indirizzarci verso l'equilibrio necessario nel tempo della grande trasformazione tecnologica». A. MASERA - G. SCORZA, *op. cit.*, p. 73: «Perché se chiunque ha diritto a far sparire dalla rete le tracce del proprio passato, tutti gli altri vengono privati del diritto di conoscere fatti, eventi e persone». Sul valore della memoria per l'umanità V. MAYER-SCHÖNBERGER, *op. cit.*, p. 15 ss.: «la memoria esterna è un'estensione di quella umana. Ma può essere utilizzata anche per contribuire alla realizzazione di una memoria comune» (p. 25).

780 È la soluzione prospettata da V. MAYER-SCHÖNBERGER, *op. cit.*, che suggerisce una data di scadenza per le informazioni. L'Autore analizza sei soluzioni per prevenire o combattere i pericoli della memoria digitale in termini di potere e tempo: l'astinenza digitale; la tutela dei dati personali; la struttura dei diritti della privacy digitale (DRM a tutela dei dati personali); l'adeguamento cognitivo; l'ecologia dell'informazione (ossia norme atte a limitare raccolta e memorizzazione delle informazioni); la contestualizzazione perfetta. Le prime tre soluzioni sono relazionali e tentano di risolvere la questione della perdita di controllo e del potere sull'informazione, ma non le problematiche legate al tempo; le ultime tre risolvono, invece, la sfida temporale. Dal momento che nell'analisi l'Autore evidenzia problematiche, difficoltà o perplessità sull'efficacia (è il caso della normativa sulla privacy) delle sei soluzioni, propende per una soluzione di "ripristino dell'oblio", grazie all'attribuzione di una data di scadenza alle informazioni digitalmente memorizzate (per mezzo di una metainformazione da collegare all'informazione) e all'eliminazione automatica successiva delle informazioni "scadute"; la soluzione secondo l'Autore, ha i vantaggi di incrementare la consapevolezza, richiedere modifiche tecniche relativamente modeste e migliorare la qualità dell'informazione, anche se presenta i rischi correlati di essere binaria (e non graduale) e di poter essere da sola insufficiente, necessitando di ulteriori misure.

non bilanciano, ma scelgono in via generale tra diritti che invece hanno pari dignità[781]. Scelte del genere esporrebbero il contesto europeo anche a problemi di natura geopolitica. Infatti, al riguardo, è necessario richiamare la grande distanza tra Europa e Stati Uniti, che sono caratterizzati da una chiara preminenza della libertà di espressione, del diritto a informare ed essere informati rispetto all'interesse ad essere dimenticati[782].

La strada quindi è il bilanciamento, da condurre come esaminato avendo riguardo alla persona, alla qualità delle informazioni, alla verità delle stesse.

Il diritto a conoscere, nella configurazione attuale dinamica e attiva, deve fare i conti e bilanciarsi non solo con il rispetto dell'identità digitale e la tutela del diritto all'oblio, ma altresì con altri interessi protetti dagli ordinamenti, in particolare la proprietà intellettuale, oggetto di analisi nei prossimi paragrafi di questo capitolo, e la protezione dei dati personali, oggetto di analisi nel prossimo capitolo.

4.4. Il diritto d'autore nella *digital age*

La rivoluzione digitale incrementa in modo esponenziale le modalità di circolazione e fruizione dei contenuti, incidendo profondamente sulla conoscenza e, quindi, sulla proprietà intellettuale: il diritto a conoscere si fortifica, si amplia e muta nell'era contemporanea, dal momento che è semplice, veloce ed economico acquisire e diffondere dati e informazioni. Di conseguenza, il cambiamento che interessa il mondo

---

781 Cfr., al riguardo, M. RIZZUTI, *op. cit.*, p. 1080 ss.; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, cit., p. 591 ss.; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 398: «Se si riconosce il diritto alla cancellazione, sciolto da ogni vincolo, allora la permanenza dell'informazione è in pericolo, l'identità diviene solo presente e sciolta dal passato, la memoria non ha più radici. La memoria-identità viene meno e rimane solo una forma di memoria come selezione arbitraria»; E. STRADELLA, *op. cit.*, p. 7, che, in caso di "oblio by default", richiama gli effetti uniformanti e distorsivi della traduzione in rete della naturale propensione a dimenticare propria della mente umana; M. D'AMBROSIO, *op. cit.*, pp. 54-55, secondo cui è necessario «uno sforzo ermeneutico costante, che non può che risolversi nell'impossibilità di adottare soluzioni tendenzialmente universali. […] In buona sostanza, i legislatori nazionale ed europeo, raccogliendo l'ammonimento sull'importanza di ricordarsi di dimenticare, fatta salva la protezione dell'inderogabile valore della persona, dovrebbero ragionevolmente prendere atto che l'oblio non può realizzarsi sempre e, soprattutto, a ogni costo».

782 E. STRADELLA, *op. cit.*, p. 13 ss.

digitale e l'ampliamento del diritto a conoscere devono necessariamente fare i conti con un interesse tutelato dall'ordinamento: il diritto d'autore[783].

Per poter analizzare la tutela del diritto d'autore nel governo dei dati e nelle diverse configurazioni assunte dai dati stessi, è necessario uno sguardo alla disciplina del diritto d'autore al fine di comprendere innanzitutto il difficile adattamento della regolazione alla realtà della rete[784]. Successivamente l'analisi si concentrerà sul governo dei dati, sulla tutela della proprietà intellettuale e sul necessario bilanciamento con altri diritti e istanze, in particolare la libertà d'informazione.

Nell'articolato contesto giuridico di riferimento a livello internazionale[785] ed europeo[786], preme ricordare in premessa che l'art. 27, comma 2, della Dichiarazione universale dei diritti dell'uomo e l'art. 17, comma 2 (dedicato al diritto di proprietà) della Carta dei diritti fondamentali dell'Unione europea tutelano la proprietà intellettuale e il diritto d'autore[787].

---

783 Secondo R. RAZZANTE, *op. cit.*, p. 343 ss. «il contemperamento di opposti interessi di autori e utenti costituisce, anche nella Rete, il principio cui deve ispirarsi la normativa in tema di diritto d'autore». Le riflessioni di questo paragrafo tengono in considerazione l'analisi contenuta in F. FAINI, Digital age *e diritto dei privati*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 203-223.

784 G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2016, pp. 499-516: storicamente il diritto d'autore è frutto della tecnologia; nasce nella rivoluzione industriale ed è "figlio" dell'invenzione della stampa e dell'esigenza di tutelare l'editoria e gli autori.

785 Sono numerosi i trattati e le convenzioni internazionali, quali la Convenzione di Berna per la protezione delle opere letterarie e artistiche, adottata nel 1886 e sottoposta a revisioni nel corso degli anni, la *Universal Copyright Convention*, adottata nel 1952 e successivamente rivista, l'accordo TRIPs (*the agreement on Trade-Related Aspects of Intellectual Property Rights*) del 1994 e i due trattati del WIPO (*World Intellectual Property Organization*), ossia il *WIPO Copyright Treaty* (WCT) e il *WIPO Performances and Phonograms Treaty* (WPPT), approvati nel 1996.

786 Tra le direttive maggiormente rilevanti a livello europeo la direttiva 91/250/CEE, la direttiva 96/9/CE, la direttiva 2001/29/CE, la direttiva 2004/48/CE, la direttiva 2006/115/CE, la direttiva 2006/116/CE, la direttiva 2009/24/CE, la direttiva 2014/26/UE.

787 Rilevante anche l'art. 1 del protocollo addizionale alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU): dispone la tutela del diritto di proprietà e la portata è estesa anche alla proprietà intellettuale, che di conseguenza può essere fatta rientrare nel comma 2 dell'art. 10 della CEDU tra i "diritti altrui" che possono limitare la libertà d'espressione; cfr. M. NINO,

4.4.1. La disciplina italiana del diritto d'autore online

Nel nostro Paese il diritto d'autore trova fondamento in un complesso combinato di norme costituzionali, quali l'art. 2 (diritti inviolabili), l'art. 3 (il pieno sviluppo della persona umana), l'art. 4 (progresso materiale o spirituale della società), l'art. 9 (sviluppo della cultura e della ricerca scientifica e tecnica), l'art. 21 (libertà di manifestazione del pensiero e di espressione), l'art. 33 (libertà dell'arte e della scienza), l'art. 35 (tutela del lavoro in tutte le sue forme e applicazioni), l'art. 36 (retribuzione del lavoratore), l'art. 41 (libertà di iniziativa economica) e l'art. 42 (tutela della proprietà); parla espressamente di "opere dell'ingegno" l'art. 117, comma 2, lett. r) della Costituzione, che prevede al riguardo la potestà legislativa esclusiva dello Stato[788].

La Dichiarazione dei diritti in Internet richiama «i diritti derivanti dal riconoscimento degli interessi morali e materiali legati alla produzione di conoscenze» e, significativamente, la previsione è contenuta nella disposizione dedicata al diritto alla conoscenza in rete, mostrando consapevolezza del complesso e necessario bilanciamento tra i due diritti[789].

A livello normativo il diritto d'autore è disciplinato dal Codice civile nel Libro V, Titolo IX, art. 2575 e ss., e dalla legge 22 aprile 1941, n. 633, come modificata e integrata nel corso degli anni, anche a seguito di impulsi internazionali ed europei[790].

Il diritto d'autore protegge ampiamente le opere dell'ingegno di carattere creativo, che appartengono alle scienze, alla letteratura, alla musica, alle arti figurative,

---

Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale, cit., p. 554 ss.

788 Cfr. sentenza della Corte costituzionale 6 aprile 1995, n. 108 e P. COSTANZO, *Quale tutela del diritto d'autore in internet?*, in *Giurisprudenza Costituzionale*, fasc. 6, 2015, p. 2347 ss.

789 Art. 3, Dichiarazione dei diritti in Internet.

790 La legge 633/1941, recante «*Protezione del diritto d'autore e di altri diritti connessi al suo esercizio*», è stata modificata, tra gli altri, dal d.lgs. 518/1992 (attuazione della direttiva 91/250/CEE), dal d.lgs. 169/1999 (attuazione della direttiva 96/9/CE), dalla legge 248/2000 e dal d.lgs. 68/2003 (attuazione della direttiva 2001/29/CE). E. BARONE, *Diritto d'autore e ICT*, in M. MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Tangram edizioni scientifiche, Trento, 2017, p. 313 ricorda, accanto alle norme principali, la presenza di altre disposizioni, come quelle sanzionatorie contenute nel codice penale.

all'architettura, al teatro e alla cinematografia, qualunque ne sia il modo o la forma di espressione[791], e i cosiddetti beni informatici (i programmi per elaboratore e le banche dati), che per le caratteristiche peculiari che li connotano e la distanza dalle opere artistiche sono state definite "opere utili"[792].

Per incontrare la relativa protezione giuridica, la creazione intellettuale deve avere un'estrinsecazione nel mondo materiale, concretizzarsi in una forma oggettivata e percepibile e non essere solo un'idea astratta; le idee astratte sono libere e non sono protette come bene giuridico[793]. Sono protette anche le opere cosiddette derivate «*senza pregiudizio dei diritti esistenti sull'opera originaria*», dove il carattere creativo è legato all'elaborazione successiva: nella realtà digitale che facilita il riutilizzo, l'elaborazione e il *mash-up*, questa disposizione risulta particolarmente significativa, così come la prevista protezione delle opere plurisoggettive e collettive, considerando la diffusione degli strumenti *wiki*[794].

La creazione dell'opera, quale particolare espressione del lavoro intellettuale, è titolo originario all'acquisto del diritto d'autore e comporta l'acquisizione automatica dei diritti, lo sfruttamento delle prerogative e dei diritti collegati[795]; la connessa protezione giuridica è automatica e non è richiesta alcuna formalità[796]. Di conseguenza,

---

791 Art. 2575 c.c. e art. 1, comma 1, legge 633/1941. L'art. 2, legge 633/1941 riporta un'elencazione non esaustiva, ma esemplificativa di opere dell'ingegno che ricadono sotto la protezione della normativa.

792 Artt. 1 e 2, legge 633/1941. Particolare opera dell'ingegno è l'opera multimediale, locuzione utilizzata nell'art. 171-ter, legge 633/1941; cfr. al riguardo C. DI COCCO, *Il diritto d'autore nell'era digitale: la tutela dei beni informatici,* in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli, Torino, 2013, p. 175 ss.

793 La stessa idea può essere alla base di diverse opere d'autore che saranno diverse per la creatività soggettiva, che è costituita dalla forma della sua espressione; cfr. Corte di Cassazione civile, sez. I, 11 agosto 2004, n. 15496. Cfr. C. DI COCCO, *op. cit.*, p. 139 ss. e G. D'AMMASSA, *La legge sul diritto d'autore nell'era multimediale*, in C. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, p. 379 ss.

794 Art. 4, legge 633/1941. La legge disciplina le opere create in rapporto di lavoro dipendente e le opere plurisoggettive, collettive, in comune o composte (artt. 7 e 10); cfr. A.M. GAMBINO - A. STAZI, *op. cit.*, p. 154 ss. e D. SBARISCIA, *La tutela attraverso la disciplina del diritto d'autore*, in G. FINOCCHIARO - F. DELFINI, *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, p. 875 ss.

795 Art. 2576 c.c. e art. 6, legge 633/1941.

796 Cfr. M. TRAVOSTINO, *op. cit.*, p. 201 ss.

è rilevante l'esatta identificazione del momento della creazione; è reputato autore chi è indicato come tale nelle forme d'uso, salvo prova contraria[797].

Il diritto d'autore, nato nell'era analogica, si compone di diritti morali, irrinunciabili, inalienabili e imprescrittibili, quale il diritto alla paternità dell'opera[798], e di diritti patrimoniali o di utilizzazione economica, che si sostanziano in una serie di privative, ossia facoltà di utilizzazione economica esclusive e indipendenti[799]. L'autore ha il diritto esclusivo di pubblicare l'opera e di utilizzarla economicamente in ogni forma e modo, originale o derivato, nei limiti e per gli effetti fissati dalla legge; i diritti esclusivi attengono a una serie di facoltà quali la pubblicazione, la riproduzione, l'esecuzione, la rappresentazione, la comunicazione al pubblico e la messa a disposizione del pubblico, la distribuzione, la traduzione, la modifica, l'elaborazione e la trasformazione. I diritti patrimoniali, tranne eccezioni e diversi termini di decorrenza, durano tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte[800].

Alla luce di tali disposizioni, i diritti patrimoniali comportano la caratteristica dell'esclusività, dal momento che le utilizzazioni possono essere precluse a soggetti diversi dal titolare, se non autorizzate nei limiti e modi che il titolare stabilisce[801]. Di conseguenza, in considerazione dei diritti spettanti al titolare del diritto d'autore, da un punto di vista legale l'utilizzo dell'opera digitale protetta dalla legge 633/1941 avviene legittimamente con l'autorizzazione da parte dell'autore per mezzo di una licenza, ossia un contratto o altro strumento negoziale, deputato a stabilire le utilizzazioni consentite giuridicamente. Per quanto riguarda i contenuti digitali, utilizzando le categorie delle licenze dei software, si distingue tra sistemi di tutela tradizionali, con le relative licenze

---

797 Art. 8, legge 633/1941.

798 I diritti morali sono il diritto alla paternità, il diritto all'integrità dell'opera, il diritto di inedito e il c.d. diritto di pentimento, che è esercitabile solo in presenza di specifiche condizioni; sono disciplinati dagli artt. 20-24, legge 633/1941.

799 Si tratta dei diritti di sfruttamento economico disciplinati dagli artt. 12-19, legge 633/1941. Ai sensi dell'art. 19, comma 1, legge 633/1941, i diritti esclusivi «*sono fra loro indipendenti. L'esercizio di uno di essi non esclude l'esercizio esclusivo di ciascuno degli altri diritti*».

800 Art. 25, legge 633/1941 e art. 17, comma 1, legge 6 febbraio 1996, n. 52. Trascorso il previsto periodo temporale le opere diventano liberamente fruibili da un punto di vista economico.

801 Art. 2577 c.c. e art. 12, legge 633/1941.

"proprietarie", e sistemi con licenze "aperte", in relazione ai diversi diritti concessi a chi fruisce di ciò che è tutelato dal diritto d'autore, seppur entrambe fondate sulla disciplina normativa della proprietà intellettuale: sono licenze aperte le *Creative Commons*, esaminate in relazione agli *open data*[802].

Nell'era digitale i contenuti, i materiali e le opere digitali cadono sotto la protezione giuridica del diritto d'autore e, come esaminato in relazione agli *open data*, anche le informazioni strutturate[803], i *dataset* e le banche dati (*database*) (analizzate più avanti), quali insiemi organizzati di dati.

Pertanto, per poter utilizzare opere e contenuti protetti dal diritto d'autore nell'ecosistema digitale, è necessario attenersi all'eventuale licenza aperta, laddove sia presente, o, altrimenti, ottenere l'autorizzazione da parte dell'autore, tranne nei casi residuali di eccezione, in cui non si applica la normativa, o nell'ipotesi di superamento del previsto lungo termine di tutela del diritto[804].

La regolazione è consapevole della realtà digitale e questo emerge chiaramente in alcune disposizioni. In considerazione proprio della rete e delle esigenze di funzionamento della stessa «*sono esentati dal diritto di riproduzione gli atti di riproduzione temporanea privi di rilievo economico proprio che sono transitori o accessori e parte integrante ed essenziale di un procedimento tecnologico, eseguiti all'unico scopo di consentire la trasmissione in rete tra terzi con l'intervento di un intermediario, o un utilizzo legittimo di un'opera o di altri materiali*» (art. 68-bis, legge 633/1941): tale tipologia di copia in senso tecnico include la realizzazione di copie *cache* necessarie al funzionamento stesso della rete. Con la consapevolezza della specificità della rete è consentita «*la libera pubblicazione attraverso la rete internet, a*

---

802 *Supra*, cap. 3. Cfr. B. CUNEGATTI, *op. cit.*, p. 641 ss.

803 Cfr. G. MANCOSU, *op. cit.*, p. 3 ss.; C. SAPPA, *op. cit.*, p. 186 ss.; A.M. ROVATI, *op. cit.*, p. 155. Al riguardo, più ampiamente, *supra*, capitolo 3.

804 In tal senso la direttiva 2014/26/UE del 26 febbraio 2014 nell'art. 3, lett. c) e lett. k) significativamente definisce titolare dei diritti «*qualsiasi persona o entità, diversa da un organismo di gestione collettiva, che detiene diritti d'autore o diritti connessi ai diritti d'autore o a cui, in base a un accordo per lo sfruttamento dei diritti o alla legge, spetta una parte dei proventi*» e utilizzatore «*qualsiasi persona o entità le cui azioni sono subordinate all'autorizzazione dei titolari dei diritti, al compenso dei titolari dei diritti o al pagamento di un indennizzo ai titolari dei diritti e che non agisce in qualità di consumatore*».

titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro» (art. 70, comma 1-bis, legge 633/1941). Sempre con riferimento a Internet, ponendo un limite di carattere generale, si precisa che le eccezioni e le limitazioni al diritto d'autore «*quando sono applicate ad opere o ad altri materiali protetti messi a disposizione del pubblico in modo che ciascuno possa avervi accesso dal luogo e nel momento scelto individualmente, non devono essere in contrasto con lo sfruttamento normale delle opere o degli altri materiali, né arrecare un ingiustificato pregiudizio agli interessi dei titolari*» (art. 71-novies).

Al di là delle singole norme, però, la disciplina del diritto d'autore, basata sul controllo della circolazione delle opere e dei contenuti, faticosamente si adegua al mutato contesto digitale, in cui diventa problematica l'applicazione dei diritti di proprietà intellettuale[805].

L'opera si distacca dalla necessità di un supporto materiale e non ha più i limiti del *corpus mechanicum*, le condizioni spazio-temporali e l'ubiquità della rete rendono globale la fruizione dei contenuti, possibile in ogni momento e in ogni luogo, e diventa agevole trarre infinite copie di un'opera con la stessa qualità dell'originale sostanzialmente a costo zero[806]. Nel mondo digitale, pertanto, diventa difficile controllare e limitare la circolazione di quanto è protetto dal diritto d'autore: mutano le condizioni economiche di creazione e distribuzione, non sembra più necessaria l'intermediazione dell'industria culturale e si generano nuovi modelli economici, insieme a inediti modelli di espressione della creatività (si pensi alle opere derivate e

---

[805] Sul diritto d'autore nell'era digitale cfr., *inter alia*, G. D'AMMASSA, *op. cit.*, p. 379 ss.; C. DI COCCO, *op. cit.*, p. 139 ss.; S. ERCOLANI, *Il diritto d'autore e i diritti connessi. La legge 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE*, Giappichelli, Torino, 2004; L.C. UBERTAZZI, *I diritti d'autore e connessi. Scritti*, II ed., Giuffrè, Milano, 2003; G. MAZZIOTTI, *Il copyright digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, pp. 175-199.

[806] Il regolamento Agcom, approvato con delibera 680/13/CONS, definisce nell'art. 1, comma 1, lett. p) l'opera digitale come «*un'opera, o parti di essa, di carattere sonoro, audiovisivo, fotografico, videoludico, editoriale e letterario, inclusi i programmi applicativi e i sistemi operativi per elaboratore, tutelata dalla Legge sul diritto d'autore e diffusa su reti di comunicazione elettronica*».

alle opere collettive, al *mash-up*[807] e al *wiki*) e di fruizione delle informazioni, che possono anche sostanziare nuove forme di violazione dei diritti (sistemi di condivisione *peer-to-peer*)[808].

Sotto il profilo economico, grazie alle tecnologie digitali, alla rete e al *web 2.0*, si crea di fatto una non-rivalità nei consumi dei contenuti digitali ed è difficile escludere utenti dal consumo, anche quando questi non siano disposti a pagare il relativo corrispettivo: la pirateria digitale è in realtà una conferma evidente della difficoltà di considerare questi beni digitali quali beni privati ed escludibili[809]. Al riguardo, peraltro, è opportuno precisare che la pirateria digitale non solo riduce i ricavi del titolare del diritto, ma riduce gli incentivi a produrre e innovare, dato che il titolare non riesce ad acquisire i frutti del proprio lavoro: per tale strada il fenomeno della pirateria si pone in contrasto diretto anche con gli interessi pubblici alla creatività, alla ricerca, alla concorrenza e allo sviluppo della conoscenza[810].

Il mondo digitale, che ha visto evolvere il web verso il *web 2.0* e il *web of data*, è profondamente caratterizzato dai principi di condivisione e dinamicità, che rendono agevole scaricare, copiare, manipolare e riprodurre, favorendo il riutilizzo capace di azionare l'intelligenza collettiva; di conseguenza diventa particolarmente complesso proteggere il diritto d'autore. Nella rete i contenuti digitali possono non essere pubblicati dall'autore, ma riutilizzati e ridistribuiti e, pertanto, diventa difficile risalire all'autore per ottenerne l'autorizzazione all'utilizzo oppure possono essere pubblicati su piattaforme di condivisione (come i *social*) e in quel caso è necessario visionare le relative *policy* e condizioni di uso per capire chi vanta diritti al riguardo.

---

807 Secondo G. MODESTI, *op. cit.*, p. 29 *mash-up* è un «termine utilizzato nell'ambito delle opere creative per cui un'opera è costituita interamente da parti di altre opere, tra loro integrate. Esso è stato poi esteso al contesto informatico ad indicare un processo in cui si integrano contenuti, dati e informazioni provenienti da fonti differenti per fornire nuovi servizi».

808 Cfr. G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., pp. 499-516.

809 Cfr. A. STAZI, *La tutela del diritto d'autore in rete: bilanciamento degli interessi, opzioni regolatorie europee e "modello italiano"*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2015, p. 89 ss.

810 Cfr. A. STAZI, *op. cit.*, p. 89 ss. e P. OTRANTO, *op. cit.*, p. 223 ss.

Nel difficile adattamento della normativa del diritto d'autore alla realtà digitale emerge nuovamente quel passaggio dal concetto di proprietà al concetto di accesso che connota l'avvento e l'impatto della realtà digitale e investe necessariamente anche la "proprietà" intellettuale. La struttura dominicale del diritto d'autore, tesa a proteggere il titolare, emerge nella relativa disciplina e mal si integra nel mutato contesto digitale, dove gli *users* acquisiscono un ruolo diverso, dinamico e attivo: diventa necessario trovare un equilibrio tra tali soggetti e i relativi interessi di cui sono portatori e sviluppare la funzione sociale e l'aspetto pubblicistico del diritto d'autore[811]. Verso questa strada, peraltro, conducono anche due caratteristiche che, a ben guardare, connotano intimamente l'opera dell'ingegno, ossia l'essere condivisibile per natura (si pensi ad esempio a un'opera letteraria fatta per essere letta e trasmessa) e l'essere originaria, ossia prodotto di un atto di creazione, ma indipendente dall'autore e capace anche di sopravvivergli[812].

In questo contesto, i diritti di proprietà intellettuale, che limitano e "chiudono" le possibilità su contenuti che spettano all'autore, si scontrano in modo aperto con le istanze di conoscenza e apertura che pervadono la realtà contemporanea.

L'ordinamento, allora, al fine di assicurare un'efficace tutela, oltre a strumenti di ordine legale, ricorre alla tecnologia stessa e si avvale di strumenti difensivi offerti dalla tecnica per garantire la sua osservanza: si prevede la possibilità di ricorrere a misure tecnologiche di protezione a presidio delle opere digitali, in modo che alcune operazioni, come accessi, utilizzi o copie non autorizzate, non solo siano giuridicamente illecite, ma siano anche inibite tecnicamente. Le misure tecnologiche di protezione comprendono ampiamente «*tutte le tecnologie, i dispositivi o i componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti non autorizzati dai titolari dei diritti*» e sono considerate efficaci «*nel caso in cui l'uso dell'opera o del materiale protetto sia controllato dai titolari tramite l'applicazione di un dispositivo di accesso o di un procedimento di protezione, quale la cifratura, la distorsione o qualsiasi altra trasformazione dell'opera o del materiale protetto, ovvero*

---

811 Cfr. G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., p. 499 ss.

812 Cfr. A.C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, II ed., Giappichelli, Torino, 2015, p. 297 ss.

sia limitato mediante un meccanismo di controllo delle copie che realizzi l'obiettivo di protezione» (art. 102-quater, legge 633/1941). In tal modo la condotta non autorizzata diventa impossibile e si tutela giuridicamente il titolare contro l'elusione delle misure tecnologiche di protezione.

Accanto alle misure tecnologiche di protezione, la normativa fornisce anche la possibilità di applicare le cosiddette informazioni elettroniche sul regime dei diritti, che semplificano la gestione dei diritti stessi e della relativa tutela giuridica: «*identificano l'opera o il materiale protetto, nonché l'autore o qualsiasi altro titolare dei diritti. Tali informazioni possono altresì contenere indicazioni circa i termini o le condizioni d'uso dell'opera o dei materiali, nonché qualunque numero o codice che rappresenti le informazioni stesse o altri elementi di identificazione*» (art. 102-quinquies, legge 633/1941)[813].

In tale contesto, la nozione di *digital rights management* (DRM) è più ampia e si riferisce all'insieme delle tecnologie informatiche e telematiche che si occupano della gestione in forma digitale dei diritti: sono sistemi che combinano misure tecnologiche di protezione e i cosiddetti *rights expression languages* (RELs), che consentono la gestione elettronica delle facoltà di utilizzazione, l'identificazione, la tracciabilità dei contenuti e il sistema di pagamento[814].

Tali strumenti, efficaci per prevenire e reprimere violazioni, possono avere però l'effetto di limitare la diffusione e la circolazione delle opere e dei contenuti digitali. E invece le istanze di condivisione e collaborazione della rete, i principi pervasivi di uguaglianza, libertà e reciprocità resi possibili da Internet, insieme all'emersione di un nuovo paradigma sociale ed economico, sono forti e capaci di andare oltre, arrivando a scardinare i modelli tradizionali*:* la rete stessa ha previsto accanto al modello *client* (utente) - *server* (fornitore di servizio) il modello *peer-to-peer* (P2P), dove ogni nodo della rete svolge entrambe le funzioni (*server* e *client*), mettendo a disposizione una

---

[813] L'art. 171-ter, legge 633/1941 prevede specifiche sanzioni a salvaguardia delle misure tecnologiche e delle informazioni elettroniche.

[814] Cfr. G. MAZZIOTTI, *op. cit.*, p. 182 ss.

parte delle proprie risorse e utilizzando risorse messe a disposizione da altri. In tal modo si possono condividere *file* (*file sharing*); è il caso di BitTorrent ed eMule[815].

Il *file sharing*, che si pone quale veicolo di opere, capace di promuovere la conoscenza e la circolazione della cultura, finisce al tempo stesso per generare violazioni del diritto d'autore e fenomeni di pirateria digitale in relazione a quanto messo in condivisione, mettendo a rischio i diritti del titolare, in particolare la sua remunerazione[816]. Il *file sharing* ha generato svariati casi giudiziari in merito alla liceità di tali sistemi, con decisioni diverse, talvolta di condanna dei fornitori di tali sistemi, quali concorrenti e partecipi delle violazioni del diritto d'autore commesse dagli utenti (il caso di *Napster*, chiuso, di conseguenza, nel 2001 e il caso *Pirate Bay* del 2009). Il dibattito è acceso e ha generato diverse posizioni: accanto a chi crede nella necessità di rigide sanzioni a tutela della proprietà intellettuale e chi, al contrario, reputa debba essere abbandonato il tradizionale modello del diritto d'autore, c'è chi propone soluzioni di compromesso consapevoli della nuova realtà, quale un pagamento ridotto, idoneo a proteggere il titolare, ma che non confini nell'illiceità tali sistemi[817].

Alla luce di quanto esaminato, la tutela del diritto d'autore è particolarmente complessa nell'era digitale della condivisione e della conoscenza e confligge in modo diretto con il *right to know*, che il mondo digitale sembra promettere in misura illimitata: diventa difficile adattare alla diversa realtà della rete regole idonee a una realtà analogica.

---

815 Tale modello ha diverse esplicazioni, che vanno dalla condivisione della potenza di calcolo, alla condivisione delle connessioni Internet fino alla realizzazione più significativa che consiste nella condivisione di *file* (*file sharing*). Esempio celebre è il sistema Napster per la condivisione di *file* musicali che, reso disponibile nel 1999, è stato rapidamente usato in larga scala come primo sistema *peer-to-peer* di massa. In realtà in Napster i *file* risiedono nei diversi calcolatori e tramite un indice allocato in un *server* centrale sono specificati i nodi presso i quali i *file* cercati sono disponibili; le reti *peer-to-peer* "pure" sono, invece, architetture "acefale" e non richiedono l'utilizzo di un *server* e di un indice centrale (es. Gnutella, BitTorrent, eMule). Cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, cit., p. 58 ss.

816 Cfr. O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, in *Giurisprudenza italiana*, fasc. 8-9, 2011, pp. 1944-1953. Per la tematica del *peer-to-peer* e del *file sharing* si rimanda alla vasta letteratura in merito.

817 Cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, cit., p. 58 ss.

Proprio in considerazione di queste difficoltà, oltre alla tutela giurisdizionale[818], al fine di proteggere in modo efficace il diritto d'autore nell'era digitale, un ruolo particolarmente incisivo è stato assunto da un'autorità amministrativa indipendente, l'Autorità per le Garanzie nelle Comunicazioni (di seguito anche Agcom o Autorità)[819], che il 12 dicembre 2013 ha approvato, a seguito di un'ampia consultazione e della notifica alla Commissione europea, con delibera 680/13/CONS, il «*Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70*» (di seguito anche reg. Agcom), entrato in vigore il 31 marzo 2014[820].

Nel regolamento Agcom, la tutela del diritto d'autore online viene attuata attraverso due ordini di interventi: da una parte, la promozione di misure per la legittima diffusione di opere digitali (misure proattive e positive), dall'altra la previsione di procedure volte all'accertamento e alla cessazione delle condotte illecite (misure di contrasto alla pirateria digitale di carattere *lato sensu* sanzionatorio, che intervengono nel momento patologico della violazione del diritto d'autore)[821].

Con il fine esplicito di promuovere lo sviluppo dell'offerta legale di opere digitali e l'educazione alla corretta fruizione delle stesse (e, in tal modo, intervenire preventivamente sul fenomeno della pirateria digitale), il regolamento Agcom prevede misure positive dirette a tale scopo, tra le quali l'istituzione di un Comitato per lo sviluppo e la tutela dell'offerta legale di opere digitali, composto da un'ampia rappresentanza dei diversi *stakeholder* in gioco, finalizzato proprio a individuare iniziative volte a tali fini, quali l'educazione alla legalità nella fruizione di opere digitali (anche attraverso l'adozione di procedure di reindirizzamento automatico ad apposite pagine Internet a ciò dedicate), la promozione di codici di condotta, il sostegno allo sviluppo di opere digitali e il monitoraggio dell'offerta legale[822].

---

818 La tutela civile, penale e amministrativa assistono la disciplina del diritto d'autore; cfr. G. D'AMMASSA, *op. cit.*, p. 395 ss.

819 Istituita dalla legge 249/1997.

820 Art. 19, reg. Agcom. Cfr. L.C. UBERTAZZI (a cura di), *Il regolamento Agcom sul diritto d'autore*, Giappichelli, Torino, 2014.

821 Art. 2, comma 1, reg. Agcom.

822 Art. 3 ss., reg. Agcom.

A queste azioni positive il regolamento accompagna in modo complementare e sinergico misure di *enforcement* di lotta alla pirateria, disciplinando le attività dell'Autorità in materia di tutela del diritto d'autore online e, in particolare, le procedure volte all'accertamento e alla cessazione delle violazioni del diritto d'autore e dei diritti connessi poste in essere sulle reti di comunicazione elettronica[823].

Nel garantire la tutela del diritto d'autore il regolamento è consapevole della necessità del bilanciamento tra gli interessi fondamentali in gioco e chiarisce espressamente che «*nell'applicazione della disciplina del diritto d'autore sulle reti di comunicazione elettronica è necessario operare un contemperamento tra i diversi diritti in gioco, rispettando le libertà di comunicazione, di espressione e di manifestazione del pensiero, il diritto alla privacy e l'accesso dei cittadini alla cultura e ad internet, alla luce di quanto sancito dall'ordinamento dell'Unione europea in materia di comunicazioni elettroniche, e tutelando il diritto d'autore e la remunerazione del titolare dei diritti*»[824].

In merito alle procedure di *enforcement*, l'intervento dell'Autorità è previsto su istanza di parte e non d'ufficio e sono state fatte salve le eventuali procedure autoregolamentate di *notice and take down* messe a disposizione dalle principali piattaforme[825].

---

823 Art. 2, reg. Agcom.

824 Tale passaggio è contenuto nella parte narrativa della delibera 680/13/CONS. Il regolamento (allegato A della delibera) chiarisce, altresì, nell'art. 2, comma 2, che nello svolgimento delle attività, «*l'Autorità opera nel rispetto dei diritti e delle libertà di comunicazione, di manifestazione del pensiero, di cronaca, di commento, critica e discussione, nonché delle eccezioni e delle limitazioni di cui alla Legge sul diritto d'autore. In particolare, l'Autorità tutela i diritti di libertà nell'uso dei mezzi di comunicazione elettronica, nonché il diritto di iniziativa economica e il suo esercizio in regime di concorrenza nel settore delle comunicazioni elettroniche, nel rispetto delle garanzie di cui alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e alla Carta dei diritti fondamentali dell'Unione europea*». Al riguardo, secondo A. STAZI, *op. cit.*, p. 89 ss., il regolamento Agcom «ha inteso proporre un modello – originale nel panorama internazionale – basato su un " 'ordine valoriale' equilibrato"», idoneo a realizzare una sintesi tra i diversi interessi in gioco.

825 Art. 5, reg. Agcom. Le procedure di *notice and take down* sono «le procedure finalizzate alla rimozione di contenuti illeciti dalle reti di comunicazione elettronica» (art. 1, lett. dd), reg. Agcom): permettono ai titolari del diritto d'autore di segnalare condotte illecite al fornitore di servizi e di chiedere la rimozione spontanea di contenuti illeciti.

Il soggetto legittimato[826], qualora ritenga che un'opera digitale sia stata resa disponibile su una pagina Internet in violazione della legge sul diritto d'autore, può presentare un'istanza all'Autorità, chiedendone la rimozione[827]. L'istanza all'Autorità è trasmessa utilizzando e compilando in ogni sua parte, a pena di irricevibilità, il modello reso disponibile sul sito Internet dell'Autorità, dedicato al diritto d'autore online, (*www.ddaonline.it*) e allegando ogni documentazione utile a comprovare la titolarità del diritto[828]; sul sito si dà anche conto degli interventi dell'Autorità, riportando i procedimenti avviati, le archiviazioni disposte e i provvedimenti adottati.

Entro sette giorni dalla ricezione dell'istanza, l'Agcom, laddove non disponga l'archiviazione[829], avvia il procedimento istruttorio e comunica l'avvio ai prestatori di servizi all'uopo individuati, nonché, ove rintracciabili, all'*uploader* e ai gestori della pagina e del sito, che possono adeguarsi spontaneamente (in tal caso, di conseguenza, l'istanza viene archiviata) o presentare controdeduzioni[830].

In assenza di adeguamento spontaneo, qualora sia ritenuta sussistente la violazione del diritto d'autore o dei diritti connessi, l'Autorità entro 35 giorni esige, nel rispetto dei criteri di gradualità, proporzionalità e adeguatezza, che i prestatori di servizi destinatari della comunicazione impediscano la violazione medesima o vi pongano fine, entro tre giorni dalla notifica, di norma attraverso la rimozione selettiva delle opere digitali (in caso di violazione su *server* ubicato in territorio nazionale) o con la disabilitazione dell'accesso alle opere o al sito (in caso di violazioni di carattere massivo o di violazione su *server* ubicato fuori dal territorio nazionale)[831]. In caso di

---

826 Ai sensi dell'art. 1, comma 1, lett. u), reg. Agcom, il soggetto legittimato è il titolare o licenziatario del diritto d'autore, ossia «*ogni soggetto titolare o licenziatario del diritto d'autore o dei diritti connessi con riferimento all'opera digitale di cui alla lettera p)*» (art. 1, comma 1, lett. t), reg. Agcom), o le associazioni di gestione collettiva o di categoria con mandato conferito dal titolare o dal licenziatario del diritto.

827 Art. 6, comma 1, reg. Agcom.

828 Art. 6, comma 2, reg. Agcom.

829 L'art. 6, comma 4, reg. Agcom prevede i casi di archiviazione in via amministrativa dell'istanza.

830 I prestatori di servizi, nonché l'*uploader* e i gestori della pagina e del sito, qualora ritengano di controdedurre in merito alla violazione contestata, trasmettono ogni elemento utile ai fini del relativo accertamento, entro il termine di cinque giorni dalla ricezione della comunicazione.

831 Artt. 7 e 8, reg. Agcom. Nel caso in cui da una prima e sommaria cognizione dei fatti oggetto dell'istanza l'Autorità ritenga che si tratti di un'ipotesi di grave lesione dei diritti di sfruttamento

disabilitazione, l'Agcom ordina di procedere a reindirizzare automaticamente verso una pagina Internet, redatta secondo le modalità indicate dall'Autorità, le richieste di accesso alla pagina Internet su cui è stata accertata la presenza di opere digitali diffuse in violazione del diritto d'autore o dei diritti connessi[832].

In caso di inottemperanza, l'Autorità applica le sanzioni amministrative previste e ne dà comunicazione agli organi di polizia giudiziaria.

È previsto il cosiddetto sistema del doppio binario che permette di rivolgersi sia all'autorità amministrativa che a quella giudiziaria: il procedimento dinanzi all'Agcom non può essere promosso qualora per il medesimo oggetto e tra le stesse parti sia pendente un procedimento dinanzi all'autorità giudiziaria; contro i provvedimenti dell'Agcom è ammesso il ricorso davanti al giudice amministrativo[833].

Anche se non manca chi ha ritenuto il regolamento ispirato a criteri di gradualità e proporzionalità dell'intervento[834], l'incisività dei poteri che il regolamento riconosce a un'autorità amministrativa (Agcom) ha sollevato forti reazioni critiche nel dibattito scientifico e pubblico, proprio in considerazione del fatto che sono disposti provvedimenti di cancellazione di contenuti pubblicati online in mancanza di una norma di legge che espressamente li preveda e al di fuori di un processo davanti all'autorità giudiziaria: il rischio è la lesione di diritti e libertà, quali la libertà di espressione e di informazione dei soggetti, costituzionalmente protetti e come tali suscettibili di limitazione solo per mezzo di norme e di provvedimenti dell'autorità giurisdizionale (riserva di legge e di giurisdizione)[835]. I dubbi si sono incentrati sull'attribuzione o

---

economico di un'opera digitale ovvero di un'ipotesi di violazione di carattere massivo, è previsto il procedimento abbreviato di cui all'art. 9.

832 Art. 8, comma 5, reg. Agcom.

833 Art. 6, comma 3, e art. 17, reg. Agcom. Inoltre, qualora nel corso del procedimento sia adita l'autorità giudiziaria per il medesimo oggetto, il soggetto istante ne informa tempestivamente l'Agcom che archivia gli atti e li trasmette all'Autorità giudiziaria (art. 7, comma 7, reg. Agcom).

834 P. OTRANTO, *op. cit.*, p. 229 ss.: sono fatte salve le procedure di *notice and take down* e l'intervento dell'Agcom non è diretto, ma si limita ad esigere l'adempimento dell'obbligo, impedire la violazione o porvi fine. In tal senso viene evidenziato anche il fatto che, di norma, si procede alla rimozione selettiva e la disabilitazione dell'accesso è confinata a ipotesi circoscritte, in cui il rimedio della rimozione selettiva sarebbe stato votato all'ineffettività.

835 F. GIOVANELLA, *La responsabilità civile degli Internet Service Provider*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, p. 243 ss.

meno da parte della legge di un potere così incisivo all'Autorità: parte della dottrina e dell'opinione pubblica ha ritenuto che l'Agcom si sia arrogata tale potere con un'interpretazione estensiva delle disposizioni e, oltretutto, senza prevedere un obbligatorio provvedimento giurisdizionale[836].

Le perplessità sono sfociate nel ricorso al TAR Lazio presentato da alcune associazioni; il TAR Lazio, con due ordinanze depositate il 26 settembre 2014, ha dichiarato rilevante e non manifestamente infondata la questione, ha sospeso il giudizio e ha rimesso alla Corte costituzionale il giudizio di legittimità costituzionale delle norme, sulla cui base l'Agcom ha approvato il regolamento[837], in relazione agli artt. 21, commi 2 e seguenti, 24 e 25, comma 1, Cost.[838].

La Corte costituzionale, con sentenza n. 247 del 21 ottobre 2015 ha ritenuto inammissibili le ordinanze per i «molteplici profili di contraddittorietà, ambiguità e oscurità nella formulazione della motivazione e del *petitum*»: anche se ha avuto modo di affermare che le disposizioni normative censurate «non attribuiscono espressamente all'Agcom un potere regolamentare in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica» quale quello esercitato[839]. Successivamente, con le sentenze n. 4100 e n. 4101 del 2017, il TAR Lazio ha respinto i due ricorsi.

---

836 P. OTRANTO, *op. cit.*, p. 231 ss. precisa come tale potere regolamentare potrebbe essere fatto rientrare, come avviene nei settori regolati dalle autorità, in un principio di legalità sostanziale, che si ritiene possa attenuarsi laddove sia compensato da un rafforzamento della legalità procedimentale con istituti di partecipazione, come la consultazione (a cui si è ricorso per il regolamento Agcom).

837 Si tratta degli artt. 5, comma 1, 14, comma 3, 15, comma 2, e 16, comma 3, d.lgs. 70/2003, nonché dell'art. 32 bis, comma 3, d.lgs. 177/2005, introdotto dal d.lgs. 44/2010.

838 Le ordinanze sono la n. 10016 e la n. 10020 del 26 settembre 2014 della Sezione Prima TAR Lazio.

839 Secondo la Corte «ciò che più rileva è che il contenuto di ciascuna delle previsioni impugnate è per alcuni aspetti più circoscritto e per altri eccedente rispetto all'oggetto del regolamento di AGCOM. Sicché, considerato che la Corte giudica su norme, ma pronuncia su disposizioni […], una decisione di accoglimento – qual è quella richiesta dal primo punto del dispositivo dell'ordinanza di rimessione – non avrebbe l'effetto auspicato dal giudice rimettente, ma finirebbe per espungere dall'ordinamento disposizioni che riguardano, o aspetti sostanziali della disciplina delle comunicazioni elettroniche, o l'attribuzione ad AGCOM di funzioni e poteri che non solo non sono in discussione, ma che devono essere attribuiti, conformemente a quanto previsto dalla direttiva europea». Sulla sentenza della Corte costituzionale cfr. P. COSTANZO, *Quale tutela del diritto d'autore in internet?*, cit., p. 2343 ss.; O. POLLICINO, *La rimessione alla Corte della questione di legittimità costituzionale in materia di diritto*

Al riguardo, è opportuno rilevare che l'Agcom ha approvato la delibera 8/18/CONS del 18 gennaio 2018, con cui ha sottoposto a consultazione pubblica lo «*schema di proposte di modifica al Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70, di cui alla delibera n. 680/13/CONS*», allegato A della delibera[840]. Accanto a modifiche di coordinamento rispetto ad atti sopravvenuti, lo schema recante proposte di modifica al regolamento prevede disposizioni in merito alla reiterazione di violazioni già accertate dall'Agcom e al procedimento cautelare nei confronti dei prestatori di servizi.

4.4.2. Il contesto internazionale

La problematica protezione del diritto d'autore in rete non è, del resto, problema solo italiano, ma ha investito parimenti anche gli altri ordinamenti europei.

In Francia l'autorità amministrativa *Hadopi* (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet*), in caso di violazioni, deve devolvere a un'autorità giurisdizionale la determinazione della sanzione che consiste nell'imposizione della sospensione dell'accesso a Internet, dal momento che inficia il diritto di accesso alla rete e la libertà di espressione costituzionalmente protetti, ai sensi della *Loi* n. 2009-1311 del 28 ottobre 2009, cosiddetta *Hadopi II*, approvata a seguito della *décision* del *Conseil Constitutionnel* n. 2009-580 DC del 10 giugno 2009, che ha dichiarato l'incostituzionalità della legge *Création et Internet*, istitutiva dell'*Hadopi*. La legge dichiarata incostituzionale prevedeva, invece, in caso di reiterate violazioni dei diritti di proprietà intellettuale, un meccanismo sanzionatorio, in particolare la disconnessione forzata da Internet, a seguito di una decisione dell'autorità

---

d'autore sulle reti di comunicazione elettronica, in *federalismi.it*, n. 3, 2014; O. POLLICINO - M. BASSINI, *"Le parole contano", ovvero "tanto rumore per nulla". Sulla (prevista) inammissibilità della questione di legittimità costituzionale della base giuridica del Regolamento AGCOM #ddaonline*, in *medialaws.eu*, 2015; G. M. SALERNO, *Le ordinanze gemelle sulla disciplina dei provvedimenti interdittivi dell'AGCom: alcune riflessioni*, in *federalismi.it*, n. 3, 2014.

[840] L'allegato B della delibera contiene il testo coordinato del regolamento, mentre l'allegato C le modalità della consultazione.

amministrativa e senza nessun controllo giurisdizionale, attribuendo così a un soggetto amministrativo un ampio margine di apprezzamento in merito alla restrizione di diritti fondamentali[841].

Nel Regno Unito, con l'emanazione del *Digital Economy Act* dell'8 aprile 2010 è stato introdotto un sistema "graduato" che mutua tratti del sistema francese, ossia una procedura di contrasto al *file sharing* secondo cui i titolari dei diritti devono informare delle violazioni del *copyright* i fornitori di accesso a Internet e chiedere che le notifichino ai loro utenti, in base al previsto "*Initial Obligations Code*" predisposto dall'*Office of Communications* (Ofcom). Secondo la disciplina inglese, il fornitore è tenuto a inserire i riferimenti dell'utente in forma anonima in un registro delle violazioni da fornire su richiesta ai titolari dei diritti, che potranno quindi chiedere a un'autorità giurisdizionale la *disclosure* dei dati personali contenuti nell'elenco, per poter intentare un'azione per danni[842].

Proprio in considerazione delle divergenti discipline tra gli Stati europei, dell'opportunità di una dimensione sovranazionale, maggiormente adeguata alla tutela, e della necessità di migliorare il bilanciamento tra diritto d'autore e diritto alla conoscenza[843], l'Europa, nell'ambito della Strategia per il mercato unico digitale[844], ha

---

841 O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., pp. 1944-1953. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 562 ss. sottolinea come la giurisprudenza francese mostri un atteggiamento di resistenza nell'ammettere restrizioni al diritto d'autore in favore della libertà d'espressione.

842 Cfr. O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, in *Giurisprudenza italiana*, fasc. 8-9, 2011, pp. 1944-1953 e A. STAZI, *op. cit.*, p. 89 ss., che sottolinea come la sezione che prevedeva la possibilità per i titolari dei diritti di richiedere a una Corte di obbligare i fornitori di servizi ad adottare misure di sospensione o limitazione dell'accesso a Internet è stata ritirata a seguito di una *review* svolta dall'Ofcom su richiesta del Governo. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 563 ss. anche nel caso britannico, come per la giurisprudenza francese, sottolinea un atteggiamento di resistenza della giurisprudenza nell'ammettere limitazioni al diritto d'autore a tutela della libertà d'espressione, salvo quando questa si esprima in manifestazioni che sollecitano considerazioni di natura politico-sociale (e non di matrice prevalentemente economica).

843 A. STAZI, *op. cit.*, p. 89 ss.

844 Comunicazione della Commissione europea «*Strategia per il mercato unico digitale in Europa*» COM (2015) 192 final del 6 maggio 2015.

individuato specifiche azioni nella comunicazione della Commissione europea «*Verso un quadro normativo moderno e più europeo sul diritto d'autore*» del dicembre 2015[845]. Tali azioni sono state poi concretizzate in alcune proposte di riforma nel 2016, tese ad aggiornare e armonizzare le norme europee in materia di diritto d'autore e diritti connessi nell'ambito del mercato interno, al fine di migliorare il coordinamento tra la tutela del diritto d'autore e il libero accesso alla conoscenza, promuovendo la circolazione della cultura e aumentando la diversità culturale e i contenuti disponibili online[846]. A questi fini, sono state adottate una proposta di direttiva sul diritto d'autore nel mercato unico digitale[847] e una proposta di regolamento relativa a talune trasmissioni online degli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici[848], insieme ad altre due proposte inerenti agli utilizzi di opere protette a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa[849].

---

845 Comunicazione della Commissione europea «*Verso un quadro normativo moderno e più europeo sul diritto d'autore*» COM (2015) 626 final del 9 dicembre 2015.

846 Cfr. G. DE SANCTIS, *Le nuove proposte di riforma della Commissione europea in materia di copyright. Analisi dei profili più rilevanti in relazione alle tematiche d'interesse dell'AGCom*, in *GiustAmm.it*, fasc. 2, 2017, p. 1 ss., che sottolinea tra gli obiettivi anche l'aumento della chiarezza e della trasparenza per tutti gli utenti online e l'inserimento di nuovi elementi per l'innovazione dell'istruzione, della ricerca e delle istituzioni che gestiscono il patrimonio culturale.

847 «*Proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale*» COM (2016) 593 final - 2016/0280 (COD) del 14 settembre 2016.

848 «*Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme relative all'esercizio del diritto d'autore e dei diritti connessi applicabili a talune trasmissioni online degli organismi di diffusione radiotelevisiva e ritrasmissioni di programmi televisivi e radiofonici*» COM (2016) 594 final - 2016/0284 (COD) del 14 settembre 2016.

849 «*Proposta di regolamento del Parlamento europeo e del Consiglio relativa allo scambio transfrontaliero tra l'Unione e i paesi terzi di copie in formato accessibile di determinate opere e altro materiale protetto da diritto d'autore e da diritti connessi, a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa*» COM (2016) 595 final - 2016/0279(COD) del 14 settembre 2016 e «*Proposta di direttiva del Parlamento europeo e del Consiglio relativa a taluni utilizzi consentiti delle opere e di altro materiale protetto da diritto d'autore e da diritti connessi a beneficio delle persone non vedenti, con disabilità visive o con altre difficoltà nella lettura di testi a stampa, e che modifica la direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto*

Ai fini di questa analisi è interessante la proposta di direttiva sul diritto d'autore nel mercato unico digitale, atto principale della riforma, che detta disposizioni generali (titolo I), misure volte ad adeguare le eccezioni e le limitazioni all'ambiente digitale e al contesto transfrontaliero (titolo II), misure volte a migliorare le procedure di concessione delle licenze e a garantire un più ampio accesso ai contenuti (titolo III) e misure volte a garantire il buon funzionamento del mercato per il diritto d'autore (titolo IV), oltre a disposizioni finali relative a modifiche di altre direttive e all'applicazione (titolo V). In merito, ad esempio, sono significative la previsione di eccezioni e limitazioni per estrazioni di testo e dati (*text mining* e *data mining*) nel campo della ricerca scientifica[850] e la disposizione relativa all'adozione di misure, quali l'uso di tecnologie efficaci per il riconoscimento dei contenuti, adeguate e proporzionate da parte delle piattaforme di condivisione, in collaborazione con i titolari dei diritti, al fine del corretto funzionamento degli accordi di licenza tra piattaforme e titolari[851].

Rispetto al diritto d'autore e alla protezione offerta dall'Europa, gli Stati Uniti si atteggiano diversamente, anche a causa della considerazione privilegiata e della tutela rafforzata che offrono alla libertà di espressione.

L'Europa mostra una concezione del diritto d'autore come strumento di stimolo all'innovazione creativa funzionale al progresso sociale e culturale, mentre gli USA lo interpretano in chiave utilitaristica, come una proiezione materiale della persona. Da ciò consegue una disciplina giuridica, basata sull'art. 1, par. 8, della Costituzione degli Stati Uniti d'America[852], che invece di ritenere prevalente la dimensione proprietaria e

---

d'autore e dei diritti connessi nella società dell'informazione» COM (2016) 596 final - 2016/0278(COD) del 14 settembre 2016.

850 Art. 3 della proposta di direttiva.

851 Art. 13 della proposta di direttiva. La norma prevede che siano date ai titolari dei diritti adeguate informazioni sul funzionamento e sull'implementazione di tali tecnologie e che siano istituiti meccanismi di reclamo e ricorso a disposizione degli utenti.

852 L'art. 1, par. 8, della Costituzione degli Stati Uniti d'America del 15 settembre 1787 conferisce al Congresso il potere di «promuovere il progresso della scienza e delle arti utili, assicurando per periodi limitati di tempo agli Autori ed agli Inventori il diritto esclusivo sui loro scritti e scoperte». Dedicati al diritto d'autore sono il *Copyright Act* statunitense del 1976 e il *Digital Millennium Copyright Act* del 1998, che prevede un meccanismo di *notice and take down* in caso di violazioni; riguardo all'esperienza americana cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., pp. 549-585.

attribuire, di conseguenza, un insieme aperto di facoltà di sfruttamento economico accompagnato da un elenco tassativo e rigido di eccezioni, prevede un'elencazione rigida delle modalità di sfruttamento economico accompagnata da una definizione ampia e aperta di eccezioni[853].

Significativo, in merito al bilanciamento tra diritto d'autore e libertà di espressione, è il caso *Harper & Row, Publishers, Inc. v. National Enterprises*[854], dove il *copyright* è descritto come motore della libertà di espressione, perché, garantendo la remunerazione dello sforzo creativo, si configura come principale incentivo allo sviluppo dell'industria culturale e, di conseguenza, più ampiamente, della libera espressione[855]. Il diritto d'autore viene interpretato, pertanto, in modo strumentale rispetto alla libertà di espressione, ma può anche sfociare in una minaccia e in una sua compressione, dal momento che può portare ad una privatizzazione della conoscenza, limitando così l'accesso alla stessa: affinché il diritto d'autore assolva alla sua funzione tipica di promozione della conoscenza è necessario che la configurazione legislativa non travalichi i limiti necessari a conseguire il suo scopo, altrimenti sconfina in un indebito sacrificio della libertà di espressione[856].

4.4.3. La proprietà intellettuale nel governo dei dati

In considerazione dell'analisi effettuata, le opere, i contenuti e le informazioni strutturate soggiacciono alla normativa sul diritto d'autore, che faticosamente si adatta al contesto digitale e che può scontrarsi con la libertà di informazione e il diritto alla

---

853 O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., pp. 1944-1953. E. BARONE, *op. cit.*, p. 315 ricorda come il *copyright* non riconosca la componente morale del diritto d'autore che invece caratterizza la normativa europea.

854 Sentenza della Corte Suprema degli Stati Uniti 471 U.S. 539 (1985).

855 O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., p. 1944 ss.

856 O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., p. 1944 ss.; M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 565 in merito alla prassi giurisprudenziale statunitense sottolinea la tendenziale negazione di un rapporto conflittuale tra diritto d'autore e libertà d'espressione, anche se non mancano sentenze che ammettono il rapporto conflittuale tra i due diritti.

conoscenza. Questi aspetti rilevano particolarmente nel governo dei dati, dal momento che è necessario prestare attenzione a tutelare quelle informazioni strutturate e quei contenuti sui quali siano vantati diritti d'autore.

Nel caso del governo dei dati, vengono spesso in gioco *dataset* e *database*; è il caso degli *open data*, ma anche dei *big data*, e, di conseguenza, deve essere tenuta in considerazione anche la tutela prevista per le banche dati. La normativa sul diritto d'autore, infatti, accanto al software, protegge anche le banche dati, a seguito delle modifiche alla legge 633/1941 da parte del d.lgs. 6 maggio 1999, n. 169, attuazione della direttiva 96/9/CE, con alcune specificità nella disciplina dovute alla particolare tipologia di opera dell'ingegno[857].

Sono oggetto di tutela le banche di dati, elettroniche e di altro tipo, ossia raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti e individualmente accessibili mediante mezzi elettronici o in altro modo, «*che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore*»: la tutela delle banche dati non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto[858].

Emergono, di conseguenza, come oggetto di tutela due tipologie di banche dati: quelle cosiddette selettive, nelle quali i contenuti sono selezionati in modo originale, e quelle cosiddette dispositive, nelle quali, seppur la selezione non sia creativa, è originale la disposizione del materiale. Il titolare vanta diritti morali e diritti patrimoniali, che consistono nel diritto esclusivo dell'autore di eseguire o autorizzare la riproduzione permanente o temporanea, totale o parziale, con qualsiasi mezzo e in qualsiasi forma, la traduzione, l'adattamento, una diversa disposizione e ogni altra modifica, qualsiasi forma di distribuzione al pubblico dell'originale o di copie e qualsiasi presentazione, dimostrazione o comunicazione in pubblico, ivi compresa la trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma[859].

---

857 Cfr. V. FALCE, *La disciplina comunitaria sulle banche dati. Un bilancio a dieci anni dall'adozione*, in *Rivista di diritto industriale*, fasc. 6, 2006, p. 227 ss.

858 Art. 1, comma 2, e art. 2, comma 1, n. 9), legge 633/1941. Le banche dati comprendono l'opera multimediale; G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., p. 499 ss.

859 Art. 64-quinquies, legge 633/1941. Il cosiddetto principio di esaurimento è limitato alla prima vendita di una copia nel territorio dell'Unione europea da parte del titolare del diritto o con il suo

Sono previsti diritti e prerogative specifiche che non richiedono l'autorizzazione da parte del titolare; si tratta delle libere utilizzazioni previste nell'art. 64-sexies, legge 633/1941, che consente l'accesso, la consultazione o l'impiego per esclusive finalità didattiche o di ricerca scientifica, per fini di sicurezza pubblica o per effetto di una procedura amministrativa o giurisdizionale. Inoltre, l'utente può porre in essere le attività che spettano al titolare, senza necessità di autorizzazione, se necessarie per l'accesso alla banca dati e il suo impiego (eventuali clausole pattuite in violazione sono nulle).

Nel caso dei *database* può accadere che non ricorrano le caratteristiche di originalità nella scelta o disposizione del materiale previste dalla normativa per azionare la relativa tutela giuridica. La normativa europea e italiana[860] ne è consapevole e, al fine di proteggere lo sforzo necessario a reperire e predisporre i contenuti e l'investimento economico e professionale, ha previsto il c.d. diritto *sui generis* o diritto del costitutore, ossia il diritto del soggetto che effettua investimenti rilevanti per la costituzione o la verifica o la presentazione di una banca dati, impegnando, a tal fine, mezzi finanziari, tempo o lavoro[861].

Il c.d. diritto *sui generis*, autonomo rispetto al diritto d'autore, prescinde dall'esistenza di qualunque requisito di creatività e originalità e tutela il costitutore, assegnandogli il diritto di vietare le operazioni di estrazione[862] o reimpiego[863] della totalità o di parti sostanziali della banca dati (art. 102-bis, legge 633/1941).

Il diritto del costitutore è indipendente dalla tutelabilità della banca dati a norma

---

consenso, che esaurisce il diritto di controllare, all'interno dell'Unione stessa, le vendite successive della copia (art. 64-quinquies, comma 1, lett. c), legge 633/1941).

860 La direttiva 96/9/CE e il relativo d.lgs. 169/1999 di attuazione si occupano di tale esigenza.

861 Art. 102-bis, comma 1, lett. a), legge 633/1941. Secondo F. AUTELITANO, *La rilevanza delle banche dati nel sistema del "cyberlaw"*, in *I Contratti*, fasc. 10, 1999, p. 925 ss. la protezione del diritto *sui generis* si colloca sul piano dei principi del diritto della concorrenza, con lo scopo di non scoraggiare lo sviluppo del settore e di prevenire atti di concorrenza sleale.

862 «*Il trasferimento permanente o temporaneo della totalità o di una parte sostanziale del contenuto di una banca di dati su un altro supporto con qualsiasi mezzo o in qualsivoglia forma*» (art. 102-bis, comma 1, lett. b), legge 633/1941).

863 «*Qualsivoglia forma di messa a disposizione del pubblico della totalità o di una parte sostanziale del contenuto della banca di dati mediante distribuzione di copie, noleggio, trasmissione effettuata con qualsiasi mezzo e in qualsiasi forma*» (art. 102-bis, comma 1, lett. c), legge 633/1941).

del diritto d'autore o di altri diritti e non pregiudica diritti sul contenuto o su parti di esso. La diversa finalità motiva anche la durata diversa rispetto al diritto d'autore: il diritto del costitutore sorge al momento del completamento della banca dati e si estingue trascorsi quindici anni dal primo gennaio dell'anno successivo alla data del completamento stesso[864]. L'utente legittimo della banca dati messa a disposizione del pubblico non può arrecare pregiudizio al titolare del diritto d'autore o di un altro diritto connesso relativo ad opere o prestazioni contenute nella banca dati e non può eseguire operazioni che siano in contrasto con la normale gestione della banca dati o che arrechino un ingiustificato pregiudizio al costitutore della stessa[865].

Nel governo dei dati, sotto il profilo del diritto d'autore, si porrà, di conseguenza, l'esigenza di tutelare eventuali diritti d'autore vantati su informazioni strutturate, ma anche il diritto *sui generis* del costitutore del *database* o, addirittura, il diritto d'autore del titolare della banca dati, laddove questa abbia le caratteristiche di originalità nella scelta o disposizione del materiale. La tutela di questi diritti, come tra poco si vedrà, è particolarmente complessa a seconda della configurazione dei dati stessi[866].

La disciplina giuridica, infatti, non è ancora completamente adeguata alle inedite questioni che riguardano la proprietà intellettuale nell'era digitale e questo provoca contrasti con altri interessi protetti dall'ordinamento, che peraltro non costituiscono neppure un *numerus clausus* definibile aprioristicamente, ma una serie aperta dipendente dalla fattispecie concreta, quali il diritto di accesso all'informazione, la

---

[864] Anche al diritto del costitutore si applica il principio dell'esaurimento: la prima vendita di una copia della banca di dati effettuata o consentita dal titolare in uno Stato membro dell'Unione europea esaurisce il diritto di controllare la rivendita della copia nel territorio dell'Unione europea (art. 102-bis, comma 2, legge 633/1941).

[865] Art. 102-ter, commi 1 e 2, legge 633/1941. Art. 102-ter, comma 3: «*Non sono soggette all'autorizzazione del costitutore della banca di dati messa per qualsiasi motivo a disposizione del pubblico le attività di estrazione o reimpiego di parti non sostanziali, valutate in termini qualitativi e quantitativi, del contenuto della banca di dati per qualsivoglia fine effettuate dall'utente legittimo*». L'art. 102-ter, comma 4, prevede la nullità delle clausole contrattuali pattuite in violazione dei commi 1, 2 e 3. «*Non sono consentiti l'estrazione o il reimpiego ripetuti e sistematici di parti non sostanziali del contenuto della banca di dati, qualora presuppongano operazioni contrarie alla normale gestione della banca di dati o arrechino un pregiudizio ingiustificato al costitutore della banca di dati*» (art. 102-bis, comma 9, legge 633/1941).

[866] *Infra*, § 4.4.

circolazione della cultura, la libertà di espressione, la protezione dei dati personali e la libertà di iniziativa economica. Esemplificativamente, in caso di richiesta ai *provider*, da parte dei titolari dei diritti d'autore, dei dati personali degli autori di violazioni di diritti di proprietà intellettuale, al fine di agire giudizialmente contro di loro, si pone un problema di bilanciamento tra il diritto d'autore e il diritto alla protezione dei dati personali, che è stato al centro di celebri sentenze, come il caso *Promusicae*[867] e il caso *Bonnier*[868]; peraltro in tali casi vengono in gioco e possono essere compromessi anche gli interessi economici dei *provider*, che rischiano di vedere pregiudicata la fiducia degli utenti attuali e potenziali verso i loro servizi[869]. Attenzione alla libertà di iniziativa economica mostra, ad esempio, il caso *Scarlet*[870]: nel dare ragione al fornitore, che si era rifiutato di predisporre un sistema di filtraggio per impedire scambi lesivi del diritto d'autore, ha ritenuto che la predisposizione di un sistema di filtraggio causerebbe una grave violazione della libertà di impresa, obbligando il *provider* a predisporre un sistema a suo carico complesso, costoso, permanente[871].

Ai fini di questa analisi verrà esaminato, in particolare, il rapporto che lega il diritto a conoscere, nelle sue diverse configurazioni e intensità, e il diritto d'autore nel governo dei dati. È, infatti, evidente il difficile bilanciamento nella realtà digitale, dal momento che una tutela "forte" del diritto d'autore online rischia di porsi in contrasto con l'esigenza di conoscenza e il correlato diritto all'informazione che connota

---

867 Caso *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, sentenza della Corte di Giustizia dell'Unione europea del 29 gennaio 2008, causa C-275/06.

868 Caso *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB c. Perfect Communication Sweden AB*, sentenza della Corte di Giustizia dell'Unione europea del 19 aprile 2012, causa C-461/10.

869 Cfr. A. STAZI, *op. cit.*, p. 89 ss.

870 Caso *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, sentenza della Corte di Giustizia dell'Unione europea del 24 novembre 2011, causa C-70/10. Nella sentenza i sistemi di filtraggio, idonei a effettuare una sorveglianza attiva e generalizzata sulla totalità delle informazioni relative agli utenti sono risultati incompatibili con il diritto dell'Unione europea ed eccessivamente lesivi di diritti fondamentali parimenti previsti e protetti dalla normativa europea; cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 577 ss.

871 Cfr. G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., p. 499 ss.

profondamente l'attuale società e che deve essere ugualmente protetto.

4.4.4. Diritto d'autore e *right to know*: alla ricerca dell'equilibrio

I diritti individuali del titolare devono rapportarsi con i diritti e le esigenze collettive relative all'accesso all'informazione e al sapere; questo genera uno "scontro" tra il diritto d'autore con le correlate facoltà esclusive e il diritto a conoscere basato su istanze di apertura e condivisione, che animano particolarmente la realtà digitale e, in specifico, vengono in gioco nel governo dei dati.

In realtà si può individuare una tensione fisiologica e costante tra diritto d'autore e libertà d'informazione, rinvenibile nella struttura genetica e ontologica dei diritti in questione: il diritto d'autore conduce a una privatizzazione dominicale della conoscenza che necessariamente "stona" e urta con la libertà di informazione, che al contrario aspira alla massima diffusione possibile dei contenuti[872].

Questo difficile compromesso tra le due istanze ha, dunque, origine risalente nel tempo, ma la realtà digitale fa esplodere con evidenza e moltiplica il momento patologico del conflitto, dal momento che ha reso globale e semplice l'accesso e la fruizione delle opere protette, che però anche nel nuovo contesto di libertà continuano ad andare incontro a limitazioni atte a proteggere la proprietà intellettuale[873]. Per questa strada il diritto d'autore e le istanze di protezione fortificata dello stesso rischiano di contrastare e limitare il più ampio e fondamentale diritto d'accesso alla rete, diritto prodromico ed essenziale anche all'accesso alla conoscenza che la rete permette, oltre che allo sviluppo della stessa creatività personale[874]. Peraltro il diritto d'autore rischia un mutamento e una degenerazione nella realtà digitale dall'autentica finalità di remunerare lo sforzo creativo verso l'attribuzione nei fatti di un privilegio a quelle che vengono definite come industrie creative[875].

---

872 In senso conforme P. OTRANTO, *op. cit.*, p. 239 ss.

873 Cfr. O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., pp. 1944-1953.

874 M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 554 ss.

875 O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., p. 1944 ss.

In questa tensione genetica tra i due diritti sono individuabili punti di equilibrio, messi in luce anche dalla giurisprudenza: nella proprietà intellettuale la protezione dei diritti patrimoniali e non patrimoniali è giustificata dalla capacità creativa della persona, cui si collega la volontà di incoraggiamento alla produzione di altre opere nell'interesse pubblico generale alla cultura e alla conoscenza; il diritto d'autore mostra allora la sua dimensione pubblica di interesse generale, che è la medesima del diritto all'informazione e alla conoscenza[876]. I due diritti, da traiettorie diverse, convergono verso un comune interesse pubblico generale legato alla conoscenza e alla cultura.

Tale aspetto è evidente nell'esperienza statunitense, ad esempio nel citato caso *Harper & Row, Publishers, Inc. v. National Enterprises*, dove il diritto d'autore è strumento della libertà d'espressione e della promozione della conoscenza e il sottile punto di equilibrio va ricercato proprio nel rispetto della funzione tipica che lo caratterizza: nell'esperienza degli Stati Uniti, pur consapevole delle contrapposizioni e dei conflitti che possono nascere tra diritto d'autore e libertà di espressione, viene evidenziato l'aspetto di convergenza che lega i due diritti[877].

A guardare bene, la relazione è biunivoca, dal momento che non solo il diritto d'autore è motore della libertà d'espressione, ma anche la libertà d'espressione è mezzo di sviluppo e promozione dello sforzo creativo[878].

Per tale via emerge come sia centrale in entrambi i diritti la persona, che è il soggetto la cui libertà di informazione e diritto d'accesso alla conoscenza da una parte va protetto (con il *right to know*) e dall'altra va promosso e incentivato al fine di far emergere l'aspetto creativo (con il diritto d'autore).

---

876 Così la sentenza della Corte costituzionale 6 aprile 1995, n. 108.

877 Nel caso americano il diritto d'autore viene definito come "motore" della libertà di espressione (*engine of free speech*), dal momento che fornisce protezione allo sforzo creativo.

878 Cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., pp. 549-585, che rileva come la connotazione sinergica tra i due diritti era maggiormente presente in passato, quando si negava il conflitto e si risolveva nelle leggi nazionali a tutela del diritto d'autore (c.d. *internalizzazione del conflitto*); negli ultimi anni, invece, grazie anche all'avvento della rete e alla libera condivisione delle informazioni (es. *file sharing*), è emerso l'aspetto conflittuale tra i due diritti, che viene risolto fuori dalla normativa interna sul diritto d'autore (c.d. *esternalizzazione del conflitt*o). Le motivazioni alla base della negazione del conflitto afferiscono alla dicotomia idea/espressione, alla presenza di eccezioni, al parametro del *fair dealing exception* e ad alcune valutazioni, tra le quali la limitata durata di protezione del diritto d'autore.

Ai fini di un efficace bilanciamento tra i due interessi contrapposti, in considerazione della tutela della libertà di informazione, uno strumento efficace consiste nell'autonomia negoziale, che consente di disporre dei diritti riconosciuti dalla legge: la possibilità di ricorrere all'autonomia negoziale per interpretare le disposizioni in materia di diritto d'autore è sfociata in strumenti concreti come le licenze aperte, quali le *Creative Commons*, maggiormente flessibili e attente a quelle istanze contrapposte di accesso alla conoscenza e circolazione della cultura, accentuando, a tale scopo, la tutela del diritto morale d'autore piuttosto che lo sfruttamento economico dell'opera e le correlate facoltà esclusive[879]. Le *Creative Commons* sono tese a concedere ampi margini di libertà e in tal modo permettono un migliore bilanciamento tra interessi contrapposti: consentono di rendere pubblici e utilizzabili, con il diverso grado di intensità deciso dal titolare, beni e contenuti, che sono così protetti in modo equo e ragionevole, adeguato alla realtà digitale di riferimento[880].

In considerazione dei punti di equilibrio e per mezzo degli utili strumenti di autonomia negoziale, il bilanciamento dovrà comunque essere effettuato caso per caso senza prevalenze assolute e aprioristiche dell'uno o dell'altro diritto, che peraltro mal si conciliano con la normativa europea e nazionale al riguardo; andrà condotto valutando la prevalenza del diritto e della relativa protezione nel caso concreto, applicando il principio di sussidiarietà tra discipline e istituzioni a tutela: ci sarà, di norma, un interesse prevalente, ma non esclusivo da tenere in considerazione[881].

---

879 In tal senso G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., p. 499 ss. Per un'analisi delle licenze *Creative Commons*, *supra*, cap. 3.

880 Cfr. G. ZICCARDI, *Informatica giuridica. Tomo I - Controcultura, informatica giuridica, libertà del software e della conoscenza*, II ed., Giuffrè, Milano, 2011, p. 323 ss., che richiama i potenziali aspetti critici delle *Creative Commons*, consistenti nel difficile successo nel lungo periodo di economie basate sulla condivisione e nel possibile impoverimento della qualità. In realtà, sottolinea l'Autore, sotto il primo profilo, nell'epoca odierna, cultura, creatività e conoscenza si pongono come risorse tipicamente non competitive e, sotto il secondo profilo, i contenuti veicolati con tali licenze sono di qualità, prodotti da professionisti come gli altri.

881 Cfr. A. STAZI, *op. cit.*, p. 89 ss., che al riguardo richiama nel bilanciamento da effettuare l'importanza dell'art. 47 (diritto a un ricorso effettivo, che impone una sussidiarietà tra discipline e istituzioni) e dell'art. 54 (divieto dell'abuso di diritto, che dovrebbe evitare che l'interesse prevalente diventi esclusivo) della Carta fondamentale dei diritti dell'Unione europea. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e*

Nella reciproca integrazione che lega i diritti va cercato il punto di equilibrio, non prefissato, ma necessariamente dinamico[882]. In tale valutazione, come già rilevato, risulta centrale porre l'attenzione sulla persona e sulla tutela effettiva da garantirle per proteggere e allo stesso tempo promuovere la libertà d'espressione, fondamento bifronte del *right to know* e del diritto d'autore.

Proprio il ricorso al bilanciamento tra diritti e interessi diversi porta la giurisprudenza della Corte di giustizia dell'Unione europea ad affermare che non sono legittimi sistemi di filtraggio preventivo dei contenuti per prevenire le violazioni del diritto d'autore, dal momento che comprimerebbero troppo la libertà di informazione, ma anche la libertà di iniziativa economica e la protezione dei dati personali, a causa del correlato monitoraggio[883]; per ragioni affini, secondo la giurisprudenza, deve essere consentito il rinvio tramite link ad opere protette dal diritto d'autore disponibili su altro sito, senza che occorra l'autorizzazione dei titolari[884]. *A contrario*, però, può essere disposto l'ordine di blocco all'accesso a un contenuto o un sito che viola il diritto d'autore, prestando attenzione a garantire comunque un giusto equilibrio tra i diritti fondamentali interessati[885]; altresì, i collegamenti ipertestuali verso opere protette

---

internazionale, cit., p. 553 sottolinea come la libertà di espressione non vada tutelata necessariamente in ogni caso, anche in considerazione del fatto che può celare interessi venali e concorrenziali di operatori economici e finanziari.

882 P. OTRANTO, *op. cit.*, p. 243 sottolinea che, nel caso del rapporto tra libertà d'informazione e diritto d'autore, deve essere garantita la conoscenza lecitamente diffusa e non l'illecito sfruttamento di diritti altrui, altrimenti la preminenza assoluta dell'accesso alla conoscenza porterebbe a dare una prevalenza aprioristica e assoluta a questo diritto rispetto agli altri.

883 Caso *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, sentenza della Corte di Giustizia dell'Unione europea del 16 febbraio 2012, causa C-360/10. I sistemi di filtraggio richiesti, prevedendo una sorveglianza totale, illimitata e indiscriminata, potendo riguardare anche opere future, si pongono in contrasto con altri diritti e libertà parimenti tutelati; cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 577 ss.

884 Caso *Svensson*, sentenza della Corte di Giustizia dell'Unione europea del 13 febbraio 2014, causa C-466/12.

885 Caso *Telekabel*, sentenza della Corte di Giustizia dell'Unione europea del 27 marzo 2014, causa C-314/12; in tal caso l'ordine di blocco è possibile se risponde a un criterio di proporzionalità e a misure ragionevoli, non comprime troppo gli interessi in gioco e, di conseguenza, non deve privare gli utenti dell'accesso ai contenuti in modo lecito, ma avere l'effetto di impedire o rendere difficoltose le

liberamente disponibili su altro sito senza l'autorizzazione del titolare costituiscono comunicazione al pubblico vietata, laddove siano a fini di lucro e nella consapevolezza dell'illegittimità della pubblicazione (da presumere nello scopo di lucro)[886].

Nel bilanciamento tra le istanze va tenuto anche in considerazione l'insegnamento della giurisprudenza della Corte europea dei diritti dell'uomo che, sulla base dell'art. 10 della Convenzione europea dei diritti dell'uomo, secondo cui la restrizione della libertà di espressione è possibile anche in caso di protezione dei diritti altrui, ha previsto la possibilità di comprimere la libertà di espressione solo dove questo risponda alla soddisfazione di un interesse pubblico e al criterio di proporzionalità, configurando la soluzione meno invasiva per l'obiettivo di tutela[887].

Nel governo dei dati, si porranno precipui e specifici problemi da risolvere nelle diverse configurazioni che i dati assumono e che sono state esaminate nei precedenti capitoli.

Nel caso della trasparenza proattiva, da realizzare con la pubblicazione, sarà necessario valutare attentamente la titolarità dei dati dal punto di vista del diritto

---

consultazioni non autorizzate. Cfr. A. STAZI, *op. cit.*, p. 89 ss. Secondo M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 577 ss. tale sentenza è molto significativa e mostra maggior coraggio rispetto ad altri casi precedenti (i casi *Scarlet* e *Netlog*) nell'individuare in modo più puntuale le indicazioni per effettuare il bilanciamento tra interessi contrapposti, realizzando così una maggiore certezza del diritto e una migliore armonizzazione tra le autorità nazionali.

886 Caso *GS Media BV c. Sanoma Media Netherlands BV et al.*, sentenza della Corte di Giustizia dell'Unione europea dell'8 settembre 2016, causa C-160/15; cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 582 ss.

887 Cfr. O. POLLICINO, *Copyright versus freedom of speech nell'era digitale*, cit., p. 1944 ss., che in merito sottolinea la riflessione da svolgere sulla riconducibilità del diritto d'autore al novero dei diritti altrui. Al riguardo è opportuno richiamare la sentenza della Corte europea dei diritti dell'uomo *Ashby Donald e altri c. Francia*, n. 36769/08 del 10 gennaio 2013, nella quale si analizza la portata applicativa dell'art. 10 CEDU, si accerta l'ingerenza nella libertà di espressione e si verifica la compatibilità dell'ingerenza con il sistema di protezione dei diritti umani previsto dalla CEDU, valutando legalità, legittimità e necessità della limitazione della libertà d'espressione; nello stesso senso il caso *The Pirate Bay Neij e Sunde Kolmisoppi c. Svezia*, ricorso n. 40397/12, del 19 febbraio 2013; in merito cfr. M. NINO, *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, cit., p. 571 ss.

d'autore e, in caso di titolarità in capo ad altre istituzioni, si dovrà porre attenzione e attenersi alla licenza prevista o, altrimenti, chiederne l'autorizzazione. Come già esaminato in relazione agli *open data*, infatti, alle amministrazioni pubbliche sono applicabili il diritto d'autore e quello *sui generis*, relativi rispettivamente alle banche dati creative e non creative: alle amministrazioni pubbliche spetta, infatti, il diritto di autore su quanto creato e pubblicato sotto il loro nome e a loro conto e spese, diritto che dura venti anni a partire dalla prima pubblicazione, qualunque sia la forma nella quale la pubblicazione è stata effettuata[888]. Nei contenuti pubblicati è necessario, altresì, non violare eventuali diritti d'autore di terzi.

In caso di trasparenza reattiva, nell'accesso documentale[889] e nell'accesso civico generalizzato, tra gli interessi da considerare c'è proprio la proprietà intellettuale. In specifico, in caso di istanza di accesso civico generalizzato «*gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali*» sono causa di diniego dell'accesso se questo è necessario per evitare un pregiudizio concreto alla tutela di tali interessi privati protetti[890]; di nuovo emerge l'esigenza di bilanciamento in concreto, con la valutazione del caso.

In presenza di *open data* il diritto d'autore deve fare i conti con il diritto al riutilizzo dei dati, che confligge in modo fisiologico ed evidente. In tal caso i profili sono regolati dalle licenze aperte e, in caso di assenza, è previsto il principio *open data by default*: i dati e i documenti che i soggetti cui si applica il Codice dell'amministrazione digitale pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza, si intendono rilasciati come dati di tipo aperto ai sensi

---

888 Artt. 11 e 29, legge 633/1941; le disposizioni della legge, ai sensi dell'art. 5, non si applicano ai testi degli atti ufficiali dello Stato e delle amministrazioni pubbliche, sia italiane che straniere.

889 Tale diritto può essere ricompreso nell'art. 24, comma 6, lett. d), legge 241/1990 nella seguente ipotesi: «*quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono*»; il regolamento del Governo relativo alla previsione dei casi di sottrazione all'accesso di documenti amministrativi, tra cui quelli richiamati, non è stato adottato.

890 Art. 5-bis, comma 2, lett. c), d.lgs. 33/2013.

all'articolo 1, comma 1, lett. l-bis) e l-ter) del Codice, ad eccezione dei casi in cui la pubblicazione riguardi dati personali[891]. Anche in tal caso la messa a disposizione dei *dataset* dovrà avvenire da parte di colui che è titolare dello stesso, tenendo conto che il trasferimento del dato non sposta la titolarità dello stesso[892].

Nel caso dei *big data* si porranno complessi problemi per stabilire la titolarità dei relativi grandi *dataset* oggetto degli algoritmi e dei processi di *data mining*, potendosi configurare diritti d'autore su informazioni strutturate contenute all'interno, diritti *sui generis* su *dataset* contenuti nell'insieme di *big data* oggetto di elaborazione e il diritto *sui generis* sull'insieme di dati che formano il *dataset* di *big data*; infatti, come già esaminato, generalmente le raccolte di *big data* sono ricondotte alle banche dati "non creative", anche a causa della estrema varietà dei dati inclusi, ma non sempre sarà facile individuare il titolare laddove nel processo intervengano attori diversi (è il caso dell'*Internet of Things*).

In considerazione poi del ruolo svolto dagli algoritmi e dai programmi di elaborazione per estrarre conoscenza dai *big data* la proprietà intellettuale emergerà anche sotto tale profilo, dal momento che i software sono beni informatici protetti dal diritto d'autore e, di conseguenza, si porrà una contrapposizione tra la dimensione "proprietaria" del titolare del software e l'istanza collettiva di conoscere lo stesso, che si traduce nell'esigenza di conoscere quanto meno la logica che guida i processi di estrazione della conoscenza e di predizione.

Come emerge dall'analisi, nel governo dei dati e nelle diverse configurazioni degli stessi è necessaria la ricerca del bilanciamento, ossia «il difficile punto di equilibrio tra sfere di proprietà e sfere di libertà, avendo comunque sempre di vista l'esigenza di fondo — che in qualche modo connota la società del nostro tempo influenzando di riflesso i criteri classificatori in chiave giuridica — riconducibile alla necessità di garantire i beni comuni della conoscenza contro la logica riduttiva della prospettiva dominicale»[893].

---

891 Art. 52, comma 2, d.lgs. 82/2005, come modificato, da ultimo, dal d.lgs. 217/2017.

892 Art. 50, comma 3-bis, d.lgs. 82/2005.

893 N. LIPARI, *Le categorie del diritto civile*, Giuffrè, Milano, 2013, p. 135 ss.; la citazione è riportata in G. FINOCCHIARO, *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, cit., p. 499 ss.

Capitolo 5

Protezione dei dati personali e *data governance*

SOMMARIO: 5.1. Il diritto alla protezione dei dati personali nell'era digitale. – 5.1.1. Il fondamento del diritto e il sistema delle fonti. – 5.1.2. La disciplina di riferimento: il regolamento europeo 2016/679 e la normativa nazionale. – 5.2. La *data protection* nel governo dei dati. – 5.3. Privacy, trasparenza proattiva e apertura dei dati pubblici. – 5.3.1. *Data protection* e pubblicazione (obbligatoria e facoltativa). – 5.3.2. I profili problematici del bilanciamento tra diritti: durata, indicizzazione e apertura (riutilizzo). – 5.4. La protezione dei dati personali e la trasparenza reattiva realizzata con l'accesso civico generalizzato. – 5.5. Equilibri tra trasparenza, apertura e privacy. – 5.6. *Data protection* e *big data*.

5.1. Il diritto alla protezione dei dati personali nell'era digitale

5.1.1. Il fondamento del diritto e il sistema delle fonti

I diritti fondamentali entrano spesso in contrasto in rete; accade così che gli esaminati diritto all'informazione e diritto d'autore entrino in conflitto con il diritto alla protezione dei dati personali[894].

Il diritto alla protezione dei dati personali[895], quale diritto fondamentale della persona, trova fonte nella normativa europea e fondamento costituzionale, seppur

[894] Si pensi al celebre caso *Peppermint* del 2007, che ha riguardato il bilanciamento tra la proprietà intellettuale e la protezione dei dati personali: dopo una serie di pronunce a favore del diritto d'autore, che sancivano il diritto del titolare di ottenere in via d'urgenza dal *provider* i dati anagrafici degli assegnatari degli indirizzi IP autori di condotte illecite attraverso piattaforme *peer-to-peer* (ordinanze Trib. Roma, 18 agosto 2006, 9 febbraio 2007, 5 aprile 2007, 20 aprile 2007 e 26 aprile 2007), l'ordinanza del Trib. Roma, 14 luglio 2007, ha accolto le istanze del Garante, costituitosi in giudizio, ritenendo prevalente nel bilanciamento la tutela della protezione dei dati personali rispetto al diritto d'autore, decidendo, di conseguenza, che non potevano essere forniti i dati anagrafici.

indiretto, nella lettura sistematica di un insieme di norme e, in particolare, nel rispetto dei diritti inviolabili dell'uomo, nello sviluppo della persona e nella pari dignità sociale, garantiti dagli articoli 2 e 3 della Costituzione[896], fornendo la matrice ideale di una serie di ulteriori diritti quali la libertà personale, di cui all'art. 13 C., l'inviolabilità del domicilio, di cui all'art. 14 C., la libertà e segretezza della corrispondenza e di ogni forma di comunicazione, di cui all'art. 15 C.[897].

Come emerso nell'analisi condotta nel precedente capitolo, il diritto alla protezione dei dati personali si lega profondamente all'identità personale e al diritto all'oblio, attribuendo al soggetto un diritto di contenuto positivo all'autodeterminazione informativa, che permette di controllare, in modo attivo, la circolazione dei dati e delle informazioni che lo riguardano, consentendo di poter accedere, rettificare e cancellare i dati e permettendo, così, di definirsi e determinarsi[898]. Si tratta di un diritto, come nel caso dell'identità, dinamico, che nell'era digitale si collega alla libertà informatica e

---

895 Nel presente lavoro il termine privacy verrà usato in modo atecnico come sinonimo di protezione dei dati personali, oltre che di riservatezza.

896 Chiarisce I. NICOTRA, *op. cit.*, p. 8 che le «disposizioni contenute negli articoli 2 e 3 della Costituzione contribuiscono a superare la prospettiva della privacy – property per edificare il nuovo paradigma della privacy – dignity, quale patrimonio inalienabile della persona». G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, p. 151 ss. sottolinea che l'art. 2 Cost. costituisce una clausola aperta e generale di tutela dello svolgimento della persona umana, che dà fondamento ai diritti della personalità.

897 La privacy viene fondata, altresì, sulla libertà di manifestazione del pensiero nell'accezione in senso negativo, come diritto a mantenere il segreto sulle proprie idee e convinzioni, di cui all'art. 21 C., che afferisce più propriamente al diritto alla riservatezza che non alla protezione dei dati personali. Cfr. C. FLICK, *Privacy e legge penale nella società dell'informazione e della comunicazione*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici,* Giuffrè editore, Milano, 2008, p. 243 ss. e G.E. VIGEVANI, *op. cit.*, pp. 473-498.

898 Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 394 ss.; S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, cit.; G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, cit., p. 151 ss.; G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civili commentate*, fasc. 1, 2017, p. 1 ss. A.C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, cit., p. 320: «se, infatti, nella società della comunicazione globale si può dire che noi siamo le nostre informazioni, quel che più conta è governarne la circolazione così da provare a recuperare il possesso di sé».

all'*habeas data*, sviluppo dell'*habeas corpus*, da cui è originata la libertà personale. Non c'è tutela dell'identità, come controllo della propria rappresentazione sociale, senza la protezione dei dati personali, come controllo sui dati[899], nella direzione condivisa della dignità e della libera costruzione della personalità[900].

In tale congiunzione con l'identità emerge anche l'accezione iniziale di privacy, il limitrofo e distinto diritto alla riservatezza, che protegge la sfera individuale dalle intrusioni esterne (diritto ad essere lasciati soli - *right to be let alone*), diritto a contenuto statico e negativo, teso a mantenere riservate alcune informazioni personali e familiari da interferenze altrui, sul modello della proprietà privata. Si tratta, nel caso della riservatezza, di un diritto di creazione giurisprudenziale, che non riguarda tutti i dati, ma solo le vicende riservate; seppur talvolta i due diritti (riservatezza e protezione dei dati personali) possano coincidere (es. i dati sanitari), sono diversi e distinti gli ambiti e gli oggetti di tutela[901]. La protezione dei dati personali tutela ampiamente la persona per mezzo della protezione di ogni informazione che la riguarda e non soltanto di quelle potenzialmente offensive[902]. Il punto di congiunzione è allocato nella tutela

---

899 G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, cit., p. 154 coglie in questo la differenza: il diritto all'identità è un diritto al controllo sull'immagine sociale, mentre il diritto alla protezione dei dati personali è un diritto al controllo sui dati.

900 M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, fasc. 4, 2016, pp. 1249-1264.

901 Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 4 ss., che ricorda come la genesi del diritto alla riservatezza sia generalmente ricondotta a un articolo di Warren e Brandeis sul *right to be let alone* e sull'inviolabilità della sfera personale e privata in relazione a interferenze giornalistiche (anche se altri la riconducono alla dottrina tedesca); cfr. S.D. WARREN - L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, vol. 4, n. 5, 15 dicembre 1890, pp. 193-220. In Italia il diritto alla riservatezza viene riconosciuto dalla giurisprudenza a partire dalla sentenza della Corte di Cassazione del 22 dicembre 1956, n. 4487, *caso Caruso*, dalla sentenza della Corte di Cassazione del 20 aprile 1963, n. 990, *caso Petacci* e, in particolare, dalla sentenza della Corte di Cassazione del 27 maggio 1975, n. 2129, *caso Soraya Esfandiary*, che ha visto contrapposti diritto alla riservatezza e diritto di cronaca. Cfr. G. PASCUZZI - F. GIOVANELLA, *Dal diritto alla riservatezza alla computer privacy*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, p. 43 ss.

902 G.E. VIGEVANI, *op. cit.*, pp. 473-498. G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, cit., p. 151 ss. sottolinea che anche le altre espressioni utilizzate per indicare il diritto alla protezione dei dati personali come *information privacy*, *informational privacy*, *data privacy* evidenziano come sia oggetto del diritto l'informazione o il dato (seppur i due termini non siano coincidenti).

complessiva della libertà e della dignità della persona, sulla quale convergono in modo unitario sia il diritto ad auto-escludersi dal flusso di informazioni come libertà dal controllo sociale, ossia il diritto alla riservatezza, sia il diritto al controllo delle informazioni come libertà dal controllo tecnologico, l'*habeas data*[903].

Dal momento che è teso alla protezione dei dati personali, si tratta di un diritto ontologicamente toccato in modo profondo dalle nuove configurazioni dei dati e forme di trasparenza: il governo dei dati deve necessariamente fare i conti con la protezione dei dati personali.

Come nel caso dell'analisi relativa al diritto d'autore, per poter esaminare il profilo della privacy in relazione al governo dei dati e nelle diverse configurazioni che i dati stessi assumono (trasparenza, *open data*, *big data*), è necessario preventivamente soffermarsi sui principi e sulla disciplina di riferimento[904].

L'Autrice evidenzia la natura di diritto della personalità (categoria aperta di diritti), come tale assoluto, indisponibile e imprescrittibile, suscettibile di ampliamento da parte della normativa o della giurisprudenza.

[903] G.E. VIGEVANI, *op. cit.*, pp. 473-498. Secondo M. CARTA, *Diritto alla vita privata ed Internet nell'esperienza giuridica europea ed internazionale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2014, pp. 1-19 il diritto del singolo di decidere in prima persona sulla cessione e sull'uso dei dati personali, ossia la sua autodeterminazione informativa, va interpretata come una delle declinazioni possibili della tutela della dignità dell'uomo, che non rendono la protezione dei dati personali assimilabile a un diritto di proprietà in quanto tale alienabile. Secondo G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, cit., p. 155 il diritto alla protezione dei dati personali e i diritti della personalità limitrofi, come il diritto all'identità e il diritto alla riservatezza, «sono tutti volti a tutelare un unico bene giuridico: l'identità. Identità che viene vista nelle sue molteplici forme ed espressioni: le informazioni concernenti un soggetto, la sua immagine sociale, la sua immagine sulla stampa, la sua immagine fisica, il suo nome»: un elemento di complessità è dato dalla possibilità di manifestazione dell'identità con mezzi digitali e dalla conseguente possibilità di assumere molteplici identità.

[904] Sulla protezione dei dati personali, *ex plurimis*, cfr. F. BERGADANO - A. MANTELERO - G. RUFFO - G. SARTOR, *Privacy digitale: giuristi e informatici a confronto*, Giappichelli, Torino, 2005; L. BOLOGNINI - D. FULCO - P. PAGANINI (a cura di), *Next privacy. Il futuro dei nostri dati nell'era digitale*, Etas RCS, Milano, 2010; V. CUFFARO - R. D'ORAZIO - V. RICCIUTO, *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007; P. PERRI, *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007; S. RODOTÀ, *Intervista su privacy e libertà*, cit.; S. SICA - P. STANZIONE (diretto da), *La nuova disciplina della privacy. Commento al D.Lgs. 30 giugno 2003, n.* 196, Zanichelli, Bologna, 2004; G. ZICCARDI, *Informatica giuridica. Tomo II – Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, II ed., Giuffrè, Milano, 2012.

Il diritto trova fondamento in significative disposizioni a livello sovranazionale[905].

La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, nell'art. 8, riconosce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, limitando l'ingerenza della pubblica autorità, disciplinando così il diritto alla riservatezza[906].

Il diritto alla protezione dei dati di carattere personale assume autonomia con la Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) del 2000, che lo tratta specificamente nell'art. 8 in modo autonomo e distinto dalla tutela del diritto al rispetto della vita privata e familiare (art. 7), seppur entrambi condividano l'essenza di diritti fondamentali di libertà, in quanto relativi al diritto del singolo a definire la propria esistenza. Nell'art. 8 si precisa che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano e si affermano alcuni principi che saranno centrali nella disciplina europea e nazionale: «*tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*». L'art. 8 chiarisce, altresì, che «*il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*».

Anche il Trattato sul funzionamento dell'Unione europea, nel suo art. 16, prevede il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano:

---

905 La regolazione della protezione dei dati personali si alloca in fonti diverse e disparate, di diversa forza giuridica, come norme vincolanti o meno, di natura nazionale e sovranazionale (si pensi alla disciplina europea), i trattati UE-USA, i rapporti e le iniziative delle Nazioni Unite e le linee guida dell'OCSE, i provvedimenti del Garante europeo e di quello nazionale, l'attività dell'*Article 29 Data Protection Working Party*, le sentenze della Corte di Giustizia dell'Unione europea e le sentenze delle Corti interne; cfr. C. FOCARELLI, *op. cit.*, p. 103, che ricostruisce il complesso insieme di fonti.

906 Al diritto alla riservatezza si riferiscono anche l'art. 12 della Dichiarazione universale dei diritti dell'uomo del 1948, l'art. 17 del Patto sui diritti civili e politici del 1966 e l'art. 1 della Dichiarazione dei diritti dell'uomo in relazione ai mezzi di comunicazione di massa del 1970; cfr. C. CANALE, *Internet e le nuove frontiere di tutela della privacy alla luce delle ultime sentenze della Corte di Cassazione e della Corte di Giustizia Europea*, in *Temi romana*, fasc. 2, 2015, p. 12 ss. e E. FALLETTI, *L'evoluzione del concetto di privacy e della sua tutela giuridica*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, 2013, pp. 23-24.

il Parlamento europeo e il Consiglio sono tenuti a stabilire le norme relative alla protezione delle persone fisiche[907].

In tale contesto va richiamata anche la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, promossa dal Consiglio d'Europa nel 1981, ossia la Convenzione di Strasburgo del 28 gennaio 1981, n. 108, ratificata in Italia con legge 21 febbraio 1989, n. 98[908].

A livello europeo sono state emanate diverse direttive in materia di privacy, delle quali quella "madre" è costituita dalla direttiva 95/46/CE [909], ed è stato di recente approvato il regolamento (UE) 2016/679, regolamento generale sulla protezione dei dati (*General Data Protection Regulation* – GDPR), che, entrato in vigore il 24 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti gli Stati membri a partire dal 25 maggio 2018[910].

---

907 Le norme sono stabilite con riguardo «*al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti*». Rileva anche l'art. 39 TUE (Trattato sull'Unione europea), che estende la protezione dei dati personali allo specifico settore della politica estera e della sicurezza comune, rimettendo la regolazione all'adozione di una decisione da parte del Consiglio.

908 Completa la Convenzione il Protocollo addizionale sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, concernente le autorità di controllo e i flussi transfrontalieri di dati, adottato l'8 novembre 2001.

909 Rilevano in materia di privacy la direttiva 2002/58/CE, la direttiva 2006/24/CE, la direttiva 2009/136/CE, la direttiva 2009/140/CE e il regolamento 2001/45/CE.

910 Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Il cosiddetto "pacchetto europeo protezione dati" consta anche della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, in vigore dal 5 maggio 2016 e che dovrà essere recepita dagli Stati membri entro 2 anni. Sull'evoluzione del diritto europeo della privacy cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. I – Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016. Sul regolamento europeo cfr., *inter alia*, F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. II – Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016 e L. BOLOGNINI - E. PELINO - C. BISTOLFI, *Il regolamento*

La direttiva 95/46/CE, recependo il pensiero e il dibattito dei decenni precedenti, aveva delineato un modello statico di trattamento dei dati personali di carattere riparatorio, centrato su un unico scambio di dati tra interessato e titolare, adatto alla realtà e alla società tecnologica dell'epoca, priva di *social* e motori di ricerca, modello ormai superato; diversamente, il regolamento (UE) 2016/679 prevede un modello di condivisione e cogestione dei dati, fin dall'origine destinati alla circolazione globale, fondato su una tutela preventiva e "attiva", maggiormente adeguato alla realtà contemporanea dominata da efficienti algoritmi, tecniche di *data mining*, ricorrenti profilazioni e rischi di sorveglianza[911].

Il regolamento, nella specifica tipologia di atto scelta (regolamento e non direttiva), origina dall'esigenza di un'applicazione omogenea della normativa nell'Unione europea necessaria per un clima di fiducia, essenziale allo sviluppo dell'economia digitale e all'efficacia dei servizi digitali pubblici e privati, a fronte della diffusa incertezza giuridica derivante dalla frammentarietà e dalle differenze tra discipline all'interno dell'Unione: il regolamento si pone come strumento di uniformazione del diritto per gli Stati membri, dal momento che si applica direttamente, senza la necessità di atti di recepimento[912].

Stesso strumento è stato adottato anche in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, il regolamento eIDAS, reg. (UE) n. 910/2014, che ha abrogato anche in quel caso una direttiva (la direttiva 1999/93/CE). In una prospettiva unitaria il legislatore europeo mostra l'intento evidente di creare un mercato unico digitale rimuovendo l'ostacolo della disomogeneità

---

privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Giuffrè, Milano, 2016.

911 Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 1 ss. e M.G. STANZIONE, *op. cit.*, p. 1249 ss., che sottolinea come in tale contesto la logica del consenso rivela comunque tutta la sua insufficienza.

912 G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 5 ss. Ciò non toglie che siano lasciati margini agli Stati, come si specifica nel considerando 10 del regolamento, liberi nel mantenere o introdurre norme per specificare ulteriormente l'applicazione del regolamento o per stabilire le condizioni per specifiche situazioni di trattamento, anche determinando più precisamente le condizioni, sempre nel quadro dei principi e delle norme del regolamento europeo; M.G. STANZIONE, *op. cit.*, p. 1249 ss.

tra normative, consolidando così la posizione europea a livello globale per mezzo di un approccio unitario.

Tale esigenza che anima il regolamento europeo emerge anche nel cosiddetto "meccanismo di coerenza", atto a garantire un'applicazione uniforme del regolamento e basato sulla cooperazione tra le autorità di controllo[913].

La finalità di omogeneizzare e rendere maggiormente efficace la tutela della privacy in Europa risulta particolarmente significativa anche in considerazione delle differenze nel riconoscimento del valore e nella regolazione della protezione dei dati personali rispetto agli Stati Uniti: anche se il concetto di privacy nasce in quell'ordinamento[914], a livello di tutela concreta al di là delle elaborazioni teoriche, la protezione statunitense ha sostanzialmente fallito e la normativa federale in materia risulta debole, settoriale e frammentaria[915].

---

913 Art. 63 ss., reg. (UE) 2016/679. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. II - Il Regolamento europeo 2016/679*, cit., p. 101 ss. sottolinea che il regolamento europeo poggia su due pilastri: «il primo, solido e fermo come una muraglia, e profondamente radicato nel tessuto normativo, mira a imporre regole uniformi e, soprattutto, ad assicurare l'attuazione delle medesime regole in tutta l'Unione; il secondo, mobile e flessibile come il braccio girevole di una gru o la piattaforma di un elevatore in movimento, assicura invece l'elasticità necessaria per trovare sempre il giusto punto di equilibrio con le tradizioni culturali dei diversi Paesi, con le caratteristiche dei loro ordinamenti giuridici, con le esigenze degli scambi internazionali». Il regolamento, per mezzo della rigidità da una parte e dell'elasticità dall'altra, assicura in ogni caso un alto livello di protezione dei dati personali «adeguato sia a garantire il diritto fondamentale dell'interessato che la tutela delle libertà in una società democratica».

914 Gli Stati Uniti non contemplano espressamente il diritto alla privacy in Costituzione, ma c'è stata l'interpretazione evolutiva del quarto emendamento, ai sensi del quale il potere esecutivo può condurre indagini o perquisizioni di beni o cose appartenenti ad individui solo se sono fondate su un mandato emesso da un'autorità giurisdizionale, in base alla probabilità (*probable cause*) che quell'attività permetta di ottenere prove relative alla commissione di un reato; cfr. M. NINO, *Il caso "Datagate": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, fasc. 3, 2013, p. 732 ss.

915 Si tratta dell'*US Privacy Act* del 1974, del *Freedom of Information Act* (FOIA), dell'*E-Government Act* del 2002 e del relativo *Federal Information Security Act*, nonché di ordinanze, codici di autoregolamentazione e politiche del Governo; cfr. M. NINO, *Il caso "Datagate": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, cit., p. 732 ss. Secondo G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 15 gli Stati Uniti hanno mostrato attenzione all'elaborazione teorica senza una reale tutela da un punto di vista pratico, mentre l'Europa, più immatura

Le divergenze tra Stati Uniti ed Europa derivano da una diversa concezione valoriale di fondo: nel contesto europeo la persona e i suoi dati sono sovraordinati ad eventuali interessi economici in conflitto, mentre negli Stati Uniti prevale la volontà di promuovere e privilegiare "il mercato dei dati" e rimettere la tutela dei dati stessi alla negoziazione tra le parti, seppur negli ultimi anni anche nel contesto statunitense si tenda a rafforzare la protezione dell'interessato. Sia Europa che Stati Uniti convergono però nel metodo e nell'approccio preventivo e proattivo, ossia nella valorizzazione del principio di *accountability* e nel ricorso a soluzioni tecnologiche e organizzative atte a prevenire le violazioni[916]. Peraltro, come si vedrà, nella disciplina europea e nel relativo regolamento emerge la tendenza ad espandere il proprio modello fuori dai confini europei.

In tale operazione di uniformazione europea, che mira al riordino e alla razionalizzazione, evidentemente rispetto alla normativa nazionale si porranno significative novità, ma anche mere integrazioni e arricchimenti e, in certi casi, emergerà la conformità con quanto già previsto a livello italiano, seppur le disposizioni del regolamento risultino comunque innovative della previgente disciplina europea[917].

Nel nostro Paese, dopo la legge 31 dicembre 1996, n. 675[918], che ha introdotto il diritto alla protezione dei dati personali in Italia, l'attuale disciplina è allocata nel d.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali* (di seguito

---

a livello teorico, ha però dedicato una protezione più concreta e decisa ai dati personali. Sui diversi modelli statunitense ed europeo cfr. P. PERRI, *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Giuffrè, Milano, 2007 e U. PAGALLO, *La tutela della "privacy" negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008.

916 A. MANTELERO, *Privacy digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet giuridica, Torino, 2012, p. 162 ss.

917 G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 5 ss.

918 La legge 675/1996 è stata abrogata dal d.lgs. 196/2003: aveva attuato la direttiva 95/46/CE, l'Accordo di Schengen ratificato dall'Italia con legge 30 settembre 1993, n. 388, la Convenzione del Consiglio d'Europa n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati personali, adottata a Strasburgo il 28 gennaio 1981 e ratificata dall'Italia con legge 21 febbraio 1989, n. 98 (senza ratifica vera e propria del Capo dello Stato a causa della mancanza di una normativa italiana sulla protezione dei dati) e le diverse Raccomandazioni del Consiglio d'Europa tese alla tutela del diritto alla riservatezza; cfr. J. MONDUCCI, *La tutela della privacy e le misure di sicurezza*, in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, Giappichelli Editore, Torino 2011, p. 109 ss.

anche Codice)[919]. Il Codice garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali: emergono le dimensioni autonome e correlate, che trovano matrice nella dignità e nello sviluppo della persona con il riconoscimento del diritto alla protezione dei dati personali nella sua indipendenza rispetto alla riservatezza e all'identità (art. 2)[920].

Nella «*Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017*», approvata con legge 25 ottobre 2017, n. 163, l'art. 13 prevede la delega al Governo ad adottare, entro sei mesi[921], acquisiti i pareri delle competenti Commissioni parlamentari e del Garante per la protezione dei dati personali, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679. Nell'esercizio della delega, come viene precisato espressamente dalla disposizione, il Governo è tenuto a rispettare i seguenti principi e criteri direttivi specifici[922]:

---

[919] Il Codice ha dato attuazione alle disposizioni europee e ha riordinato la norme in materia di privacy, tra le quali la direttiva europea 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. Nell'art. 1 si sancisce con forza: «*chiunque ha diritto alla protezione dei dati personali che lo riguardano*». Secondo G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, cit., p. 156 ss. il Codice detta norme essenzialmente procedurali sul modo di utilizzare le informazioni, siano esse riservate o meno.

[920] Art. 2, d.lgs. 196/2003, che al secondo comma prevede: «*il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà fondamentali nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento*». Cfr. G. PASCUZZI - F. GIOVANELLA, *Dal diritto alla riservatezza alla computer privacy*, cit., p. 43 ss. e R. BRENNA, *La protezione dei dati nel Codice della privacy*, in M. MEGALE (a cura di), *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2012, p. 127.

[921] Con le procedure di cui all'art. 31 della legge 24 dicembre 2012, n. 234, ossia le procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea.

[922] Oltre ai principi e criteri direttivi generali di cui all'art. 32 della legge 234/2012, ossia quelli generali di delega per l'attuazione del diritto dell'Unione europea.

a) abrogare espressamente le disposizioni del Codice, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
b) modificare il Codice, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679;
d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;
e) adeguare, nell'ambito delle modifiche al Codice, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

Nel percorso di adeguamento italiano al regolamento europeo, rileva, altresì, l'art. 28 della legge 20 novembre 2017, n. 167[923], che apporta le prime modifiche e integrazioni al Codice in materia di protezione dei dati personali, di cui al d.lgs. 196/2003, in specifico in relazione al responsabile del trattamento (di cui all'art. 29 del d.lgs. 196/2003) e al riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici (viene introdotto al riguardo l'art. 110-bis al d.lgs. 196/2003)[924].

---

[923] Merita precisare che, oltre all'art. 28, l'art. 29 della legge 167/2017 interviene potenziando le risorse finanziarie e organiche del Garante per la protezione dei dati personali. Infine, degno di nota è anche l'art. 24 della legge 167/2017, che (in deroga all'art. 132, commi 1 e 1-bis, d.lgs. 196/2003) estende a 72 mesi i termini di conservazione dei dati di traffico telefonico e telematico e dei dati relativi alle chiamate senza risposta, «*al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale*».

[924] L'art. 110-bis del d.lgs. 196/2003, introdotto con la legge 167/2017, dispone quanto segue: «*Nell'ambito delle finalità di ricerca scientifica ovvero per scopi statistici può essere autorizzato dal Garante il riutilizzo dei dati, anche sensibili, ad esclusione di quelli genetici, a condizione che siano adottate forme preventive di minimizzazione e di anonimizzazione dei dati ritenute idonee a tutela degli interessati*». Il secondo comma della disposizione prevede le modalità relative all'autorizzazione del Garante, che, inoltre, «*con il provvedimento di autorizzazione o anche successivamente, sulla base di*

In attesa del completo adeguamento italiano, la disciplina sarà esaminata, dando conto delle disposizioni europee che si applicheranno in modo diretto dal 25 maggio 2018, disapplicando e prevalendo sulle norme interne in contrasto, e volgendo uno sguardo anche alle disposizioni nazionali, tenendo conto di quanto già espresso al riguardo dal Garante[925].

In merito, è opportuno rilevare che la Dichiarazione dei diritti in Internet tratta ampiamente il diritto alla protezione dei dati personali nelle sue dimensioni, che trovano spazio in diversi articoli (artt. 5, 6, 7 e 8). Le disposizioni risultano interessanti, perché seppur l'atto non abbia valore giuridico, contiene aspetti che derivano dalla riflessione e dal dibattito in materia e sono presenti nella disciplina europea recata dal regolamento (UE) 2016/679.

Ai sensi dell'art. 5, specificamente dedicato alla tutela dei dati personali, ogni persona ha «diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza»; nella *data protection* emergono il valore della dignità e le dimensioni correlate di identità e riservatezza. Viene chiarita la tipologia di dati interessati dalla tutela: si tratta dei dati che permettono di identificare una persona, comprendendo anche i dati dei dispositivi e le loro ulteriori acquisizioni ed elaborazioni, come quelle dei profili. Si prevede il diritto di ogni persona di accedere ai dati raccolti, ottenerne la rettifica e la cancellazione per motivi legittimi. Sono richiamati i principi cui deve informarsi il trattamento: necessità, finalità, pertinenza, proporzionalità e prevalenza del diritto di ogni persona all'autodeterminazione informativa. Condizione necessaria per un legittimo trattamento è il consenso effettivamente informato dell'interessato o altro fondamento legittimo; il consenso è in via di principio revocabile e, in caso di dati sensibili, la legge può prevedere che debba essere accompagnato da specifiche autorizzazioni. In ogni caso il consenso «non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento»; è posto il divieto di accesso e

---

eventuali verifiche, […] *stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza*».

925 Ad esempio è il caso della Guida all'applicazione del regolamento europeo in materia di protezione dei dati personali, predisposta dal Garante e disponibile al seguente link: *www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*.

trattamento dei dati con finalità anche indirettamente discriminatorie[926]. Tali passaggi tengono evidentemente conto dell'attuale società degli algoritmi, attraversata da asimmetrie di potere e soggetta al rischio di discriminazioni.

L'art. 6 della Dichiarazione, valorizzando il contenuto positivo e dinamico della privacy, si riferisce al diritto all'autodeterminazione informativa, quale diritto di controllo relativo alle informazioni e ai dati sulla propria persona (*habeas data*). Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto e il luogo di conservazione, per chiederne integrazione, rettifica e cancellazione secondo le modalità previste dalla legge, nonché di conoscere le modalità tecniche di trattamento dei dati. In ogni caso la raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando i principi di finalità e proporzionalità e il diritto all'autodeterminazione[927].

L'art. 7 è dedicato al diritto all'inviolabilità dei sistemi, dei dispositivi e dei domicili informatici e, richiamando anche la problematica della sorveglianza di massa, fa riferimento all'inviolabilità della libertà e segretezza delle informazioni e delle comunicazioni elettroniche delle persone, che possono essere derogate nei soli casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria[928].

Infine, anche l'art. 8 della Dichiarazione dei diritti in Internet è particolarmente adeguato alla società contemporanea e agli strumenti che la caratterizzano, dal momento che richiama la necessità di garantire la persona da trattamenti automatizzati che possano profilarla o definirne la personalità: «nessun atto, provvedimento giudiziario o amministrativo, decisione comunque destinata ad incidere in maniera significativa nella

---

926 A. MASERA - G. SCORZA, *op. cit.*, p. 34 ss. Secondo C. FOCARELLI, *op. cit.*, p. 151 ss. la bozza di Dichiarazione (che l'Autore commenta prima del testo definitivo) sembra condizionata dal *Datagate* e «pare trascurare, anche se non vengono omessi, gli aspetti di innovazione e crescita economica dei *big data* (sul piano tecnologico ed economico) e quelli di sicurezza (sul piano politico e di difesa)» (p. 153).

927 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 77.

928 Secondo G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 78 l'articolo sembra fare riferimento, oltre alle azioni di sorveglianza indiscriminata, al problema delle investigazioni digitali in ambito penale, ai tipici *computer crimes* come l'accesso abusivo a un sistema informatico, seppur marginalmente, e, infine, all'importanza delle procedure di autenticazione.

sfera delle persone possono essere fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato».

5.1.2. La disciplina di riferimento: il regolamento europeo 2016/679 e la normativa nazionale

L'intreccio di disposizioni e di livelli normativi che intervengono nella materia mostra la centralità del diritto alla protezione dei dati personali nei rapporti inediti tra evoluzione tecnologica e dimensione globale, al fine di un corretto utilizzo della tecnologia nei confronti della persona, su cui il diritto è chiamato a intervenire[929].

La tutela del diritto alla protezione dei dati personali, come scaturisce dalla normativa europea di riferimento, si basa su una disciplina che chiarisce la tipologia dei dati, dei soggetti e dei trattamenti coinvolti.

Il diritto alla protezione dei dati personali tutela le persone fisiche[930] e riguarda i dati personali, ossia qualsiasi informazione riguardante una persona fisica, identificata o identificabile (il cosiddetto interessato), 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[931].

---

929 R. BIFULCO, *op. cit.*, pp. 289-307. Secondo S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 396, nel riferirsi ai dati ceduti e continuamente monitorati e alle tracce lasciate nello spazio digitale, «questa gran massa di dati personali, raccolta su scala sempre più larga e fatta circolare intensamente, modifica la conoscenza e l'identità stessa delle persone, spesso conosciute soltanto attraverso il trattamento elettronico delle informazioni che le riguardano».

930 Art. 1, reg. (UE) 2016/679. Anche la disciplina nazionale non tutela più, come in passato, i dati delle persone giuridiche; l'art. 40, comma 2, lett. a) e b) del d.l. 6 dicembre 2011, n. 201, convertito con modificazioni dalla legge 22 dicembre 2011, n. 214 (il cosiddetto decreto Salva Italia), ha, infatti, modificato l'art. 4, comma 1, lett. b) e i) del Codice.

931 Art. 4, paragrafo 1, n. 1), reg. (UE) 2016/679 e, analogamente, art. 4, comma 1, lett. b), d.lgs. 196/2003: l'interessato è definito nell'art. 4, comma 1, lett. i), d.lgs. 196/2003 come «*la persona fisica, cui si riferiscono i dati personali*». Come esempio di dato indirettamente identificativo si può pensare ai *nickname* o codici utenti che si utilizzano con i fornitori di servizi; G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 29.

L'ambito è molto vasto ed evidenzia l'ampiezza dell'oggetto del diritto costituito da dati e informazioni. Emerge un approccio e una regolazione basata sui dati[932]: si tratta sostanzialmente di qualunque informazione riferibile a qualunque soggetto di qualunque tipologia (anche immagini e suoni)[933]. Sono esclusi dall'applicazione della normativa i cosiddetti dati anonimi, ossia dati che in origine, o a seguito di trattamento, non possono essere riferiti ad una persona fisica identificata o identificabile[934]; al riguardo, il regolamento introduce il concetto di pseudonimizzazione, che si differenzia dall'anonimizzazione[935].

---

[932] A. MANTELERO, *Privacy digitale*, cit., p. 163 ss. parla di regolamentazione dato-centrica, dato il rilievo attribuito alle operazioni sulle informazioni e ai rapporti tra i soggetti che trattano i dati e i dati stessi.

[933] G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 3. Il considerando 26 precisa che per stabilire l'identificabilità di una persona «*è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente*» e per il considerando 30 le persone fisiche possono essere associate «*a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*».

[934] Il considerando 26 del reg. (UE) 2016/679 parla di mancata applicazione alle «*informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato*». L'art. 4, comma 1, lett. n), d.lgs. 196/2003 definisce il dato anonimo «*il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile*».

[935] La pseudonimizzazione, ai sensi dell'art. 4, paragrafo 1, n. 5), reg. (UE) 2016/679 è «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile*»; al riguardo il considerando 28 precisa che l'introduzione esplicita della «pseudonimizzazione» non è intesa a precludere altre misure di protezione dei dati. G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 31 distinguono i due termini: l'anonimizzazione si basa sull'introduzione di incertezze nell'attribuzione di un dato ad un soggetto, mentre la pseudonimizzazione consiste nel sostituire un attributo, solitamente univoco, di un dato con un altro, univoco e solitamente non immediatamente intellegibile e, quindi, rende più complessa

Tra i dati personali, per la tipologia delle informazioni coinvolte e l'incidenza nella sfera intima della persona, specifica e più elevata tutela è garantita a «*categorie particolari di dati*», i dati sensibili[936], e, altresì, ai dati relativi a condanne penali e reati[937]: i dati che non rientrano in tali tipologie sono detti generalmente comuni (es. nome, cognome, indirizzo, titolo di studio, etc.). In merito il regolamento europeo prevede la necessità di condizioni specifiche per effettuare il trattamento, altrimenti vietato, di particolari categorie di dati[938] e, nel considerando 10, prevede un margine di manovra degli Stati membri per precisarne le norme, anche proprio con riguardo al trattamento di categorie particolari di dati personali (dati sensibili): sotto tale profilo il

---

l'identificazione, garantendo confidenzialità e integrità dalle manipolazioni, ma non muta il quadro di certezze nella concatenazione di passaggi per l'attribuzione del dato pseudonimo alla persona: in tale ultimo caso l'operazione è reversibile e a ritroso il dato è riferibile alla persona. La pseudonimizzazione costituisce quindi una misura di sicurezza utile, ma non un metodo di anonimizzazione. Le diverse tecniche di anonimizzazione sono raggruppabili nelle due categorie della distorsione (o randomizzazione) e della generalizzazione dei dati.

936 Si tratta dei «*dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale*», nonché «*dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*», ai sensi dell'art. 9, paragrafo 1, reg. (UE) 2016/679; il considerando 10 chiarisce esplicitamente che per «*categorie particolari di dati personali*» si intendono i dati sensibili. Il Codice italiano qualifica come dati sensibili «*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*» (art. 4, comma 1, lett. d), d.lgs. 196/2003); questi ultimi sono anche definiti sensibilissimi, a causa del loro particolare impatto nella sfera intima del soggetto e della conseguente peculiare disciplina.

937 In tal caso, ai sensi dell'art. 10, reg. (UE) 2016/679, il trattamento deve avvenire «*sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati*». Anche il Codice garantisce maggiore tutela ai dati giudiziari, ossia i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), d.p.r. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del codice di procedura penale (art. 4, comma 1, lett. e), d.lgs. 196/2003).

938 L'art. 9, paragrafo 2, reg. (UE) 2016/679 prevede i casi in cui è lecito effettuare il trattamento di tali dati.

regolamento «*non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito*». Il regolamento definisce esplicitamente i dati genetici[939], quelli biometrici[940] e i dati relativi alla salute[941].

Oltre all'interessato, ossia la persona fisica cui i dati personali si riferiscono, vengono in gioco nel trattamento dei dati personali altri soggetti: il titolare del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che, singolarmente o insieme ad altri titolari, determina le finalità del trattamento di dati personali[942]; il responsabile del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo eventualmente preposto dal titolare che tratta dati personali per conto del titolare del trattamento[943]; gli incaricati, ossia le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile[944].

---

939 Art. 4, paragrafo 1, n. 13), reg. (UE) 2016/679: «*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione*».

940 Art. 4, paragrafo 1, n. 14), reg. (UE) 2016/679: «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*».

941 Art. 4, paragrafo 1, n. 15), reg. (UE) 2016/679: «*i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

942 Art. 4, paragrafo 1, n. 7), reg. (UE) 2016/679 e, analogamente a livello nazionale, art. 4, comma 1, lett. f) (che parla più specificamente di «*finalità, modalità del trattamento di dati personali e strumenti utilizzati, ivi compreso il profilo della sicurezza*») e art. 28, d.lgs. 196/2003.

943 Art. 4, paragrafo 1, n. 8), reg. (UE) 2016/679 e, a livello nazionale, art. 4, comma 1, lett. g) («*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo eventualmente preposto dal titolare al trattamento di dati personali*») e art. 29, d.lgs. 196/2003, quest'ultimo modificato dalla legge 167/2017.

944 Art. 4, comma 1, lett. h), e art. 30, d.lgs. 196/2003. Pur non prevedendo espressamente la figura dell'incaricato, il regolamento (UE) 2016/679 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*» (art. 4, n. 10); in tal senso la Guida all'applicazione del regolamento europeo in materia di

Il regolamento europeo prevede, inoltre, la designazione del responsabile della protezione dei dati (RDP) o *Data Protection Officer* (DPO), di cui all'art. 37 e seguenti del reg. (UE) 2016/679, nei casi previsti dalla disposizione; tale figura viene designata in base alle qualità professionali, in particolare alla conoscenza specialistica della normativa e delle prassi in materia e alla capacità di assolvere i compiti previsti dall'art. 39[945]. Si tratta di un soggetto autonomo, dal momento che non deve ricevere istruzioni e neppure incorrere in rimozioni o penalizzazioni per l'esecuzione dei propri compiti e deve riferire direttamente al vertice gerarchico del titolare o del responsabile (art. 38)[946].

Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e devono essergli attribuite le risorse necessarie per assolvere i propri compiti, che consistono essenzialmente nel vigilare sul rispetto della normativa e nel fornire consulenza[947]. Nello svolgere le proprie funzioni, tale figura deve considerare debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso[948].

Il trattamento, come il dato personale, ha una definizione ampia ed estesa, dal momento che riguarda sostanzialmente qualsiasi attività che abbia ad oggetto i dati

---

protezione dei dati personali, predisposta dal Garante (*www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali*).

945 Art. 37, paragrafo 5, reg. (UE) 2016/679.

946 La nomina del DPO è prevista in una serie di casi con la funzione di garantire una corretta gestione dei dati: ad esempio se il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (eccetto autorità giurisdizionali) o se il trattamento, per sua natura, ambito di applicazione e/o finalità, richiede il monitoraggio regolare e sistematico degli interessati su larga scala. Al riguardo cfr. «*Guidelines on Data Protection Officers ("DPOs")*», 16/EN WP 243 rev.01, adottate il 13 dicembre 2016 e riviste il 5 aprile 2017 dall'*Article 29 Data Protection Working Party*, al fine di agevolare l'individuazione di tale figura. In aggiunta a tali linee guida e al relativo allegato contenente indicazioni essenziali in forma di faq, il Garante per la protezione dei dati personali ha adottato specifiche faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico.

947 Art. 38, paragrafi 1 e 2, e art. 39, paragrafo 1, reg. (UE) 2016/679. Il DPO è il punto di contatto con l'autorità di controllo per questioni connesse al trattamento, ai sensi dell'art. 39, paragrafo 1, lett. e), reg. (UE) 2016/679.

948 Art. 39, paragrafo 2, reg. (UE) 2016/679. Il *Data Protection Officer*, oggi previsto nella normativa europea, era già disciplinato in alcuni ordinamenti, come Francia, Germania e Svezia; cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 15.

personali: viene identificato, infatti, a livello europeo in «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*»[949]. I trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico sono esclusi dalla disciplina[950]; sono esclusi, altresì, i trattamenti di dati personali effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse[951].

Sotto il profilo dell'ambito di applicazione territoriale, il regolamento europeo applica il c.d. *target principle*.

Il regolamento «*si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione, ma anche al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico*». Si prevede, anche, l'applicazione «*al trattamento dei dati personali di*

---

[949] Art. 4, paragrafo 1, n. 2), reg. (UE) 2016/679 e, in senso analogo (seppur più ristretto), art. 4, comma 1, lett. a), d.lgs. 196/2003.

[950] Art. 2, paragrafo 2, lett. c), reg. (UE) 2016/679. In senso analogo l'art. 5, comma 3, d.lgs. 196/2003 prevede che il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali sia soggetto all'applicazione del Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione (e quindi di fatto non si tratti di un uso esclusivamente personale o domestico).

[951] Art. 2, paragrafo 2, lett. d), reg. (UE) 2016/679. Sono esclusi anche i trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione e quelli effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE, dedicato alla politica di sicurezza e di difesa comune, ai sensi dell'art. 2, paragrafo 2, lett. a) e lett. b), reg. (UE) 2016/679.

interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione»[952]. Nell'affermare l'applicabilità del regolamento anche nel caso di trattamento di dati personali di interessati che si trovano nell'Unione da parte di un titolare o responsabile non stabilito nell'Unione si scorge l'influenza della giurisprudenza e, in particolare, delle celebri sentenze *Schrems* e *Google Spain*[953].

Le modalità di trattamento sono governate da una serie di principi previsti dagli articoli 5 e 6 del reg. (UE) 2016/679[954]: liceità, correttezza e trasparenza[955]; limitazione della finalità (i dati devono essere «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*») [956]; adeguatezza, pertinenza e non eccedenza dei dati rispetto alle finalità del

---

952 Art. 3, reg. (UE) 2016/679. Secondo il considerando 22 «*lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile*».

953 *Supra*, cap. 4. Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 16 ss., secondo la quale al riguardo «si tratta di indirizzi profondamente politici in cui la Corte orgogliosamente sceglie cultura, principi e diritto europeo. Lo strumento tecnico è costituito dall'interpretazione estensiva della nozione di "stabilimento"» (p. 17); la protezione dei dati personali, infatti, è tema politico di grande rilevanza, in cui sono sempre più evidenti gli interessi economici relativi al bene costituito dall'informazione.

954 Principi analoghi sono previsti attualmente, a livello nazionale, dagli articoli 3 e 11, comma 1, d.lgs. 196/2003.

955 Art. 5, paragrafo 1, lett. a), reg. (UE) 2016/679: i dati devono essere *«trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*»; nello stesso senso art. 11, comma 1, lett. a), d.lgs. 196/2003.

956 Art. 5, paragrafo 1, lett. b), reg. (UE) 2016/679, che aggiunge: «*un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali*». In senso analogo art. 11, comma 1, lett. b), d.lgs. 196/2003: i dati personali devono essere «*raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi*». È opportuno evidenziare un aspetto in cui i due testi si esprimono diversamente: mentre il Codice italiano parla di compatibilità dei successivi trattamenti, il regolamento

trattamento (minimizzazione dei dati)[957]; esattezza e, se necessario, aggiornamento dei dati, ossia qualità dei dati[958]; limitazione della conservazione[959]; integrità e riservatezza[960]. In relazione al rispetto di tali criteri, il regolamento chiarisce la competenza del titolare del trattamento, che deve essere in grado di comprovarlo (principio di responsabilizzazione)[961].

Ogni trattamento deve essere lecito e, di conseguenza, trovare fondamento in un'idonea base giuridica, ai sensi del regolamento europeo; i fondamenti di liceità del

---

europeo richiede che i successivi trattamenti non siano incompatibili con le originarie finalità. Pertanto, piuttosto che imporre la compatibilità, il regolamento europeo vieta l'incompatibilità e lascia così un margine di manovra e flessibilità opportuno anche nel contesto dei *big data*; in tal senso G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 31 ss., secondo i quali, alla luce delle disposizioni del regolamento, la finalità ulteriore perseguita con l'anonimizzazione va considerata non incompatibile con qualsiasi finalità originaria del trattamento.

[957] Art. 5, paragrafo 1, lett. c), reg. (UE) 2016/679 («*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*») e, in senso analogo, art. 11, comma 1, lett. d), d.lgs. 196/2003 («*pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*»). Il Codice prevede il principio di necessità all'art. 3, preferendo sempre l'utilizzo di dati anonimi: «*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*».

[958] Art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679, che precisa che «*devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*» e, in senso analogo, art. 11, comma 1, lett. c), d.lgs. 196/2003.

[959] Art. 5, paragrafo 1, lett. e), reg. (UE) 2016/679: «*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato*». In tal senso anche l'art. 11, comma 1, lett. e), d.lgs. 196/2003, che parla di conservazione in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi del trattamento (diritto all'oblio).

[960] Art. 5, paragrafo 1, lett. f), reg. (UE) 2016/679: «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*».

[961] Art. 5, paragrafo 2, reg. (UE) 2016/679.

trattamento sono indicati nell'art. 6 del regolamento (UE) 2016/679 e, in linea di massima, mostrano coincidenza con quelli previsti attualmente dal Codice, come affermato dallo stesso Garante[962]. Si tratta delle seguenti condizioni di liceità del trattamento:

a) consenso espresso dall'interessato per una o più specifiche finalità;
b) adempimento di obblighi contrattuali, ossia esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato;
c) adempimento di obblighi di legge cui è soggetto il titolare;
d) salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare;
f) perseguimento del legittimo interesse del titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali (in particolare se è un minore).

Alla luce del forte collegamento con l'identità e della profonda incidenza sulla persona, la disciplina in materia di *data protection* ruota intorno all'informativa e al consenso dell'interessato, che deve essere informato dettagliatamente in merito al trattamento dei suoi dati e, se non ricorrono altri fondamenti di liceità, deve esplicitamente consentire al trattamento stesso.

In specifico, ai sensi degli artt. 12, 13 e 14 del reg. (UE) 2016/679 (e, analogamente dell'art. 13 del Codice italiano, d.lgs. 196/2003) devono essere fornite, salve eccezioni, informazioni all'interessato «*per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici*»[963], in relazione a una serie di dati che sono in parte più ampi nel regolamento europeo rispetto al Codice italiano[964]: l'identità e i dati di contatto del titolare e, ove applicabile, del rappresentante e i dati di contatto del responsabile della protezione dei dati (*Data Protection Officer*), ove applicabile; le finalità del trattamento

---

962 Si esprime così la già richiamata Guida all'applicazione del regolamento europeo.

963 Si esprime così l'art. 12, paragrafo 1, reg. (UE) 2016/679, che precisa «*se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*».

964 Le informazioni da fornire all'interessato sono previste dall'art. 13, paragrafo 1, reg. (UE) 2016/679: gli artt. 13 e 14 trattano rispettivamente i casi in cui i dati siano o non siano raccolti presso l'interessato.

cui sono destinati i dati personali e la base giuridica del trattamento stesso; l'interesse legittimo perseguito dal titolare o dai terzi se questo costituisce la base giuridica del trattamento; eventuali destinatari o eventuali categorie di destinatari dei dati personali; l'intenzione del titolare di trasferire i dati personali in Paesi terzi o a un'organizzazione internazionale e attraverso quali strumenti[965].

Le informazioni devono essere rese «*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori*»: è posto un esplicito dovere di trasparenza in capo al titolare[966].

Il regolamento prevede anche ulteriori informazioni «*necessarie per garantire un trattamento corretto e trasparente*»: in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri utilizzati per determinare tale periodo di conservazione; l'esistenza del diritto di accesso, rettifica, cancellazione, limitazione e opposizione dell'interessato, il diritto alla portabilità dei dati e l'eventuale esistenza del diritto di revoca; il diritto di presentare un reclamo all'autorità di controllo; se esiste un obbligo legale o contrattuale di comunicazione dei dati o se è un requisito necessario a concludere un contratto, e se l'interessato è obbligato a fornire i dati e le possibili conseguenze della mancata comunicazione. Inoltre, se il trattamento comporta processi decisionali automatizzati, compresa la profilazione, l'informativa deve specificarlo e deve indicare anche la logica utilizzata da tali processi decisionali, nonché l'importanza e le conseguenze previste per l'interessato[967]; in tal modo il regolamento europeo mostra

---

965 In specifico, l'esistenza o meno di una decisione di adeguatezza della Commissione oppure il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere copia dei dati o il luogo dove sono stati resi disponibili.

966 Art. 12, paragrafo 1, reg. (UE) 2016/679. La disposizione prevede al comma 7 la possibilità di fornire le informazioni di cui agli artt. 13 e 14 «*in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico*». Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 7.

967 Art. 13, paragrafo 2, reg. (UE) 2016/679; in modo analogo art. 14, paragrafo 2, reg. (UE) 2016/679 per il caso di informazioni non raccolte presso l'interessato con le differenze dovute alla diversa fattispecie. L'art. 13 del d.lgs. 196/2003, in modo meno ampio del regolamento europeo, prevede quali informazioni fornire nell'informativa: le finalità e modalità del trattamento cui sono destinati i dati; la natura obbligatoria o facoltativa del conferimento dei dati; le conseguenze di un eventuale rifiuto a

di essere calato nell'odierna società degli algoritmi, che comporta la necessità di ulteriori specifiche garanzie a tutela della persona.

L'informativa deve essere fornita all'interessato al momento della raccolta dei dati, se raccolti direttamente presso l'interessato (art. 13, reg. (UE) 2016/679), mentre se i dati non sono raccolti direttamente presso l'interessato (art. 14, reg. (UE) 2016/679), l'informativa va fornita in un termine ragionevole dall'ottenimento dei dati e negli altri termini previsti dalla norma, a seconda dei casi, e deve comprendere anche le categorie dei dati personali oggetto di trattamento[968]. Inoltre il principio di limitazione della finalità determina che ogni volta che il titolare intenda trattare i dati per finalità diverse, devono essere fornite le informazioni all'interessato prima di procedere al trattamento ulteriore[969].

Insieme all'informativa, l'altro elemento fondamentale della disciplina è il consenso di cui all'art. 7 del reg. (UE) 2016/679 (e, altresì, attualmente, art. 23 del Codice): qualora il trattamento sia basato sul consenso, il titolare deve essere sempre in grado di dimostrare che l'interessato ha prestato il proprio consenso; a tutela dell'interessato, il regolamento sembra porre in capo al titolare un vero e proprio onere della prova sulla raccolta del consenso[970].

Il consenso deve consistere, in tutti i casi, in una manifestazione di volontà libera, informata, specifica e inequivocabile, con la quale si esprime l'assenso al trattamento dei dati personali che riguardano l'interessato, mediante dichiarazione o azione positiva inequivocabile (non è ammesso il consenso tacito o presunto)[971] e, se è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, deve essere presentato in modo chiaramente distinguibile dalle altre, in forma comprensibile e

---

rendere disponibili i propri dati; i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza come responsabili o incaricati e l'ambito di diffusione dei dati stessi; i diritti dell'interessato previsti dall'art. 7 del d.lgs. 196/2003; gli estremi identificativi del titolare e, se designato, del responsabile.

968 L'art. 12 e seguenti del reg. (UE) 2016/679 specificano tempi e modalità dell'informativa, alla lettura dei quali si rinvia.

969 Art. 13, paragrafo 3, e art. 14, paragrafo 4, reg. (UE) 2016/679.

970 Art. 7, paragrafo 1, reg. (UE) 2016/679. Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 7.

971 Art. 4, paragrafo 1, n. 11) e considerando 39 e 42, reg. (UE) 2016/679.

facilmente accessibile, utilizzando un linguaggio semplice e chiaro: viene posto anche in tal caso un chiaro dovere di trasparenza in capo al titolare[972]. Per i dati sensibili il consenso deve essere esplicito[973]; lo stesso vale per il consenso fornito a decisioni basate su trattamenti automatizzati, compresa la profilazione[974]. Di conseguenza, non deve essere necessariamente documentato per iscritto[975], né è richiesta la forma scritta, anche se questa è una modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (nei casi previsti)[976].

Emerge un modello di *opt-in* per la prestazione del consenso, che comporta l'invalidità di sistemi basati sul silenzio dell'utente o su caselle e campi "pre-spuntati" sui moduli[977].

I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, dal momento che, come esaminato, in tal caso la liceità del trattamento deriva dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui all'art. 6, comma 1, lett. e), reg. (UE) 2016/679[978].

Alla luce della disciplina, le regole che informano qualsiasi tipo di trattamento valgono anche nell'era digitale e *social*: anche nella condivisione enfatizzata e nella

---

[972] Art. 7, paragrafo 2, reg. (UE) 2016/679. Per quanto attiene all'offerta diretta di servizi della società dell'informazione ai minori, il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale (genitori o chi ne fa le veci), ai sensi dell'art. 8, reg. (UE) 2016/679. Per quanto riguarda il Codice italiano, il consenso è disciplinato dall'art. 23: può riguardare l'intero trattamento ovvero una o più operazioni dello stesso ed è validamente prestato solo se è espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato, è documentato per iscritto ed è stata resa all'interessato l'informativa di cui all'art. 13 del Codice. I dati sensibili possono essere oggetto di trattamento, salvo eccezioni, solo con il consenso in forma scritta e la previa autorizzazione del Garante (art. 26, d.lgs. 196/2003).

[973] Art. 9, reg. (UE) 2016/679.

[974] Art. 22, reg. (UE) 2016/679.

[975] Come richiede, invece, l'art. 23, comma 3, d.lgs. 196/2003.

[976] Guida all'applicazione del regolamento europeo.

[977] Cfr. Guida all'applicazione del regolamento europeo e G. PASCUZZI - F. GIOVANELLA, *Dal diritto alla riservatezza alla computer privacy*, cit., p. 53. L'*opt-in* fa riferimento alla necessità di acquisire un'esplicita dichiarazione di consenso da parte dell'interessato prima dell'inizio del trattamento, mentre l'*opt-out* si riferisce al consenso presunto, salvo esplicito diniego da parte dell'interessato; cfr. A. MANTELERO, *Privacy digitale*, cit., p. 164.

[978] Considerando 43 del reg. (UE) 2016/679 e, nello stesso senso, artt. 18 e 20, d.lgs. 196/2003.

dinamicità rapida della rete, il trattamento dei dati personali, per essere legittimo, deve avvenire in modo trasparente, previa un'informativa dettagliata e, in assenza di altri idonei fondamenti giuridici previsti, chiedendo il consenso dell'interessato, che conserva specifici diritti nei confronti del titolare del trattamento.

Dal momento che il diritto alla protezione dei dati personali è anche diritto all'autodeterminazione informativa, all'interessato, infatti, sono riconosciuti dal regolamento (UE) 2016/679 diritti esercitabili nei confronti del titolare[979]: diritto di conoscenza del trattamento e di accesso ai dati e alle informazioni (art. 15); diritto di rettifica e integrazione (art. 16)[980]; diritto alla cancellazione ("diritto all'oblio") (art. 17)[981]; diritto di limitazione di trattamento (art. 18), che si configura diverso e più esteso rispetto al blocco del trattamento di cui al Codice italiano; diritto di opposizione (art. 21); diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che riguardano il soggetto o incida in modo analogo significativamente sulla persona (art. 22)[982].

In merito ai diritti attribuiti all'interessato, una significativa novità è il diritto alla portabilità dei dati (*data portability*) di cui all'art. 20, ossia il diritto dell'interessato a ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare e il diritto di trasmettere tali dati a un altro titolare, senza impedimenti da parte del primo titolare cui li ha forniti: si tratta del diritto di trasferire i propri dati da un sistema di trattamento elettronico a un altro; si pensi al proprio profilo utente trasferito da una piattaforma a un'altra[983]. L'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del

---

979 I diritti sono previsti negli artt. 7 e seguenti del d.lgs. 196/2003 in modo analogo, seppur con alcune differenze.

980 Si può ritenere vi rientri anche il diritto alla modifica e all'aggiornamento, previsti esplicitamente nell'art. 7, comma 3, d.lgs. 196/2003; negli artt. 8, 9 e 10 sono disciplinate le modalità di esercizio dei diritti.

981 *Supra*, cap. 4, § 3.2.

982 Cfr. «*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*», 17/EN WP 251 rev.01, adottate il 3 ottobre 2017 e successivamente riviste e adottate il 6 febbraio 2018 dall'*Article 29 Data Protection Working Party*. Tale disposizione trova il suo precedente affine nell'art. 15 della direttiva 95/46.

983 G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 8. Tale disposizione amplia il diritto di accesso dell'interessato.

trattamento all'altro, se tecnicamente fattibile. Tale diritto non si applica ai trattamenti non automatizzati (quindi archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio: sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi, ad esempio, non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare) e solo i dati che siano stati forniti dall'interessato al titolare (art. 20 e considerando 68)[984].

Il regolamento europeo, con la finalità di responsabilizzare e rendere maggiormente efficace la protezione dei dati personali, rafforzando il diritto all'autodeterminazione informativa della persona, ha previsto una serie di misure particolarmente rilevanti, alcune delle quali saranno specificamente trattate successivamente perché significative ai fini della presente analisi[985].

Senza pretesa di esausitività, oltre ad alcuni profili esaminati come il diritto alla portabilità e la previsione del *Data Protection Officer*, sono particolarmente significativi il principio *privacy by design* (art. 25, comma 1)[986], il principio *privacy by default* (art. 25, comma 2)[987] e il c.d. *Data Protection Impact Assessment* (art. 35)[988], che mirano a un approccio e a una ponderazione *ex ante* dell'impatto e dei rischi sulla *data*

---

984 Guida all'applicazione del regolamento europeo. Ai sensi dell'art. 20, comma 3, reg. (UE) 2016/679 «*tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*». Cfr. «*Guidelines on the right to data portability*», 16/EN WP 242 rev.01, adottate il 13 dicembre 2016 e successivamente riviste e adottate il 5 aprile 2017 *dall'Article 29 Data Protection Working Party*.

985 In particolare, *infra*, § 6.

986 In proposito si parla anche di *privacy enhancing technologies* – PETs.

987 G. PASCUZZI - F. GIOVANELLA, *Dal diritto alla riservatezza alla computer privacy*, cit., p. 43 ss. sottolineano che i due principi sono le due facce della stessa medaglia: la *data protection by design* è rivolta all'interno con un obbligo di implementazione della disciplina fin dalla progettazione e la *data protection by default* è rivolta all'esterno e prevede che al cittadino sia offerto un prodotto le cui impostazioni predefinite garantiscano il massimo livello di tutela della privacy.

988 In merito alla valutazione d'impatto sulla protezione dei dati cfr. «*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*», 17/EN WP 248 rev.01, adottate in data 4 aprile 2017 e successivamente riviste e adottate il 4 ottobre 2017 dall'*Article 29 Data Protection Working Party*.

protection; la disciplina della contitolarità del trattamento (art. 26)[989]; il registro delle attività di trattamento (art. 30); le misure di sicurezza (art. 32); la consultazione preventiva (art. 36)[990]; la *data breach notification* (artt. 33 e 34) [991]; la certificazione (artt. 42 e 43)[992]; i trasferimenti di dati personali verso paesi terzi e organizzazioni internazionali, disciplina più articolata e strutturata del passato (art. 44 ss.)[993].

In particolare, alla luce dei nuovi principi e strumenti previsti dal regolamento europeo, emerge un cambiamento di paradigma rispetto al passato: l'approccio basato sul rischio si basa su un meccanismo di *accountability*, su un concetto dinamico e integrato di sicurezza, in cui le misure previste non sono solo tecnologiche, ma anche organizzative e, condivisibilmente, mostrano la necessità di integrazione tra professionalità e competenze in informatica, diritto e organizzazione[994]. Si tratta di un approccio proattivo e non reattivo, in un'ottica di prevenzione, riduzione ed eliminazione di possibili problematiche[995].

L'*accountability* si nutre dei principi che pervadono il regolamento: trasparenza, *compliance*, responsabilità, sanzioni effettive e attenzione alla sicurezza. Alla luce di tale concezione spetta, quindi, al titolare mettere in atto «*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*»,

---

989 La disposizione è molto utile per affrontare la complessa catena di valore dei *big data*; G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 31.

990 Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto ai sensi dell'art. 35 «*indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*».

991 Il titolare ha l'obbligo di notificare la violazione dei dati personali all'autorità di controllo (art. 33) e, quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ha l'obbligo di comunicare la violazione all'interessato senza ingiustificato ritardo, tranne nei casi previsti dalla norma (art. 34). Sulla *data breach notification* cfr. «*Guidelines on Personal data breach notification under Regulation 2016/679*», 17/EN WP250 rev.01, adottate il 3 ottobre 2017 e successivamente riviste e adottate il 6 febbraio 2018 dall'*Article 29 Data Protection Working Party*.

992 Si promuove l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati, allo scopo di dimostrare la conformità al regolamento dei trattamenti effettuati dai titolari e dai responsabili del trattamento.

993 Al riguardo cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 9.

994 G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 10 ss.

995 In tal senso Relazione del Garante sull'attività svolta nell'anno 2015.

tenendo conto «*dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento*», prevedendo *policy*, monitorando l'efficacia ed essendo in grado di dimostrare le misure e le procedure, appropriate ed efficaci, adottate[996]. Si richiede, infatti, al titolare di mettere in atto «*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare*» che il trattamento è effettuato conformemente al regolamento «*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*». Si tratta di un *work in progress* permanente, dal momento che le misure devono essere riesaminate e aggiornate qualora necessario[997].

In caso di violazioni, scatta il diritto al risarcimento e si prevede una responsabilità civile, che non sembra più basata sulla responsabilità oggettiva come nella normativa italiana[998]; a fini di efficacia, le sanzioni amministrative pecuniarie sono incisive e possono arrivare in alcuni casi a 10 o 20 milioni di euro o, per le imprese, al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Il regolamento prevede significativamente che ogni autorità di controllo provveda affinché le sanzioni amministrative pecuniarie inflitte in relazione alle violazioni del regolamento «*siano in ogni singolo caso effettive, proporzionate e dissuasive*»[999].

---

[996] Art. 32, reg. (UE) 2016/679; a livello nazionale le misure di sicurezza sono trattate nell'art. 31 e seguenti, d.lgs. 196/2003. Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 10 ss. Sulla tutela da offrire alla protezione dei dati personali S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 398 parla di «una strategia integrata, affidata a strumenti diversi, che tuttavia hanno il loro comune fondamento nel riconoscimento alla persona del diritto di seguire i dati ovunque essi si trovino, potendo così continuare a governarli».

[997] Art. 24, reg. (UE) 2016/679, dedicato alla responsabilità del titolare; l'adesione ai codici di condotta o a un meccanismo di certificazione può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento (comma 3).

[998] Art. 82, reg. (UE) 2016/679; cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 8.

[999] Art. 83, reg. (UE) 2016/679. Sulle sanzioni amministrative cfr. «*Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*», 17/EN WP 253, adottate in data 3 ottobre 2017 dall'*Article 29 Data Protection Working Party*. Nel Codice italiano il trattamento effettuato in mancanza di idonei presupposti normativi, oltre che con la sanzione amministrativa del pagamento di una somma, in presenza dei requisiti previsti, può configurare la fattispecie penale di

Ai fini della presente riflessione, è interessante osservare che, oltre alle sanzioni previste dalla normativa in caso di violazione delle disposizioni e al possibile ricorso all'autorità giudiziaria, in caso di violazione delle norme e più in generale nella disciplina, anche per la *data protection*, come nel caso del diritto d'autore, emerge la centralità di un'autorità di controllo, quale "custode dei diritti e delle libertà fondamentali"[1000], il Garante per la protezione dei dati personali, previsto dall'art. 51 e seguenti del regolamento (UE) 2016/679 (di seguito anche Garante)[1001]. Tale figura opera in piena indipendenza[1002] e ha lo specifico compito di sorvegliare e assicurare la corretta applicazione delle disposizioni europee e nazionali; a tal fine sono attribuiti al Garante compiti e poteri di natura consultiva, regolamentare e giurisdizionale[1003].

Merita rilevare ai fini di questa analisi che, tra le ampie funzioni attribuite al Garante, è prevista l'adozione dei provvedimenti disposti dalla normativa e la consulenza (attraverso la formulazione di pareri) al Parlamento nazionale, al Governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al

---

illecito trattamento di dati personali (artt. 162 e 167, d.lgs. 196/2003); in tal senso anche il Garante, nelle linee guida adottate con provvedimento n. 243 del 15 maggio 2014.

[1000] Sentenza della Corte di Giustizia dell'Unione europea del 9 marzo 2010, causa C-518/07, *Commissione europea c. Repubblica federale di Germania*. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 398 sottolinea che i poteri di controllo e d'intervento non sono solo attribuiti ai diretti interessati, ma sono affidati anche a un'autorità indipendente e, di conseguenza, «la tutela non è più soltanto individualistica, ma coinvolge una specifica responsabilità pubblica. Siamo così di fronte anche a una redistribuzione di poteri sociali e giuridici».

[1001] Nella normativa italiana è previsto dall'art. 153 e seguenti del d.lgs. 196/2003. Il Garante «*è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni*» (art. 153, comma 2, d.lgs. 196/2003).

[1002] Art. 52, reg. (UE) 2016/679 e art. 153, comma 1, d.lgs. 196/2003.

[1003] Art. 57 ss., reg. (UE) 2016/67; in senso analogo art. 154, d.lgs. 196/2003. Ai sensi del Codice i diritti stessi dell'interessato di cui all'art. 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante: il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria e, parimenti, la presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto (art. 145, d.lgs. 196/2003).

trattamento[1004]. In relazione a questa funzione, come emergerà più avanti, l'azione del Garante talvolta può dare adito a riflessioni, soprattutto nei casi in cui le interpretazioni delle norme vengono strettamente ridimensionate dai provvedimenti dell'autorità di controllo, che di fatto si riserva una sorta di interpretazione autentica della normativa, peraltro anche laddove la normativa stessa si sia discostata dal parere preventivo espresso dal Garante sul provvedimento[1005].

5.2. La *data protection* nel governo dei dati

Alla luce della disciplina di riferimento in materia di *data protection*, l'analisi si concentrerà sul governo dei dati, al fine di valutare come si atteggia la tutela della protezione dei dati personali nelle configurazioni che i dati assumono e nei diversi gradi di trasparenza e apertura (o chiusura), soprattutto nel bilanciamento con il diritto a conoscere che le stesse istanze di *disclosure* e *openness* sostanziano. Merita precisare che, anche in questo caso, come già in precedenza, il diritto all'informazione oggetto di analisi consisterà specificamente nel diritto a conoscere nei confronti delle istituzioni e non sarà trattata l'accezione di diritto ad informare ed essere informati quale libertà giornalistica di cronaca e di stampa[1006].

Il bilanciamento tra *right to know* e *data protection*, entrambi implicitamente diritti costituzionali[1007], è intuitivamente particolarmente complesso, dal momento che il

---

[1004] Art. 57, paragrafo 1, lett. c), reg. (UE) 2016/679 e art. 154, d.lgs. 196/2003.

[1005] È il caso del d.lgs. 33/2013, su cui il Garante ha espresso un parere preventivo che non è stato accolto integralmente. Nelle successive *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* del 15 maggio 2014, pubblicate sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014 (doc. web n. 3134436), il Garante ha dato indicazioni sull'attuazione delle disposizioni del d.lgs. 33/2013, facendo riemergere quelle indicazioni che il testo legislativo non aveva accolto e quindi, in sostanza, producendo il risultato di un'interpretazione autentica della normativa.

[1006] Sul bilanciamento tra il diritto all'informazione giornalistica e il diritto alla privacy, che mostra peculiarità in quanto soggetto a una disciplina speciale, cfr. G.E. VIGEVANI, *op. cit.*, p. 473 ss.

[1007] Come già esaminato, il diritto a conoscere e il diritto alla protezione dei dati personali trovano indiretta fonte costituzionale in una serie di norme e relativi principi contenuti nella Carta fondamentale; *supra*, cap. 4, § 2, e in questo capitolo, § 1.

primo muove e si nutre di disponibilità, apertura e utilizzo dei dati, mentre il secondo aspira al controllo dei dati e anche alla "chiusura" degli stessi se necessaria a tutela della persona. Si tratta di un equilibrio difficile e dinamico, cui però non è possibile rinunciare perché l'estensione dell'uno o dell'altro è capace di limitare e danneggiare l'altra istanza. In una società dominata dagli algoritmi come quella attuale, dove protagonisti sono i *big data*, è quanto mai necessario adattare la protezione dei dati personali per non esporla ad una sostanziale inefficacia e, di conseguenza, non esporre l'individuo a lesioni intime e fondamentali del suo essere[1008].

Sotto tale profilo, in relazione al governo dei dati, è necessaria una considerazione preventiva sistematica, derivante dal quadro normativo e dall'evoluzione giurisprudenziale in materia: oltre all'autorità giudiziaria, a occuparsi della *data protection* non è più soltanto l'autorità di controllo costituita dal Garante per la protezione dei dati personali, ma nei fatti entrano in scena con ruolo di protagonisti anche soggetti privati, ossia nello specifico i motori di ricerca, a seguito della esaminata sentenza della Corte di giustizia *Google Spain*[1009], che ha inciso sul diritto all'oblio. Del resto, un pericolo significativo consiste proprio nella perdita del controllo sui dati personali con il rischio che siano "intrappolati" nella rete e, di conseguenza, possano ledere la persona interessata.

Le conseguenze della sentenza e, in particolare, il fatto che soggetti come Google abbiano un ruolo centrale in merito al bilanciamento tra protezione dei dati personali e, in specifico, diritto all'oblio, da una parte, e diritto all'informazione e alla memoria, dall'altra, sollevano molte perplessità: un soggetto privato di fatto ha assunto il ruolo di arbitro e detentore della luce e dell'ombra sulle informazioni nel web, laddove queste siano segnalate dai privati come dati da oscurare. Nella nuova funzione, i motori di ricerca possono concretamente ledere il diritto del singolo alla *data protection*, laddove non accolgano richieste legittime, oppure possono ledere il diritto della collettività all'informazione, laddove al contrario accolgano con facilità le richieste degli utenti, impoverendo di conseguenza il web. Il ruolo delicato e complesso, afferente al bilanciamento di diritti fondamentali di matrice costituzionale, quali il diritto del singolo alla protezione dei dati personali e il diritto della collettività all'informazione, risulta

---

1008 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 396.

1009 *Supra*, cap. 4, § 3.2.

difficilmente attribuibile a un soggetto che è mosso da scopi diversi dall'autorità giudiziaria e che può decidere con modalità e parametri che non tutelano in modo adeguato i diritti fondamentali in oggetto.

Oltre a questa funzione specifica, di estrema rilevanza, più ampiamente il ruolo giocato nel governo dei dati dai colossi del web rende difficile la protezione dei diritti. La tutela dei dati personali e il bilanciamento con gli altri interessi protetti dall'ordinamento si fanno, infatti, particolarmente complessi nel contesto contemporaneo: i giganti della rete procedono a trattare i dati senza alcun reale consenso, ma a seguito delle semplici interazioni sul web che permettono la profilazione e la collegata implementazione di altri servizi (come la pubblicità)[1010], i rapporti tra i singoli e le piattaforme dei *big player* sono caratterizzati da un'asimmetria informativa e di potere difficilmente sanabile e gli algoritmi si spingono a determinare non solo il presente, ma anche il futuro.

Di conseguenza, il bilanciamento tra istanze diverse nella rete vede coinvolti diversi soggetti: la persona fisica dei cui dati si parla; i soggetti pubblici tenuti ad adottare e a far rispettare la regolazione adeguata a tutela della persona; i soggetti privati, come i motori di ricerca, che incessantemente e in dimensioni enormi trattano i dati di tutti noi.

Gli atti normativi che regolano il profilo hanno piena contezza dell'importanza dell'equilibrio tra i diritti da garantire a tutela della dignità e dello sviluppo della persona. In specifico, il regolamento (UE) 2016/679 in materia di *data protection* mostra esplicita consapevolezza della centralità del bilanciamento tra interessi diversi, in cui nessun diritto ha una prevalenza assoluta e aprioristica, neppure la protezione dei dati personali: «*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà*

[1010] M. CARTA, *op. cit.*, pp. 1-19.

d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica» (considerando 4). Il regolamento europeo dichiara esplicitamente l'ampiezza del suo raggio d'azione che abbraccia non solo la *data protection*, ma l'intera *data governance*; in tale ottica emerge la centralità della persona, sulla cui base costruire il complesso equilibrio tra diritti sotto l'egida del principio di proporzionalità.

In tal senso, nel nostro ordinamento si esprime la sentenza della Corte di Cassazione, sezione III, 20 maggio 2015, n. 10280, secondo cui «il diritto ad esigere una corretta gestione dei propri dati personali, pur se rientrante nei diritti fondamentali di cui all'art. 2 Cost., non è un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale»[1011].

Nell'evoluzione del principio di trasparenza originata dalle recenti riforme, da ultimo dal d.lgs. 97/2016, si configura l'esigenza di bilanciamento fra il diritto alla protezione dei dati personali e il diritto all'informazione, connesso alla pubblicità, alla trasparenza e all'apertura dei dati pubblici, quale interesse generale al controllo democratico dell'esercizio delle funzioni pubbliche da parte dei cittadini[1012]. Della necessità di equilibrio è pienamente consapevole il d.lgs. 33/2013 che, fin dal primo articolo, chiarisce che il principio di trasparenza deve essere realizzato nel rispetto delle disposizioni in materia di protezione dei dati personali (art. 1, comma 2) e lo ribadisce più volte nella disposizione dedicata ai limiti della trasparenza (art. 7-bis, commi 1 e 2): la protezione dei dati personali si pone come protagonista del «continuo bilanciamento "mobile"» che deve assicurare la tutela di «tutti gli interessi coinvolti secondo una lettura costituzionalmente orientata»[1013].

I dati personali hanno assunto una nuova valenza nella rivoluzione informatica e nel passaggio dall'identità personale all'identità digitale, dal momento che nel web la

---

1011 G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, cit., p. 18.

1012 Secondo G. ARMAO, *op. cit.*, p. 3 la trasparenza totale e gli *open data* rappresentano «presidi di legalità ed efficienza ai quali le amministrazioni non possono sottrarsi poiché costituiscono la nuova frontiera dei diritti di cittadinanza e della democrazia partecipativa»; la rete coniugata agli strumenti dell'*open government* costituisce «uno straordinario strumento di controllo da parte dei cittadini per contrastare inefficienze, corruzione e malamministrazione, ed invera i principi fondamentali di trasparenza e di partecipazione».

1013 Così I. NICOTRA, *op. cit.*, p. 9.

dimensione informativa risulta dominante e può configurarsi una potenziale frammentazione dell'io in un insieme di dati che riguardano il soggetto insieme alla "cristallizzazione" degli stessi, con conseguenti possibili effetti lesivi e distorsivi, eventuali fenomeni di decontestualizzazione e difficoltà pratiche e giuridiche di cancellazione dei dati (e di rispetto del diritto all'oblio)[1014].

È consapevole di questo e si esprime in tal senso il Garante quando invita a trattare il bilanciamento con «un approccio equilibrato per evitare che i diritti fondamentali alla riservatezza e alla protezione dei dati personali, nonché la dignità dell'individuo […] possano essere gravemente pregiudicati da una indiscriminata diffusione di documenti riportanti dati personali»; «occorre, infatti, tenere in adeguata considerazione le conseguenze e i rischi per la vita privata e per la dignità della persone interessate derivanti dal crescente e generalizzato obbligo di pubblicazione delle informazioni del settore pubblico». E tale attenzione deve essere particolarmente alta, perché, con espressione volutamente forte, secondo il Garante in materia di protezione dei dati personali «il danno derivante dalla semplice conoscenza di un'informazione è *in re ipsa* e non c'è risarcimento che possa riparare al danno effettuato (si pensi ad esempio alla rivelazione di dati idonei a rivelare lo stato di salute)»[1015]. A tal fine il Garante si riferisce al rispetto degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, nonché alla disciplina europea e nazionale in materia di protezione dei dati personali.

Del resto, con estrema chiarezza, il Garante puntualizza che «la trasparenza, affinché sia effettiva "garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali", integrando "il diritto ad una buona amministrazione e concorrendo alla realizzazione di una amministrazione aperta, al servizio del cittadino" (art. 1, comma 2, del d. lgs. n. 33/2013), non può essere realizzata violando la dignità e i diritti fondamentali della persona, come il diritto alla riservatezza e il diritto alla protezione dei dati personali, costituzionalmente garantiti e previsti anche dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà

1014 Cfr. C. FLICK, *op. cit.*, p. 243 ss. e A. MANTELERO, *Privacy digitale*, cit., p. 159 ss.

1015 Provvedimento n. 92 del 3 marzo 2016, con il quale il Garante ha reso il parere sullo schema di quello che è diventato il d.lgs. 97/2016.

fondamentali (artt. 7 e 8) nonché dalla Carta dei diritti fondamentali dell'Unione europea»[1016].

Nelle diverse configurazioni assunte dai dati e nelle gradazioni di trasparenza si atteggia diversamente il complesso bilanciamento tra il diritto alla conoscenza nei confronti delle istituzioni, che quelle configurazioni promuovono, e la protezione dei dati personali: di conseguenza, sono diverse e specifiche le problematiche che si generano sotto tale profilo.

L'esigenza di trovare un equilibrio fra le opposte istanze di trasparenza (proattiva e reattiva) e apertura, da una parte, e *data protection*, dall'altra, porta alla necessità di esaminare la disciplina nel nostro ordinamento giuridico, tenendo in considerazione anche le previsioni al riguardo del regolamento (UE) 2016/679.

Di conseguenza saranno oggetto di analisi, in primo luogo, il caso della trasparenza proattiva, che si attua con la pubblicazione, valutandone anche i profili problematici, come quello legato all'apertura (*open data*) e, successivamente, il caso della trasparenza reattiva, in particolare nella sua nuova forma costituita dal diritto di accesso civico generalizzato. Solo successivamente verrà trattato il complesso caso dei *big data*.

5.3. Privacy, trasparenza proattiva e apertura dei dati pubblici

5.3.1. *Data protection* e pubblicazione (obbligatoria e facoltativa)

La pubblicazione dei dati sul web esprime uno specifico trattamento, la diffusione, identificato dal d.lgs. 196/2003 nel «*dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o*

[1016] Provvedimento n. 92 del 3 marzo 2016, reso sullo schema del d.lgs. 97/2016. Nel provvedimento il Garante ha richiamato il proprio parere sulla schema di decreto legislativo n. 33/2013, «a fronte del quale occorre far presente che mentre alcune indicazioni sono state recepite dal Governo in maniera integrale, altre non sono state accolte o lo sono state solo parzialmente e restano quindi pienamente valide e riproducibili in relazione allo schema di decreto in esame».

consultazione»[1017]. Come espresso dal Garante, la diffusione di dati sul web «è, per definizione, la forma più ampia e più invasiva di diffusione di dati»[1018].

Nel caso della trasparenza e dell'apertura messe in atto dalle amministrazioni, rileva la specifica disciplina del trattamento dei dati personali da parte di soggetti pubblici, che si differenziano dalle regole in caso di trattamento da parte di soggetti privati. Nell'analisi, sarà esaminata anche la disciplina del Codice, il d.lgs. 196/2003, che potrebbe essere modificata o integrata nell'adeguamento al regolamento europeo 2016/679. Al riguardo, è opportuno evidenziare che il regolamento europeo prevede un margine di manovra degli Stati membri: «*per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme*» del regolamento, che non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito (considerando 10). In tali casi (adempimento di un obbligo legale ed esecuzione di un compito pubblico), nella disposizione relativa alla liceità del trattamento, si chiarisce che gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del regolamento con riguardo al trattamento, determinando con maggiore

---

[1017] Art. 4, comma 1, lett. m), d.lgs. 196/2003. La diffusione si distingue dalla comunicazione, identificata dal Codice nel «*dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*» (art. 4, comma 1, lett. l), d.lgs. 196/2003): in tal caso, a differenza della diffusione, è possibile determinare i soggetti che vengono a conoscenza dei dati personali. Il regolamento (UE) 2016/679 richiama i termini diffusione e comunicazione nella definizione di trattamento, ma non li definisce.

[1018] Così il Garante per la protezione dei dati personali, provvedimento n. 49 del 7 febbraio 2013, recante «*Parere del Garante su uno schema di decreto legislativo concernente il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle Pa*», doc. web. n. 2243168, che ha dato parere favorevole "condizionato" allo schema di quello che è diventato il d.lgs. 33/2013. Il Garante si è espresso in tal senso anche nel provvedimento n. 92 del 3 marzo 2016 relativo allo schema di quello che è diventato il d.lgs. 97/2016.

precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento[1019].

Nel caso dei soggetti pubblici qualunque trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali e, di norma, come esaminato, i soggetti pubblici non devono richiedere il consenso dell'interessato. Tale potere risulta pertanto implicito e connesso alle funzioni istituzionali delle amministrazioni pubbliche, configurandosi al tempo stesso come presupposto di legittimazione del trattamento e limite generale dello stesso[1020].

Per quanto attiene alla diffusione, la disciplina recata dal Codice è specifica e si differenzia in base alla tipologia di dati personali che vengono in gioco, a seconda che si tratti di dati personali comuni o dati sensibili e giudiziari.

La diffusione di dati comuni da parte di un soggetto pubblico è ammessa unicamente quando è prevista da una norma di legge o di regolamento[1021], rientrando così nel caso del trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, previsto dal regolamento europeo, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute dei singoli interessati[1022].

In caso di trattamento (e quindi anche di diffusione) di dati sensibili e giudiziari, alla luce della particolare invasività, si eleva il livello di protezione e il relativo trattamento è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite[1023]: il trattamento quindi deve essere legittimato da una fonte di rango primario che in modo espresso dettagli dati, operazioni e finalità. In caso di assenza di una norma con questi requisiti, se la disposizione di legge si limita a specificare la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che effettuano il

---

1019 Art. 6, comma 2, regolamento (UE) 2016/679. Le disposizioni relative a specifiche situazioni di trattamento sono contenute nel capo IX del regolamento (UE) 2016/679.

1020 Cfr. F. G. ANGELINI, *op. cit.*, p. 249 ss.

1021 Art. 19, comma 3, d.lgs. 196/2003.

1022 Art. 22, comma 8, art. 65, comma 5, e art. 68, comma 3, d.lgs. 196/2003.

1023 Art. 20, comma 1, d.lgs. 196/2003.

trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi applicabili al trattamento di dati sensibili e giudiziari, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante, anche su schemi tipo, aggiornati e integrati periodicamente[1024]. Nel caso di dati sensibili e giudiziari andranno osservati i principi previsti espressamente dal Codice: il c.d. principio di indispensabilità[1025] e la verifica periodica circa «*l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa*»[1026].

In tale contesto normativo, le istanze contrapposte di trasparenza/apertura e protezione dei dati personali, anche alla luce della particolare *vis* costituzionale che le caratterizza, risultano entrambe fondamentali per informare l'agire pubblico, ma operano in senso divergente e persino opposto, provocando la necessità di trovare un equilibrio che ne consenta la "pacifica" convivenza.

L'esigenza del rispetto della protezione dei dati personali è affrontata già dal Codice dell'amministrazione digitale, nell'art. 2, comma 5, d.lgs. 82/2005, come modificato dal d.lgs. 179/2016, secondo cui le disposizioni del Codice si applicano nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice approvato con d.lgs. 196/2003. Nel contesto digitale, dove la diffusione è agevolata dall'assenza di barriere spazio-temporali, emerge il diritto

---

[1024] Art. 20, commi 2 e 4, d.lgs. 196/2003. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate agli stessi dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi previsti (art. 20, comma 3, d.lgs. 196/2003). L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente (art. 20, comma 4, d.lgs. 196/2003).

[1025] Art. 22, comma 3, d.lgs. 196/2003, secondo cui i soggetti pubblici «*possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa*».

[1026] Art. 22, comma 5, d.lgs. 196/2003. I soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi (art. 22, comma 9, d.lgs. 196/2003).

all'autodeterminazione informativa quale diritto attivo di controllo dell'*homo technologicus* sulle modalità di circolazione e utilizzo dei dati personali.

Al bilanciamento fra trasparenza e privacy è dedicato l'art. 7-bis del d.lgs. 33/2013, come modificato dal d.lgs. 97/2016[1027], rubricato significativamente «*riutilizzo dei dati pubblicati*», facendo emergere la complessa e problematica dimensione dell'apertura relativa agli *open data*, anche se nella disposizione si tracciano più ampiamente i limiti alla trasparenza necessari per realizzare un equilibrio con la protezione dei dati personali.

È opportuno esaminare la norma, al fine di analizzare i punti di convergenza ed equilibrio fra trasparenza e *data protection* raggiunti dal legislatore e quelli invece in cui il bilanciamento resta complesso e la bilancia si trova a pendere in favore dell'una o dell'altra istanza.

La norma esamina tale aspetto distinguendo tra i casi di pubblicazione obbligatoria e quelli di pubblicazione facoltativa.

Innanzitutto la norma prende in considerazione il caso di pubblicazione obbligatoria: gli obblighi di pubblicazione dei dati personali comuni (diversi dai dati sensibili e dai dati giudiziari) comportano la possibilità di:

- diffusione dei dati medesimi attraverso siti istituzionali;
- trattamento secondo modalità che ne consentono:
    - la indicizzazione e la rintracciabilità tramite i motori di ricerca web;
    - il loro riutilizzo ai sensi dell'art. 7 nel rispetto dei principi sul trattamento dei dati personali[1028].

Pertanto per tale tipologia di dati la norma prevede la possibilità di diffusione e altresì l'indicizzazione e la rintracciabilità tramite i motori di ricerca web, senza lasciare margine di discrezionalità alle amministrazioni, mostrando un chiaro *favor* verso il valore della trasparenza[1029], mentre esclude *tout court* i dati sensibili e giudiziari, evidentemente ritenendo in tal caso una previsione del genere non conforme al principio

---

1027 Prima si trattava dell'art. 4 rubricato «*limiti alla trasparenza*», oggi abrogato: i contenuti sono stati spostati nell'art. 7-bis, d.lgs. 33/2013.

1028 Art. 7-bis, comma 1, d.lgs. 33/2013.

1029 Significativo, a tale proposito, il lessico usato: gli obblighi di pubblicazione "comportano" la possibilità di una diffusione che dà il senso di una conseguenza legalmente statuita.

di proporzionalità rispetto alla finalità di trasparenza[1030]. In caso di dati comuni, la disposizione consente anche il riutilizzo ai sensi dell'art. 7 (*open data*), ma lo condiziona esplicitamente al rispetto dei principi sul trattamento dei dati personali[1031].

Il legislatore non interpreta il valore della trasparenza in modo aprioristico ritenendolo *ex se* superiore alla protezione dei dati personali, ma si limita ad operare il bilanciamento, a favore della trasparenza soltanto laddove siano dati comuni. Questo non significa che venga meno la tutela dei dati personali, ma solo che per tali dati perdono peso i meccanismi di tutela preventiva a favore del contrapposto valore della trasparenza; restano fermi i meccanismi di tutela successiva cui può ricorrere l'interessato per reprimere eventuali violazioni o abusi eventualmente commessi nell'utilizzo di dati diffusi[1032].

Di conseguenza, per quanto riguarda gli obblighi di pubblicazione, si può ritenere, come espresso da autorevole dottrina, che le amministrazioni non debbano valutare le specifiche finalità, dal momento che il legislatore ha esplicitamente finalizzato le fattispecie di pubblicazione alla trasparenza amministrativa, nel corretto esercizio del suo ruolo di "regolatore dei confini"[1033]; allo stesso modo la valutazione circa la pertinenza e l'indispensabilità dei dati personali pertinenti allo scopo si può ritenere già compiuta *ex ante* dal legislatore[1034].

La pubblicazione obbligatoria è prevista esplicitamente anche nel caso dei dati personali dei soggetti titolari di incarichi pubblici, dal momento che la pubblicazione è finalizzata alla realizzazione della trasparenza, che integra una finalità di rilevante interesse pubblico nel rispetto dei principi della disciplina in materia di protezione dei

---

1030 S. VACCARI, *op. cit.*, p. 160.

1031 Allo stesso limite del rispetto dei principi della disciplina in materia di protezione dei dati personali è sottoposta la pubblicazione di cui all'art. 7-bis, comma 2, d.lgs. 33/2013, trattata più avanti.

1032 S. VACCARI, *op. cit.*, p. 161 e F. PATRONI GRIFFI, *op. cit.*, p. 10.

1033 E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1119.

1034 In tal senso B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 75 ss. Secondo F. TENTONI, *Trasparenza "Riservata"*, in *Azienditalia - Il Personale,* fasc. 5, 2013, p. 236 ss. dovranno essere pubblicati solo i dati personali pertinenti allo scopo di trasparenza fissato dalla norma.

dati personali, "limite" che in tal caso il legislatore richiama espressamente in modo ampio, mostrando già un diverso bilanciamento rispetto al primo comma[1035].

Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, il legislatore si mostra più garantista e interessato a ridurre al minimo l'utilizzo dei dati personali per rispetto del principio di proporzionalità e, in specifico, dei criteri di pertinenza, non eccedenza e indispensabilità[1036]: le amministrazioni «*provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*»[1037]; pertanto andrà effettuato il bilanciamento e, a tal fine, dovranno essere applicati i principi e le regole che informano il trattamento[1038], il che si traduce, in caso di presenza di dati sensibili o giudiziari, nel fatto che il principio di pertinenza si "acutizza" in quello di indispensabilità[1039].

[1035] Al limite del rispetto dei principi della disciplina in materia di protezione dei dati personali è sottoposta la pubblicazione e la diffusione dei dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi: la pubblicazione è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico (art. 7-bis, comma 2, d.lgs. 33/2013). Secondo B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 87 la disposizione legittima la diffusione sia con riferimento ai dati personali comuni, sia con riferimento ai dati sensibili o giudiziari. *Contra* M.C. CAVALLARO, *op. cit.*, p. 121 ss., secondo cui il legislatore in tal caso riduce il margine di discrezionalità delle amministrazioni, che permane non per l'*an* della pubblicazione, ma solo per il *quomodo* della stessa, che si traduce nella valutazione sulla sussistenza di quali dati, all'interno di una pubblicazione obbligatoria, debbano essere omessi o schermati; si può aggiungere che la valutazione dovrà tenere conto della pertinenza alla finalità della trasparenza.

[1036] S. VACCARI, *op. cit.*, p. 162 ss.

[1037] Art. 7-bis, comma 4, d.lgs. 33/2013. Il comma 5 dell'art. 7-bis prevede il bilanciamento da compiere in caso di addetti a una funzione pubblica: sono rese accessibili le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione, mentre non sono ostensibili, salvo i casi previsti dalla legge, le notizie riguardanti la natura delle infermità e degli impedimenti personali o familiari causa di astensione dal lavoro, le componenti della valutazione e le notizie concernenti il rapporto di lavoro, idonee a rivelare dati sensibili.

[1038] In tal caso il testo si è uniformato alle indicazioni espresse dal Garante nel provvedimento n. 49 del 7 febbraio 2013 (contenente il parere del Garante sullo schema del d.lgs. 33/2013).

[1039] Cfr. F. TENTONI, *op. cit.*, p. 236 ss.

In considerazione della natura dei dati interessati, resta fermo il fatto che la diffusione non può riguardare dati idonei a rivelare lo stato di salute e la vita sessuale delle persone, limite espressamente richiamato dall'art. 7-bis, comma 6, del decreto[1040].

I dati idonei a rivelare lo stato di salute o la vita sessuale non sono l'unico limite, è necessario infatti porre attenzione ad alcune clausole di salvaguardia poste dal legislatore nei commi 6 e 8.

La norma esclude espressamente dall'ambito di applicazione del decreto legislativo «*i servizi di aggregazione, estrazione e trasmissione massiva degli atti memorizzati in banche dati rese disponibili sul web*»[1041]. La norma viene ricostruita ritenendo che l'oggetto sia costituito non da informazioni e dati, ma da servizi[1042].

Inoltre l'art. 7-bis, comma 6, d.lgs. 33/2013, accanto ai limiti relativi alla diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale, fa salvi i limiti all'accesso e alla diffusione delle informazioni, relativamente a:

- accesso documentale di cui all'art. 24, commi 1 e 6, legge 241/1990;
- tutti i dati raccolti nell'ambito di rilevazioni statistiche, comprese nel programma statistico nazionale di cui all'art. 9, d.lgs. 322/1989;
- quelli previsti dalla normativa europea in materia di tutela del segreto statistico;

1040 Anche in tal caso il testo del d.lgs. 33/2013 si è uniformato alle indicazioni espresse dal Garante nel provvedimento n. 49 del 7 febbraio 2013. È opportuno richiamare l'art. 26, comma 4, d.lgs. 33/2013, relativo agli obblighi di pubblicazione degli atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici a persone fisiche ed enti pubblici e privati, che esclude la pubblicazione dei dati identificativi delle persone fisiche destinatarie di tali provvedimenti, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute ovvero alla situazione di disagio economico-sociale degli interessati. Al riguardo la sentenza della Corte di Cassazione, sez. III, 13 ottobre 2016, n. 20615 ha specificato che sono notizie idonee a rivelare lo stato di salute quelle destinate a svelare patologie, terapie, anamnesi familiari e accertamenti diagnostici e non, per esempio, un infortunio al ginocchio (caso oggetto della sentenza).

1041 Art. 7-bis, comma 8, d.lgs. 33/2013.

1042 Così B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 93 ss., secondo cui «la *ratio* della clausola di salvaguardia pare essere quella di impedire l'estrazione e lo scarico "massivo" degli atti resi disponibili (ciò che potrebbe preludere alla costituzione di una banca dati parallela)» (pp. 94-95), trovando una possibile motivazione nella prevalenza in tali casi del profilo (finalità) di servizio rispetto a quello della trasparenza, con la volontà di voler preservare l'esclusività della fornitura e l'investimento.

- quelli che siano espressamente qualificati come riservati dalla normativa nazionale ed europea in materia statistica.

Accanto agli obblighi di pubblicazione e alla conseguente pubblicità necessaria, è diverso il caso della prevista trasparenza facoltativa[1043]. Le amministrazioni possono disporre, infatti, la pubblicazione di ulteriori dati, informazioni e documenti, che non hanno l'obbligo di pubblicare in base a specifica disposizione di legge o di regolamento, nel rispetto dei limiti previsti per l'accesso civico generalizzato (art. 5-bis): in tal caso devono procedere all'indicazione in forma anonima dei dati personali eventualmente presenti[1044]. Pertanto può essere assicurata la conoscibilità di ulteriori dati e documenti, ma vanno rispettati i limiti previsti e attivate le idonee misure di anonimizzazione: anche in questa ipotesi alle amministrazioni non resta alcun margine di discrezionalità, dal momento che il legislatore nel bilanciare gli interessi in gioco qui, diversamente dal primo comma, pone in rilievo l'esigenza della *data protection* e, di conseguenza, preclude *ipso iure* ogni diffusione dei dati personali presenti negli atti che in via aggiuntiva si vogliano pubblicare[1045].

Si conferma chiaramente la mancanza di prevalenze aprioristiche dell'uno o dell'altro valore (diritto alla conoscenza e diritto alla protezione dei dati personali): il bilanciamento è "mobile" e cambia in base al mutare delle circostanze di riferimento.

Interessante è anche il richiamo, frutto della riforma avvenuta con d.lgs. 97/2016, all'art. 5-bis e ai limiti all'accesso civico generalizzato: la disposizione prevede, infatti, il diniego dell'accesso se necessario ad evitare un pregiudizio concreto alla tutela di alcuni interessi privati, tra i quali «*la protezione dei dati personali, in conformità con la disciplina legislativa in materia*». Dal momento che si tratta di ipotesi di trasparenza facoltativa, ne possiamo dedurre che, in caso di diniego di accesso, l'utilizzo della

---

1043 Cfr. M. SAVINO, *La nuova disciplina della trasparenza amministrativa*, cit., pp. 795-805.

1044 Art. 7-bis, comma 3, d.lgs. 33/2013. Anche in tal caso il testo del d.lgs. 33/2013 si è uniformato alle indicazioni espresse dal Garante nel provvedimento n. 49 del 7 febbraio 2013.

1045 Cfr. S. VACCARI, *op. cit.*, p. 163 ss., che sottolinea come il legislatore abbia recepito le indicazioni del Garante sullo schema di decreto legislativo. Secondo l'Autore tale opzione è condivisibile e maggiormente coerente con il sistema di protezione dei dati personali; se tale oscuramento non fosse stato imposto, ma lasciato alla discrezionalità delle amministrazioni avrebbe causato una possibile disomogeneità non auspicabile in una visione di uniforme protezione dei dati personali.

discrezionalità amministrativa non dovrebbe certo portare alla pubblicazione dei relativi atti.

Sulla diffusione dei dati personali tramite pubblicazione sul sito web è intervenuto anche il Garante per la protezione dei dati personali, con le linee guida del 15 maggio 2014[1046]. Il Garante, oltre a trattare i profili attinenti alla pubblicità per finalità di trasparenza e gli aspetti più problematici, che saranno esaminati tra poco, distingue la pubblicità online per finalità di trasparenza da quella effettuata per finalità diverse (forme di pubblicità dichiarativa, notizia o integrativa dell'efficacia) e richiama le amministrazioni al rispetto dei principi della disciplina nel caso della pubblicità per finalità diverse dalla trasparenza (come l'albo pretorio online e le graduatorie): in particolare, le invita all'individuazione della specifica finalità perseguita su cui calibrare le modalità, anche tecniche, di pubblicazione, rispettando i principi di necessità, pertinenza e non eccedenza, garantendo i principi di qualità, esattezza ed aggiornamento dei dati, delimitando la durata della disponibilità online a tempi limitati e proporzionati, evitando la rintracciabilità e l'indicizzazione per mezzo di motori esterni di ricerca (capaci di decontestualizzare il dato[1047]) e adottando opportune cautele per ostacolare operazioni di duplicazione massiva[1048].

[1046] Provvedimento n. 243 del 15 maggio 2014, doc. web n. 3134436. Il Garante si era già occupato della pubblicazione di dati personali sui siti web istituzionali nel provvedimento n. 88 del 2 marzo 2011, «*Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web*», in *G.U.* n. 64 del 19 marzo 2011, doc. web n. 1793203; nel provvedimento n. 17 del 19 aprile 2007, «*Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali*», in *G.U.* n. 120 del 25 maggio 2007, doc. web n. 1407101; nel provvedimento n. 31 del 25 gennaio 2012, «*Linee guida in tema di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute*», in *G.U.* n. 42 del 20 febbraio 2012, doc. web n. 1870212.

[1047] Il Garante evidenzia «il pericolo di decontestualizzazione del dato personale e la riorganizzazione delle informazioni restituite dal motore di ricerca secondo una logica di priorità di importanza del tutto sconosciuta, non conoscibile e non modificabile dall'utente».

[1048] Cfr. B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 75 ss.

Pertanto, nella disciplina normativa recata dal d.lgs. 33/2013 e, in specifico, nelle diverse forme di trasparenza proattiva si colgono significativi punti di equilibrio e criteri da seguire nel bilanciamento fra le diverse istanze afferenti al *right to know* e alla *data protection*, cui va sommata una dimensione ulteriore di convergenza: la qualità dei dati.

Il principio emerge, come esaminato, nella disciplina europea e nazionale, dove si stabilisce che i dati personali oggetto di trattamento devono essere esatti e, se necessario, aggiornati[1049].

La qualità delle informazioni, già presente nell'art. 53 del d.lgs. 82/2005 fra le caratteristiche che i siti istituzionali devono rispettare[1050], viene valorizzata e disciplinata in una disposizione specifica, l'art. 6 del d.lgs. 33/2013, nella consapevolezza che è essenziale per assicurare autentica trasparenza. Le pubbliche amministrazioni devono garantire la qualità delle informazioni riportate nei siti istituzionali nel rispetto degli obblighi di pubblicazione previsti, assicurando all'informazione una serie di caratteristiche che formano il concetto di "qualità": l'integrità, il costante aggiornamento, la completezza, la tempestività, la semplicità di consultazione, la comprensibilità, l'omogeneità, la facile accessibilità, la conformità ai documenti originali in possesso dell'amministrazione, l'indicazione della loro provenienza e la riutilizzabilità. Al fine di garantire effettività alla disposizione è precisato che l'esigenza di assicurare adeguata qualità delle informazioni diffuse non può, in ogni caso, costituire motivo per l'omessa o ritardata pubblicazione dei dati, delle informazioni e dei documenti[1051].

Sugli esaminati aspetti di disciplina, alla luce dei principi e delle disposizioni di riferimento, si può ritenere realizzato già *ex ante*, grazie al puntuale intervento del legislatore, un bilanciamento tra le istanze di trasparenza proattiva e *data protection*,

---

1049 Art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679 e art. 11, comma 1, lett. c), d.lgs. 196/2003.

1050 Art. 53, comma 1, d.lgs. 82/2005: «*Le pubbliche amministrazioni realizzano siti istituzionali su reti telematiche che rispettano i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilià, semplicità di consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54*».

1051 Art. 6, commi 1 e 2, d.lgs. 33/2013.

bilanciamento guidato anche da quanto espresso al riguardo dal Garante e rafforzato dalla condivisa esigenza di qualità dei dati[1052].

5.3.2. I profili problematici del bilanciamento tra diritti: durata, indicizzazione e apertura (riutilizzo)

Mentre sui profili esaminati la normativa chiarisce le modalità con cui garantire l'equilibrio tra istanze diverse, tre profili restano maggiormente problematici per la realizzazione del bilanciamento, dal momento che la scelta relativa a questi aspetti riguarda la profondità, l'ampiezza e gli effetti della diffusione[1053] e, di conseguenza, porta la bilancia a pendere inevitabilmente verso una delle due istanze, trasparenza o protezione dei dati personali.

I tre profili sono relativi alla durata della pubblicazione, che chiama in gioco il rispetto del principio di non eccedenza, specificamente in relazione alla dimensione temporale (diritto all'oblio), all'indicizzazione da parte di motori di ricerca esterni, dove viene in rilievo il rispetto del principio di proporzionalità, e, infine, al riutilizzo e all'apertura dei dati, profilo particolarmente complesso che porta a esaminare il rispetto del principio di finalità. Si tratta di aspetti particolarmente significativi, dal momento che emerge con chiarezza che i nodi problematici del bilanciamento si annidano non tanto nella trasparenza in quanto tale, ma nelle potenzialità particolarmente incisive e diffusive della rete e, quindi, nelle modalità digitali della trasparenza, nella sua digitalizzazione e, altresì, nel paradigma dell'*open government*[1054].

[1052] Significativamente il d.lgs. 33/2013 ha recepito le indicazioni fornite al riguardo dal Garante per la protezione dei dati personali, espresse nel provvedimento n. 49 del 7 febbraio 2013 recante il parere sullo schema del decreto legislativo. Dopo l'intervento del d.lgs. 97/2016 l'attuale disposizione dell'art. 7-bis non reca differenze rispetto alle previsioni dell'art. 4, se non proprio la collocazione.

[1053] Si riferisce all'ampiezza, agli effetti e alla profondità della diffusione con particolare riguardo al profilo dell'indicizzazione e rintracciabilità dei dati mediante motori di ricerca B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 90 ss.

[1054] S. CALZOLAIO, *op. cit.*, p. 189. Secondo E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1114 «a rilevare in modo decisivo è il contrasto tra i paradigmi

Per quanto attiene al primo profilo legato al tempo, ai sensi dell'art. 8 del d.lgs. 33/2013, i documenti contenenti atti oggetto di pubblicazione obbligatoria sono pubblicati tempestivamente sul sito istituzionale; i documenti contenenti altre informazioni e dati oggetto di pubblicazione obbligatoria sono pubblicati e mantenuti aggiornati ai sensi delle disposizioni[1055]. Nella tempestività e nell'aggiornamento emerge la qualità da garantire ai dati, su cui convergono entrambe le istanze, come già esaminato.

In merito alla decorrenza e alla durata della pubblicazione, invece, nascono i problemi. Nel proprio parere allo schema del d.lgs. 33/2013, posizione confermata in occasione del parere allo schema del d.lgs. 97/2017[1056], il Garante aveva richiesto un'attenzione particolare al riguardo, suggerendo di stabilire periodi di permanenza online differenziati in base alla natura dei documenti, garantendo altresì un'accessibilità selettiva in base alla scadenza del termine di pubblicazione, motivando con il fatto che un termine generalizzato non rispetta il principio di proporzionalità di matrice europea nella conservazione dei dati personali rispetto alle finalità perseguite. Invece, ai sensi della normativa vigente, i dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria devono essere pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e dagli artt. 14, comma 2, e 15, comma 4; decorsi i termini previsti, i relativi dati e documenti sono accessibili ai sensi dell'articolo 5, che prevede l'accesso civico generalizzato[1057].

---

dell'amministrazione aperta e quelli della privacy, che ha i suoi punti più evidenti nelle contrapposizioni tra riutilizzo (per qualsiasi finalità) e principi di finalità e necessità; tra indicizzazione e pericolo di decontestualizzazione; tra completezza e pertinenza-non eccedenza; più complessivamente tra dati di tipo aperto e dati oggetto di protezione, tra *open data* e *habeas data*».

[1055] Art. 8, commi 1 e 2, d.lgs. 33/2013.

[1056] Provvedimenti n. 49 del 7 febbraio 2013 e n. 92 del 3 marzo 2016.

[1057] Art. 8, comma 3, d.lgs. 33/2013. Gli artt. 14, comma 2, e 15, comma 4, prevedono disposizioni specifiche per i componenti degli organi di indirizzo politico e per i titolari di incarichi dirigenziali e di collaborazione o consulenza. Il d.lgs. 97/2016, opportunamente, ha abrogato il secondo comma dell'art. 9, ai sensi del quale, alla scadenza del termine dell'obbligo di pubblicazione, o anche prima, i documenti, le informazioni e i dati dovevano essere conservati e resi disponibili in distinte sezioni del sito di archivio, collocate e debitamente segnalate nella sezione "Amministrazione trasparente": in tal modo i dati

La normativa, pertanto, prevede un termine unico e generalizzato per tutti i dati, che pone possibili profili di contrasto con il principio di proporzionalità e non eccedenza e che comunque, alla luce della normativa e dei principi in materia di *data protection*, deve essere interpretato come derogabile[1058]. In tal senso, nelle linee guida del 2014 e nel parere sullo schema di d.lgs. 97/2016, in merito alla durata, il Garante ha sollevato la necessità di oscurare i dati anche prima del termine di 5 anni, quando sono stati raggiunti gli scopi per i quali sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

A seguito della riforma del d.lgs. 97/2016, accogliendo quanto previsto dal Garante per la protezione dei dati personali, l'Anac, sulla base della valutazione del rischio corruttivo, delle esigenze di semplificazione e delle richieste di accesso, determina, anche su proposta del Garante, i casi in cui la durata della pubblicazione del dato e del documento può essere inferiore a 5 anni[1059].

Profilo particolarmente delicato per il bilanciamento fra trasparenza e protezione dei dati personali è quello relativo all'indicizzazione e alla rintracciabilità dei dati da parte dei motori di ricerca esterni al sito di provenienza, che li porta a "uscire" dall'alveo del sito web istituzionale, in cui i dati sono stati pubblicati, e a un'esposizione che, come esaminato, può essere latrice di violazioni a danno della persona e della stessa fiducia della comunità nell'operato dei poteri pubblici[1060]. Secondo il Garante «un malinteso (e dilatato) principio di trasparenza» può determinare «conseguenze gravi e

---

permanevano sul sito, seppur in sezioni diverse, senza l'espressa previsione di un termine. Tale disposizione sembrava vanificare e contraddire la *ratio* di una pubblicazione di natura temporanea, cristallizzando e immobilizzando *sine die* i dati e interferendo evidentemente con il rispetto del diritto all'oblio; S. VACCARI, *op. cit.*, p. 174 ss.

1058 Cfr. S. VACCARI, *op. cit.*, p. 172 ss., che, peraltro, come il Garante, sottolinea l'inutilità del richiamo ai diversi termini previsti dalla normativa in materia di protezione dei dati personali, dal momento che in realtà non sono previsti: di conseguenza, la disposizione va interpretata come possibilità di deroga e modulazione di termini proporzionati, differenziati e conformi ai principi in materia di *data protection*.

1059 Art. 8, comma 3-bis, d.lgs. 33/2013.

1060 I motori di ricerca pongono problematiche in relazione alla *data protection* per il fatto che per il loro funzionamento non hanno limiti alla cattura e all'utilizzo dei dati; in proposito cfr. R. RAZZANTE, *op. cit.*, p. 181 ss.

pregiudizievoli tanto della dignità delle persone quanto della stessa convivenza sociale»[1061].

L'indicizzazione e la rintracciabilità da parte dei motori di ricerca, infatti, espongono a pericolose decontestualizzazioni dei dati «estrapolandoli dal sito in cui sono contenuti e trasformandoli in una parte – non controllata e non controllabile – secondo una "logica" di priorità di importanza del tutto sconosciuta e non conoscibile all'utente»[1062], oltre al rischio di permanenza in rete, compromettendo così il diritto all'oblio degli interessati, aspetto che è stato protagonista della celebre sentenza della Corte di giustizia *Google Spain*, già esaminata[1063].

Secondo il Garante «un obbligo così ampio e indifferenziato di indicizzare la documentazione pubblicata è contrario al principio di proporzionalità nel trattamento dei dati personali rispetto alle specifiche finalità di trasparenza di volta in volta perseguite e non tiene in considerazione le esigenze di avere dati esatti, aggiornati e contestualizzati» e, di conseguenza, espone la vita privata «alla generale curiosità del pubblico, determinando conseguenze ultronee rispetto agli obiettivi di trasparenza già efficacemente raggiunti attraverso la pubblicazione dei medesimi dati sui siti web istituzionali delle amministrazioni»[1064].

Peraltro l'indicizzazione, la rintracciabilità e la diffusione per mezzo dei motori di ricerca hanno anche l'effetto negativo di rendere estranee le amministrazioni al possibile governo e controllo sui dati pubblicati e sulle caratteristiche di qualità che devono connotarli (esattezza e aggiornamento)[1065].

1061 Provvedimento n. 92 del 3 marzo 2016.

1062 Provvedimento n. 92 del 3 marzo 2016.

1063 *Supra*, cap. 4, § 3.2. Cfr. L. CALIFANO, *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014, p. 64; I. NICOTRA, *op. cit.*, p. 8; S. VACCARI, *op. cit.*, p. 165 ss.; E. FURIOSI, *op. cit.*, p. 1 ss., secondo la quale il regime previsto è sproporzionato *ex se* e non c'è modo di riequilibrarlo: peraltro espone anche al rischio di voyerismo amministrativo.

1064 Provvedimento n. 92 del 3 marzo 2016.

1065 S. VACCARI, *op. cit.*, p. 167.

L'art. 7-bis, comma 1, discostandosi dal parere sullo schema del d.lgs. 33/2013 del Garante che aveva suggerito il ricorso solo a motori di ricerca interni[1066], prevede espressamente per i dati personali diversi dai dati sensibili e giudiziari, oggetto di pubblicazione obbligatoria, il trattamento «*secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web*». Evidentemente il legislatore ha ritenuto l'utilizzo di motori di ricerca interni al sito limitante rispetto alle potenzialità offerte dalla rete di conoscere, ricercare, reperire agevolmente e fare uso di informazioni, finendo altrimenti per replicare le logiche di una diffusione realizzabile con mezzi tradizionali[1067]. Le norme interpretano quindi il principio di trasparenza nel suo concetto più profondo, favorendo forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche, nella prospettiva tipica del modello di *open government*[1068].

Nel parere sullo schema del d.lgs. 97/2016 il Garante aveva invitato il legislatore a «una graduazione delle modalità di reperibilità in rete delle informazioni, oggetto degli obblighi di trasparenza, tramite i motori di ricerca», ritenendo giustificata «l'indicizzazione da parte dei comuni motori di ricerca dei dati personali riferiti a soggetti che ricoprono cariche politiche per la rilevanza pubblica del ruolo ricoperto o della funzione esercitata», ma non degli altri, non ritenendo giustificabile «che la trasparenza dell'amministrazione si trasformi nella "trasparenza delle persone"»[1069].

[1066] Il testo si discosta dalle indicazioni fornite nel parere espresso dal Garante sullo schema del d.lgs. 33/2013 (provvedimento del Garante n. 49 del 7 febbraio 2013), che aveva raccomandato l'utilizzo di motori di ricerca interni al sito dell'amministrazione, non consentendo l'indicizzazione e la facile rintracciabilità degli stessi attraverso i comuni motori di ricerca, ritenendo tale misura, ampia e indifferenziata, contraria al principio di proporzionalità nel trattamento dei dati personali rispetto alle specifiche finalità di trasparenza di volta in volta perseguite (art. 11, comma 1, lett. b), d.lgs. 196/2003) e rilevando che la misura incide negativamente sull'esigenza di avere dati esatti, aggiornati e contestualizzati.

[1067] In tal senso B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 90 ss.

[1068] Così B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 90 ss.

[1069] Provvedimento del Garante n. 92 del 3 marzo 2016.

La norma sembra, invece, aver privilegiato le istanze di trasparenza e apertura che connotano la contemporaneità. Conferma e rafforza tale impostazione, atta a favorire il diritto alla conoscenza e a sfruttare le potenzialità del web, anche la disposizione secondo cui le amministrazioni «*non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente"*» (art. 9, comma 1, d.lgs. 33/2013), che il Garante anche in occasione del parere sullo schema di d.lgs. 97/2016 aveva invitato il legislatore a sopprimere.

Al riguardo, nelle linee guida del 2014, il Garante ha avuto modo di precisare che tale obbligo di indicizzazione da parte dei motori generalisti, come Google, durante il periodo di pubblicazione obbligatoria deve intendersi limitato ai soli dati tassativamente individuati dalle disposizioni da collocarsi nella sezione "Amministrazione trasparente" con esclusione di altri dati che si ha obbligo di pubblicare per altre finalità di pubblicità diverse da quella di trasparenza (es. albo pretorio).

Se indicizzazione e rintracciabilità per mezzo dei motori di ricerca web sono esplicitamente previste per i dati c.d. comuni, potrebbero permanere dubbi per quanto attiene ai dati sensibili e giudiziari, anche in considerazione del fatto che la norma che vieta filtri e altre soluzioni atte ad impedire l'indicizzazione si riferisce a tutti i contenuti della sezione[1070]. Nelle linee guida del 2014, il Garante ha chiarito il profilo, precisando che i dati sensibili e giudiziari sono sottratti all'indicizzazione e alla rintracciabilità.

Nell'evoluzione normativa che ha riguardato il principio di *disclosure* e nell'affermarsi del modello di *open government*, la trasparenza diventa paradigma e pilastro dell'intera attività amministrativa, assumendo una nuova configurazione "attiva" nel legame con l'apertura (*open data*) e trovando cornice normativa nel riordino compiuto dal d.lgs. 33/2013, poi rafforzato dal d.lgs. 97/2016. Il "matrimonio" tra trasparenza e apertura impone l'esigenza di analizzare il terzo profilo problematico,

---

[1070] Secondo B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 90 ss. l'interpretazione che include nella possibilità di indicizzazione anche tali dati, tranne naturalmente quelli per i quali è imposto il mascheramento e per i quali, di conseguenza, risulta vanificata l'indicizzazione stessa, non annulla la tutela dei dati personali, dal momento che è possibile attivare meccanismi di repressione e quindi di tutela successiva in caso di eventuali abusi.

quello relativo al bilanciamento tra il diritto del singolo alla *data protection* e il diritto di chiunque altro al riutilizzo.

L'aspetto forse più problematico del bilanciamento si trova proprio negli *open data* e nella possibilità di riutilizzo dei dati, prevista dal combinato disposto degli articoli 3, comma 1, 7 e 7-bis, comma 1, d.lgs. 33/2013.

Tutti i documenti, le informazioni e i dati oggetto di accesso civico, compresi quelli oggetto di pubblicazione obbligatoria[1071], ai sensi dell'art. 3 del d.lgs. 33/2013, sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, utilizzarli e riutilizzarli ai sensi dell'art. 7 del d.lgs. 33/2013, significativamente rubricato «*dati aperti e riutilizzo*»: tali documenti, informazioni e dati devono essere pubblicati in formato aperto e devono essere riutilizzabili ai sensi dei d.lgs. 36/2006, d.lgs. 82/2005 e d.lgs. 196/2003, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità. Come esaminato, conferma tale approccio l'art. 7-bis del d.lgs. 33/2013, ai sensi del quale gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari comportano, accanto a diffusione, indicizzazione e rintracciabilità da parte dei motori di ricerca, anche il riutilizzo ai sensi dell'art. 7 nel rispetto dei principi sul trattamento dei dati personali.

Il combinato disposto di norme fonda non solo il diritto alla conoscenza, ma anche il diritto all'apertura e al riutilizzo di documenti, informazioni e dati, limitato solo dall'attribuzione della paternità/titolarità dei dati e dal rispetto dell'integrità, profilo che fa emergere anche in tale contesto la rilevanza della qualità del dato. È evidente l'attenzione all'*openness* e al correlato sviluppo sociale ed economico, aspetti chiariti anche nella relazione illustrativa di accompagnamento allo schema del d.lgs. 33/2013, che sottolinea l'importanza della messa a disposizione di cittadini e imprese di una vasta mole di dati pubblici da poter utilizzare per realizzare servizi a valore aggiunto e migliorare la qualità di vita, finalità tipiche delle strategie di *open data*.

Il riutilizzo prevede e auspica la possibilità che i dati non solo fuoriescano dal sito di riferimento, ma vengano utilizzati in nuovi contesti e quindi siano sottoposti a

[1071] La disposizione, frutto della riforma del d.lgs. 97/2016, risulta più ampia rispetto alla versione originaria che parlava solo di dati oggetto di pubblicazione obbligatoria, anche in conseguenza dell'assenza dell'accesso civico generalizzato, introdotto dal d.lgs. 97/2016.

ulteriori "trattamenti" successivi effettuati con scopi diversi dall'originario[1072]: in tal modo, si pone in modo evidente la problematica del rispetto della *data protection* e, in specifico, del principio di finalità, in base al quale i dati personali, legittimamente raccolti, possono essere utilizzati in altre operazioni del trattamento solo in modi che non siano incompatibili con gli scopi per i quali sono stati trattati[1073]. Una tale limitazione può compromettere infatti le potenzialità stesse del riutilizzo, dal momento che nelle strategie di apertura si auspica l'utilizzo proprio per scopi diversi, anche di natura commerciale, poiché ciò consente di favorire lo sviluppo economico legato a dati pubblicati in formato aperto e rielaborabili, che le aziende e i privati potranno impiegare per realizzare servizi a valore aggiunto.

In proposito l'art. 3, comma 1, e, altresì, l'art. 7-bis, comma 1, prevedono il riutilizzo ai sensi dell'articolo 7 «*nel rispetto dei principi sul trattamento dei dati personali*» (così specifica l'art. 7-bis, comma 1), fondamentalmente senza sciogliere il nodo circa le modalità concrete per realizzare il complesso bilanciamento tra l'istanza di apertura, da una parte, e l'esigenza di rispettare la protezione dei dati personali, dall'altra.

Sul profilo è intervenuto il Garante nelle linee guida del 2014[1074], riequilibrando la bilancia verso la *data protection*, a fronte di possibili estremismi a favore dell'apertura: secondo l'Autorità il principio generale del riutilizzo non deve essere

---

[1072] E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1120.

[1073] Art. 5, paragrafo 1, lett. b), regolamento (UE) 2016/679 e art. 11, comma 1, lett. b), d.lgs. 196/2003. Secondo E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1119 ss. la trasparenza impone gli *open data* e, anche con riferimento ad alcuni dati personali, «l'immagine di una trasparenza fatta di informazioni anonime è inadeguata alla finalità di un principio che (a prendere sul serio il d.lgs. 33), realizzando fondamentali principi costituzionali ha in sé un valore non minore della stessa protezione dei dati personali rispetto a dati non sensibili o giudiziari», anche in considerazione del fatto che fin dalla nascita del modello di *open government* negli Stati Uniti «la democrazia richiede accountability, l'accountability richiede trasparenza».

[1074] Secondo F. CARDARELLI, *op. cit.*, p. 227 ss., dal momento che nel tentativo di una mediazione *a priori* degli interessi in gioco la disciplina normativa non si può ritenere giunga a realizzare un bilanciamento soddisfacente, è necessario leggerla alla luce delle regole di *soft law* elaborate dal Garante, che attua i principi europei e nazionali in materia di protezione dei dati personali.

automatico quando coinvolge dati personali e non può prevalere sulla disciplina a tutela dei dati personali[1075].

Nelle linee guida, innanzitutto, il Garante sottolinea che il riutilizzo «riguarda essenzialmente documenti che non contengono dati personali oppure riguarda dati personali opportunamente aggregati e resi anonimi». Il Garante precisa poi, attraverso una forzatura del testo normativo, che la pubblicazione dei dati "in formato aperto" non comporta che siano anche "dati di tipo aperto", che attengono precipuamente alla disponibilità unita alla riutilizzabilità da parte di chiunque anche per finalità commerciali e in modo disaggregato[1076]. Di conseguenza, il Garante specifica che la pubblicazione online dei dati per finalità di trasparenza non comporta che siano liberamente riutilizzabili da chiunque e per qualunque finalità, ma siano riutilizzabili solo in termini compatibili (ora, ai sensi del regolamento, non incompatibili) con gli scopi per i quali sono stati raccolti e resi accessibili e nel rispetto delle norme in materia di protezione dei dati personali[1077].

Il Garante richiama, pertanto, nel bilanciamento il principio cardine di finalità, idoneo ad arginare in tale contesto manipolazioni che possano incrinare il valore della verità[1078]. Per tale motivo, il soggetto chiamato a dare attuazione agli obblighi di pubblicazione sul proprio sito web istituzionale è tenuto a «determinare – qualora intenda rendere i dati riutilizzabili – se, per quali finalità e secondo quali limiti e condizioni eventuali utilizzi ulteriori dei dati personali resi pubblici possano ritenersi leciti alla luce del "principio di finalità" e degli altri principi di matrice europea in materia di protezione dei dati personali». Secondo il Garante, pertanto, al fine di evitare di perdere il controllo sui dati personali pubblicati online in attuazione degli obblighi di trasparenza e di ridurre i rischi di loro usi indebiti, è opportuno che le pubbliche amministrazioni inseriscano nella sezione "Amministrazione trasparente" un *alert* generale atto a informare il pubblico che i dati personali sono riutilizzabili solo alle

---

1075 Cfr. G. ARMAO, *op. cit.*, p. 7.

1076 G. GARDINI, *op. cit.*, p. 875 ss.

1077 F. TENTONI, *op. cit.*, p. 236 ss. spiega come in concreto questo significhi riutilizzare esclusivamente i dati per le finalità di trasparenza per le quali sono stati raccolti e pubblicati e, quindi, per ragioni di informazione alla collettività, indirizzo e controllo politico, mentre non sarebbe possibile il riutilizzo per scopi diversi quali finalità di pubblicità commerciale, indagini etc.

1078 S. VACCARI, *op. cit.*, p. 170 ss.

condizioni previste dalla normativa vigente sul riutilizzo, in termini compatibili (ora, ai sensi del regolamento, non incompatibili) con gli scopi per i quali sono raccolti e nel rispetto delle norme in materia di protezione dei dati personali.

Una volta effettuata la pubblicazione online dei dati personali prevista dalla normativa in materia di trasparenza, il Garante precisa che il soggetto pubblico può rendere riutilizzabili tali dati o accogliere eventuali richieste di riutilizzo degli stessi da parte di terzi, solamente dopo avere effettuato una rigorosa valutazione d'impatto in materia di protezione dei dati personali, al fine di ridurre il rischio di perdere il controllo sulle medesime informazioni o di dover far fronte a richieste di risarcimento del danno da parte degli interessati. Tale valutazione deve essere volta a:

a) stabilire, alla luce dell'esistenza di un presupposto normativo idoneo, la liceità del riutilizzo di dati personali pubblicamente accessibili sui siti web istituzionali da parte di terzi e per scopi ulteriori;
b) in caso di valutazione positiva circa la liceità, è necessario verificare se l'utilizzo ulteriore di questi dati possa essere consentito:
    - «limitatamente ai dati rielaborati in forma anonima e aggregata, individuando il livello appropriato di aggregazione e la specifica tecnica di anonimizzazione da utilizzare sulla base di una ponderata valutazione del rischio di re-identificazione degli interessati oppure rispetto a tutti o soltanto ad alcuni dei dati personali resi pubblici, in considerazione della difficoltà di ottenere dati effettivamente anonimi»;
    - «per qualsiasi scopo ulteriore o solo per taluni scopi determinati» (per esempio fini commerciali o non commerciali);
    - «secondo modalità di messa a disposizione online conformi ai principi di necessità, proporzionalità e pertinenza», sulla base di una ponderazione dei rischi di utilizzi impropri e degli effetti negativi che possono derivare agli interessati;
    - «a condizione che gli utilizzatori adottino modalità tecniche e rispettino specifici vincoli giuridici definiti in apposite licenze predisposte al fine di individuare idonee cautele per tutelare i diritti degli interessati nei successivi trattamenti di dati a fini di riutilizzo» (come le questioni inerenti la responsabilità in capo agli utilizzatori e l'uso corretto dei dati).

Il Garante porta un esempio concreto: è illecito riutilizzare a fini di *marketing* o di propaganda elettorale i recapiti e gli indirizzi di posta elettronica del personale pubblico oggetto di pubblicazione obbligatoria, dal momento che tale ulteriore trattamento deve ritenersi incompatibile con le originarie finalità di trasparenza[1079].

Nella valutazione d'impatto, anche alla luce dell'intepretazione sistematica delle disposizioni, il Garante precisa che i dati personali sensibili e giudiziari sono espressamente esclusi dal riutilizzo.

Il Garante si sofferma anche sulle licenze: «non è ammesso l'incondizionato riutilizzo di dati personali oggetto di pubblicazione obbligatoria sulla base di mere licenze aperte che non pongano alcuna limitazione all'ulteriore trattamento dei dati». Infatti per rendere riutilizzabili, a seguito della valutazione d'impatto, i dati personali oggetto di obblighi di pubblicazione, è indispensabile che il soggetto predisponga sul proprio sito istituzionale «licenze standard, in formato elettronico e rese facilmente conoscibili ai potenziali utilizzatori, le quali stabiliscano chiaramente le modalità di carattere giuridico e tecnico che presiedono al corretto riutilizzo di tali dati».

Per garantire il rispetto dei diritti degli interessati da parte degli utilizzatori, i termini delle licenze dovrebbero contenere una clausola di protezione dei dati, quando il riuso riguardi dati personali, e dovrebbero indicare chiaramente le finalità e le modalità degli ulteriori trattamenti consentiti. Invece laddove riguardino dati anonimi derivati da dati personali, le condizioni di licenza dovrebbero «vietare ai titolari delle licenze di re-identificare gli interessati e di assumere qualsiasi decisione o provvedimento che possa riguardarli individualmente sulla base dei dati personali così ottenuti, nonché prevedere in capo ai medesimi titolari l'obbligo di informare l'organismo pubblico nel caso in cui venisse rilevato che gli individui interessati possano essere o siano stati re-identificati».

Nelle linee guida, il Garante fornisce anche indicazioni di ordine tecnico, esortando a considerare con attenzione quali accorgimenti tecnologici possono essere

---

[1079] La finalità perseguita dalle disposizioni che impongono la pubblicazione dei dati del personale, secondo il Garante, seppure non espressamente indicata, è quella di aiutare i consociati a individuare i soggetti e i recapiti da contattare per presentare istanze o ottenere informazioni relative a procedimenti di competenza delle pubbliche amministrazioni (es. art. 35, d.lgs. n. 33/2013). Di conseguenza, il personale interessato, tenuto conto del contesto in cui i dati che lo riguardano sono stati raccolti, non potrebbe ragionevolmente prevedere che questi possano essere utilizzati per scopi non collegati alle proprie attività lavorative.

messi in atto per ridurre i rischi di usi impropri e delle conseguenze negative che possono derivarne agli interessati, privilegiando «modalità tecniche di messa a disposizione dei dati a fini di riutilizzo che consentano di controllare gli accessi a tali dati da parte degli utilizzatori e che impediscano la possibilità di scaricare o di duplicare in maniera massiva e incondizionata le informazioni rese disponibili, nonché l'indiscriminato utilizzo di software o programmi automatici».

Le indicazioni fornite dal Garante, nelle linee guida del 2014, risultano in linea con il regolamento (UE) 2016/679, che tra i nuovi principi fondamentali pone in via generale proprio la valutazione d'impatto sulla protezione dei dati (art. 35), anche se indubbiamente, come rilevato in dottrina, consistono in una rilettura restrittiva delle norme che finisce per negare al legislatore il ruolo di regolatore dei confini e di responsabile dell'equilibrio tra pubblicità e protezione dei dati personali[1080].

In caso di riutilizzo, oltre al Garante, viene in gioco anche l'AgID, che ha un ruolo significativo nelle strategie di apertura.

Nelle linee guida per la valorizzazione del patrimonio informativo pubblico per l'anno 2017, si perimetra l'applicazione delle stesse, precisando che ci si riferisce ai dati pubblici, da intendersi quali dati conoscibili da chiunque e non soggetti a restrizioni temporali e, di conseguenza, si escludono esplicitamente i dati personali, per i quali, si precisa, trovano applicazione le norme del Codice, il d.lgs. 196/2003, e le linee guida del Garante[1081]. Nella consapevolezza dei rischi di identificazione dei soggetti, si richiama l'attenzione «a non esporre quasi-identificatori (e.g., data di nascita, domicilio, residenza, sesso, razza, etnia, composizione nucleo famigliare, status giuridico, ecc.) che possono facilmente re-identificare i soggetti che si intende invece tutelare o che hanno una tutela speciale perché appartenenti a fasce protette (e.g., testimoni giudiziari, profughi, rifugiati, pentiti, ecc.)». Le linee guida invitano le amministrazioni a tenere conto delle differenze specifiche tra *open data*, trasparenza e condivisione dei dati tra pubbliche amministrazioni per finalità istituzionali: questi tre concetti e le correlate azioni svolgono differenti ruoli funzionali, mirano a soddisfare esigenze diverse e,

---

[1080] E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1113 ss.

[1081] Le linee guida dell'AgID escludono, altresì, quelli che sono definiti "dati a conoscibilità limitata", come i dati coperti da segreto di Stato o le opere d'ingegno coperte dal diritto d'autore.

nonostante la convergenza su alcuni aspetti, fanno sempre riferimento a obiettivi specifici[1082].

Alla luce dell'analisi condotta, emerge che i profili sui quali maggiormente si disputa la battaglia fra trasparenza, apertura e *data protection* (durata della pubblicazione, indicizzazione dei motori di ricerca e riutilizzo dei dati) appaiono "risolti" dalla normativa in modo maggiormente favorevole alle istanze di trasparenza, mentre il Garante nei suoi interventi tende a bilanciare in direzione di protezione dei dati personali.

Di nuovo, anche in tale contesto, si conferma la necessità di un bilanciamento "mobile" che non ceda a prevalenze aprioristiche, automatiche e assolute di un interesse rispetto all'altro, ma sia condotto valutando i casi in concreto, anche in considerazione del fatto che una lesione del diritto alla protezione dei dati personali in rete può essere irreparabile e non reversibile[1083]. Peraltro nel bilanciamento, in caso di riutilizzo, il diritto alla protezione dei dati personali si trova di fronte non solo il principio di trasparenza e il diritto alla conoscenza, ma anche ulteriori diritti, quale il diritto di iniziativa economica delle imprese intenzionate a riutilizzare i dati[1084].

1082 Al riguardo sono portati alcuni esempi: in termini di trasparenza, alcuni documenti resi pubblici in conformità al d.lgs. 33/2013 nella sezione "Amministrazione Trasparente" del sito web istituzionale devono essere rimossi dopo aver svolto la loro funzione (es. 3 anni, ai sensi degli artt. 14 e 15, d.lgs. 33/2013): in questo senso, non possono essere propriamente considerati *open data*, ai quali tali restrizioni temporali non si applicano. Diversamente, ci sono dati delle pubbliche amministrazioni che assumono un ruolo significativo nell'ecosistema degli *open data* e nella creazione di nuove forme di partecipazione (come edifici, farmacie, musei, turismo, etc.), ma che non figurano nell'elenco dei dati obbligatori da pubblicare ai sensi del d.lgs. 33/2013.

1083 Cfr. sentenza della Corte di Giustizia dell'Unione europea del 9 novembre 2010, *Volker und Markus Schecke GbR e al*., cause riunite C-92/09 e C-93/09, secondo la quale con riferimento alla divulgazione da parte di istituzioni pubbliche di informazioni riguardanti una persona fisica deve essere soppesato l'interesse dell'Unione a garantire la trasparenza delle proprie azioni con la lesione dei diritti riconosciuti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, senza che possa riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali, anche qualora siano coinvolti rilevanti interessi economici.

1084 M. ALOVISIO, *Criticità Privacy nel riuso dei dati pubblici*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 45-64.

Si tratta allora di immaginare un governo dei dati e correlati sistemi informativi capaci di realizzare una visione cooperativa dei valori di rilevanza costituzionale[1085] e una convergenza tra i principi recati dalla normativa, *digital by default*, ma anche *privacy by default* e *by design*, considerando fin dal momento della progettazione i contrapposti interessi in gioco e l'esigenza di una loro armonia a tutela della persona e della sua dignità[1086].

Naturalmente ci sono strumenti, misure e accorgimenti che permettono di realizzare più agevolmente questa impostazione.

Innanzitutto, sarà fondamentale accompagnare la pubblicazione sul sito web, ossia la diffusione dei dati, con un'accurata informativa preventiva circa le finalità perseguite, le modalità del trattamento, l'ambito di diffusione, i diritti e le relative modalità di esercizio[1087].

Un grande ausilio è poi offerto dalle licenze standard per il riutilizzo, strumento giuridico necessario, che deve accompagnare l'apertura dei dati; attenzione va prestata anche ai metadati di accompagnamento, previsti a livello normativo ed essenziali per garantire qualità all'apertura dei dati stessi.

In questi casi, poi, come suggerisce anche il Garante, risulta opportuno disporre da parte dell'amministrazione titolare dei dati strumenti e misure tecniche di sicurezza idonee a evitare trattamenti illegittimi dei dati pubblicati, ad esempio trasferimenti massivi per via telematica, e tesi a evitare il rischio di re-identificazione di dati anonimi e quindi della loro trasformazione in dati personali in una prospettiva *privacy by design* conforme al regolamento europeo[1088].

1085 F. PATRONI GRIFFI, *op. cit.*, p. 10.

1086 S. CALZOLAIO, *op. cit.*, p. 198 ss.

1087 M. ALOVISIO, *op. cit.*, pp. 45-64. Anche nella nota vicenda della pubblicazione su Internet dei redditi dei cittadini italiani relativi all'anno 2005, uno dei profili rilevati dal Garante nella censura di illegittimità della pubblicazione consisteva nella mancata idonea e preventiva informativa ai contribuenti relativa all'ambito di diffusione dei dati; sulla vicenda M. CONTE, *E-government e privacy*, in L. DE PIETRO (a cura di), *Dieci lezioni per capire e attuare l'e-government*, Marsilio Editori, Venezia, 2011, p. 186 ss.

1088 E. BASSI, *PSI, protezione dei dati personali, anonimizzazione*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 65-83.

Nel bilanciamento da compiere da parte delle amministrazioni, sono da tenere in considerazione, quale ausilio, proprio gli atti, i provvedimenti e le linee guida delle diverse autorità coinvolte, in particolare il Garante per la protezione dei dati personali, ma anche l'Anac e l'AgID: nell'intreccio complesso tra istanze e interessi diversi si intrecciano anche le competenze delle autorità previste a tutela dei diversi interessi in gioco, che sono chiamate a collaborare ed evitare tensioni che, confondendo ulteriormente i soggetti deputati ad applicare le norme, nuocerebbero all'intero sistema[1089].

Se è vero che le amministrazioni non sono responsabili di eventuali trattamenti illeciti da parte di soggetti privati riutilizzatori dei dati delle amministrazioni, dal momento che i riutilizzatori saranno a loro volta tenuti a rispettare le disposizioni in materia, il ruolo dei poteri pubblici è fondamentale per diminuire il rischio di abusi e favorire un generale clima di fiducia della collettività verso l'operato pubblico[1090].

Naturalmente, in caso di violazioni e abusi, si configurerà la possibilità di azionare meccanismi di controllo, tutela e sanzione "successivi", in modo conforme

---

[1089] Secondo E. CARLONI, *Le linee guida del Garante: protezione dei dati e protezione dell'opacità*, cit., p. 1113 ss., mentre nelle linee guida del 2011 non si percepisce una funzione di contenimento, ma al contrario di promozione della trasparenza, nelle linee guida del 2014 si coglie un "arroccamento" del Garante a difesa dell'equilibrio, trovandosi in una potenziale tensione istituzionale con l'autorità che si trova davanti e che è in qualche modo speculare sulla trasparenza, Anac. Di conseguenza, secondo l'Autore, l'interpretazione della normativa da parte del Garante è restrittiva, piena di carica ideologica, antagonista del concetto di trasparenza recato nel d.lgs. 33/2013 e incline anche a una serie di forzature del testo, in particolare nella lettura restrittiva e parziale della norma del riutilizzo (ossia formato di dati aperto e non dato di tipo aperto). In tal modo si assiste a un'evoluzione del Garante verso un ruolo di «garante dell'opacità: un'opacità funzionale al potere, più che alla tutela dei diritti, nel momento in cui si dà sponda, così facendo, ad istanze di riserbo cui da più parti dentro le amministrazioni si aspira»: negando la funzionalità dei principi di trasparenza e apertura si rischia di trasformare la privacy «in alibi di un'amministrazione che rimane restia a riconoscere lo spostamento di potere (a vantaggio non solo del cittadino interessato, ma del "chiunque") […]» (p. 1118).

[1090] Cfr. M. ALOVISIO, *op. cit.*, pp. 45-64, che richiama il provvedimento del Garante per la protezione dei dati personali del 26 marzo 2010, recante *Esonero dall'informativa per un sito web che raccoglie e diffonde dati già disponibili online* (doc. web n. 1721169), in cui il Garante specifica che «è la stessa legge a consentire ai soggetti privati, nei termini e alle condizioni ivi previste, di riutilizzare le informazioni del settore pubblico per finalità anche commerciali (art. 2, comma 1, lett. *e*) del d.lgs. 24 gennaio 2006, n. 36, attuativo della direttiva 2003/98/CE)».

anche in tal caso all'ottica perseguita dal regolamento europeo, ossia garantendo l'efficacia del momento sanzionatorio[1091].

5.4. La protezione dei dati personali e la trasparenza reattiva realizzata con l'accesso civico generalizzato

Il bilanciamento tra il diritto a conoscere e la protezione dei dati personali non riguarda solo la trasparenza proattiva realizzata con la diffusione, ma anche quella reattiva, in particolare quella ottenuta con l'accesso civico generalizzato, strumento previsto dal d.lgs. 33/2013 a seguito delle modifiche e integrazioni del d.lgs. 97/2016 (cosiddetto *Freedom of Information Act* italiano)[1092].

L'introduzione dell'accesso civico generalizzato rende complesso trovare un adeguato bilanciamento tra *right to know* e *data protection*; l'art. 5-bis del d.lgs. 33/2013, inserito dal d.lgs. 97/2016, come esaminato, prevede, infatti, il diniego di accesso se necessario per evitare un pregiudizio concreto alla tutela, tra gli altri interessi privati previsti, della protezione dei dati personali, in conformità con la disciplina legislativa in materia[1093]: ciò implica la necessità di un bilanciamento tra i due diritti in gioco.

Al fine di esaminare l'equilibrio in questo nuovo caso di trasparenza reattiva, particolarmente significativo è il ruolo che hanno giocato le autorità amministrative indipendenti, il Garante per la protezione dei dati personali e l'Anac[1094]: al riguardo è sufficiente pensare alle linee guida adottate da quest'ultima con delibera n. 1309 del 28

1091 Tale spostamento dei meccanismi di tutela dalla protezione preventiva al controllo e sanzione successivi sia per quanto attiene al profilo dell'indicizzazione e della rintracciabilità tramite motori di ricerca web, sia per quanto riguarda il profilo del riutilizzo dei dati è messo in evidenza in B. PONTI, *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, cit., p. 90 ss. e p. 124 ss.

1092 *Supra*, cap. 2.

1093 Art. 5-bis, comma 2, lett. a), d.lgs. 33/2013.

1094 Cfr. A. MONEA, *La nuova trasparenza amministrativa alla luce del d.lgs. 97/2016. L'accesso civico*, cit., p. 1040 ss.

dicembre 2016, recanti indicazioni operative tese proprio alla definizione delle esclusioni e dei limiti all'accesso civico[1095].

Le linee guida dell'Anac, ai fini del bilanciamento, suggeriscono opportunamente, in applicazione del principio di limitazione della finalità, di attenersi alle finalità dell'accesso civico generalizzato, previste esplicitamente all'art. 5, comma 2 del d.lgs. 33/2013 nel «*favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*» e nel *«promuovere la partecipazione al dibattito pubblico*», rispetto alle quali l'accesso civico generalizzato è strumentale e servente.

L'Anac suggerisce di avvalersi del possibile oscuramento dei dati personali, in caso di accoglimento dell'istanza, e di tenere in considerazione le motivazioni addotte dal soggetto interessato che, in tal caso, deve essere obbligatoriamente interpellato[1096], seppur tali motivazioni siano solo un'indicazione e la valutazione spetti all'amministrazione, che deve condurla anche in caso di silenzio dell'interessato.

Le linee guida richiamano le disposizioni sovranazionali e i principi che informano il trattamento, sui quali effettuare il bilanciamento e la valutazione relativa all'accesso, dovendo «scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei "dati personali" in esso presenti, laddove l'esigenza informativa, alla base dell'accesso generalizzato, possa essere raggiunta senza implicare il trattamento dei dati personali»[1097].

In considerazione del rischio di lesione alla tutela dei dati personali e alla dignità stessa della persona, che induce ad attenersi scrupolosamente al principio di proporzionalità e a tutti i criteri della disciplina in materia, le linee guida invitano le amministrazioni a valutare anche le conseguenze scaturenti dal fatto che i dati, laddove forniti a seguito di istanza, sono pubblici (art. 3, comma 1, e art. 7, d.lgs. 33/2013): il rischio consiste in possibili future azioni da parte di terzi nei confronti dell'interessato o

---

1095 L'adozione delle linee guida è prevista dall'art. 5-bis, comma 6, d.lgs. 33/2013.

1096 L'istanza di accesso civico generalizzato, infatti, non richiede motivazione (art. 5, comma 3, d.lgs. 33/2013).

1097 Le linee guida sottolineano al riguardo la maggior celerità del procedimento in caso di oscuramento, potendo accogliere l'istanza senza dover attivare la procedura prevista in caso di controinteressati, ai sensi dell'art. 5, comma 5, d.lgs. 33/2013.

situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso o, ancora, altri svantaggi personali o sociali, come in particolare esposizione a minacce, intimidazioni, ritorsioni o turbative al regolare svolgimento delle funzioni pubbliche o delle attività di pubblico interesse esercitate e, altresì, eventuali furti di identità o di creazione di identità fittizie attraverso le quali esercitare attività fraudolente.

Data la delicatezza del bilanciamento e la gravità delle potenziali lesioni, ai fini di tale valutazione viene suggerito di fare riferimento anche alla natura dei dati e all'eventuale ruolo ricoperto nella vita pubblica dall'interessato; inoltre deve essere posta particolare attenzione nel caso in cui i dati riguardino minori. Tutto ciò porta a ritenere che, in merito alla natura dei dati, sicuramente in caso di dati idonei a rivelare lo stato di salute o la vita sessuale, ma anche in caso di dati sensibili o giudiziari, il bilanciamento, in linea con la diversa natura dello strumento (più ampio, ma meno profondo), si atteggerà diversamente e, in linea di principio, l'accesso andrà negato[1098].

Accanto all'Anac, che si è occupata, nelle proprie linee guida, del profilo del bilanciamento tra istanze di conoscenza e istanze di protezione dei dati personali, al riguardo è significativo anche il parere del Garante per la protezione dei dati personali, reso con provvedimento n. 92 del 3 marzo 2016 sullo schema di quello che poi è diventato il d.lgs. 97/2016.

In merito all'accesso civico generalizzato introdotto dalla riforma, «che estende, in misura rilevante e con pochissimi limiti, i casi di ostensione di dati personali a terzi», il Garante parla chiaramente di significativa compressione del diritto alla protezione dei dati personali. In particolare, il Garante si domanda «come i soggetti pubblici, che detengono grandi banche di dati, anche sensibili, dei cittadini decideranno se accogliere o meno le istanze di accesso al documento contenente dati personali, in assenza di un parametro per effettuare il bilanciamento fra la protezione dei dati personali e l'interesse del richiedente, dal momento che l'istanza non è motivata ed è dunque carente dell'indicazione della finalità perseguita, che costituisce elemento determinante ai fini

[1098] Cfr. E. FURIOSI, *op. cit.*, p. 1 ss. I dati idonei a rivelare lo stato di salute o la vita sessuale tornano in gioco anche nel bilanciamento da compiere in caso di istanza di accesso documentale: il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; art. 60, d.lgs. 196/2003. È il caso del diritto alla difesa; cfr. M.C. CAVALLARO, *op. cit.*, p. 121 ss.

della valutazione della legittimità del trattamento»; questo espone a rischi di applicazione non omogenea delle disposizioni.

La soluzione adeguata per il Garante consiste nella seguente: laddove l'accoglimento dell'istanza possa determinare la comunicazione al richiedente di dati personali di terzi, «l'ostensione del documento può essere effettuata soltanto ove risulti accertata, in atti, la prevalenza dell'interesse perseguito dall'accesso ovvero, previo oscuramento dei dati personali presenti». Tale accertamento, inoltre, deve tenere ovviamente conto di quanto manifestato dal controinteressato, «al quale deve essere sempre data comunicazione della richiesta di accesso», in linea con quanto poi è stato espresso dalle linee guida adottate dall'Anac, che sembrano aver tenuto conto delle parole del Garante. Il Garante, inoltre, ritiene ci sia «un generale divieto di comunicazione di dati sensibili o giudiziari nonché di dati personali di minorenni, in osservanza della tutela rafforzata accordata dall'ordinamento interno e dal diritto dell'Unione europea a tali categorie di dati personali».

Nella sua relazione sull'attività svolta nell'anno 2016, il Garante si è espresso sulla versione finale delle linee guida dell'Anac, in particolare criticando il passaggio secondo cui l'amministrazione è tenuta «a privilegiare la scelta che, pur non oltrepassando i limiti di ciò che può essere ragionevolmente richiesto, sia la più favorevole al diritto di accesso del richiedente»: in proposito il Garante ha ribadito che tale passaggio non può essere interpretato «nel senso di accordare una generale prevalenza al diritto di accesso generalizzato a scapito di altri diritti ugualmente riconosciuti dall'ordinamento (quali, ad es., quello alla riservatezza e alla protezione dei dati personali)». In tal modo, infatti, «si vanificherebbe il necessario bilanciamento degli interessi in gioco che richiede un approccio equilibrato nella ponderazione dei diversi diritti coinvolti, tale da evitare che i diritti fondamentali di eventuali controinteressati possano essere gravemente pregiudicati dalla messa a disposizione a terzi – non adeguatamente ponderata – di dati, informazioni e documenti che li riguardano», bilanciamento cui sono tenute le amministrazioni nel dare applicazione alla disciplina in materia di accesso generalizzato, come peraltro ribadito dalle stesse linee guida sull'accesso civico.

In caso contrario, secondo il Garante si genera il rischio di comportamenti irragionevoli in contrasto con la disciplina internazionale ed europea per quanto attiene

alla tutela della riservatezza e del diritto alla protezione dei dati personali (vengono espressamente richiamati l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, la direttiva 95/46/CE, il regolamento (UE) 2016/679)[1099].

5.5. Equilibri tra trasparenza, apertura e privacy

In conclusione, l'analisi relativa alle contrapposte istanze di trasparenza (proattiva e reattiva) e apertura, da un lato, e protezione dei dati personali, dall'altro, mostra che su alcuni profili si riesce a raggiungere un bilanciamento già all'interno delle disposizioni, che devono semplicemente essere applicate, grazie a valutazioni compiute *ex ante* dal legislatore e basate su criteri quali la proporzionalità rispetto alla finalità di trasparenza[1100], mentre su altri profili l'equilibrio diventa problematico ed emerge il nuovo corso intrapreso dalla trasparenza, con un suo rafforzamento nel senso dell'apertura, in coerenza con l'evoluzione impressa dalle norme al modello di amministrazione digitale che guarda all'*open government*[1101].

Tale potenziamento del valore della trasparenza, della conoscibilità e dell'informazione ai cittadini deriva dal fatto che questi principi, anche grazie alle ultime riforme, diventano regola nell'agire dei pubblici poteri[1102]. Ciò non porta a inficiare la tutela del diritto alla *data protection*, ma comporta in concreto la necessità di garantire *ex ante* trasparenza e apertura, tese a realizzare valori costituzionali quali il buon andamento dell'amministrazione (grazie al controllo pubblico) e lo sviluppo culturale, sociale ed economico (grazie al riutilizzo dei dati), con un'attenzione alla "realizzazione tecnica della *data protection*" per mezzo di *privacy by design*, *privacy by default*, valutazione d'impatto sulla protezione dei dati e *accountability* (strumenti previsti nella disciplina europea), intervenendo successivamente in via repressiva ed

---

1099 Relazione del Garante sull'attività svolta nell'anno 2016, sezione quarta, p. 31 ss.

1100 I. NICOTRA, *op. cit.*, p. 10.

1101 *Supra*, cap. 1, § 2.

1102 I. NICOTRA, *op. cit.*, p. 1 ss.

efficace al verificarsi di violazioni o abusi sui dati personali. L'alternativa di una preventiva e cautelare maggiore chiusura non risulta coerente con la società contemporanea e con i pilastri di un'amministrazione digitale aperta, rischiando di distanziare maggiormente istituzioni e cittadini, in direzione inversa rispetto all'epoca contemporanea che chiede a gran voce fiducia, partecipazione, collaborazione e capacità di bilanciamento dei diritti.

5.6. *Data protection* e *big data*

L'economia dei dati deve basarsi sulla fiducia, che a sua volta si traduce in efficaci strumenti di protezione della persona e dei suoi dati personali, riducendo al minimo i rischi. Ne è consapevole l'Europa e per questo da anni una significativa sfida consiste proprio nel «fare in modo che i pertinenti quadri giuridici e le politiche, ad esempio in materia di interoperabilità, protezione dei dati, sicurezza e diritti di proprietà intellettuale, favoriscano l'uso dei dati, al fine di rafforzare la certezza giuridica per le imprese e infondere nei consumatori la fiducia nei confronti delle tecnologie per i dati»[1103].

Anche a tali fini nasce il processo di riforma che ha portato al regolamento europeo in materia di protezione dei dati personali, teso a rendere omogenea la tutela, a migliorare la certezza giuridica e a rafforzarne l'effettività e la correlata fiducia, ben sapendo quanto siano a rischio i dati personali nell'era contemporanea, caratterizzata dalle correlazioni algoritmiche dei *big data*[1104].

Il regolamento (UE) 2016/679 mostra la consapevolezza di dover disciplinare la società degli algoritmi e un mondo dominato dai *big data*, consapevolezza che emerge

---

[1103] Comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014. In tal senso anche la comunicazione della Commissione europea «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017, che però avverte anche: «le preoccupazioni relative alla privacy sono legittime, ma non devono essere utilizzate dalle amministrazioni pubbliche come motivo per limitare il libero flusso dei dati in modo ingiustificato».

[1104] Comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014: l'intenzione dell'Europa è di «definire un unico quadro normativo per la protezione dei dati che sia moderno, solido, coerente ed esaustivo».

sia nei principi che negli strumenti, così come nell'attenzione ad alcuni aspetti, si pensi alla profilazione, esplicitamente definita[1105], ma non scioglie in modo espresso le problematiche giuridiche che originano dai *big data* né si riferisce mai in modo esplicito agli stessi[1106].

La natura e le caratteristiche che connotano i *big data* e le relative modalità di utilizzo mostrano con evidenza elementi di criticità nel rispetto della disciplina in materia di protezione dei dati personali[1107]. Al riguardo, è sufficiente pensare alla mancata consapevolezza e conoscenza degli individui in merito a ciò che sarà fatto con i loro dati o allo sviluppo delle analisi predittive, che aspirano a trarre inferenze sul futuro partendo da correlazioni e analisi algoritmiche, superando lo stesso concetto di profilazione cui guarda la disciplina in materia di *data protection* e rischiando di minare profondamente il diritto all'autodeterminanzione informativa degli individui e la loro libertà[1108]. La "svendita" al ribasso dei dati personali a fronte di servizi migliori e calibrati sull'individuo rischiano di rendere la privacy un privilegio di cui può beneficiare solo chi è disposto a pagare in termini monetari e di tempo per servizi maggiormente "costosi" e, allo stesso tempo, maggiormente rispettosi dei dati personali: risulta evidente come questo possa creare nuove forme di discriminazione e disuguaglianza[1109].

[1105] L'art. 4, paragrafo 1, n. 4), reg. (UE) 2016/679 la definisce 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*».

[1106] Sulla tematica cfr. i documenti dell'*European Data Protection Supervisor* (di seguito anche EDPS).

[1107] G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 23: «nel rendere i dati "più grandi" e nel "trovare", che sono le due attività che caratterizzano lo schema Big Data, non si può escludere che le "sfere di influenza dei dati" collidano le nostre "sfere private", ovvero implichino il trattamento dei nostri dati personali, o interessino dati relativi a "cose" che ci appartengono o che sono a noi intimamente legate».

[1108] A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 138 ss. e M. OREFICE, *op. cit.*, p. 711.

[1109] Cfr. M. OREFICE, *op. cit.*, p. 711 e G. COLANGELO, *op. cit.*, p. 451, che ricorda in proposito come alcuni *provider* offrano ai propri utenti anche una riduzione del corrispettivo pagato per i servizi offerti in cambio dell'autorizzazione all'utilizzo e alla condivisione dei dati personali (*pay-for-pricing*).

La tutela dei dati personali necessita di una ridefinizione per adeguarsi ai *big data*, che lungi dall'essere uno strumento della nostra epoca contemporanea, costituiscono più ampiamente la nuova configurazione dei dati capace di informare la realtà digitale stessa: come si è avuto modo di esaminare, non si limitano a una diversa e più ampia dimensione quantitativa, ma determinano un cambiamento di natura sostanziale capace di mutare il modo di conoscere presente e futuro, il controllo e la "misurazione" di fatti e persone e le capacità di analisi e predizione dell'uomo[1110].

Sotto il profilo della *data protection*, in specifico, l'utilizzo dei *big data*, laddove siano presenti dati personali, rende particolarmente difficile il rispetto del principio di limitazione della finalità che permea la normativa, dal momento che spesso nelle strategie basate sui *big data* al momento della raccolta non si conosce il risultato atteso, essendo capaci di condurre a risultati imprevisti di indubbio interesse. Nei *big data*, inoltre, proprio per le dimensioni e la varietà di fonti e per la correlata tendenza a utilizzare quanti più dati possibili per aumentare la probabilità di avere risultati interessanti, è difficile rispettare anche adeguatezza, pertinenza e limitazione dei dati personali a quanto necessario rispetto alle finalità del trattamento (minimizzazione dei dati).

I principi di limitazione della finalità e di minimizzazione dei dati, particolarmente difficili da rispettare nell'era dei *big data* e degli algoritmi, costituiscono però il fondamento della disciplina europea, garantendo da una parte il rispetto dell'individuo e della sua libertà di autodeterminazione e dall'altra, altresì, lo stesso mercato, ponendosi come limite alla creazione di posizioni dominanti[1111].

Di conseguenza, in specifico, l'uso dei *big data* rischia costantemente di scontrarsi con i principi di cui all'art. 5, comma 1, regolamento (UE) 2016/679, secondo cui i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (limitazione della finalità) (lett. b) e devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati) (lett. c). Il principio di finalità

1110 Più ampiamente, *supra*, cap. 3.

1111 E. NUNZIANTE, *op. cit.*, p. 9.

e gli altri principi relativi al trattamento dei dati personali sono presenti e regolati anche nella vigente normativa italiana[1112].

Il profilo relativo al difficile rispetto dei principi di limitazione della finalità e *data minimization* comporta conseguenti difficoltà a garantire l'informativa e il consenso, elementi fondamentali sui cui ruota ancora l'attuale disciplina a livello europeo, che rischiano di vanificarsi dal momento che nell'utilizzo dei *big data* non si conoscono preventivamente gli scopi: tutto questo, di conseguenza, può inficiare la stessa liceità del trattamento[1113]. Si pongono, infatti, problemi al momento di fornire le informazioni previste, che includono il fatto che gli interessati debbano sapere anche se i loro dati saranno trasmessi al di fuori dell'Unione europea e con quali garanzie[1114], e al momento di acquisizione del consenso, che deve essere libero, preventivo, specifico, inequivocabile, revocabile[1115]: in merito a cosa viene prestato il consenso se non si conoscono preventivamente le finalità di utilizzo dei *big data*?

La raccolta e l'analisi di enormi insiemi di dati rischia, inoltre, di inficiare la qualità, l'esattezza e l'accuratezza dei dati, principi di riferimento della disciplina in materia di privacy[1116].

1112 In specifico, nell'art. 11, comma 1, lett. b), d.lgs. 196/2003 si prevede che questi siano «*raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi*» e nell'art. 11, comma 1, lett. d), d.lgs. 196/2003, altresì, che siano «*pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati*». Rileva anche l'art. 3 del d.lgs. 196/2003, secondo cui «*i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità*».

1113 Cfr. F.H. CATE - V. MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, vol. 3, n. 2, 2013, pp. 67-73.

1114 Artt. 13-14, reg. (UE) 2016/679.

1115 Art. 7, reg. (UE) 2016/679. La vigente normativa italiana, il d.lgs. 196/2003, prevede parimenti l'informativa all'art. 13 e il consenso all'art. 23, elementi cardine sui quali ruota la *data protection* europea e nazionale.

1116 Art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679 e art. 11, comma 1, lett. c), d.lgs. 196/2003. Cfr. E. NUNZIANTE, *op. cit.*, p. 8.

Pertanto, nei *big data* e nelle caratteristiche che li connotano si annidano criticità ontologiche rispetto alla disciplina prevista a tutela dei dati personali.

Fermi tali aspetti problematici, nella gestione giuridica dei *big data* possono rivelarsi di proficuo utilizzo alcuni principi contenuti nel regolamento (UE) 2016/679, che mirano a un approccio sistematico, a un atteggiamento proattivo e a una ponderazione *ex ante* dell'impatto e dei rischi sulla *data protection*. È il caso dei principi paradigmatici della nuova disciplina europea: *privacy by design*, *privacy by default* e *Data Protection Impact Assessment*.

L'art. 25 del regolamento (UE) 2016/679, nel primo comma recante il principio *privacy by design*, prevede, infatti, 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, 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 debba mettere in atto «*misure tecniche e organizzative adeguate, quali la pseudonimizzazione*»[1117], «*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 regolamento e tutelare i diritti degli interessati*». Emerge l'approccio proattivo e preventivo, centrato sull'utente fin dalla progettazione.

A questo paradigma di *privacy by design* si collega strettamente quello di *privacy by default*, significativamente posto nel secondo comma dell'art. 25 del regolamento (UE) 2016/679: il titolare deve mettere 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*»[1118]. Di

---

[1117] La pseudonimizzazione è prevista nell'art. 4, paragrafo 1, n. 5), reg. (UE) 2016/679.

[1118] Art. 25, paragrafo 2, reg. (UE) 2016/679; il terzo comma prevede che un meccanismo di certificazione, approvato ai sensi della normativa, possa esser utilizzato come elemento per dimostrare la conformità ai requisiti dell'approccio *privacy by design* e *privacy by default*.

conseguenza, le impostazioni predefinite devono rispettare i principi della disciplina in materia di protezione dei dati personali, quali la minimizzazione dei dati e la limitazione della finalità.

In questa disposizione si coglie l'attenzione all'utente e all'inevitabile squilibrio di potere in cui verte nella società dominata dai *big data*: mantenendo la sua libertà, lo si tutela in modo rafforzato per mezzo di misure tecniche e organizzative adeguate. La norma è calata nella realtà dei "grandi dati": si diffida e si impedisce opportunamente l'accesso a un numero indefinito di persone fisiche da parte di macchine (senza l'intervento della persona fisica) e l'obbligo si calibra su aspetti centrali e problematici dei *big data* quali la quantità di dati, la portata del trattamento, il periodo di conservazione e l'accessibilità.

I due principi, *data protection by design* e *data protection by default*, inverano un concetto di privacy all'interno della stessa tecnologia, una *privacy tecnica* per impostazione predefinita: il diritto si serve della tecnologia per assicurare il rispetto dei suoi principi imprescindibili e garantire la tutela della dignità e dello sviluppo della persona[1119]. Si comprende intuitivamente l'importanza di questo aspetto nelle recenti evoluzioni tecnologiche, si pensi all'*Internet of Things*.

Interessante, altresì, l'art. 35 del regolamento (UE) 2016/679, relativo al c.d. *Data Protection Impact Assessment*: quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento, «*una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*»; una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati

[1119] Cfr. A. MANTELERO, *Privacy digitale*, cit., p. 159, secondo cui il ricorso a regole volte a conformare le tecnologie al dettato normativo permette di innalzare la soglia di prevenzione «inibendo sin dall'origine già a livello tecnico la realizzazione dei comportamenti vietati, rendendo così il mezzo stesso inadeguato alla commissione di attività dannose o illecite, con un'efficacia che sarà tanto maggiore quanto più risulterà arduo superare la barriera strutturale apposta» (p. 162). C. FOCARELLI, *op. cit.*, p. 63 parla della tecnologia che "aggiusta" se stessa, "antidoto" sistemico ai rischi della raccolta e dell'utilizzo di dati personali di massa, di solito più efficace di qualsiasi rimedio giuridico, ma avverte, altresì, sui limiti e sui rischi della sostituzione del diritto con la tecnica.

analoghi. In particolare la valutazione d'impatto sulla protezione dei dati è richiesta nei casi seguenti:

«*a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico»[1120].

I casi previsti, che riguardano principalmente operazioni di profilazione e monitoraggio degli utenti, trattamenti su larga scala di particolari categorie di dati e sorveglianza sistematica[1121], si attagliano particolarmente bene al contesto dei *big data*.

Il verificarsi delle ipotesi previste comporta la necessità di svolgere la valutazione d'impatto sulla protezione dei dati, che si prevede debba possedere dei requisiti minimi, dal momento che deve contenere almeno: una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione dei rischi per i diritti e le libertà degli interessati; le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione[1122].

L'approccio preventivo, trasparente e proattivo, che responsabilizza il titolare del trattamento e, sinergicamente, attribuisce strumenti di consapevolezza e poteri all'individuo a tutela dei suoi dati, è evidente anche nell'esaminato diritto alla portabilità dei dati (art. 20), che riduce il rischio di *lock-in* e favorisce la concorrenza tra

---

1120 Art. 35, comma 3, reg. (UE) 2017/679.

1121 M.G. STANZIONE, *op. cit.*, p. 1249 ss.

1122 Così art. 35, comma 7, reg. (UE) 2017/679.

le piattaforme[1123]. Anche altre norme del regolamento europeo 2016/679 in materia di protezione dei dati personali possono risultare funzionali sotto il profilo della gestione dei *big data*, come la consultazione preventiva (art. 36)[1124], la figura del *Data Protection Officer* (art. 37)[1125] e la *data breach notification* (artt. 33-34)[1126].

Particolarmente interessante nel contesto dei *big data* è la previsione dedicata al «*processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*», di cui all'art. 22 del regolamento (UE) 2016/679. Si chiarisce che «*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*». Ma la portata della previsione si riduce nel comma 2, dal momento che non si applica al verificarsi di alcune condizioni, in particolare «*nel caso in cui la decisione:*

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato».

1123 *Supra*, § 1.2. G. COLANGELO, *op. cit.*, p. 455 e E. NUNZIANTE, *op. cit.*, p. 11.

1124 Il titolare, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto di cui all'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate per attenuare il rischio.

1125 La nomina è prevista con la funzione di garantire una corretta gestione dei dati in una serie di casi, come quello in cui il trattamento richieda il monitoraggio regolare e sistematico degli interessati su larga scala e quello di trattamento, su larga scala, di categorie particolari di dati personali.

1126 Il titolare ha l'obbligo di notificare eventuali violazioni dei dati personali all'autorità nazionale nei tempi e nelle modalità previste dall'art. 33. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo, ai sensi dell'art. 34. Sono previsti casi in cui la comunicazione non è richiesta: sostanzialmente il titolare può evitare di informare gli interessati se dimostra di aver utilizzato adeguate misure di sicurezza tecniche e organizzative, se ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato o se informarli può comportare sforzi sproporzionati (un caso può essere il numero particolarmente elevato dei soggetti coinvolti): in tale ultima ipotesi è richiesta una comunicazione pubblica o misure simili.

Nel caso del consenso, come laddove sia necessaria per la conclusione o l'esecuzione del contratto, il titolare del trattamento deve attuare «*misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*»[1127].

L'approccio preventivo al rischio, che scaturisce dalla *privacy by design*, dalla *privacy by default*, dalla valutazione d'impatto e dagli altri strumenti analizzati, comporta la volontà di ridurre, se non eliminare, le possibili violazioni del diritto alla protezione dei dati personali nella società dei *big data* e degli algoritmi[1128].

Emerge, altresì, l'attenzione alla sicurezza e il ricorso ad effettive tecniche di anonimizzazione che permettano di non applicare la disciplina, ma che per farlo non devono consentire la reversibilità[1129]. Il rischio però si annida proprio qui, ossia nelle inferenze che possono essere tratte su gruppi o individui da dati anonimi, grazie anche alla disponibilità di dati ausiliari riferibili alle persone[1130]: emerge la conseguenza che, di fatto, nessun dato è totalmente anonimo e può finire per essere personale e, come tale, esigere l'applicazione della relativa disciplina[1131]. Da questo punto di vista la stessa definizione di "dato personale" può generare problemi, dal momento che, oltre a quelli anonimi (che non è detto restino tali), ci possono essere dati afferenti a gruppi o comunità, che appartengono cioè a più persone, oltre ad essere in gioco anche i metadati

---

1127 Art. 22, paragrafo 3, reg. (UE) 2016/679. Ai sensi del comma 4 dell'art. 22 «*le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato*».

1128 M. MENNELLA, *Privacy e nuove tecnologie*, in M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014, p. 207 ss.

1129 E. NUNZIANTE, *op. cit.*, p. 11.

1130 Secondo G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 34 ss. la disponibilità di dati ausiliari riferibili alla persona cui collegare il dato anonimizzato è in grado di compromettere le tutele dell'anonimizzazione: l'operazione di valutazione non dovrà essere *una tantum*, ma periodica, dal momento che i dati disponibili cambiano nel tempo, così come le tecnologie di riferimento.

1131 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 33 ss. Secondo G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 34 ss., in linea di principio, in relazione a un dato anonimizzato non può mai essere scongiurato il rischio di attribuzione arbitraria a una persona, ma laddove il processo di anonimizzazione sia corretto, l'attribuzione sarà casuale.

e i frammentari *digital exhaust* delle operazioni compiute in rete, estremamente significativi nel contesto dei *big data*[1132]: questi dati sono personali e possono riceverne la relativa tutela[1133]?

Inoltre, a fronte degli strumenti esaminati del regolamento europeo, che si attagliano, seppur con alcune criticità, al nuovo contesto e possono essere impiegati proficuamente nell'ambito dei *big data*, non mancano disposizioni che fanno storcere il naso, come la norma che prevede la finalità del *marketing* diretto e la connessa profilazione come legittimo interesse che consente e giustifica il trattamento dei dati personali, con un meccanismo di tutela di *opt-out* tramite opposizione dell'interessato, che non sembra congruo e conforme all'intenzione di elevare la tutela dei dati personali[1134].

Anche sul consenso preventivo grazie a sistemi di *opt-in* va constatato che in realtà il problema sta nel continuare a considerare il consenso individuale come elemento capace di legittimare il trattamento e perfino il processo decisionale automatizzato (in tal caso deve trattarsi di un consenso esplicito), anche nel mutato contesto dei *big data*, dove il consenso preventivo, libero ed esplicito può essere ottenuto a fronte di vantaggi perseguibili, come prezzi personalizzati, mercificando e sicuramente svendendo la protezione dei dati personali[1135].

1132 C. FOCARELLI, *op. cit.*, p. 28 ss. sottolinea come non sia chiaro se i metadati, ossia "i dati sui dati", debbano rientrare o meno nel concetto di "dati". In proposito l'Autore richiama il Report del maggio 2014 dell'*Executive Office* del Presidente degli Stati Uniti «*Big Data: Seizing Opportunities, Preserving Values*», in cui si rileva che nell'era dei *big data* a tali dati dovrebbe essere accordata una tutela rafforzata, dal momento che possono rivelare dati sulla persona e non sono meno problematici dei dati personali veri e propri sotto il profilo della *data protection*.

1133 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 33 ss.

1134 Considerando 47 e art. 21, paragrafo 2, reg. (UE) 2016/679: «*Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto*». Cfr. M. OREFICE, *op. cit.*, p. 736.

1135 G. COLANGELO, *op. cit.*, p. 455: «La convinzione che il consenso possa rappresentare il principale elemento di legittimazione anche nel contesto digitale espone ogni intervento normativo (compreso il recente Regolamento europeo 2016/679) all'esito tragico dello sforzo di Sisifo, specie se si considera che non si intravedono modelli di business alternativi rispetto a quelli che ricavano profitti dalla profilazione degli utenti e dalla pubblicità».

In altre parole risulta questionabile che sia ancora solido il paradigma basato su informativa e consenso, replicato e presente nel regolamento europeo, e che il consenso possa considerarsi libero e informato e tale da poter rendere legittimo il trattamento o il processo decisionale automatizzato. Del resto ne è consapevole anche il regolamento quando al considerando 42 chiarisce che «*il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio*»: non è forse questa la condizione nei rapporti con le piattaforme dei colossi della rete e in un mondo di *big data*? Tutti i trattamenti che necessariamente avvengono nelle elaborazioni algoritmiche sui *big data* che comprendono dati personali necessitano allora di altri fondamenti di liceità? Non è un caso che le stesse imprese spesso ricorrano ad altre condizioni legittimanti per fondare la liceità delle proprie attività, quali l'esecuzione di un contratto di cui l'interessato è parte o il legittimo interesse di cui all'art. 6, comma 1, lett. b) e f) del regolamento europeo[1136]. Ma anche in relazione a questi fondamenti emergono perplessità, a ben vedere, nel primo caso (esecuzione di un contratto) in considerazione dello squilibrio tra le parti e nell'altro per il dubbio che prevalga il legittimo interesse sui diritti e sulle libertà fondamentali dell'interessato, che richiedono la protezione dei dati personali.

Inoltre non va dimenticato che nel caso dei soggetti pubblici il trattamento è possibile senza il consenso, dal momento che si fonda su altri presupposti di liceità. In tali casi, però, i poteri possono anche essere più incisivi di quelli privati, proprio in considerazione del ruolo rivestito e delle connesse prerogative impositive e sanzionatorie: risulta evidente come un uso distorto, finalizzato per esempio al controllo o alla sorveglianza, che possa ledere la protezione dei dati personali, nel contesto pubblico possa essere persino più grave in termini di danni arrecati, che comprendono anche la perdita di fiducia dei consociati verso le istituzioni[1137]. Sui pericoli che si corrono non va dimenticata la *lectio magistralis* a livello planetario offerta in proposito dal *Datagate*.

In considerazione di tali pericoli, di conseguenza, in ambito pubblico è necessario mantenere uno stretto collegamento tra trattamento e governo dei dati, da una parte, e

---

[1136] Cfr. E. NUNZIANTE, *op. cit.*, p. 8.

[1137] G. CARULLO, *op. cit.*, p. 193 ss.

funzione istituzionale esercitata, dall'altra, in un'ottica di funzionalizzazione che opportunamente emerge nel regolamento (UE) 2016/679, nell'art. 6, comma 1, lett. e) e nei considerando 45 e 46: la gestione del dato deve essere strettamente correlata all'esercizio in concreto di una funzione pubblica e rispettare il principio di proporzionalità, altrimenti si verificherà un'illegittimità, per violazione di legge o per eccesso di potere[1138]. Questo vale anche nel rapporto tra istituzioni: il trasferimento non giustifica l'utilizzo per fini incompatibili con quelli della raccolta. La natura pubblica del soggetto che gestisce i *big data*, infatti, non mitiga necessariamente le problematiche e i pericoli posti da questi dati, ma, in considerazione dei poteri posseduti, può addirittura aggravarli in caso di abusi[1139].

L'approccio preventivo di analisi sui rischi per la protezione dei dati personali è fatto proprio anche dalle «*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*», adottate il 23 gennaio 2017 dal Comitato della Convenzione del Consiglio d'Europa per la protezione dei dati (nota anche come "Convenzione 108") e dedicate proprio alla protezione dei dati personali nel contesto dei *big data*. Nelle linee guida la definizione di *big data* non riguarda solo i *big data ex se* nelle loro caratteristiche di volume, velocità e varietà, ma anche l'analisi dei dati stessi con l'uso di software allo scopo di estrarre conoscenze nuove e predittive per finalità decisionali relative a individui e gruppi (*big data analytics*).

Le linee guida precisano opportunamente la necessità di un diritto di controllo sui dati più ampio, non circoscritto all'individuo, ma tale da comprendere una valutazione dei rischi per la collettività, che tenga conto del contesto sociale e tecnologico. L'esigenza, infatti, è prevenire i potenziali effetti negativi dell'utilizzo dei *big data* sulla dignità umana, sulle libertà e sui diritti fondamentali degli individui, quali polarizzazioni dell'analisi, pregiudizi e discriminazioni, la sottovalutazione delle implicazioni legali, sociali ed etiche, la marginalizzazione di un efficace e informato coinvolgimento dell'individuo.

In merito sono richiamati i principi del regolamento (UE) 2016/679 sulla protezione dei dati personali, quali la minimizzazione dei dati, la limitazione delle finalità, la correttezza e la trasparenza, il consenso libero, specifico e informato, che,

---

1138 G. CARULLO, *op. cit.*, p. 193 ss.

1139 M. FALCONE, *op. cit.*, p. 601 ss.

come esaminato, risultano di difficile attuazione e che, di conseguenza, vanno adeguati al nuovo contesto. Per farlo e renderli più efficaci nella realtà dei *big data*, nelle *guidelines* sono indicate alcune direttrici da seguire:

- è necessario rispettare l'uso etico, consapevole e socialmente responsabile dei dati, che comporta al momento dell'analisi del rischio la valutazione circa la possibilità di conflitto con altri diritti e valori, soprattutto laddove le informazioni siano impiegate per scopi predittivi nei processi decisionali[1140];
- l'approccio preventivo di valutazione dei rischi, sopra richiamato, deve considerare anche l'impatto giuridico, sociale ed etico dell'utilizzo dei *big data* sia a livello individuale che collettivo (garantendo parità e non discriminazione) e condurre a sviluppare e implementare misure appropriate per mitigare il rischio (soluzioni *by design* e *by default*), accompagnandole dal monitoraggio sull'adozione e sull'efficacia delle stesse[1141];
- il rispetto del principio di limitazione delle finalità e del principio di trasparenza deve essere garantito, in modo da evitare che i dati siano ulteriormente elaborati in modo inaspettato, inappropriato o discutibile per l'interessato;
- è necessaria l'implementazione dei paradigmi *privacy by design* e *privacy by default* volti alla minimizzazione dei dati, sia nella raccolta che nell'analisi degli stessi per mezzo di anonimizzazione e pseudonimizzazione, che è utile a ridurre i rischi per gli interessati;
- in merito al consenso, deve essere agevolata la comprensione delle operazioni sulle quali l'interessato deve esprimere il relativo consenso per mezzo dell'utilizzo di interfacce grafiche che simulino l'utilizzo dei dati e il potenziale impatto sull'interessato, fermo restando che il consenso non è da intendersi liberamente reso in condizioni di chiaro squilibrio di potere, atto a influenzare le decisioni dell'interessato, e che l'onere della prova al riguardo spetta al titolare (la

---

[1140] In tal caso le linee guida, laddove emerga un forte impatto, suggeriscono ai titolari l'istituzione di un comitato etico *ad hoc* o l'affidamento a quelli esistenti, in ogni caso soggetti indipendenti.

[1141] Le verifiche da parte dei titolari devono essere periodiche, documentate e vanno tenute in considerazione nella valutazione di possibili sanzioni amministrative; se l'impatto è significativo sui diritti e sulle libertà fondamentali, i titolari dovrebbero consultare le autorità di controllo per chiedere consigli.

prova riguarda il fatto che non esiste squilibrio o che questo non pregiudica il consenso);

- l'anonimizzazione comporta la valutazione del rischio di re-identificazione tenendo conto del tempo, degli sforzi o delle risorse necessarie alla luce della natura dei dati, del contesto, delle tecnologie e dei costi. La prova sull'adeguatezza delle misure di anonimizzazione spetta ai titolari, che possono combinarle ad obblighi legali e contrattuali e devono esaminare regolarmente i rischi di re-identificazione;
- l'importanza del ruolo dell'intervento umano nei processi decisionali basati sull'analisi dei *big data*, che va preservato nella sua autonomia, deve tenere conto di tutte le circostanze (e non basarsi su informazioni decontestualizzate o semplici elaborazioni di dati) e deve consentire la libertà di non fare affidamento e la relativa possibilità di assumere decisioni diverse da quelle consentite dall'analisi dei dati, fornendo peraltro all'interessato informazioni circa le modalità di assunzione delle decisioni[1142];
- la cultura digitale, l'istruzione, l'informazione e la formazione dovrebbero essere considerate abilità educative essenziali degli individui, da sviluppare al fine di comprendere le implicazioni sottese all'utilizzo dei *big data*.

Le linee guida, peraltro, prevedono l'applicazione del procedimento di analisi del rischio anche agli *open data*, in considerazione dei pregiudizi che possono causare, laddove siano usati per estrarre inferenze e informazioni su singoli e gruppi, anche se anonimizzati, in considerazione della fusione di *dataset* diversi.

Le *guidelines* evidenziano la centralità che va garantita alla persona, alla sua autonomia e al suo diritto di controllo sui dati nel contesto dei *big data*.

Sulla necessità di porre al centro l'individuo e consentirgli di scegliere se vuole o meno essere tracciato si è espresso anche l'*European Data Protection Supervisor* (EDPS), che ai fini della protezione dei dati personali ritiene sia necessaria una stretta cooperazione tra autorità distinte e una connessione forte tra tutele giuridiche diverse

---

[1142] Anche in tal caso spetta ai titolari dimostrare l'assenza di discriminazioni, laddove ci siano indicazioni che portano a supporre che si sia generata una discriminazione diretta o indiretta basata sull'analisi dei *big data*. I soggetti, interessati da una decisione basata sui *big data*, la possono contestare davanti all'autorità competente.

che si intrecciano nei *big data*: privacy, tutela della concorrenza e dei consumatori; tra i casi di operazione congiunta tra autorità si richiamano le procedure concernenti le condizioni contrattuali e l'informativa per la protezione dei dati personali[1143].

Nel complesso bilanciamento tra la conoscenza ottenuta dall'utilizzo dei *big data* e la protezione dei dati personali risulta centrale esaminare le finalità dell'utilizzo dei *big data*: se le finalità non sono connesse alla tutela di interessi generali, quali l'uguaglianza, l'ampliamento dei diritti e l'esercizio della sovranità popolare, ma al contrario sono tese al potere o a ragioni economiche e di controllo sociale (anche laddove motivato da esigenze di sicurezza), la compressione della protezione dei dati personali sarà da considerare eccessiva e sproporzionata. È pur vero che la Carta costituzionale protegge il titolare del trattamento, per mezzo della tutela statica della proprietà e della tutela dinamica dell'iniziativa economica privata (artt. 41 e 42), così come forse anche nella libera manifestazione del pensiero configurata dal trattamento (art. 21)[1144], ma dall'altra parte la protezione dei dati personali, seppur non espressamente e direttamente prevista, è funzionale agli articoli 1, 2 e 3 della Costituzione e, dunque, ai diritti fondamentali dell'uomo: da un punto di vista gerarchico e valoriale, non è giustificabile una compressione e un indebolimento della stessa a fronte di quelle istanze, se non a rischio di inficiare i valori fondanti delle società democratiche, basate saldamente sulla dignità e sullo sviluppo della persona[1145]. È necessario quindi bilanciare i diritti in gioco, prestando attenzione all'interesse pubblico generale che si viene a proteggere[1146].

Alla luce di tali considerazioni, gli strumenti del regolamento europeo 2016/679, per quanto consapevoli e mirati a perseguire un rafforzamento della protezione dei dati

---

1143 *Preliminary Opinion* dell'EDPS *«Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*», marzo 2014 e *Opinion* 8/2016 dell'EDPS «*Opinion on coherent enforcement of fundamental rights in the age of big data*» del 23 settembre 2016. Nel parere preliminare del 2014 il Garante europeo sottolinea la catena del valore dei dati personali composta da quattro fasi: raccolta e accesso; *storage* e aggregazione; analisi e distribuzione; utilizzo di *dataset* personali.

1144 A.C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, cit., p. 324.

1145 M.F. DE TULLIO, *op. cit.*, p. 637 ss.

1146 C. FOCARELLI, *op. cit.*, p. 163 ss.

personali nell'era dei *big data* e degli algoritmi, non risultano sufficienti, perché, anche se riescono ad arricchire il quadro con elementi e approcci proattivi e preventivi al rischio, non mutano radicalmente la logica sottesa, che resta basata sulla minimizzazione dei dati, sulla limitazione della finalità, sull'informativa e sul consenso del singolo, che come esaminato in tale contesto sono sostanzialmente svuotati di contenuto e rischiano di ridursi a meri formalismi, alla luce dell'abissale squilibrio tra le parti in gioco[1147]. È difficile nel mondo dei *big data*, infatti, informare, chiedere e dare il consenso su elaborazioni che non si sa dove porteranno e su scopi per lo più ignoti al momento della raccolta[1148]. L'informativa deve diventare in realtà un'operazione reale di trasparenza e un modo per rendere consapevole la persona: per tali motivi deve essere capace di attirarne l'attenzione (e un'informativa testuale non è affatto detto raggiunga lo scopo), senza ridursi ad un passaggio burocratico e noioso che divide l'utente dal servizio cui vuole accedere e che, di conseguenza, viene saltato fornendo una rapida e inconsapevole accettazione[1149]. Il consenso e l'esercizio dei diritti condividono questa stessa esigenza: la consapevolezza della persona, che significa anche la sua libertà.

Lo stesso approccio preventivo e tecnico alla *data protection*, che emerge dal regolamento, rischia di scricchiolare nell'efficacia laddove si basi anche sull'anonimizzazione, che è sostanzialmente irraggiungibile ed espone sempre al rischio di re-identificazione, facilitata dai *big data* stessi[1150].

Nel mutato contesto, invece, può effettivamente essere fruttuosa la maggiore responsabilizzazione e la logica di *accountability* dei soggetti che trattano i dati personali, che pervade oggi il regolamento europeo, accompagnata dall'effettività e dall'efficacia del sistema sanzionatorio correlato[1151].

I diritti fondamentali della dignità e dello sviluppo della persona perseguiti dalla protezione dei dati personali, così come dagli altri diritti oggetto di analisi, fanno emergere la necessità dell'intervento dei poteri pubblici, ontologicamente chiamati a

---

1147 M. FALCONE, *op. cit.*, p. 601 ss.

1148 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 208: «Nel contesto dei big data, la vecchia e fidata idea dell'informazione preventiva a cui segue il libero consenso appare spesso troppo restrittiva per fare emergere il valore latente dei dati, o troppo vaga per proteggere la privacy degli individui».

1149 G. D'ACQUISTO - M. NALDI, *op. cit.*, p. 31 ss.

1150 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, pp. 208-209.

1151 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 231 ss.

tutelarli. Per farlo, come sarà esaminato nel prossimo capitolo, è necessario immaginare nuove tutele dei diritti e più ampiamente un nuovo diritto adatto a una realtà fatta di intrecci di dati e di algoritmi[1152].

[1152] In merito alla *data protection*, secondo V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 207 l'interrogativo da porsi «non è se i big data accrescono il rischio per la privacy (questo è sicuro), ma se vengono a modificare la natura del rischio. Se la minaccia è semplicemente più estesa, la legge e le regole che tutelano la privacy potrebbero funzionare ancora nell'era dei big data; basta solo raddoppiare gli sforzi. Ma se il problema si modifica, dovremo trovare nuove soluzioni. Sfortunatamente, il problema si è trasformato», dal momento che il valore delle informazioni non sta più esclusivamente nello scopo primario, ma negli utilizzi secondari e questo mina la disciplina basata sull'individuo, sulla sua informazione preventiva e sul suo consenso.

Capitolo 6

Dati, diritto e diritti: conclusioni e scenari futuri

SOMMARIO: 6.1. La centralità della persona nel governo dei dati: una nuova etica digitale. – 6.2. Il cambiamento nell'articolazione del rapporto tra pubblico e privato. – 6.2.1. Pericoli di *closed government*, asimmetria, controllo e sorveglianza. – 6.2.2. Possibili rimedi: verso gli *open big data* e le tutele collettive dei diritti? – 6.3. I nuovi equilibri tra diritti e la nuova fisionomia del diritto: suggestioni future.

6.1. La centralità della persona nel governo dei dati: una nuova etica digitale

La società contemporanea poggia sui dati, capaci di caratterizzare intimamente la vita presente e futura: le attività, i processi, le relazioni, le decisioni e persino le predizioni si basano sui dati. I dati e le informazioni, protagonisti indiscussi dell'era digitale, si stagliano come risorse essenziali e strategiche per lo sviluppo economico, sociale e culturale, sulle quali i tradizionali poteri statuali cercano di confermare la propria sovranità, ma nuovi dinamici soggetti privati sono capaci di affermare il proprio dominio: la crescita, il progresso e l'innovazione sono inscindibilmente legati alla gestione dei dati[1153].

La centralità acquisita dai dati è capace di coinvolgere l'essere umano stesso: come rileva Floridi, tramite i dati le tecnologie si atteggiano come "tecnologie del sé" e

[1153] L'Europa è consapevole della centralità dei dati e tale convinzione emerge nelle esaminate comunicazioni della Commissione europea, quali «*Dati aperti. Un motore per l'innovazione, la crescita e una governance trasparente*», COM(2011) 882 def. del 12 dicembre 2011, «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014 e «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017.

arrivano a plasmare le persone e le loro identità[1154]. Non a caso si parla di *data subject*[1155]: «noi siamo le nostre informazioni»[1156], vale a dire che «il sé è concepito come un sistema informazionale complesso, costituito da attività, ricordi e storie in cui si esprime la nostra coscienza di sé»[1157]. Di conseguenza, oggi i dati formano la

---

[1154] Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., p. 67 ss., secondo cui «ogni singolo dato può contribuire a descrivere l'identità personale di qualcuno» (p. 71). L'Autore sottolinea quanto le ICT siano diventate importanti «nel dare forma alle nostre identità personali. Si tratta infatti delle più potenti *tecnologie del sé* alle quali siamo mai stati esposti», da gestire con attenzione, «poiché stanno modificando in maniera significativa i contesti e le pratiche attraverso le quali diamo forma a noi stessi. […] Il sé sociale è il principale canale attraverso cui le ICT, e in particolar modo i social media interattivi, esercitano il loro profondo impatto sulle nostre identità personali».

[1155] Nell'*Opinion* 4/2015 «*Towards a new digital ethics. Data, dignity and technology*» dell'11 settembre 2015, l'*European Data Protection Supervisor* (EDPS) avverte sul pericolo che le pratiche di potenti governi e soggetti privati possano ridurre la persona a mero *data subject*, minacciando i diritti e le libertà fondamentali.

[1156] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., p. 78. In merito S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 394 ss. «Anche se è eccessivo, e persino pericoloso, dire che "noi siamo i nostri dati", è tuttavia vero che la nostra rappresentazione sociale è sempre più affidata a informazioni sparse in una molteplicità di banche dati, ed ai "profili" che su questa base vengono costruiti, alle simulazioni che permettono. Siamo sempre più conosciuti da soggetti pubblici e privati attraverso i dati che ci riguardano, in forme che possono incidere sull'eguaglianza, sulla libertà di comunicazione, di espressione o di circolazione, sul diritto alla salute, sulla condizione di lavoratore, sull'accesso al credito e alle assicurazioni, e via elencando. Divenute entità disincarnate, le persone hanno sempre più bisogno di una tutela del loro "corpo elettronico"» (pp. 396-397).

[1157] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., p. 78. Questo, come spiega l'Autore, ha implicazioni estremamente significative sull'incoporazione del sé (il sé richiede una piattaforma fisica, che non è detto debba essere il corpo, a sua volta costituito da informazioni), sullo spazio (si trascorre larga parte del tempo in un luogo consentito dalle ICT diverso dal luogo dove siamo fisicamente collocati), sul tempo, sulla memoria e sulle interazioni, sulla percezione (lo sguardo digitale), sulla salute e sull'istruzione. In merito alla percezione «il sé cerca di percepire se stesso come percepito dagli altri, facendo affidamento sulle ICT che agevolano fortemente l'esperienza dello sguardo rivolto su di sé» (p. 83). L'Autore parla di quarta rivoluzione, in considerazione del «modo in cui le ICT hanno prodotto talune significative trasformazioni nella nostra storia (l'iperstoria), nel nostro ambiente (l'infosfera) e nello sviluppo dei nostri sé (l'esperienza onlife). Alle radici di queste trasformazioni sembra esserci una profonda svolta filosofica nel nostro modo di concepire il posto e il ruolo "speciali" che abbiamo nell'Universo. Si tratta di una quarta rivoluzione nella comprensione di noi stessi […]» (pp. 97-98).

proiezione sociale dell'identità; la persistenza o meno dei dati determina il ricordo individuale e collettivo[1158]; la capacità di controllare i dati personali plasma il rispetto della privacy e la propria autodeterminazione informativa; i dati generano diritti di proprietà intellettuale, ma, al tempo stesso, facendo leva sui pilastri dell'accesso e della condivisione, permettono un'espansione inedita del diritto a conoscere, anche nei confronti delle istituzioni.

In questo coinvolgimento profondo dell'uomo, i dati necessariamente investono i complessi equilibri tra diritti e libertà, il bilanciamento tra interessi contrapposti e la tenuta dei principi democratici fondamentali, determinando giustizia e progresso della convivenza civile e influenzando fortemente la direzione etica del futuro. Di conseguenza, il diritto all'esistenza digitale, quale metaforico ombrello atto a ricomprendere i diversi diritti scaturenti dalla libertà informatica, è anche diritto al governo dei dati, sui quali l'esistenza digitale si basa, e analogamente il governo della *digital society* passa necessariamente dalla *data governance*, da intendersi proprio come tutela delle libertà e dei diritti nelle diverse fasi di gestione e nelle differenti configurazioni dei dati: l'impatto profondo e pervasivo sulla vita umana da parte dei dati, quali cellule elementari delle informazioni e della conoscenza, consente di poter parlare oggi di *data society*.

Il governo dei dati e la correlata tutela dei diritti sono questioni ineludibili per il diritto, affinché sia capace di proteggere la persona nella sua esistenza nell'era digitale.

Nel mondo dei dati, nelle loro diverse "forme" e nei relativi strumenti di conoscenza (trasparenza, *open data*, *big data*)[1159] diventano difficili gli equilibri tra diritti che paiono confliggere tra loro nella loro essenza ontologica, senza possibilità di

---

[1158] Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., p. 81, che sottolinea come il virtuale non funziona sempre correttamente e ciò che è vecchio e datato può non invecchiare. Peraltro «quanto più accumuliamo ed esternalizziamo i nostri ricordi, tanto più delimitiamo dal punto di vista narrativo la costruzione e lo sviluppo delle nostre identità personali. Accrescendo i nostri ricordi, riduciamo anche lo spazio di libertà di cui godiamo nel ridefinire noi stessi. Dimenticare è parte integrante del processo di costruzione di sé» (p. 82).

[1159] Per l'analisi dei *closed data* e della trasparenza, *supra*, capitolo 2; per l'analisi degli *open data* e dei *big data*, *supra*, capitolo 3.

giungere a una pace duratura, che certo non può essere trovata stabilendo una gerarchia, in quanto sono tutti dotati di indiretto fondamento costituzionale[1160].

La possibilità e la libertà di avere, diffondere e condividere informazioni possono violare i dati della persona e, allo stesso tempo, la sua identità; l'ubiquità e la persistenza delle informazioni, che facilitano conoscenza e memoria, possono, però, confliggere con il diritto ad essere dimenticati; la libera circolazione dei contenuti e la libertà di informazione, la condivisione della conoscenza e la volontà di generare nuova conoscenza possono intaccare la protezione del diritto d'autore, che a sua volta può entrare in conflitto con la *data protection*; *a contrario* il rafforzamento e l'ampliamento del diritto all'identità, alla protezione dei dati personali, all'oblio e alla proprietà intellettuale possono limitare il diritto all'informazione, alla conoscenza e alla memoria[1161].

Connessioni di dati generano connessioni e scontri tra diritti, cui è necessario rivolgere l'attenzione.

L'impossibilità di risolvere "gerarchicamente" i conflitti, soprattutto laddove si voglia stilare una "classifica" assoluta di vincitori e vinti in caso di scontro tra istanze afferenti ai diversi diritti esaminati, porta a un bilanciamento necessariamente "mobile", che però a ben guardare trova un fondamento solido su cui far leva, che rende i diversi diritti indivisibili, seppur nella loro conflittualità[1162].

[1160] Attraverso l'interpretazione evolutiva della clausola aperta dei diritti della personalità contenuta nell'art. 2 della Costituzione è possibile includere le molteplici libertà coinvolte dalle tecnologie informatiche, che per lo più sono fondate anche su una serie di ulteriori norme costituzionali, come già esaminato nel corso dell'analisi. In specifico, trovano fondamento nell'art. 2 Cost. il diritto all'identità e il diritto all'oblio, quest'ultimo correlato anche strettamente al diritto alla protezione dei dati personali, che si fonda a sua volta, oltre che sull'art. 2, anche sull'art. 3 e fornisce matrice ideale agli artt. 13, 14 e 15, il diritto a conoscere, che si basa anche sull'art. 21 C. e sugli artt. 1, 3 e 9 Cost., e il diritto d'autore, fondato altresì su un complesso combinato di ulteriori norme costituzionali, in particolare gli artt. 3, 9, 21, 33, 35, 36, 41 e 42. Più ampiamente, *supra*, capitoli 4 e 5.

[1161] Si pensi al *caso Peppermint* del 2007; *supra*, cap. 4.

[1162] S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 394 parla di indivisibilità e non gerarchizzabilità dei diritti in rete.

Tutti i diritti esaminati, infatti, poggiano e convergono sulla centralità della tutela della persona[1163], in particolare sulla dignità e sullo sviluppo della stessa e questo, peraltro, costituisce il condiviso fondamento costituzionale[1164], che si situa nella clausola aperta dei diritti della personalità di cui all'art. 2 Cost.

La persona con la sua identità, intesa in un'accezione ampia[1165], fondata sull'art. 2 della Costituzione, funge da prisma i cui riflessi sono costituiti dai diversi diritti in gioco: l'identità digitale valorizza la rappresentazione sociale di sé e quindi la persona calata nel proprio contesto sociale di riferimento; il diritto all'oblio esplode la proiezione di quella identità nel tempo ed evidenzia l'esigenza della sua contestualizzazione, dal momento che la persona cambia e simmetricamente deve mutare anche la percezione esterna per mezzo di una contestualizzazione delle sue informazioni; la protezione dei dati personali fa emergere il diritto di controllo da parte

---

1163 Chiara la centralità della persona nel regolamento (UE) 2016/679 in materia di *data protection*; si pensi al considerando 4, secondo cui «*il trattamento dei dati personali dovrebbe essere al servizio dell'uomo*». G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 32 pone come punti fermi, anche in periodi di emergenza, «i diritti dell'uomo e la garanzia di un'attenzione ai principi fondamentali e alla libertà della persona nell'era tecnologica e del controllo, ponendo al centro dell'analisi l'individuo e la sua azione in una società che, comunque, vede nella sicurezza un obiettivo ormai irrinunciabile, ma nella quale non risulta sempre facile trovare un fruttuoso equilibrio tra tessuto normativo, terrore diffuso e privacy dell'individuo».

1164 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 154 ss.: nella Costituzione non compare il termine "soggetto", ma ci si riferisce alla "persona", oltre che nell'art. 2, in diversi articoli significativi, quali gli articoli 3, 13, 23, 27, 32, 111, 119. La "persona", nella ricostruzione costituzionale, si lega al principio di dignità di cui agli artt. 3, 32, 36 e 41: persona e dignità sono concetti inseparabili nell'art. 1 della Carta dei diritti fondamentali dell'Unione europea. Sulla centralità della persona e della sua dignità si esprime l'*European Data Protection Supervisor* (EDPS) nell'*Opinion* 4/2015 «*Towards a new digital ethics. Data, dignity and technology*» dell'11 settembre 2015, che richiama l'art. 1 della Carta dei diritti fondamentali dell'Unione europea: «*la dignità umana è inviolabile. Essa deve essere rispettata e tutelata*».

1165 Secondo G. RESTA, *Identità personale e identità digitale*, cit., p. 511 ss. l'identità «non viene più vista come dato preesistente (ossia come proiezione esterna di un patrimonio individuale già delineato nelle sue caratteristiche distintive), bensì come processo, costantemente in atto, aperto ad una pluralità di esiti e continuamente esposto all'interferenza, capillare e pervasiva, delle varie forme di potere sociale»: l'ordinamento esercita un ruolo attivo di supervisione e controllo (e non di astensione e non interferenza), al fine di restituire il più possibile all'individuo la capacità di perseguire politiche dell'identità personale liberamente definite, sottraendolo al rischio di normalizzazione.

della persona e la sua autodeterminazione informativa, permettendo di tutelare i dati che costituiscono la persona stessa; la persona, oltre al diritto a essere "conosciuta" correttamente nella sua rappresentazione "qui e ora" ha anche diritto a conoscere, dal momento che la conoscenza è determinante nella costruzione e nello sviluppo della propria identità e, in particolare, ha diritto a conoscere nei confronti dei poteri pubblici per essere "informata" e consapevole, potendo di conseguenza agire pienamente il suo ruolo di cittadino e svolgere le connesse prerogative; la protezione del diritto d'autore mira a tutelare i frutti della creazione intellettuale della persona, che concretizzano l'estrinsecazione "materiale" dello sviluppo della stessa.

Allora sono davvero ontologicamente in conflitto i diritti che maggiormente vengono in gioco nel governo dei dati o è errato l'assunto di partenza e qui si annida parte del problema e anche della soluzione?

Nelle fasi di gestione e nelle diverse configurazioni dei dati i diritti possono certamente entrare in contrasto, ma il bilanciamento "mobile" può fondarsi saldamente sulla persona, con un ripensamento del presunto conflitto tra i diritti sotto l'alveo dello stesso "io digitale" da proteggere e senza bisogno di trovare né vincitori, né vinti. Emerge la persona con la sua identità ampiamente intesa quale *data subject*, come luogo di sintesi dei diversi diritti che sono indirizzati in modo convergente alla sua protezione. Di conseguenza, il complesso bilanciamento, da effettuarsi caso per caso, si fonderà sulla tutela della persona, che tutti quei diritti in diverso modo esprimono, e sugli interessi pubblici generali coinvolti nei diversi casi concreti[1166].

Del resto anche le esaminate[1167] «*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*», adottate il 23 gennaio 2017 dal Comitato della Convenzione del Consiglio d'Europa per la protezione

---

[1166] In tal senso G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 591 ss., in relazione specificamente al bilanciamento tra diritto all'oblio e gli altri diritti che vengono in gioco. In tale ottica, in relazione alla privacy, secondo M.F. DE TULLIO, *op. cit.*, p. 646 «i *big data* possono essere funzionali tanto allo sviluppo economico o al potere autoritario quanto all'uguaglianza, ai diritti fondamentali e all'esercizio consapevole della sovranità popolare, che costituiscono il valore-scopo […]. In base a tale valore-scopo, il valore-mezzo – cioè lo sfruttamento dei dati – può pesare di più o di meno nel bilanciamento con la *privacy*; quindi l'equilibrio ottimale potrà variare a seconda di quale sia il valore-scopo concretamente perseguito, visto che ve n'è più d'uno teoricamente possibile».

[1167] *Supra*, cap. 5.

dei dati, si preoccupano «*to ensure that persons are placed at the centre of our digital economies and that their rights and fundamental freedoms are upheld*».

Basandosi sul fondamento costituito dalla protezione della persona quale *data subject*, tra i diversi diritti emergono significativi punti di contatto e convergenza, che si deducono proprio dai dati stessi.

In ogni configurazione di dati (*small*, *big*, *closed*, *open*) rileva l'importanza dei metadati per descrivere i dati stessi. La rilevanza dei metadati si connette più ampiamente all'esigenza di qualità dei dati, che afferisce alla loro esattezza, al loro aggiornamento e alla loro contestualizzazione. La qualità è, del resto, richiesta e prevista nelle diverse normative e nei vari atti di riferimento[1168] e, nelle caratteristiche specifiche in cui si concretizza, emerge come aspetto importante e, a volte, dirimente nei casi giurisprudenziali di conflitto tra interessi, si pensi alla contestualizzazione per la tutela dell'identità e del diritto all'oblio[1169].

Sull'esigenza di qualità e sulla presenza di adeguati metadati convergono, pertanto, i diversi diritti confliggenti, dal momento che la qualità garantisce un'informazione capace di generare conoscenza e non un'oscura trasparenza e di tutelare l'identità, permette di proteggere i dati personali in conformità alle previsioni normative, consente di collocare temporalmente il dato in conformità con il diritto all'oblio e si traduce nella corretta attribuzione della paternità/titolarità dei dati stessi.

Sotto tale profilo emerge un altro strumento utile nei rapporti tra soggetti e nelle relazioni tra diritti: le licenze, che permettono la contestualizzazione dell'informazione e l'emergere delle limitazioni al suo utilizzo.

La tutela dei diversi diritti implicati nel governo dei dati trova un significativo punto di convergenza anche nell'approccio preventivo *by default* e *by design* basato sull'*accountability*, che fa leva sulla tecnologia e sulla sicurezza, da una parte, e sulla responsabilizzazione e sulla consapevolezza dei soggetti, dall'altra, grazie anche ad efficaci sistemi sanzionatori: si tratta di un metodo preventivo atto a confinare le repressioni prevalentemente alla tutela sanzionatoria successiva, anche al fine di non

---

[1168] Art. 53, d.lgs. 82/2005; art. 6, d.lgs. 33/2013; art. 5, paragrafo 1, lett. d), reg. (UE) 2016/679; art. 11, comma 1, lett. c), d.lgs. 196/2003.

[1169] Cfr. sentenza della Corte di Cassazione 5 aprile 2012, n. 5525.

reprimere eccessivamente la libera circolazione dei dati e la diffusione della conoscenza[1170].

Tale approccio al rischio, che emerge nel regolamento europeo 2016/679 sulla *data protection*, ben si attaglia al rispetto anche degli altri diritti esaminati: sicuramente ne guadagnano la protezione dell'identità e dell'oblio, strettamente connessi alla tutela dei dati personali, ma anche il diritto alla conoscenza, che poggia su informazioni integre, contestualizzate e veritiere, e il diritto d'autore, che potrebbe parimenti trovare una forma di protezione tecnica, ad esempio nelle informazioni elettroniche sul regime dei diritti o nei *digital rights management* (DRM), quali informazioni associate ai dati che recano le regole di utilizzo dei dati stessi[1171], rimettendo a un momento successivo una repressione efficace che concretizzi l'importanza della responsabilità, in linea con tale ottica.

Si delinea un approccio centrato sulla persona, fondato sulla qualità dei dati, sulla presenza di metadati e su adeguate licenze, che si serve della tecnica per una tutela *by default* e *by design* e che responsabilizza i soggetti, reprimendo in modo efficace le violazioni. Una tale logica, attenta alla sicurezza e alla conformazione dei sistemi

---

[1170] In relazione al diritto all'oblio e alla protezione dei dati personali, G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 402 ss. suggerisce una revisione del modello con alcuni necessari aggiustamenti e il necessario supporto della tecnologia, in particolare suggerisce di non basarsi solo sul consenso dell'interessato, ma sulla maggiore responsabilità e *accountability* del titolare, affidandosi anche alla tecnologia: «il giurista, sistematizzato lo scenario e individuati i valori di riferimento, non può non affidarsi alla tecnologia. L'apporto della tecnologia è essenziale, e appare chiaro che l'effettività del diritto in un mondo digitale possa essere garantita solo attraverso la tecnologia. Una volta che il diritto ha stabilito le regole e i principi, compito della tecnologia è attuarli» (p. 403). L'Autrice fa l'esempio di molte tecnologie utilizzabili a questi scopi: DRM, scadenza nell'uso dei dati personali, contestualizzazione; mancano infatti in Internet l'attribuzione di un peso relativo, di una valutazione dell'informazione pubblicata, e la presenza di informazioni atte a completare o anche modificare il quadro. In relazione al diritto all'oblio, E. STRADELLA, *op. cit.*, p. 28 ss. sottolinea l'opportunità di spostarsi da una tutela *ex post* a una protezione *ex ante*, rafforzando la responsabilità in termini di *accountability* dei gestori dei dati e fortificando la cultura degli individui, superando i tradizionali schemi di consenso informato che non proteggono sufficientemente il singolo nel contesto dei *big data*.

[1171] Deve essere posta attenzione, però, a non prevedere misure tecnologiche di protezione particolarmente restrittive della libertà e della condivisione. *Supra*, capitolo 4, § 4.1. Sull'utilizzo a tali fini dei *Digital Rights Management* (DRM) anche in associazione ai dati personali (ad esempio natura, finalità, interessato, titolare), cfr. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, cit., p. 403.

tecnologici per mezzo dei quali si governano i dati, si basa su una valutazione di impatto preventiva ai rischi atta a confinare le repressioni prevalentemente *ex post* e capace, in tal modo, di conferire il corretto risalto al potere giurisdizionale, senza dover arrivare ad attribuire bilanciamenti e poteri troppo incisivi ad autorità amministrative indipendenti diverse dall'autorità giudiziaria.

Nell'analisi della disciplina emerge con evidenza, infatti, che il bilanciamento fra diritti di fondamento costituzionale si basa principalmente e naturalmente sul quadro normativo, che però talvolta è incapace di dare indicazioni puntuali in merito al complesso equilibrio da trovare in casi concreti di governo dei dati. Come esaminato nel corso dell'analisi, la normativa di riferimento in alcuni casi (come il diritto d'autore) nasce in un diverso momento storico e risulta particolarmente adeguata alla realtà analogica, ma gli adattamenti nel tempo non sono sufficienti a permettere di tutelare e conciliare in modo soddisfacente i diritti nel mondo digitale; in altri casi (la normativa sulla protezione dei dati personali e la normativa sulla trasparenza) la disciplina, seppur nuova e innovativa in relazione a molti aspetti, mantiene logiche del passato e non tratta esplicitamente problematiche, che si trovano rimesse al bilanciamento da effettuare nel momento conflittuale[1172].

Di conseguenza, al fine di assicurare effettiva protezione ai diritti, nella normativa si assiste al ricorso a soluzioni dotate di una medesima matrice a fondamento, che consiste nell'attribuzione a un'autorità o ad altro soggetto indipendente, quale sorta di "garante" dello specifico diritto, dell'onere di gestire amministrativamente la tutela concreta, i bilanciamenti e le questioni di conflitto, assolvendo all'arduo compito di cercare l'equilibrio tra diverse istanze. Fermo il possibile ricorso alla magistratura, questi soggetti assumono inevitabilmente un ruolo centrale, incisivo e profondo nel governo dei dati e nella tutela dei diritti, nell'attuazione delle disposizioni e nella gestione delle fattispecie concrete.

È il caso dell'Anac per quanto concerne la *freedom of information* e il diritto alla conoscenza nei confronti delle istituzioni: il ruolo dell'autorità nell'interpretazione delle norme, nei bilanciamenti tra interessi e nell'attuazione delle disposizioni è centrale,

[1172] *Supra*, capitolo 2, capitolo 4, § 4, e capitolo 5.

come emerge, ad esempio, nelle linee guida sui limiti al diritto di accesso civico generalizzato[1173].

Nel caso del diritto d'autore un ruolo, fin troppo incisivo secondo alcuni, che ha fatto sollevare anche una questione di legittimità costituzionale, assume l'Agcom con le previsioni del regolamento che le attribuiscono poteri effettivi di una certa rilevanza nel bilanciamento tra diritto d'autore e conoscenza[1174].

Sulla protezione dei dati personali, ma anche su identità e oblio un ruolo di estremo rilievo, confermato nella sua strategicità anche dal nuovo regolamento europeo, possiede l'autorità di controllo, il Garante per la protezione dei dati personali, solidamente previsto dalla normativa e accompagnato da figure analoghe europee e dall'*European Data Protection Supervisor* (EDPS); nei provvedimenti e linee guida, come esaminato, il Garante spesso affronta il bilanciamento tra *data protection* e trasparenza, la complessa tutela della privacy nelle diverse configurazioni dei dati (*open data*, *big data*) e anche il rapporto con il diritto d'autore, oltre ad affrontare identità e oblio. Di conseguenza, il ruolo del Garante sui dati personali inevitabilmente si amplia e investe il governo dei dati *tout court*, parallelamente all'ampio raggio d'azione della disciplina (come esaminato in relazione al regolamento europeo) che si occupa non solo di *data protection*, ma più ampiamente di *data governance*. Questa opera di bilanciamento, però, non ha mancato di sollevare perplessità nei casi in cui ha fortemente ridimensionato o forzato la normativa, per mezzo di una sorta di interpretazione autentica, anche quando le disposizioni non si sono conformate al parere preventivo espresso dal Garante stesso, mostrando quindi una diversa volontà del legislatore: è il caso degli *open data* e del diritto al riutilizzo[1175].

Nel governo dei dati, al fine condiviso di tutelare i singoli diritti, si profilano contrasti tra i poteri dell'ordinamento: il potere legislativo viene "corretto", ridimensionato o spinto a normare da interventi del potere giurisdizionale, ma anche delle autorità amministrative indipendenti, cui è attribuita la tutela dei singoli diritti e il cui ruolo nel governo dei dati risulta, di conseguenza, particolarmente significativo.

1173 Le linee guida sono state adottate dall'Anac con delibera n. 1309 del 28 dicembre 2016; *supra*, capitolo 2, § 4.2.

1174 Il regolamento è stato adottato dall'Agcom con delibera 680/13/CONS; *supra*, capitolo 4, § 4.1.

1175 *Supra*, capitolo 5, § 3.2.

Nel bilanciamento tra conoscenza, memoria e privacy non va poi dimenticato il ruolo che, oltre al potere giurisdizionale e alle autorità amministrative di controllo, detengono di fatto soggetti di natura privata, i motori di ricerca, in seguito alla sentenza *Google Spain*[1176], potenti arbitri di fatto della visibilità o meno dei dati nelle ricerche, capaci di incidere profondamente, di conseguenza, sulla libertà di conoscenza e sulla necessità di memoria. È un bilanciamento tra il diritto del singolo alla protezione dei dati personali e il diritto della collettività all'informazione e alla conoscenza, che desta particolari perplessità in considerazione della tipologia di soggetto che lo compie, mosso non certo dall'interesse pubblico generale, ma da un più concreto interesse economico, che inevitabilmente e fisiologicamente rischia di influenzarne le decisioni.

Immaginare e implementare un approccio preventivo e tecnologico al governo dei dati, centrato sulla tutela della persona, basato sulla qualità dei dati e sulla presenza di metadati, può consentire di superare nei fatti le problematiche ingenerate dalla necessità di garantire la tutela affidandosi alle autorità indipendenti per un "supplemento" di regolazione o al potere giurisdizionale per indicazioni sui complessi bilanciamenti o ai colossi del web nella gestione concreta, finendo per attribuire a questi soggetti funzioni che non appartengono loro. Le problematiche che nascono dai conflitti fra i diritti nel governo dei dati talvolta rischiano, infatti, di divenire più complesse nelle regolamentazioni e nelle soluzioni atte a dirimerli, foriere di ulteriori e talvolta persino peggiori contrazioni dei diritti, soprattutto laddove comminate da autorità e soggetti diversi dall'autorità giudiziaria e, in maniera particolarmente preoccupante, da soggetti privati (come Google), in una deriva pericolosa capace di arrecare un *vulnus* ai diritti e al diritto.

La centralità della persona nei bilanciamenti tra diritti e l'approccio descritto al governo dei dati richiamano la necessità che la *data governance* sia guidata non solo da regole giuridiche, che ancora per lo più sono insufficienti o non completamente idonee alla funzione che devono assolvere, ma anche da un nuovo approccio etico[1177]. Per

---

1176 *Supra*, cap. 4, § 3.2.

1177 Sulla necessità di formulare «un quadro etico che possa trattare l'infosfera come un nuovo ambiente meritevole di cura e di attenzione morale da parte degli inforg umani che la abitano» (pp. 253-254), cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., p. 251 ss., secondo cui «ci siamo trasferiti nell'infosfera» ed è mutata la concezione di noi stessi, del mondo e della cultura che avviene adesso «in chiave iperstorica e informazionale, e non più in termini storici e

meglio dire, le regole giuridiche devono derivare ed essere coadiuvate da una nuova etica sociale, che richiama il diritto a svolgere la propria funzione ontologica nella società[1178].

Il diritto, lungi dal potersi atteggiare soprattutto oggi in modo neutrale, deve indirizzare la regolamentazione verso la direzione "positiva" dei valori e dei principi della società democratica, che permettono di ampliare le libertà e rafforzare i diritti, mettere al centro e accrescere le potenzialità di sviluppo della persona nel rispetto della sua dignità, aumentare la partecipazione, migliorare le relazioni e le attività, diffondere e condividere la conoscenza e rendere più eguale e democratica la società. Si tratta, del resto, dei valori che animano gli atti sovranazionali e la stessa Carta costituzionale italiana.

Allo stesso tempo una nuova etica calata nel contesto digitale e il conseguente diritto a quella informato, nel perseguimento di questi valori, sono capaci di comprimere pericolose fughe verso la direzione "negativa" del controllo sociale e della sorveglianza, del dominio incontrollato del potere economico, della conseguente perdita di libertà dei singoli e dell'aggressione nell'identità delle persone, della mercificazione dei dati e della violazione della dignità, dell'asimmetria informativa e dello squilibrio di potere fra chi lo detiene (Stati e soggetti economici) e chi lo subisce.

A rischio, a ben guardare, sono le fondamenta di ogni società democratica e spetta all'uomo impegnarsi in un approccio filosofico ed etico in relazione ai dati, che consideri i cambiamenti imponenti della rivoluzione digitale senza smarrire i propri

---

meccanici». Di conseguenza non rileva tanto il fatto di spostare bit invece di atomi, quanto piuttosto il fatto che la nostra comprensione e teorizzazione dell'essenza e della trama del reale sta mutando e in questo nuovo contesto dati e informazione costituiscono il «nuovo oro digitale e autentica fonte del valore aggiunto» (p. 252): «le ICT stanno creando il nuovo ambiente informazionale in cui le generazioni future trascorreranno la maggior parte del loro tempo» (p. 253).

[1178] Nello specifico ambito dei *big data*, V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 53 ss., dal momento che la legge riguarda valori e non numeri e adesso contano i numeri, si chiedono se la legge possa essere conciliata con i *big data*, sottolineando i problemi etici e filosofici che si pongono al riguardo anche in relazione alla capacità predittiva dei *big data*: è compito del diritto dare un senso al principio di non discriminazione in un contesto di analisi predittive, senza utilizzarle per il controllo sociale e mantenendo la libera volontà degli individui, la loro capacità di scegliere, senza cedere ad approcci deterministici, che rischiano di violare anche i principi di uguaglianza sostanziale.

valori e i propri diritti fondamentali[1179]. Come verrà esaminato più avanti tutto ciò porta più ampiamente a dover riflettere sul ruolo del diritto nella società digitale contemporanea.

Orientata a una nuova etica digitale è l'*Opinion* 4/2015 «*Towards a new digital ethics. Data, dignity and technology*» dell'*European Data Protection Supervisor* (EDPS) dell'11 settembre 2015, secondo cui «*in today's digital environment, adherence to the law is not enough; we have to consider the ethical dimension of data processing*», anche in considerazione del fatto che le problematiche poste dalla *data society* hanno «*engineering, philosophical, legal and moral implications*».

Tra le tendenze che secondo l'EDPS sollevano le più significative questioni etiche e sociali, in particolare in merito all'applicazione dei principi di protezione dei dati, sono richiamati i *big data* (che non a caso figurano come la prima voce), *Internet of Things*, *ambient computing*, *cloud computing*, *personal-data business models*, droni e veicoli autonomi e tendenze con un impatto potenzialmente più ampio a lungo termine, come il *3D bioprinting* e l'intelligenza artificiale.

Per tali motivi è necessario definire «*a new digital ethics, allowing to realise better the benefits of technology for society and the economy in ways which reinforce the rights and freedoms of individuals*». In particolare, per rispondere alla sfida digitale, l'*European Data Protection Supervisor* delinea un «*big data protection ecosystem*» a quattro livelli «*to reinforce rights and to steer, not to block, technological innovation*»[1180]:

«(1) *Future-oriented regulation of data processing and respect for the rights to privacy and to data protection*[1181].

[1179] Secondo T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 676 «le tecnologie non producono solo libertà, per così dire: la tecnologia può essere al servizio dell'uomo buono o cattivo, del governante illuminato o del despota; in uno Stato costituzionale liberale, però, l'indirizzo politico dovrebbe essere sempre rivolto verso interventi che valorizzano e accrescono le libertà dell'individuo, e l'utilizzo delle tecnologie non può che essere strumentale a questo obiettivo».

[1180] In merito spiega l'EDPS che, infatti, le tendenze in corso hanno allargato il divario tra ciò che è possibile e ciò che è legalmente permesso: la protezione dei dati non è un ostacolo, ma è necessaria per un ambiente sostenibile e dinamico.

[1181] In specifico, sono necessarie regole più semplici per la gestione dei dati personali (il regolamento europeo va in questa direzione) e un dialogo più stretto tra i regolatori dei diversi settori che conduca a

(2) *Accountable controllers who determine personal information processing*[1182].

(3) *Privacy conscious engineering and design of data processing products and services*[1183].

(4) *Empowered individuals*[1184]».

Pertanto, seppur con una focalizzazione sui dati personali, l'*European Data Protection Supervisor* tratteggia un approccio etico al trattamento dei dati basato sulla prevenzione, sull'*accountability* e sulla responsabilizzazione, capace di guidare e avvalersi della tecnica e di realizzare soluzioni tecnologiche *by default* e *by design*, servendosi anche di metadati, al fine di rispettare la dignità e i diritti della persona, che anche in tale approccio è messa al centro[1185]. Del resto, lo stesso regolamento europeo in materia di privacy fa riferimento a principi e valori etici, nel momento in cui chiarisce di essere «*inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento*

---

una visione maggiormente coerente e olistica delle diverse problematiche (privacy, tutela dei consumatori, concorrenza).

[1182] La responsabilità richiede l'attuazione di politiche interne e di sistemi di controllo sulla conformità. A questo proposito l'EDPS ribadisce la bontà e la necessità del principio secondo cui i dati devono essere trattati per scopi compatibili (ora, secondo il regolamento europeo, non incompatibili) rispetto a quello specifico della raccolta, al fine di rispettare le legittime aspettative degli individui.

[1183] Al riguardo l'EDPS sottolinea che l'innovazione sociale è sempre stata il prodotto di attività che riflettono le norme sociali del tempo, ma le decisioni di progettazione tecnica non devono dettare la struttura sociale della comunità e delle interazioni, ma piuttosto sostenerne i valori e i diritti fondamentali.

[1184] L'EDPS si riferisce a un «"*prosumer" environment*», che rafforzi e renda responsabili i cittadini circa la necessità di essere consapevoli, critici e informati nelle scelte che compiono. In tale contesto, l'EDPS parla del consenso, che non è l'unica base giuridica di fondamento e, in ogni caso, non assolve i titolari da ciò che fanno con i dati, soprattutto quando ottengono consensi generalizzati all'elaborazione per un'ampia gamma di scopi. Si afferma anche la necessità di poter mettere in discussione e rilevare errori o risultati fuorvianti provenienti dalle elaborazioni degli algoritmi. Viene posta l'attenzione, altresì, alla necessità di un maggior controllo sui dati da parte degli individui, che potrebbe essere raggiunto con l'uso di archivi e banche dati personali, che faciliterebbero la condivisione e la portabilità, essenziale per garantire scelte libere ai consumatori.

[1185] Nell'*Opinion* 4/2015 i metadati sono immaginati per taggare ogni unità di dati personali in modo da descrivere i requisiti della protezione dei dati, ma la soluzione è replicabile anche nel contesto degli altri diritti (identità, oblio, diritto d'autore).

e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche»[1186].

Un nuovo approccio etico è quanto mai necessario, come messo in evidenza anche dall'*European Data Protection Supervisor*, in considerazione del fatto che nelle nuove configurazioni di rapporti tra governanti e governati e, più ampiamente, tra poteri pubblici e soggetti privati si annidano inediti rischi di asimmetrie di potere e nuovi pericoli di sorveglianza, che si stanno già concretizzando e che esigono rapidi rimedi per non rischiare di inficiare il nucleo fondamentale della stessa società democratica e dare spazio a un futuro che non somiglia all'altezza delle aspettative e alla profondità dei valori dell'uomo[1187].

6.2. Il cambiamento nell'articolazione del rapporto tra pubblico e privato

6.2.1. Pericoli di *closed government*, asimmetria, controllo e sorveglianza

I dati sono capaci di ridefinire la sfera pubblica e privata e disegnare nuove geometrie di potere.

Il cambiamento indotto dalla *data society*, come esaminato, investe e forza il rapporto tra governanti e governati che, sotto la spinta della centralità dei dati, della circolazione delle informazioni e del valore della conoscenza, diventa maggiormente orizzontale, connotandosi per l'emersione di un maggiore controllo democratico e dei principi di *open government*[1188]: il nuovo modello prende forma in strumenti di trasparenza proattiva e reattiva, che danno sostanza alla *freedom of information* (è il

---

[1186] Considerando 2, reg. (UE) 2016/679.

[1187] Secondo l'EDPS l'ecosistema digitale delineato nella *Opinion* 4/2015, al centro di una nuova etica digitale, può fungere da contrappeso rispetto alla sorveglianza pervasiva e alle asimmetrie di potere. Tanto più che la dignità, oltre che essere diritto fondamentale in sé, è anche base per altre libertà e altri diritti, come la privacy, e deve in ogni caso essere rispettata. Al riguardo l'EDPS avverte sui rischi che in futuro gli individui siano determinati dalle elaborazioni algoritmiche.

[1188] *Supra*, cap. 1.

caso dell'accesso civico generalizzato introdotto con il d.lgs. 97/2016)[1189], e in strumenti di trasparenza attiva come gli *open data* con il relativo diritto al loro riutilizzo[1190].

Accanto alla promessa di una società più equilibrata, democratica e, alla fine, più giusta, la *data society* mostra anche l'altra faccia della medaglia, il volto oscuro che va in direzione esattamente opposta rispetto ai principi di trasparenza, partecipazione e collaborazione, pilastri di un governo aperto.

Insieme al valore dei dati e della correlata conoscenza, crescono le torsioni tese a limitare l'utilizzo di quei dati in mano a pochi soggetti, sfruttando anche lacune e vuoti normativi e insinuandosi tra i meandri di discipline non perfettamente allineate alla società da regolare. Sulla scena della contemporaneità compaiono i "signori dei dati"[1191]: governi e grandi poteri privati detengono enormi quantità di dati, *i big data*, dai quali estrapolare con rapidi algoritmi un'ampia conoscenza del presente, ma anche del futuro, in relazione ai più svariati ambiti afferenti a fatti, beni e persone[1192].

La società odierna si trova inevitabilmente di fronte a un bivio cruciale: i beni odierni costituiti dai dati, dalle informazioni e dalla conoscenza possono essere utilizzati in direzione di sviluppo e di apertura, ma allo stesso tempo possono condurre a pericolose derive caratterizzate da nuove asimmetrie e squilibri di potere[1193]. A ben vedere si tratta di una dicotomia che caratterizza più ampiamente le tecnologie come "lame a doppio taglio" per dirla con Bauman: servono per un utilizzo, ma tagliano anche da un'altra parte e sono pericolose da utilizzare perché tendono a colpire anche

---

1189 *Supra*, cap. 2.

1190 *Supra*, cap. 3.

1191 A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 135.

1192 *Supra*, cap. 3.

1193 Cfr. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 57 ss., secondo cui la tecnologia è libera dalle antiche schiavitù dello spazio e del tempo, ma porta criticità come il controllo: «l'innovazione porta in dono libertà in misura, e con modalità, mai viste prima ma, al contempo, può garantire grandi poteri di controllo a chi li voglia utilizzare contro l'individuo stesso» (p. 58).

obiettivi non designati e possono servire a scopi non previsti e ad applicazioni non prefigurate[1194].

Nel ruolo cruciale giocato nel governo dei dati dai colossi del web, spinti da finalità economiche e dal profitto, possono configurarsi rischi tangibili per l'intera società: alcuni *big player* grazie ai dati possono, infatti, divenire dominanti sul mercato con rischio di violazione delle norme *antitrust*, delle regole a tutela dei consumatori e dei principi a protezione dei dati personali[1195].

Più ampiamente le azioni dei giganti della rete possono realizzare una sistematica, ampia e profonda violazione dei diritti e delle libertà delle persone. L'asimmetria di potere, infatti, si palesa in diverse e connesse forme: nei tentativi di predire i comportamenti e, di conseguenza, indirizzare l'individuo in rete grazie alle elaborazioni algoritmiche sulle sue tracce digitali e su quelle di coloro che gli somigliano[1196]; nella frammentazione della persona tra profili, navigazioni, *like* e *cookie*; nelle commercializzazioni aggressive, nelle trattazioni e contrattazioni inique, celate dietro formali richieste di consenso e di accettazione di condizioni generali, presentate a soggetti inconsapevoli imprigionati in un'apparente libertà di scelta; nelle conseguenti discriminazioni di prezzo e disuguaglianze economiche, disparità di trattamento e distorsioni del mercato[1197].

Per mezzo di dati, calcoli e algoritmi si creano nel contesto digitale le asimmetrie, le gerarchie, le disparità tipiche della società: la realtà digitale finisce per somigliare nel volto oscuro a quella analogica. Peraltro, al riguardo, come esaminato, anche laddove i dati trattati siano anonimi e non si applichi, di conseguenza, la normativa in materia di protezione dei dati personali, non è affatto detto che attraverso processi di elaborazione non si riesca a identificare i soggetti[1198].

1194 Cfr. Z. BAUMAN - D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, trad. it., GLF Editori Laterza, Economica, Roma-Bari, 2015, p. 86 ss.

1195 *Preliminary Opinion* dell'EDPS *«Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy»*, marzo 2014.

1196 Cfr. D. CARDON, *op. cit.*, p. 31 ss.

1197 Cfr. M.F. DE TULLIO, *op. cit.*, p. 651 ss. e M. OREFICE, *op. cit.*

1198 V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 203 ss.

Il paradosso della società contemporanea basata sui dati sta nel fatto che gli individui si sentono più liberi delle loro scelte, mentre sono costantemente eterodiretti da potenti algoritmi[1199]; dalla soddisfazione dei bisogni si passa alla creazione degli stessi, con un'opera che tenta e seduce consumatori e utenti e offre loro quel che desiderano in base alle preferenze rilevate per mezzo delle loro stesse tracce, in una "scomposizione" e "ricomposizione" che rischia di perdere e dimenticare "l'uomo" da un punto di vista etico[1200]. Nell'assenza di modelli e direzioni[1201], gli utenti cedono dati personali e li scambiano per ottenere vantaggi: non sono forzati, ma in libertà (non autentica) si fanno sorvegliare, ritenendo ragionevole il prezzo da pagare a fronte di ciò che viene offerto[1202].

Mentre i colossi privati sono mossi dalla logica economica del profitto, i soggetti pubblici, invece, sono ontologicamente tenuti a perseguire gli interessi generali, garantire i diritti fondamentali e stabilire, di conseguenza, i principi e le direttrici del governo dei dati: le istituzioni sono tenute a realizzare le condizioni necessarie per il rispetto della dignità e il pieno sviluppo della persona umana nel governo dei dati per mezzo di azioni positive, specifiche e concrete. Si configura una conseguente responsabilità pubblica nel garantire diritti e libertà, componenti essenziali della cittadinanza e precondizione della democrazia.

Di conseguenza, nel caso dei poteri pubblici, il pericolo si fa ancora più minaccioso e si annida nella capacità della "dittatura dei dati" di asservire, oltre ai soggetti privati, anche i governi: come esaminato nel corso dell'analisi, i *big data* possono essere impiegati non solo dalle grandi imprese private, ma anche dai poteri pubblici come supporto alle decisioni e alle previsioni politiche e strategiche in relazione ai diversi ambiti di interesse. Sotto l'egida della protezione di interessi generali, spesso ampliati oltre misura, come la sicurezza nazionale e internazionale, la

---

1199 D. CARDON, *op. cit.*, p. 89 ss. In merito alla "svendita della privacy" G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 25 sottolinea da parte dei cittadini «la percezione quasi naturale di uno Stato di sorveglianza e, in molti casi, la sua accettazione a capo chino» (p. 28).

1200 Z. BAUMAN - D. LYON, *op. cit.*, p. 115 ss.

1201 Secondo C. FOCARELLI, *op. cit.*, p. 169 ss. «il controllo non deriva dall'imposizione di modelli, ma dall'*assenza* di modelli prestabiliti».

1202 Z. BAUMAN-D. LYON, *op. cit.*, p. 3 ss. e C. FOCARELLI, *op. cit.*, p. 155 ss.

lotta al crimine e al terrorismo, l'ordine pubblico e altre esigenze afferenti al "bene collettivo", i dati possono essere gestiti dai pubblici poteri in modo improprio e, da strumento utile per razionalizzare le decisioni, possono trasformarsi in uno strumento di controllo[1203], monitoraggio e sorveglianza della collettività, che incide sull'autodeterminazione del controllato, fino a poter diventare un mezzo inedito di repressione[1204].

Il mondo rischia di prendere la piega distopica del *Panopticon* di Bentham[1205] o della sorveglianza di Orwell in 1984[1206], consentendo modalità più pervasive, capillari e continue rispetto a quei metodi di controllo; c'è chi parla di *superpanopticon* o *post-panopticon*[1207] per evidenziare il rafforzamento del potere dei dominanti sui dominati, ma anche il cambiamento nelle modalità oggi flessibili, seducenti e divertenti tipiche del

---

1203 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 50 ss. individua quattro modalità tipiche di controllo tecnologico, accanto alle modalità tradizionali di controllo che continuano a sopravvivere, magari coadiuvate dalla potenza tecnologica: il dominio della macchina sull'individuo (favorito dalla potenza delle tecnologie e dall'inconsapevolezza dell'utente); il controllo da parte di un individuo verso un altro individuo (controllo *one-to-one*; es. stalking); il controllo aziendale; il controllo globale.

1204 P. TINCANI, *Controllo e sorveglianza*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, p. 19 ss.: «Sebbene alla sorveglianza si guardi spesso con fastidio e con sospetto, è innegabile che essa sia necessaria per rispondere alla richiesta di sicurezza che i cittadini rivolgono alle istituzioni; una richiesta legittima e ragionevole che si associa a una delle ragioni fondamentali – la protezione – per le quali troviamo conveniente vivere in società. Tuttavia, (anche) quando si tratta di protezione e di sicurezza, il passo dal ragionevole all'irragionevole è breve». M.F. DE TULLIO, *op. cit.*, p. 645 individua tre ragioni per le quali la sorveglianza influisce sull'autodeterminazione del controllato: la possibilità di influenzare il soggetto con la minaccia di rivelare particolari compromettenti; la propensione all'autocensura del controllato, dettata dal timore delle conseguenze dei propri comportamenti e delle proprie affermazioni; l'influenza occulta di chi controlla sulle scelte di chi è controllato.

1205 J. BENTHAM, *Panopticon ovvero la casa d'ispezione*, a cura di M. FOUCAULT - M. PERROT, trad. it., Marsilio, Venezia, 1983.

1206 G. ORWELL*, 1984*, trad. it. a cura di G. BALDINI, Mondadori, Milano, 1989.

1207 Cfr. Z. BAUMAN - D. LYON, *op. cit.*, p. 43: secondo Z. BAUMAN «il Panopticon è vivo e vegeto e gode di ottima salute, ha anzi sviluppato muscoli più robusti (elettronicamente potenziati, "cyborghizzati") di quanto avessero mai immaginato Bentham e Foucault», ma oggi non è più il modello o la strategia principale di dominio ed è confinato nelle zone "ingestibili" della società.

consumismo, distanti da connotazioni carcerarie e capaci di incidere anche sul futuro[1208].

Peraltro, come già rilevato, oltre ai *big data* prodotti dai poteri pubblici, in considerazione dei reciproci interessi, i governi possono decidere di servirsi dei dati raccolti e utilizzati dai *big player*, per mezzo di accordi negoziali di collaborazione e, di conseguenza, dare luogo a un controllo indiretto, non certo meno problematico[1209]. Nasce, così, secondo Lessig, una sorta di *Big Brother* moderno, generato dalla collaborazione tra il controllo governativo (*Big Government*) e le grandi aziende tecnologiche (*Big Business*)[1210].

Il *Datagate*, del resto, ha portato alla luce l'esistenza di accordi tra il governo degli Stati Uniti e svariati colossi privati[1211] e ha messo il mondo di fronte a una concreta sorveglianza di massa a livello globale, condotta scandagliando le enormi

---

[1208] Cfr. Z. BAUMAN - D. LYON, *op. cit.* e P. TINCANI, *op. cit.*, p. 35 ss., che contesta il termine Panopticon per l'epoca contemporanea, dal momento che non esiste un monopolio nel controllo, ma si moltiplicano i centri di dominio con il conseguente indebolimento dei governi; inoltre, per essere tale, non dovrebbe rimanere scoperto alcun aspetto della vita dei dominati. I punti deboli stanno, inoltre, nel fatto che è un sistema penetrabile da operatori esperti, cosiddetti pirati informatici (basta pensare al caso *WikiLeaks*), e nel fatto che, laddove alle violazioni non corrispondano le sanzioni, la percezione di efficacia del sistema si indebolisce. Secondo C. FOCARELLI, *op. cit.*, p. 169 ss. il modello è quello del «*Mondo Nuovo*» di A. Huxley (A. HUXLEY, *Il mondo nuovo*, trad. it di L. GIGLI, Mondadori, Milano, 1933), dove la brama di potere si soddisfa infliggendo piacere e non dolore: «il problema non è più tanto lo stato che sorveglia quanto il crescente desiderio delle persone di farsi sorvegliare autorivelandosi pur di sentirsi esistere come individualità assoluta» (p. 172).

[1209] Cfr. G. AZZARITI, *op. cit.*, pp. 4-5; A. MASERA - G. SCORZA, *op. cit.*, p. 60 ss.; M. CUNIBERTI, *Nuove tecnologie della comunicazione e trasformazioni della democrazia*, cit., p. 364 ss.

[1210] Intervista tra Moyers e Lessig su *Big Brother's Prying Eyes* del 14 giugno 2013, riportata da G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 63 ss. e consultabile al link *billmoyers.com/episode/big-brothers-prying-eyes*.

[1211] Nel caso svelato da Snowden è emersa la sorveglianza condotta dall'NSA statunitense e da altre agenzie governative (Canada, Gran Bretagna, Australia e Nuova Zelanda), detti "i cinque occhi", in collaborazione con aziende come Google, Skype, Facebook, Microsoft, Apple, Yahoo. Al riguardo P. MARSOCCI, *op. cit.*, p. 6 sottolinea che l'acquisizione e la diffusione di dati può costituire un rischio come nel caso del *Datagate*, in cui si traduce in una forma di controllo da parte delle autorità verso i cittadini, ma anche un'opportunità, come emerso nel caso *WikiLeaks*, in cui si traduce in controllo delle autorità da parte dei consociati, come esercizio della sovranità popolare.

quantità di dati che transitano negli strumenti digitali di utilizzo quotidiano da parte di ciascuno di noi[1212]. Anche in tal caso la motivazione, individuata nella necessità di garantire sicurezza e lotta efficace a fenomeni come il terrorismo, soprattutto dopo l'attentato dell'11 settembre 2001, non sembra sufficiente a bilanciare la violazione indiscriminata, estesa e profonda dei diritti e delle libertà.

A dire il vero, come opportunamente si rileva in dottrina, l'obiettivo di massima sicurezza implica ontologicamente un controllo costante e invasivo e, di conseguenza, è difficile che questo non si traduca in una concreta violazione di diritti occasionale o sistematica. Seppur possa avere questo margine di ineludibilità laddove si persegua la sicurezza totale, dal momento che l'abuso di potere e la violazione dei diritti non è accettabile dai governati, spesso alla sorveglianza si accompagnano la menzogna e il segreto da parte dei governi al fine di conservare il potere[1213].

[1212] G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 25 ss. sottolinea la specificità degli Stati Uniti, territorio di grandi contraddizioni dove si è realizzata la sorveglianza di massa esplosa nel caso *Datagate*, ma dove trovano sede anche fenomeni di *leaking* e *whistleblowing*, si pensi ad Assange, Snowden e Manning. In proposito, G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, cit., p. 697 ss. rileva che la sorveglianza è stata condotta grazie all'intercettazione delle comunicazioni telefoniche e telematiche e all'accesso sistematico ai dati dei colossi del web. Al riguardo, salve alcune zone grigie e dubbie, «il meccanismo di sorveglianza elettronica posto in essere dalle agenzie di sicurezza statunitensi non ha operato al di fuori dei circuiti della legalità, ma ha sfruttato alcune falle, o meglio alcune caratteristiche distintive, del regime statunitense di tutela della riservatezza».

[1213] Cfr. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 18 ss. secondo cui l'idea di segreto «è da sempre vista come lo strumento essenziale, caratteristico e irrinunciabile per ottenere il potere e per il suo mantenimento. Essa assume, nell'era tecnologica, nuove sfumature di grande interesse. *In primis*, ci si è resi conto che custodire il segreto in un'era *liquida*, in un mondo digitale e dell'informazione costituito di reti, di segnali, di sensori e di impulsi (e documenti) elettronici, è diventato estremamente difficile. Si potrebbe affermare, senza timore di smentita, che il mondo elettronico e delle reti sia *geneticamente* un mondo non adatto ai segreti», ma nonostante sia uno dei fattori più difficili da mantenere nell'era digitale, «è cercato con sempre maggiore intensità».

Sorveglianza, menzogna[1214] e segreto[1215] sono gli strumenti tipici della relazione di potere tra governanti e governati e della relativa asimmetria informativa, ossia il più ampio possesso di informazioni dei primi sui secondi rispetto al contrario[1216].

Sicuramente nell'era digitale il segreto si trasforma anche in una potenziale vulnerabilità, da poter attaccare da un punto di vista tecnico-informatico, come nei progetti di *leaking* e di *whistleblowing*; allo stesso tempo, esiste un "segreto domestico" che i cittadini possono mettere in campo per proteggere i propri dati: insieme al controllo e alla sorveglianza si affermano anche fenomeni di *digital resistance* e l'uso di *liberation technologies*[1217]. Ma ciò non toglie i pericoli per la democrazia da parte della sorveglianza di massa perpetrata dai pubblici poteri.

Nell'età contemporanea, peraltro, la sorveglianza non è più intermittente e mirata su soggetti determinati, ma è indiscriminata, continua, capillare e diffusa, "liquida"[1218]:

1214 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 24 parla di una sorta di *diritto di mentire* in capo a chi governa, in quanto mezzo necessario per conservare il potere e garantire il bene dello Stato.

1215 Sui rapporti tra segreto e potere cfr. A. MORRONE, *Il* nomos *del segreto di Stato*, in G. ILLUMINATI (a cura di), *Nuovi profili del segreto di Stato e dell'attività di* intelligence, Giappichelli, Torino, 2010, pp. 3-52.

1216 Secondo P. TINCANI, *op. cit.*, p. 22 «a grandi paure corrispondono grandi richieste di sicurezza, e l'unico modo per soddisfarle è un incremento del controllo statale sulle vite dei singoli, che a sua volta è possibile soltanto a patto di ampliare i poteri delle istituzioni incaricate del controllo»; l'Autore sottolinea, al riguardo, come l'ultima grande paura sia costituita dal terrorismo e, di conseguenza, tra le priorità politiche emerga la lotta al terrorismo: tra l'altro in merito dubita dell'efficacia delle misure attivate per il contrasto del fenomeno. Al riguardo, secondo G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 11 sorveglianza, controllo, segreto e trasparenza sono i quattro elementi fondamentali che stanno caratterizzando molti aspetti della società dell'informazione.

1217 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 22 ss.

1218 Così Z. BAUMAN - D. LYON, *op. cit.*: «l'espressione "sorveglianza liquida", più che una definizione esauriente della sorveglianza, è soprattutto un orientamento, un modo di contestualizzarne gli sviluppi nella modernità fluida e inquietante di oggi. La sorveglianza tende a farsi liquida soprattutto nella sfera dei consumi. Nel momento in cui frammenti di dati personali estratti per un determinato scopo divengono facilmente utilizzabili per altri scopi, gli antichi punti di riferimento vengono meno» (p. X); la sorveglianza è divenuta flessibile e mobile. In tal senso anche G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 223 ss., secondo cui il controllo capillare

è più facile compiere una sorveglianza generale sulla globalità dei soggetti tramite un'attività cosiddetta a strascico, atta a raccogliere in modo indiscriminato tutti i flussi di dati e metadati, e poi, in un secondo momento, dalla mole dei *big data* ottenuta inferire con analisi ed estrazioni algoritmiche e di *data mining* i dati di interesse, attuando così una sorveglianza particolare o mirata[1219].

La sorveglianza nell'era digitale, di conseguenza, è una sorveglianza di massa, impossibile prima dell'avvento e della diffusione endemica degli strumenti digitali e del loro utilizzo da parte della popolazione globale[1220]. Ogni individuo, infatti, tranne una parte della popolazione che va continuamente riducendosi, utilizza costantemente strumenti digitali che possono essere oggetto di controllo: fa ricerche, comunica, fruisce di servizi, conclude contratti, effettua pagamenti, si esprime, pubblica dettagli della sua vita privata e in tutte le sue azioni lascia tracce che consentono di monitorarlo[1221]. Le tracce e i dati formano una sorta di duplicato della persona di cui ci si tende a fidare più che della persona stessa per indurne inferenze e decisioni[1222]. La "scelta" di usare tali strumenti è, peraltro, al di là dell'apparenza, sempre meno libera nella sostanza e sempre più obbligata al fine di avere rapporti sociali e professionali, opportunità,

---

non è più solo appannaggio di regimi, ma può avvenire in qualsiasi contesto politico e costituzionale in modo complesso e subdolo.

1219 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 22 ss.

1220 P. TINCANI, *op. cit.*, p. 27 ss.

1221 G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 25, in merito all'invasività delle tecnologie attuali e alla loro presenza costante nella vita quotidiana, parla di «una sorta di dipendenza dalle tecnologie (che, sovente, incorporano strumenti di controllo) che facilita, tramite i comportamenti dell'essere umano, il controllo stesso». «In poche parole: è aumentato incredibilmente il lato *esposto* dell'individuo nel mondo elettronico, e ciò si rivela un ulteriore, grande vantaggio per chi ha intenzione di sorvegliarlo» (p. 227); secondo l'Autore gran parte dell'attività di sorveglianza, di conseguenza, avviene semplicemente ordinando informazioni che il soggetto ha già fatto circolare, più o meno consapevolmente, ed è favorita dalla frammentazione dei dati e dalla duplicazione delle informazioni.

1222 Cfr. Z. BAUMAN - D. LYON, *op. cit*., p. XV ss., secondo i quali i *social media* dipendono ontologicamente dal monitoraggio e dalla vendita dei dati a terzi; il potere di sorveglianza al loro interno è endemico e consequenziale. Gli Autori sottolineano le profonde conseguenze politiche e sociali non solo nelle problematiche specifiche relative all'anonimato, alla riservatezza e alla privacy, ma anche più ampiamente nelle questioni etiche di equità e giustizia, libertà civili e diritti.

vantaggi, risparmi di tempo e denaro: più ampiamente è inevitabile al fine di svolgere la propria esistenza digitale[1223].

Non si tratta, quindi, di pericoli meramente immaginati, ma di rischi reali e già realizzati in larga scala, intaccando le persone e i propri dati e, insieme a loro, i diritti che caratterizzano il governo dei dati. Incurante di ogni bilanciamento tra diritti, la possibilità di sorvegliare è stata messa in atto. I *big data,* infatti, privi di direzione e regolamentazione, permettono *ex se* una sorveglianza più semplice, economica ed efficace, che peraltro consente di sfruttare anche l'insita capacità predittiva, anche se non sono certo indenni da errori, interpretazioni fuorvianti e possibili manipolazioni e da rischi tecnici e legali concreti di intaccare la dignità, favorire discriminazioni e finire per negare la libertà umana[1224].

Allora, per adempiere alla promessa insita nell'espressione società della conoscenza, i dati, *closed*, *open*, *small* o *big*, devono rimanere uno strumento e «il futuro deve restare nelle nostre mani»[1225].

6.2.2. Possibili rimedi: verso gli *open big data* e le tutele collettive dei diritti?

Al fine di orientare la *data society* verso la direzione positiva del rispetto dei valori e delle libertà, della tutela della dignità e dello sviluppo della persona, dell'evoluzione di governi più aperti e democratici è necessario l'intervento del diritto

---

[1223] G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 228 sottolinea la scarsa sensibilità sul tema del controllo quotidiano che non induce a mutare i propri comportamenti in rete.

[1224] Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 203 ss., secondo i quali «per fare in modo che le persone vengano protette mentre si promuove la tecnologia, non dobbiamo permettere che i big data si sviluppino al di là della nostra capacità di influenzare la tecnologia» (p. 249).

[1225] V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 261 aggiungono: «se non sarà così, i big data avranno sovvertito l'essenza stessa della natura umana, ovvero il pensiero razionale e la libera scelta». «I big data sono una risorsa e uno strumento. Servono a informare, più che a spiegare; ci aiutano a capire, ma possono indurci anche al fraintendimento, a seconda di come vengono utilizzati» (p. 266).

che deve mostrarsi capace di appianare le asimmetrie e riequilibrare con misure concrete gli squilibri, frenando il controllo sociale e inibendo la sorveglianza di massa.

Per farlo, in considerazione della funzione stessa del diritto di regolare la realtà, sono necessarie soluzioni capaci di innovare i paradigmi tradizionali, oggi insufficienti, sulla base di una "nuova etica digitale" che minimizzi i rischi di distorsioni e discriminazioni[1226].

Di conseguenza, è necessario immaginare tutele inedite che, da una parte, siano capaci di equilibrare l'asimmetria a favore della collettività e, dall'altra, siano idonee a proteggere in modo efficace la persona.

Sotto il primo punto di vista, al fine di sanare l'asimmetria informativa e di potere, si può immaginare un utilizzo sinergico di *open data* e *big data* per favorire la crescita e generare un nuovo rapporto tra governi e mercati, tra soggetti pubblici e privati[1227]. In altre parole, è possibile immaginare una sorta di "sanatoria" al momento della diffusione, "aprendo" i *big data* e mettendoli a disposizione della collettività come *open data* da poter riutilizzare, per mezzo della concessione con licenza del diritto al riutilizzo, abbandonando una gestione spesso "chiusa" e opaca degli stessi, facendoli diventare un "bene comune" e, così, strumenti di democrazia economica[1228].

[1226] G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 12 parla della «necessità di un ripensamento globale – e dell'avvio di un nuovo processo d'interpretazione – di regole ormai note ma che, per molti versi, si stanno sgretolando, o stanno mutando forma e natura». Secondo l'Autore sono tre i fattori che contribuiranno a migliorare il quadro giuridico e politico attuale, che vede la crisi di privacy e democrazia: la tecnica adoperata per la protezione dei dati, incorporata nelle tecnologie stesse; il mutamento dei comportamenti umani; una politica legislativa di riforme che ponga attenzione e metta al centro dei provvedimenti i diritti dell'uomo.

[1227] V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 246 ss. ritengono che i governi dovrebbero rendere pubblici i dati che conservano.

[1228] Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., pp. 135-136 e M. OREFICE, *op. cit.*, p. 713 ss., che suggerisce di accompagnare la messa a disposizione con la definizione di uno standard di privacy cui adeguarsi e con rimedi quali il *do not track* che nasconda l'attività degli utenti agli inserzionisti, la trasparenza nell'azione dei colossi del web e la portabilità dei dati tra i servizi. Parla del collegamento tra *big data* e *open data* e delle interessanti prospettive correlate per una migliore partecipazione attiva dei cittadini M. FALCONE, *op. cit.*, p. 601 ss.

Si potrebbe, insomma, pensare a "*open big data*", che genererebbero innumerevoli possibilità e che potrebbero equilibrare le asimmetrie informative, anche se inevitabilmente provocherebbero una perdita di potere per le grandi *corporation* e gli Stati[1229]. In tal modo, però, sarebbero protetti maggiormente cittadini e imprese, per mezzo di un accesso equo e della libera concorrenza[1230], aprendosi scenari di trasparenza, partecipazione e collaborazione in una dimensione maggiormente orizzontale del rapporto tra governi e privati in direzione dell'*open government*, atta a ridurre i rischi di sorveglianza e a rafforzare il ruolo degli individui[1231].

Tra l'altro, così, il bene peculiare della conoscenza potrebbe recuperare le caratteristiche ontologiche della non escludibilità e della non rivalità, che rischia invece di perdere laddove l'utilizzo da parte di alcuni possa portare difficoltà di accesso al bene da parte di altri e conseguenti disparità nella fruizione: il potere economico deriva dalla disponibilità esclusiva nelle mani di pochi, ma "liberando" i *big data* si consentirebbe ad altri soggetti di trarre valore economico da quei dati, in uno scenario atto a mettere in equilibrio l'attuale asimmetria di potere, ma anche a delineare un contesto economico più equo e competitivo, anche in considerazione del fatto che gli interessi economici non possono prevalere sui diritti e sulla dignità dell'uomo[1232]. Al riguardo, allude

---

1229 In merito A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 140 ss. individua come strumenti utili a limitare le asimmetrie informative l'accessibilità, la condivisione delle informazioni, il pluralismo di attori e l'adozione di forme di controllo attraverso la previsione di specifiche autorità sovranazionali indipendenti: l'Autore sottolinea il ruolo evidente che possono avere gli *open data*. Al riguardo M. OREFICE, *op. cit.*, p. 713 ss. parla di *Super Data* quando i *big data* vengono aperti, dal momento che si elevano consentendo per mezzo dell'accesso conoscenza, ricchezza economica ed esercizio di diritti e libertà.

1230 V. ZENO-ZENCOVICH - G. GIANNONE CODIGLIONE, *op. cit.*, p. 36 ss. sottolineano che i dati sono un'infrastruttura essenziale delle regole della concorrenza e che si potrebbe immaginare un obbligo per il detentore di fornirli ai concorrenti.

1231 Nell'*Opinion* 4/2015 «*Towards a new digital ethics. Data, dignity and technology*» dell'11 settembre 2015, l'*European Data Protection Supervisor* (EDPS) parla di dati aperti come bene comune da condividere nell'interesse pubblico, in modo da ridurre i rischi di sorveglianza e attribuire un'influenza maggiore agli individui sulle decisioni che li riguardano.

1232 Cfr. E. NUNZIANTE, *op. cit.*, p. 12, secondo la quale «l'equilibrio tra accesso e chiusura è il vero tema alla base dei Big Data e della rivoluzione informatica, dove l'informazione assume allo stesso tempo il ruolo di motore dell'economia e di strumento per l'espansione dell'autonomia dell'individuo».

chiaramente alla necessità di un maggior accesso ai *big data* da parte dei soggetti pubblici e privati la comunicazione della Commissione europea «*Costruire un'economia dei dati europea*» COM(2017) 9 *final* del 10 gennaio 2017.

Per eliminare le disparità delle interazioni sul mercato dei dati è necessaria la messa a disposizione in modo aperto per consentire la fruizione diffusa e plurale dei *big data*, la partecipazione consapevole e il controllo pubblico[1233]. Aprendo i *big data*, questi vengono restituiti e destinati a beneficio dell'intera comunità, al fine di godere i diritti fondamentali ed esercitare la sovranità popolare: a tali scopi la regola dovrebbe consistere nell'apertura accompagnata da eccezioni finalizzate sempre al perseguimento di interessi generali, come i diritti inviolabili o la sicurezza[1234]. In tal modo il diritto orienterebbe la tecnica verso i valori costituzionali della società democratica e il governo dei dati verso un modello partecipato dalla comunità, permettendo negoziazioni consapevoli ed eventuali azioni di classe[1235].

Nella prospettiva dell'apertura naturalmente il caso dei *big data* pubblici differisce da quello dei *big data* privati.

Nella prima ipotesi l'apertura è in linea con le politiche, le strategie e le normative in materia orientate agli *open data*, trovando fondamento negli artt. 3, 97 e 118 della Costituzione[1236].

Gli artt. 3 e 118 vengono in gioco anche nel caso dell'apertura dei *big data* privati, ma in tal caso vanno considerati anche gli artt. 41 e 42 Cost. Tali disposizioni non si devono, però, ritenere violate dall'apertura, dal momento che questa tutela mercato e concorrenza, favorendo altresì uguaglianza e diritti fondamentali: l'innovazione e l'iniziativa economica sarebbero realizzati per mezzo dell'apertura in modo più conforme al modello costituzionale, ossia in modo strumentale allo sviluppo, ma anche

---

1233 M.F. DE TULLIO, *op. cit.*, p. 675 ss. lega l'apertura dei dati al secondo aspetto che sarà esaminato in questo paragrafo (la tutela collettiva dei diritti): la comunità deve essere messa in condizione di partecipare in modo informato alla negoziazione collettiva e di controllarne l'adempimento, altrimenti le asimmetrie peserebbero sulla possibilità di autodeterminarsi nella contrattazione.

1234 M.F. DE TULLIO, *op. cit.*, p. 678 ss.

1235 M.F. DE TULLIO, *op. cit.*, p. 679 ss.

1236 *Supra*, cap. 3.

ai diritti fondamentali, seguendo il principio di sussidiarietà orizzontale[1237]. Peraltro questo scenario non "svuoterebbe" il potere dei colossi del web, dal momento che l'apertura dovrebbe attenere semplicemente ai dati e non certo agli algoritmi e alle tecniche utilizzate dalle imprese per estrarre conoscenza dai dati stessi, che costituiscono l'autentico valore in termini economici; al riguardo, sarebbe necessaria invece maggiore trasparenza sulla logica utilizzata dagli algoritmi, anche ai fini di una consapevole autodeterminazione degli individui.

Il modello attuale, basato sull'acquisizione dei dati per personalizzare e migliorare piattaforme e servizi e profilare gli utenti, "vendendo" tali dati a fini di *marketing* e di pubblicità mirata, è *closed* e concentrato: risulta vantaggioso solo per pochissimi grandi soggetti privati e persegue fini che non sono di interesse prioritario per la collettività (come la profilazione a fini di *marketing*), venendo a ledere concorrenza e uguaglianza[1238]: questo scenario verrebbe drasticamente ridimensionato dall'apertura dei dati, che non renderebbe più conveniente a nessuno acquisire dati per i quali è consentito il libero accesso[1239].

[1237] Cfr. M.F. DE TULLIO, *op. cit.*, p. 692, secondo la quale per il momento attuativo della disciplina di apertura il protagonista più idoneo è «un organo collettivo, distinto da quello deliberante: non dovrebbe trattarsi né di un ente governativo né di uno dei grandi giocatori dell'attuale mercato di Internet», in modo da non lasciare il governo dei dati ad attori che hanno interesse a gestirlo a proprio vantaggio.

[1238] M.F. DE TULLIO, *op. cit.*, p. 694: «Il bilanciamento attuale appare dunque illegittimo, perché fa prevalere gli interessi economici di pochi su una prerogativa inviolabile della collettività, e realizza una sproporzione tra esigenze di sicurezza e tutela dei diritti».

[1239] Cfr. M.F. DE TULLIO, *op. cit.*, p. 675 ss., che ritiene, a causa di tali motivi, il mercato attuale non più concorrenziale «perché nessuna "buona idea" potrebbe migliorare il servizio al pari degli enormi archivi in possesso del soggetto già dominante: è dimostrato che l'implementazione dell'algoritmo non dà la stessa resa dell'incremento della base di dati su cui è applicato. Questo mette in difficoltà i nuovi entranti, che non hanno i mezzi per procurarsi un set di informazioni paragonabile a quello del dominante» (p. 684): si producono "effetti di rete" che inevitabilmente favoriscono chi è già forte, oltre al fatto che gli stessi utenti sono maggiormente attratti dalle aziende già affermate, che migliorano maggiormente i servizi adattandoli all'utenza. Peraltro, «oggi le imprese non hanno interesse a fornire un servizio che sia il più possibile utile all'utente, ma a trattenere il navigante sulla propria pagina» e le due esigenze non sempre coincidono (p. 690). In tal senso anche M. OREFICE, *op. cit.*, p. 730, secondo la quale «nessun programma innovativo potrà superare il vantaggio di *Google* nella raccolta dei dati» e, di conseguenza, il fine ultimo consiste nel «salvaguardare i mercati competitivi dei *Big Data* per impedire l'ascesa dei *data barons, Google* seguito da *Facebook, Twitter, Microsoft, Amazon,* che oggi hanno

Pertanto l'apertura consente alle imprese di esercitare il proprio diritto di iniziativa economica, in modo conforme all'art. 41 Cost., utilizzando i dati per l'avvio di un'attività o per lo sviluppo di applicazioni, servizi e prodotti e ai cittadini di esercitare i diritti fondamentali, grazie alla conoscenza, al controllo democratico e alla conseguente determinazione più consapevole nello svolgimento delle prerogative dell'essere persona e cittadino, nel fare ricerca a favore della collettività e nello svolgere attività autonome di interesse generale, dando forma al principio di sussidiarietà orizzontale[1240]. A ben vedere, la ricchezza dei dati si connette strettamente alla loro apertura generalizzata[1241].

Sotto il secondo punto di vista, relativo all'esigenza di soluzioni in grado di proteggere efficacemente la persona nel governo dei dati, è necessaria una premessa: come già evidenziato, l'aggressività dei comportamenti dei giganti della rete nei confronti della persona porta nei fatti a svuotare di contenuto strumenti preventivi di garanzia come informativa e consenso e toglie libertà al soggetto, che pur di ottenere accesso a piattaforme e servizi è portato a "svendere" i propri dati con scarsa consapevolezza delle conseguenze[1242]. Pertanto, rimettere la tutela ai singoli spesso si traduce in una mercificazione dei dati e in un'incapacità ontologica dell'individuo di proteggersi nei confronti dei colossi del web. Nella realtà dei fatti l'utilizzo dei *big data*, che potrebbe servire a interessi generali, avviene per esercitare e mantenere un potere economico, nel caso dei soggetti privati, o autoritario, nel caso dei soggetti pubblici[1243].

A questo deve essere sommato il complesso bilanciamento tra diritti nel governo dei dati, che rende difficile e anche pericoloso il bilanciamento concreto realizzato dal

---

sostituito i *robber barons* che nell'800 dominavano le ferrovie, l'industria dell'acciaio e le reti telegrafiche in America» (pp. 732-733).

1240 M. OREFICE, *op. cit.*, p. 713 ss.: «L'accesso ai dati consente di pensare migliori politiche pubbliche, analizzare problemi sociali ed economici, contrastare corruzione e criminalità organizzata, ma anche di organizzare più razionalmente la propria quotidianità: conoscendo gli sviluppi del piano asili nido comunale, le strade chiuse al traffico, le linee tramviarie sospese» (p. 715).

1241 M. OREFICE, *op. cit.*, p. 717.

1242 Cfr. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, cit., p. 148, secondo cui la "svendita" della privacy da parte del cittadino si profila «a causa sia dell'utilizzo di applicazioni che si basano sulla gestione dei dati personali, sia di una mancanza di percezione del valore della protezione del dato».

1243 M.F. DE TULLIO, *op. cit.*, p. 651.

potere giurisidizionale nel momento conflittuale della singola fattispecie: esempio paradigmatico è il caso *Google Spain*, dove lo "sconfitto" Google in realtà ha acquisito ulteriore potere nel bilanciamento tra i diritti. Non solo: la necessità di garantire effettiva tutela porta anche ad avvalersi in modo ampio dell'azione di autorità amministrative indipendenti, come visto, con rischi ancora maggiori rispetto al potere giurisdizionale di far pendere la bilancia sull'uno o sull'altro diritto a protezione del quale la specifica autorità è istituita e conseguentemente si muove.

Dal momento che tali strumenti incorrono in queste problematiche e al tempo stesso occorrono strumenti di tutela efficace per non rischiare di sgretolare i diritti fondamentali e le libertà degli individui e, con questi, l'essenza democratica degli ordinamenti, è opportuno pensare a soluzioni diverse calate come un guanto alla mano sul governo dei dati e sulle peculiari caratteristiche che lo connotano.

I "beni" che caratterizzano la *data society*, come esaminato nel corso dell'analisi, sono dati, informazioni e conoscenza, beni collettivi e a titolarità diffusa, che permettono di realizzare interessi generali come trasparenza, partecipazione, democrazia, sviluppo economico, culturale e sociale: in conformità alla loro natura ontologica necessitano di una tutela collettiva da parte della comunità, che in parte già avviene con la previsione di autorità amministrative indipendenti a protezione dei diritti e che, per essere effettiva, deve sostanziarsi in una capacità di disposizione da parte della comunità al posto e anche contro la volontà del singolo.

Inoltre, al riguardo, i *big data* che dominano la scena contemporanea, per loro natura, tendono a identificare modelli di comportamento e a predire comportamenti di gruppi e comunità con un impatto su un insieme ampio di soggetti, mostrando una dimensione collettiva dei profili e dei rischi connessi al loro utilizzo, come rilevano le stesse «*Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*», adottate il 23 gennaio 2017 dal Comitato della Convenzione del Consiglio d'Europa per la protezione dei dati[1244]. La "massa" finisce

[1244] M. FALCONE, *op. cit.*, p. 601 ss.: «L'azione dello Stato in funzione di controllo e di prevenzione insieme all'utilizzo predittivo e pervasivo dei *big data* nei processi decisionali, quindi, rischiano di ledere profondamente il principio di eguaglianza e i diritti di libertà. Un ragionamento per cui la possibilità che una persona possa compiere determinate scelte o assumere determinati comportamenti semplicemente perché possiede alcune caratteristiche o perché appartiene a determinati gruppi sociali o a determinate etnie o semplicemente perché così ha previsto il risultato di un analisi algoritmica con i *big data*, può

per dettare legge, grazie alle inferenze algoritmiche, e orienta in modo automatizzato decisioni e predizioni pubbliche e private anche laddove il singolo non si riconosca e si discosti da quella massa: nelle configurazioni odierne dei dati emerge l'impatto collettivo e sociale del loro utilizzo[1245].

I complessi bilanciamenti tra diritti diversi fanno emergere le connessioni forti non solo tra interessi, ma anche tra diversi soggetti da tutelare: decidere di rispettare l'oblio del singolo può inficiare il diritto all'informazione e alla memoria della collettività; il consenso concesso senza consapevolezza va ad accrescere i dati in possesso del soggetto privato e pubblico relativamente a una comunità o un gruppo del quale fa parte anche chi quel consenso non ha prestato, ma che potrebbe subire decisioni prese in considerazione di quei dati afferenti alla comunità di cui fa parte; una rigida applicazione dei diritti di proprietà intellettuale, se tutela l'autore, ostacola altri soggetti creativi, che non potranno riutilizzare quei dati e, *a contrario*, una circolazione incurante del diritto d'autore danneggerebbe coloro che hanno creato qualcosa. La tutela del diritto dell'uno ha effetto sulla tutela dei diritti degli altri, all'espansione di una libertà consegue la riduzione di un'altra.

Di conseguenza, si configura la necessità di una protezione collettiva, che limiti il diritto individuale del singolo anche in relazione al fatto che i suoi atti dispositivi hanno effetto anche sugli altri consociati: ogni consenso al trattamento dei dati aumenta il dominio di pochi centri di potere sul governo dei dati e, in tal modo, reca un pregiudizio alla collettività; i pericoli di discriminazione insiti nella profilazione e nel *data mining* hanno impatto generale su tutta la collettività; le scelte, rese possibili grazie ai dati acquisiti individualmente, avvengono non solo sul singolo, ma sull'intero gruppo di cui fa parte[1246]. Nella circolazione, nel trasferimento e nel riutilizzo dei dati non è coinvolto solo l'individuo, ma l'intera comunità e, certamente, il singolo da solo non è in grado di

---

produrre delle forti discriminazioni per associazione che penalizzano la persona, non solo perché valutata al netto della propria volontà personale, ma soprattutto in quanto facente parte di un gruppo sociale o di una determinata etnia».

1245 Cfr. C. FOCARELLI, *op. cit.*, p. 169 ss., che sottolinea il modellamento che disincentiva la diversità, e M. FALCONE, *op. cit.*, p. 601 ss.

1246 M.F. DE TULLIO, *op. cit.*, p. 658 ss.: «Ciascuno quindi è giuridicamente interessato a quanti e quali dati rivelano gli altri e alla correttezza di queste informazioni, perché anche in base a questi parametri vengono prese delle decisioni su di lui» (p. 664).

manifestare la volontà dell'intera comunità coinvolta dal suo esercizio dei diritti[1247]: la lesione dei diritti non si limita al singolo, ma mina la vita collettiva e i diritti di tutti nel lungo periodo[1248].

Allora l'intreccio tra dati, diritti e soggetti provoca la necessità di bilanciamenti attenti a un quadro collettivo e, di conseguenza, determina l'opportunità di non affidare la protezione al singolo, ma direzionarsi verso tutele collettive dei diritti, ossia verso una sorta di titolarità collettiva della tutela dei relativi diritti[1249]. Solo quando sono gestiti dalle comunità di riferimento i *big data* diventano *commons*, anche sul piano soggettivo: andrebbero, di conseguenza, affidati alla comunità i diritti al controllo strategico e alla gestione operativa[1250]. Specularmente all'impatto collettivo prodotto dal volto oscuro della *data society*, che consiste nel controllo, nella sorveglianza e in ogni altra operazione lesiva della persona e dei suoi diritti, la tutela deve essere collettiva, abbandonare una dimensione esclusivamente individuale, che risulta inefficace, e acquisire anche dimensioni collettive[1251].

Se non intervengono fonti sovraordinate e imperative l'autonomia contrattuale del singolo dispone e consegna un potere quasi normativo ai *big player*, che consiste nel vincolare al proprio sistema di regole una generalità di soggetti anche non contraenti, dettando così nei fatti un bilanciamento tra diritti che ontologicamente non può spettare ai soggetti privati, ma solo ai soggetti pubblici capaci di interpretare la tutela di interessi generali[1252]: per mezzo delle norme, capaci di valere *erga omnes*, è possibile recuperare questo bilanciamento nelle mani pubbliche, fisiologicamente deputate, sottraendolo a quelle private, mosse da logiche di profitto.

Dato che l'effetto delle scelte individuali è collettivo, non è infatti possibile affidarsi alla scelta del singolo, che proteggerà o magari deciderà di barattare i propri dati in base a una convenienza individuale e non certo guardando all'interesse generale,

---

1247 M.F. DE TULLIO, *op. cit.*, p. 664 ss.

1248 C. FOCARELLI, *op. cit.*, p. 169 ss.

1249 M.F. DE TULLIO, *op. cit.*, p. 641 ss., soprattutto in relazione alla privacy: «se la riservatezza vanta una titolarità collettiva, il soggetto dell'autodeterminazione informativa dovrà essere la comunità, e non più l'individuo».

1250 M. OREFICE, *op. cit.*, p. 712 ss.

1251 M. FALCONE, *op. cit.*, p. 601 ss.

1252 M.F. DE TULLIO, *op. cit.*, p. 665 ss.

che però dalla sua azione è inevitabilmente toccato, o ponendo attenzione agli altri individui, che però sono "conosciuti" anche grazie a quei dati (perché magari fanno parte dello stesso gruppo o comunità) e magari contro la loro volontà.

Si tratta di immaginare una limitazione del potere individuale e la corrispettiva introduzione di uno strumento di negoziazione collettiva in merito al governo dei dati: muta in tal modo l'esercizio delle prerogative connesse ai diritti, al fine di proteggere due beni di rilevanza collettiva, l'uguaglianza sostanziale nel godimento degli stessi, che inevitabilmente sfuma negli squilibri economici, informativi e di potere, e l'autodeterminazione informativa della collettività, che può arrivare a limitare posizioni giuridiche individuali, capaci altrimenti di creare effetti negativi anche su terzi e sulla comunità[1253]. Il pericolo, altrimenti, sta nell'automatico coinvolgimento collettivo, che può tradursi in manipolazione sociale, controllo e sorveglianza e può essere arginato proprio immaginando una speculare protezione collettiva di diritti e interessi, capace di tutelare in modo nuovo la democrazia e i suoi valori[1254].

Alla luce di queste considerazioni, è necessario immaginare un'autodeterminazione informativa della collettività sui propri dati, che si traduce nella previsione di norme, atte a individuare il bilanciamento tra diritti a fondamento

---

[1253] Nello stesso senso M.F. DE TULLIO, *op. cit.*, p. 655 ss., secondo la quale «il fuoco dovrebbe essere spostato verso diversi punti nevralgici. Il primo dovrebbe essere una legislazione che tuteli il singolo e la collettività rispetto ai contraenti forti, vietando – a prescindere dal consenso – alcuni trattamenti lesivi dei valori costituzionali e impedendo alle aziende di condizionare la fornitura di servizi alla cessione di dati non necessari. Il secondo dovrebbe essere una negoziazione collettiva e paritaria sulla cessione dei dati, assistita da un'ampia trasparenza, che permetterebbe a tutti una partecipazione consapevole all'autoregolazione e un controllo sulla sua attuazione. Posti questi limiti, la visione politica di fondo dovrebbe comunque tendere verso una fruizione diffusa e plurale dei *big data*, che dovrebbe attaccare più in radice le disuguaglianze sostanziali, creando le precondizioni per un'autentica autodeterminazione» (pp. 677-678).

[1254] Cfr. C. FOCARELLI, *op. cit.*, p. 169 ss. e p. 179 ss. e M.F. DE TULLIO, *op. cit.*, p. 696, secondo la quale «la sfida dei *big data* oggi è rovesciare il controllo dominicale pubblico e privato sulle informazioni e realizzare l'autodeterminazione conoscitiva della comunità. Dunque i dati dovrebbero costituire un'infrastruttura gestita e fruita dalla collettività, come premessa tecnica necessaria per amplificare la sovranità popolare e rendere effettivo l'uguale godimento dei diritti fondamentali. Ma tale risultato ha come condizione prima che la tecnica sia orientata all'utilità sociale, e non al calcolo egoistico di pochi».

costituzionale[1255], e nella negoziazione collettiva, regolata dalle norme, entrambe deputate a coadiuvare l'autonomia negoziale del singolo[1256].

Sotto la lente della protezione dei dati personali, questo si traduce nell'interpretazione dei diritti coinvolti nel governo dei dati quali libertà collettive e nella deroga conseguente alla libertà negoziale del singolo, vietando per mezzo di norme imperative all'autonomia negoziale alcune operazioni anche se il consenso sussiste[1257] o imponendole anche se manca[1258]: si tratta di deroghe *in melius* al consenso individuale, al fine di garantire una maggiore tutela anche al singolo[1259], in una logica che peraltro è in linea con l'approccio preventivo e tecnologico, *by design* e *by default*, prima esaminato, che "decide" *ex ante* al posto del singolo, al fine di tutelarlo[1260].

1255 M.F. DE TULLIO, *op. cit.*, p. 671 ss. sottolinea in proposito che il regolamento europeo sulla privacy non pone alcuna gerarchia tra i valori in gioco, senza individuare quelli che non possono comprimere la protezione dei dati personali, mentre avrebbe potuto limitare, ad esempio, il trattamento per finalità economiche e pubblicitarie, adeguandosi così all'indirizzo espresso dalla giurisprudenza.

1256 Cfr. M.F. DE TULLIO, *op. cit.*, p. 665 ss., che poggia tale ricostruzione su due ragioni principali: la libertà di Internet, che impone di rifiutare domini privati o pubblici capaci di limitare la libertà di espressione, e la natura della protezione dei dati personali, che comporta la necessità per la collettività di uno strumento decisionale collettivo per esercitare il suo diritto. «Posto che il consenso individuale deve essere circoscritto da fonti eteronome e di autoregolazione, sarà utile capire quale sia il contenuto minimo delle prime, e cosa debba essere lasciato alle seconde» (p. 668). Le norme, oltre al bilanciamento, secondo l'Autrice, dovrebbero dettare requisiti circa il soggetto dell'autoregolazione, che dovrebbe essere rappresentativo dei diversi interessi in gioco.

1257 Ad esempio il caso del trattamento per finalità puramente economiche e pubblicitarie, che in considerazione delle finalità lede in modo irragionevole il diritto alla protezione dei dati personali; cfr. M.F. DE TULLIO, *op. cit.*, p. 672.

1258 È il caso di un trattamento finalizzato a perseguire interessi generali; M.F. DE TULLIO, *op. cit.*, pp. 672-673.

1259 M.F. DE TULLIO, *op. cit.*, p. 673.

1260 Cfr. M.F. DE TULLIO, *op. cit.*, p. 665 ss. e C. FOCARELLI, *op. cit.*, p. 155 ss., che sottolinea come nell'era dei *big data* spesso il consenso è impraticabile o fittizio e, di conseguenza, inutile. «Non può essere lasciata al mercato, ad esempio, la libertà di costruire a piacere, soltanto secondo la domanda, un frigorifero smart. Il diritto deve imporre ai produttori una serie di requisiti *incorporati* nei prodotti e nei servizi a tutela sia delle persone sia della collettività e sanzionare efficacemente le trasgressioni, esattamente come oggi il diritto impone requisiti di commestibilità degli alimenti o di sicurezza dei giocattoli» (p. 181).

Il regolamento europeo 2016/679 in materia di *data protection*, in tale direzione, ha previsto requisiti analitici per le informazioni da fornire all'interessato, basi giuridiche che legittimano il trattamento diverse dal consenso e le caratteristiche di inequivocabilità e specificità del consenso con l'onere della prova a carico del titolare. Però è mancata incisività in merito all'aspetto cruciale del diverso potere negoziale tra le parti, che comporta la mancanza di libertà del consenso, dal momento che questo è condizione necessaria per l'accesso a servizi di cui il soggetto ha bisogno: il regolamento considera il profilo, ma in modo descrittivo e non prescrittivo, mentre dovrebbe essere impedita la cessione di dati non necessari quale condizione di accesso a piattaforme e servizi[1261].

Al riguardo, significativamente il regolamento europeo 2016/679 ha previsto nell'art. 80, comma 1, il diritto dell'interessato di «*dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti* […]», «*nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento* […]». Ma ancora più interessante, sotto il profilo della tutela collettiva del diritto, è la previsione del secondo comma: «*Gli Stati membri possono prevedere che un organismo, organizzazione o associazione* […]*, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79* [diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo e diritto a un ricorso

---

[1261] M.F. DE TULLIO, *op. cit.*, p. 674 ss.: parlano di tali aspetti il considerando 43 e l'art. 7 in modo non prescrittivo; inoltre, ai sensi del regolamento (considerando 47), il *marketing* diretto e i trattamenti per finalità pubblicitarie sono permessi anche senza accettazione dell'interessato, sotto la copertura della qualificazione come legittimi interessi dell'art. 6, comma 1, lett. f), seppur ci sia la clausola «*a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali*», per la quale andrà vista l'interpretazione della giurisprudenza. «La *ratio* del Regolamento appare annacquata rispetto alla difesa di valori economici, che pure dovrebbero essere subordinati alla protezione dei dati. La norma dovrebbe invece vietare all'imprenditore di condizionare la fruizione di un servizio alla cessione di informazioni non necessarie alla prestazione» (p. 675).

giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento]*, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento*»; emerge una protezione collettiva, la cui previsione viene raccomandata anche dall'*European Data Protection Supervisor* (EDPS) nell'*Opinion* n. 8 del 2016[1262].

Sul governo dei dati, sulla tutela effettiva dei diritti e sul bilanciamento tra interessi che il diritto sarà capace di realizzare si decideranno gli equilibri futuri tra poteri, il destino stesso del diritto e la sua capacità di regolare l'esistenza.

6.3. I nuovi equilibri tra diritti e la nuova fisionomia del diritto: suggestioni future

Il governo dei dati, sui quali si fonda l'esistenza digitale, parte integrante e ormai indistinguibile della vita, necessita di una riflessione ampia e profonda, che partendo dalla persona sia capace di ridisegnare i diritti che la riguardano, adeguandoli alla nuova realtà.

L'analisi condotta porta a ritenere che il bilanciamento tra diritti, da condurre sul singolo caso di specie senza prevalenze aprioristiche, debba poggiare sulla centralità della persona protetta da tutele non solo individuali, spesso insufficienti o inutili, ma anche da forme di tutela collettiva, in considerazione della corrispondente natura collettiva dei beni che si vogliono proteggere e dell'impatto sulla comunità degli atti di disposizione sui dati da parte di tutti e ciascuno. Nel ridisegno complessivo che coinvolge dati, persone e diritti, anche i rapporti tra i soggetti protagonisti devono conseguentemente mutare in direzione di apertura, per consentire non solo un reale *open government* capace di tenere lontani rischi di controllo e sorveglianza, ma anche un riequilibrio delle asimmetrie proprie del mercato e dei poteri pubblici grazie agli *open big data*.

La tutela giuridica per essere efficace nel governo dei dati, pertanto, può e deve avvalersi della tecnica per un approccio etico, tecnologico e preventivo, *by default* e *by*

[1262] *Opinion* 8/2016 dell'EDPS «*Opinion on coherent enforcement of fundamental rights in the age of big data*», 23 settembre 2016.

design, come quello disegnato dal regolamento europeo 2016/679 in materia di *data protection*, che ricorra opportunamente ai metadati, garantisca qualità alle informazioni e faccia leva su adeguate licenze, responsabilizzando i protagonisti della filiera dei dati e confinando al momento successivo delle sanzioni una repressione efficace delle violazioni.

Questo approccio non significa indulgere alla fallace promessa che la tecnica possa sostituirsi al diritto e quindi all'uomo. Semplicemente emerge la necessità di un'evoluzione del diritto, capace di servirsi della tecnica ai propri scopi, dirigendola con approccio etico verso i valori della società democratica del futuro. Nello svolgimento di questo ruolo, il diritto deve riuscire a mantenere in modo appropriato l'equilibrio che permetta alla tecnica di non prevalere sul diritto, ma neppure al diritto di limitare le potenzialità della tecnologia[1263].

Lungi dal rendere la tecnica sufficiente da sola a regolare la realtà, l'era contemporanea e il governo dei dati necessitano prepotentemente della funzione e della certezza del diritto, che è deputato per natura a dettare le regole della società, a disciplinare i comportamenti e le attività, a proteggere diritti e tutelare libertà, a rispettare la dignità e consentire lo sviluppo della persona[1264]. Gli individui, infatti,

---

[1263] Cfr. N. IRTI - E. SEVERINO, *op. cit.*; V. FROSINI, *Il diritto nella società tecnologica*, cit.; V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, cit., p. 89 ss.; G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, cit., p. 831 ss. Al riguardo S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 414: «Proprio nel mondo della rete, dove i potentati economici si strutturano come detentori di poteri incontrollati, la supremazia dei diritti fondamentali deve essere affermata, anche per escludere forme di "bilanciamento" degli interessi che, nella sostanza, si traducano nella prevalenza di quello materialmente più forte o più strutturato. La rete ha cambiato la società, ma è quest'ultima che agisce per determinare le modalità di funzionamento, e dunque essa stessa cambia la rete».

[1264] La stessa comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014 ribadisce la necessità di pertinenti quadri giuridici e politiche anche in materia di diritti che favoriscano l'uso dei dati, per rafforzare la certezza giuridica delle imprese e infondere la necessaria fiducia nelle tecnologie da parte dei consumatori. Cfr. G. DE MINICO, *Internet e le sue fonti*, in *Osservatorio sulle fonti*, fasc. 2, 2013, p. 1 ss., secondo la quale «il diritto giusto per Internet non può che riflettere le caratteristiche fondamentali della rete» e, di conseguenza, un territorio unico e globale, caratterizzato da eguaglianza e capacità espansiva di diritti e libertà: «oggi l'ipotesi di un diritto globale ed elastico volto a massimizzare le potenzialità di Internet è una proiezione astratta e di principio, che esprime una precisa scelta di valori, e che si scontra non di rado con una realtà diversa».

hanno bisogno di conoscere preventivamente come sono regolate le fattispecie e i bilanciamenti tra diritti per non incorrere in conflitti e contenziosi: per il buon andamento della società e l'armonia dell'ordinamento, la certezza del diritto è ineludibile anche nella società digitale. Se il diritto smarrisce la propria funzione preventiva, insieme ai conflitti crescerà il ruolo del potere giurisdizionale, che verrà caricato di una funzione suppletiva che non è consona e può produrre conseguenze profonde sullo stesso bilanciamento tra diritti, si pensi al paradigmatico caso *Google Spain* sui rapporti tra diritto all'informazione, memoria e oblio.

I nuovi equilibri tra diritti che si realizzano nel governo dei dati, in cui si gioca la tutela della persona stessa e della sua identità latamente intesa, esigono un nuovo diritto rispetto al tradizionale diritto statuale, dal momento che la regolazione giuridica deve interfacciarsi con altri e diversi sistemi di regole e non incontra più i confini dello Stato, ma si connota per la sua globalità.

Nel governo dei dati, infatti, il diritto non è solo, ma deve confrontarsi con altri sistemi di regole che hanno un ruolo significativo nell'era contemporanea.

Innanzitutto le "leggi del ciberspazio", ossia le regole informatiche, determinano ciò che è tecnologicamente possibile abilitando o meno determinate azioni e collegando effetti alle stesse[1265] e, in tal modo, hanno la capacità di condizionare ogni altra forma di regolazione, anche quella giuridica, che, di conseguenza, dovrà intervenire a sua volta con regole legislative e indirizzare le regole informatiche, al fine di non far scivolare l'ordinamento in tecnocrazie: il giuridicamente lecito deve restare un sottoinsieme del tecnologicamente possibile[1266]. Come esaminato, il diritto può fare di più: servirsi della

---

[1265] Cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, cit., pp. 501-546; G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione - Corso d'informatica giuridica*, cit., p. 37 ss.; G. SARTOR, *Internet e il diritto*, cit., p. 1 ss.

[1266] Più ampiamente sul rapporto tra macchine e uomini, D. CARDON, *op. cit.*, p. 88: «Piuttosto che fare un dramma del conflitto tra gli umani e le macchine, è più saggio considerarli come elementi di una coppia che non cessano di retroagire e di influenzarsi reciprocamente. La società dei calcoli realizza un nuovo accoppiamento tra individui sempre più potenti e sistemi sociotecnici che a loro volta impongono strutture sempre più forti. Si è ancora in tempo per dire agli algoritmi che noi non siamo la somma imprecisa e incompleta dei nostri comportamenti». Secondo l'Autore, infatti, «è fondamentale lottare contro quella sorta di fatalismo che ci porta a imputare ai sistemi di misura ciò che, in realtà, noi stessi abbiamo chiesto loro di fare» (p. 8).

tecnica per garantire il suo rispetto attraverso soluzioni che preventivamente risolvano aspetti giuridici, ad esempio rendendo impossibili o disabilitando tecnicamente azioni illecite.

Oltre alle regole informatiche, che condizionano il comportamento dell'uomo, nel mondo digitale il diritto si trova di fronte alle regole, per lo più unilaterali, dettate dai colossi del web, potenti controllori del pedaggio per lo svolgimento della vita digitale, privi di legittimazione democratica, guidati non dall'interesse pubblico, ma dalle logiche economiche del mercato e del profitto: le grandi imprese affidano l'applicazione delle proprie regole al codice (non giuridico), foraggiando la dittatura degli algoritmi. Lo spazio di regolazione dei colossi del web deriva proprio dall'assenza e dall'inefficacia di norme a tutela dei diritti, dal carattere sovranazionale delle questioni e dal rispetto sacrale nei confronti della libertà di commercio e dello sviluppo economico[1267].

Pertanto sulla scena digitale, insieme al diritto, convivono, si condizionano e talvolta si integrano altri ecosistemi di regole, quelle informatiche (*lex informatica o digitalis*), quelle dei colossi del web e del mercato (nuova *lex mercatoria*), quelle sociali e la *soft law*[1268]. Di conseguenza il diritto deve recuperare spazio mostrandosi capace di

---

[1267] S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 414: «nuovi e vitalissimi giganti di silicio, i grandi soggetti economici che si identificano con la rete, esercitano estesi e incontrollati poteri di governo, si coalizzano per chiedere regole alla loro misura, mettendo ad esempio in discussione le garanzie previste per la privacy delle persone». Secondo l'Autore «non è possibile lasciare questa tutela soltanto all'iniziativa di soggetti privati, che tendenzialmente offriranno solo le garanzie compatibili con i loro interessi e che, in assenza di altre iniziative, appariranno come le uniche "istituzioni" capaci di intervenire. Non si può accettare una privatizzazione del governo di Internet, ed è indispensabile far sì che una pluralità di attori, ai livelli più diversi, possa dialogare e mettere a punto regole comuni» (p. 415).

[1268] In merito cfr. L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, cit., pp. 501-546, che per determinare il ruolo del diritto nel regolare il ciberspazio richiama i quattro fattori costituiti dalle regole giuridiche, dalle regole sociali, dal mercato e dalle regole informatiche. G. SARTOR, *Internet e il diritto*, cit., p. 5: «Una volta che le regole virtuali abbiano stabilito quali azioni siano virtualmente possibili, a quali condizioni e in quali modi, allora il mercato può stabilire i prezzi per ottenere il consenso o la cooperazione altrui nel compimento di tali azioni. Infine, regole sociali possono qualificare come ammissibili o inammissibili (in certi contesti e in certe comunità) alcune delle azioni abilitate dalle regole virtuali. Allo stesso modo, regole giuridiche possono qualificare le azioni virtualmente possibili come giuridicamente permesse, prescritte o vietate». Come esempio di norme sociali basta pensare alle regole della *netiquette* o all'etica degli *hacker*. Per *soft law* si intendono quelle regole non vincolanti, ma

incidere sulla realtà che vuole regolare: per farlo è necessario acquisisca un approccio *multistakeholder*, che tenga conto dei diversi soggetti e dei differenti interessi implicati nel governo dei dati e riesca a integrare i diversi ecosistemi di regole.

La realtà globale della rete, inoltre, implica un mutamento nei confini geografici della regolamentazione e rende necessario arrivare a soluzioni condivise a livello sovranazionale e internazionale in merito alla protezione dei diritti, che nel web "vivono globalmente", possono essere oggetto di violazioni da qualsiasi parte del mondo e che, di conseguenza, hanno bisogno di una tutela globale[1269]. La veste sovranazionale è necessaria a garantire efficacia alle norme, evitando la tensione altrimenti fisiologica tra la dimensione globale delle questioni e la dimensione territoriale delle disposizioni da applicare.

---

non irrilevanti per il diritto che propongono soluzioni, anche basate sulla prassi, svolgendo una funzione ausiliaria di indirizzo che influisce sul comportamento dei destinatari, sia per interpretare norme che per sopperire a lacune normative, come linee guida, *policy*, comunicazioni; in senso analogo, nella prospettiva internazionale cfr. U. DRAETTA, *Internet nel diritto internazionale*, in G. FINOCCHIARO - F. DELFINI (a cura di), *op. cit.*, p. 15 e G. NOTO LA DIEGA, *Il cloud computing. Alla ricerca del diritto perduto nel web 3.0*, in *Europa e diritto privato*, fasc. 2, 2014, pp. 577-658, che mette in evidenza la centralità della *soft law* e della produzione normativa delle autorità amministrative indipendenti nell'attualità.

[1269] Sul carattere aterritoriale della rete, fattore e prodotto della globalizzazione, e sugli effetti della deterritorializzazione cfr. G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., p. 323 ss., che sottolinea come ci siano altri fenomeni per i quali i confini statuali appaiono irrilevanti, come l'ambiente, il contrasto alla criminalità internazionale, i beni culturali dell'umanità; l'emersione del pluralismo giuridico è particolarmente visibile nelle aree della *lex mercatoria*, delle imprese multinazionali, dei diritti umani, del diritto del lavoro. La globalizzazione mette in crisi il concetto di sovranità dello Stato, aggrega i soggetti sulla base del loro *status* e dell'appartenza a comunità digitali indipendenti dai luoghi territoriali. In merito G. AZZARITI, *op. cit.*, p. 1 ss. suggerisce di non affidarsi a processi spontanei di autoregolamentazione che inevitabilmente condurrebbero alla concentrazione di potere nelle mani dei soggetti attualmente più forti, Stato e *corporation*, con possibili torsioni autoritarie, ma ritiene sia necessaria una regolamentazione, un *corpus* complesso e articolato sul piano globale in conformità alla dimensione di Internet, che non consiste in una immaginifica costituzione globale, ma in un percorso che è quello della «lenta definizione di Carte internazionali di principi elaborate dai diversi attori non necessariamente istituzionali, ma anche espressione della società civile globale».

La riflessione e la regolamentazione deve essere ampia non solo nello spazio, ma anche nell'oggetto di analisi, partendo dai principi cardine e dalle relazioni tra i diritti che caratterizzano le diverse configurazioni dei dati, sui quali si erge l'esistenza digitale.

In questo senso è da accogliere con favore il tentativo di emanare una Dichiarazione dei diritti in Internet, proprio per la centralità della questione relativa alla protezione delle libertà nell'era contemporanea[1270], anche se necessariamente, per quanto suddetto, non potrà limitarsi solo ai confini nazionali, ma auspicabilmente dovrà essere base di riflessione per una Dichiarazione condivisa a livello sovranazionale, come del resto la stessa Dichiarazione italiana evidenzia nel preambolo[1271]. Una Dichiarazione dei diritti appare atto adeguato per frenare l'invadenza degli Stati, ma anche la nuova "signoria" dei colossi del web, altrettanto capaci di governare le nostre esistenze[1272].

1270 S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 94: «La lotta per i diritti è l'unica, vera, grande narrazione del millennio appena iniziato. Si distende sull'intero mondo globalizzato, costruisce modalità nuove dell'azione e soggetti che la incarnano, e va oltre la tradizionale e indispensabile difesa contro ogni potere oppressivo, perché si presenta come la sola in grado di contrapporsi alla volontà di imporre al mondo una nuova e invincibile legge naturale, quella del mercato, con la sua pretesa di incorporare e definire anche le condizioni per il riconoscimento dei diritti». Secondo l'Autore «è in corso una ininterrotta, inedita, quasi quotidiana dichiarazione dei diritti, che nasce dai comportamenti rivendicativi di una molteplicità crescente di soggetti. La rete è, al tempo stesso, luogo e condizione perché tutto questo assuma forma concreta» (p. 416).

1271 Nel Preambolo della Dichiarazione dei diritti in Internet si precisa che «una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale». Secondo A. MASERA - G. SCORZA, *op. cit.*, pp. 87-88 la Dichiarazione dei diritti in Internet «non è che il primo approdo del dibattito sulla necessità di condivisione democratica di principi, norme, regole, procedure decisionali che accompagnino l'evoluzione di Internet, lo spazio più grande in cui l'umanità si trova a interagire senza limiti né confini». S. CASSESE, *Stato in trasformazione*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 2016, p. 331 ss.: «i confini divengono manipolabili. La cittadinanza perde importanza. La sovranità esclusiva diventa condivisa»; «i confini sono sempre di più "porosi" e "malleabili": vengono varcati, si perdono, si rafforzano, avanzano, arretrano, si ridefiniscono. Sono, in una parola, soggetti a forti mutamenti, dettati da esigenze diverse, alcune di chiusura, altre di apertura (elasticità delle frontiere)».

1272 Cfr. S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 417.

La nuova realtà esige, pertanto, un inedito percorso costituente globale, idoneo a delineare condivisi principi e comuni direttrici del governo dei dati[1273] e capace di individuare principi comuni tra sistemi giuridici molto diversi (europeo e statunitense) e anche tra diversi ecosistemi di regole[1274]: tale percorso, che per le caratteristiche che deve possedere può proficuamente aver luogo all'interno dell'*Internet Governance Forum*[1275], dovrebbe condurre all'approvazione di una costituzione globale, auspicata da Rodotà, fonte normativa condivisa in cui l'approccio al governo dei dati, che è stato esaminato, possa trovare espressione[1276]. L'approdo a un atto del genere non significa

---

[1273] Secondo S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 425 nel contenuto di una Costituzione per Internet «s'intrecciano finalità d'ordine generale, veri e propri principi direttivi, con la loro traduzione in specifici diritti. Se, ad esempio, si muove dalla constatazione che Internet rappresenta il più largo spazio pubblico che l'umanità abbia conosciuto, la salvaguardia di questa sua "natura" implica l'irriducibilità alla dimensione sempre più assorbente del mercato, che vuol dire non solo un generico riconoscimento della libertà in rete, ma la concreta possibilità di esercitare "virtù civiche", dunque di dar corpo a una cittadinanza attiva».

[1274] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, cit., p. 683 ss.: «La circostanza che nessuno fisicamente possieda le onde del mare, l'aria attraverso la quale volano gli aerei o sono trasmesse le onde radio, e che lo spazio extra-terrestre è al di fuori dell'ordinario controllo degli Stati non ha impedito lo sviluppo di regole comuni le quali consentono la cooperazione internazionale nelle attività marittime, aeree, di telecomunicazione e satellitari. Anche in questi casi si è di fronte ad attività che originano da un paese e sono destinate ad altri paesi, spesso attraverso o sopra altri paesi, o su territori internazionali».

[1275] L'*Internet Governance Forum* (IGF) è un forum multilaterale e *multistakeholder* teso a facilitare il dibattito circa le principali problematiche relative alla *governance* di Internet, promosso dalle Nazioni Unite, istituito e convocato per la prima volta nel 2006: non ha poteri decisionali, ma un ruolo propositivo che si esprime per mezzo di raccomandazioni. Si riunisce periodicamente a livello mondiale, regionale e locale; il dibattito avviene tra i soggetti interessati (rappresentanti del settore pubblico, privato e società civile), in modo aperto e paritario. Cfr. *www.intgovforum.org*.

[1276] S. RODOTÀ, *Il diritto di avere diritti,* cit., p. 426 parla di «destrutturazione/ricostruzione del rapporto tra sfera pubblica e sfera privata» e individua le vie di un costituzionalismo globale possibile in «una costruzione del diritto per espansione, orizzontale, un insieme di ordini giuridici correlati, non punto d'arrivo, ma strutturati in modo da sostenere la sfida di un tempo sempre mutevole, quasi una costituzione infinita». In merito T.E. FROSINI, *Costituzionalismo 2.0*, cit., p. 673 ss. parla del costituzionalismo come "tecnica della libertà", che si declina «nella separazione dei poteri, nelle garanzie costituzionali e nella tutela dei diritti fondamentali, che sono, infatti, delle tecniche per l'affermazione della libertà dell'individuo, ovvero rappresentano il modo attraverso il quale svolgere una continua ricerca sul come

inficiare le sovranità statuali, dal momento che naturalmente la regolazione di dettaglio resterebbe affidata ai sistemi sovranazionali (come gli atti dell'Unione europea) e ai singoli ordinamenti giuridici e la regolamentazione dei singoli rapporti, altresì, sarebbe rimessa all'autonomia negoziale, guidata da norme e linee guida, talvolta limitata da tutele collettive finalizzate a preservare libertà e diritti[1277].

Infatti, il cambiamento indotto dai *big data* e dalla società degli algoritmi non consente di accontentarsi di modifiche e integrazioni, che finiscono per essere semplici "toppe" giuridiche e aggiustamenti di disciplina idonei ad adattare la protezione analogica dei diritti alla realtà digitale, dal momento che il cambiamento quantitativo dei dati, come esaminato, ha indotto un cambiamento di stato che necessita a sua volta di un cambiamento di paradigma anche giuridico[1278].

---

affermare e garantire il diritto di libertà individuale»; secondo l'Autore il costituzionalismo è «un percorso attraverso il quale si delinea l'assetto del convivere civile, dove si costruisce un sistema ordinamentale che si fonda sulla libertà dell'individuo» (p. 674). Nell'era digitale la sfida del costituzionalismo «è, prevalentemente, quella riferita alla tecnologia, ovvero come dare forza e protezione ai diritti di libertà dell'individuo in un contesto sociale profondamente mutato dall'innovazione tecnologica e i suoi derivati in punto di diritto» (p. 675). L'Autore parla di un "costituzionalismo 2.0" per caratterizzare «il connubio fra il costituzionalismo e la tecnologia, e quindi come i diritti di libertà possono trovare espressione e tutela nella società tecnologica» (p. 676); per Internet parla di ordinamento autonomo come un diritto spontaneo, simile alla *lex mercatoria*, una *lex informatica* che si avvale della *co-regulation* degli Stati che viene in sussidio della *self-regulation* degli utenti, secondo una sorta di principio di sussidiarietà.

[1277] V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, cit., p. 683 ss.: «Qualche indicazione potrebbe trarsi dal c.d. "Internet Bill of Rights", ma questo copre solo una parte assai limitata di un quadro ben più ampio. Il governo di uno "spazio" così grande come le reti globali richiede certamente l'individuazione e l'affermazione di diritti individuali, ma anche obblighi, doveri, norme dispositive, rimedi, regole per risolvere le controversie. Da questo punto di vista, da una prospettiva internazionale siamo ancora lontani da un assetto ancora embrionale».

[1278] V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 231 ss. Secondo G. PELLERINO, *op. cit.*, p. 256 il diritto in una prima fase ha tentato di adattarsi alla nuova realtà utilizzando teorie e argomentazioni tradizionali, tentando di "addomesticare" i fenomeni in istituti e categorie del diritto, spesso senza coglierne le peculiarità (è il caso del diritto d'autore) o ha abdicato alla regolazione come nel caso della *governance* di Internet.

Sotto l'evoluzione della realtà sta mutando il sistema giuridico, che vede una dimensione globale di riferimento, la destatalizzazione delle fonti di diritto, l'autoregolamentazione e l'affermazione di sistemi diversi da quello giuridico capaci di produrre regole, il mutamento e l'evoluzione dei diritti fondamentali[1279]. Qualcosa di simile è avvenuto con la regolazione del mare, ugualmente privo di frontiere, confini e sovrani, per il quale si sviluppò un diritto pattizio, una *lex mercatoria* nella cui formazione grande influenza hanno avuto i destinatari delle norme[1280].

Di conseguenza, è necessaria una tutela giuridica che innovi in profondità i meccanismi di protezione e sia capace di riportare il bilanciamento tra interessi al diritto, ossia alle norme deputate ontologicamente a farlo, fornisca tutele individuali e collettive e attribuisca il momento conflittuale all'autorità giudiziaria, senza affidarsi in modo incongruo ad autorità amministrative, snaturandole, o, ancora peggio, a soggetti privati, fortificando il loro dominio in materia[1281].

[1279] Cfr. G. PELLERINO, *op. cit.*, p. 256 ss., che ricorda la funzione di sistema immunitario svolta dal diritto, che consente di reagire a situazioni impreviste, e sottolinea come nella concezione giuspositivista il diritto non debba tollerare lacune: si tratta di aspetti difficili da rispettare nel mutato contesto della società tecnologica. F. DI CIOMMO, *op. cit.*, p. 548 ss. reputa tale rivoluzione tecnologica più inesorabile delle precedenti e sottolinea come questo metta in crisi il diritto, che «soffre la fissità e la vetustà delle sue categorie tradizionali» e vede travolta la sua concezione formale e statuale. Nella rete cambia il rapporto dell'individuo «con il tempo, con lo spazio, con le informazioni, con la propria identità nazionale, con la propria lingua, con le altre persone, con i mercati e con le cose. Parlare di svolta epocale e di nuova era non è, dunque, esagerato. Il punto, per il giurista, è capire come (e se) il diritto è realmente pronto per svolgere, nei confronti del "ciberspazio", la sua funzione ordinatrice». Peraltro si pongono problemi significativi in merito a chi sia legittimato a regolare Internet e in relazione a quale efficacia abbiano le regole: le posizioni sono svariate tra autoregolazione, regolazione statale e regolazione mista tra Stato e mercato.

[1280] In proposito cfr. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 378 ss., che ricorda l'utilizzo della locuzione "navigare in rete"; L. NANNIPIERI, *op.cit.*, p. 2; G. PELLERINO, *op. cit.*, p. 262 ss., che si chiede come debba intervenire il diritto, se con fonte pattizia o autoritativa, se attraverso meccanismi di controllo o aumento delle libertà.

[1281] In questo senso si può leggere anche il preambolo della Dichiarazione dei diritti in Internet: «La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale».

Punto di partenza e di arrivo di questa nuova riflessione e della conseguente regolamentazione è in ogni caso la persona da tutelare nella sua esistenza digitale, che deve mantenere il libero arbitrio, la propria autonomia e la responsabilità individuale senza cadere sotto l'ottimismo dell'affidamento alle predizioni[1282]. In questo senso è opportuno pretendere maggiore trasparenza da parte del mercato e, in particolare, da parte dei *big player*, chiedendo non certo di svelare segreti aziendali legati agli algoritmi, ma di rendere evidenti e trasparenti la logica e i criteri seguiti dagli algoritmi, ossia cosa determina le decisioni all'interno dei servizi che utilizzano gli utenti, in linea peraltro con le previsioni del regolamento (UE) 2016/679[1283].

Deve essere affrontata con coraggio la sfida di adeguare la tutela giuridica alla realtà attuale, facendo sì che il diritto assolva al suo compito di fornire regole su cui fondare la civile e democratica convivenza.

In tal senso e per tali motivi anche lo stesso regolamento europeo 2016/679 in materia di *data protection* rischia di non essere sufficientemente innovativo laddove propone ancora con forza la logica dell'informativa e del consenso, che si motivano col rispetto dell'autonomia della persona, ma opportunamente accompagna le tradizionali metodologie a soluzioni in linea con il mondo dei *big data* e degli algoritmi, come l'approccio preventivo e tecnologico *by design* e *by default*, il rafforzamento dell'*accountability* di chi utilizza i dati e la presenza di efficaci sistemi sanzionatori.

Il futuro necessita di un complesso e coraggioso percorso corale che conduca a una costituzione globale, capace di disegnare una base solida e condivisa per la tutela dei diritti e la protezione delle libertà nel governo dei dati[1284].

1282 Cfr. V. MAYER-SCHÖNBERGER - K. CUKIER, *op. cit.*, p. 261 ss., secondo i quali la potenzialità non deve essere sacrificata sull'altare della probabilità, imprigionando gli individui alle azioni precedenti usate per prevedere i comportamenti ed, eventualmente, punirli.

1283 Nelle informazioni da fornire all'interessato, necessarie «*per garantire un trattamento corretto e trasparente*», gli artt. 13 e 14, reg. (UE) 2016/679 pongono «*l'esistenza di un processo decisionale automatizzato, compresa la profilazione […], e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*». D. CARDON, *op. cit.*, p. 68 ss. parla di «nuova rivendicazione di un *dovere di lealtà* delle piattaforme nei confronti dei loro utenti» (p. 69).

1284 F. AMORETTI - E. GARGIULO, *Dall'appartenenza materiale all'appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, cit., p. 25: «Soltanto attraverso un sistema di limiti e vincoli imposti tanto al potere arbitrario esercitato dagli

Alla luce di quanto detto, il metodo di formazione di questo atto costituzionale globale dovrebbe essere diverso rispetto ai tradizionali; per poter essere efficace ed effettivo necessita di una genesi *multilevel* che, in un approccio *multistakeholder*, si avvalga dei diversi portatori di interessi e di una conseguente corresponsabilità da parte dei differenti produttori di norme, giuridiche o meno, della nostra contemporaneità[1285]: poteri pubblici, ma anche poteri privati, capaci di dettare regole di accesso all'esistenza digitale, università e mondo della ricerca ed associazioni e organismi collettivi capaci di interpretare gli interessi di cittadini e imprese. In questo contesto gli Stati sono chiamati a nuove forme di cooperazione e collaborazione[1286].

Nella sua natura globale, dovrebbe trattarsi di un atto snello e leggero, ma significativo, un *Internet Bill of Rights*, una Dichiarazione dei diritti, capace di

---

Stati nei confronti degli individui quanto al potere – altrettanto arbitrario ma forse ancora più insidioso, perché meno visibile – esercitato dalle grandi *corporations* nei confronti degli stessi soggetti è infatti possibile sperare che la cittadinanza, a livello mondiale, divenga più inclusiva. Strada ardua, si è detto, e purtroppo ancora estranea a molte delle forze in gioco».

[1285] In merito la comunicazione della Commissione europea «*Verso una florida economia basata sui dati*» COM(2014) 442 *final* del 2 luglio 2014 parla di partenariati pubblico-privato per una cooperazione strategica sui dati, creando incentivi alla condivisione e meccanismi che facilitino il trasferimento delle conoscenze e delle tecnologie, collaborando a tal fine anche con istituti di ricerca e università. Secondo S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 418 «è indispensabile far sì che una pluralità di attori, ai livelli più diversi, possa dialogare e mettere a punto regole comuni, secondo un modello definito appunto *multistakeholder* e *multilevel*. Soggetti diversi, a livelli diversi, con strumenti diversi negoziano e si legano con impegni reciproci per individuare e rendere effettivo un patrimonio comune di diritti». Secondo A. MASERA - G. SCORZA, *op. cit.*, pp. 92-93 una regolamentazione efficace di Internet deve integrare i diversi livelli territoriali e tre diverse fonti normative, di per sé necessarie ma non sufficienti: le tre fonti sono costituite dall'autoregolamentazione di Internet, molto importante per la definizione delle regole tecniche, la regolamentazione degli Stati nazionali con i loro intrinseci limiti territoriali e il sistema di direttive, accordi, protocolli, europei e internazionali, che di norma hanno maggiore efficacia e minore cogenza.

[1286] Sulla *co-regulation* cfr. L. LESSIG*, Code and Other Law of Cyberspace*, cit. Secondo S. RODOTÀ*, Il diritto di avere diritti,* cit., p. 419 è necessaria «una partecipazione larga di una molteplicità di soggetti che possono intervenire in modo attivo, grazie soprattutto a una tecnologia che mette tutti e ciascuno in grado di formulare progetti, di metterli a confronto, di modificarli, in definitiva di sottoporli a un controllo e a una elaborazione comuni, di trasferire nel settore della regolazione giuridica forme e procedure tipiche del "metodo *wiki*", dunque con progressivi aggiustamenti e messe a punto dei testi proposti».

disegnare quell'approccio etico, preventivo e tecnologico di tutela *by design* e *by default* che si avvalga delle soluzioni di riequilibrio delle asimmetrie di tutele collettive e apertura dei *big data*, responsabilizzi e punisca in modo efficace le violazioni. Tale atto, sottoposto a meccanismi di consultazione pubblica, dovrebbe porsi come vera e propria fonte del diritto capace di realizzare un equilibrio "attivo" con la tecnica, senza domarla, ma senza neppure essere dominato[1287].

Al fine di consentire il rispetto di un tale atto, può essere opportuno immaginare autorità sovranazionali indipendenti da quei poteri che hanno interesse a indirizzare il governo dei dati (mercato e governi), alle quali sia deputata, fermo il ruolo del potere giurisdizionale in relazione ai conflitti, la tutela dei diritti nella *data governance*, in un'ottica che non sia verticale sui singoli diritti, ma che più ampiamente tratti in modo unitario il governo dei dati e i diritti che ne sono implicati (identità, protezione dei dati personali, oblio, diritto d'autore, tutela della concorrenza, tutela dei consumatori), fornendo *policy*, linee guida, standardizzazioni in termini di sicurezza e indicazioni per

---

[1287] Cfr. M. PIETRANGELO, *Il diritto e le tecnologie informative: qualche proposta per il nuovo millennio*, in G. PERUGINELLI - M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, Napoli, 2014, p. 621 ss., che auspica per il diritto «un ruolo attivo, ma *leggero*, privo di peso» (p. 623) e suggerisce di guardare alla necessaria complementarietà tra tecnica e diritto, fino ad arrivare a ripensare alcune categorie giuridiche tradizionali. M. OREFICE, *op. cit.*, p. 733 ss., sembra preferire la strada dell'*hard law*, quale parametro vincolante per i giudici, che comunque ne rafforzerebbe il ruolo come via per un riconoscimento di diritti più visibili. Altrimenti la via della *soft law* renderebbe la Carta punto di riferimento ermeneutico normativo e giurisprudenziale e elemento di orientamento, ma possedendo una natura sostanzialmente politica affiderebbe alla sorte di fatto il rispetto di regole, principi e diritti, ossia un'elencazione di diritti non rivendibili di fronte al potere giurisdizionale. Cfr. G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, cit., p. 831 ss., la quale ritiene che «il diritto (o la politica, in taluni casi) debba stabilire gli obiettivi (se non addirittura i valori) e che la tecnica debba essere il mezzo per raggiungerli. La tecnica deve essere etero-diretta o quanto meno dall'esterno controllata» (p. 838). «Il dialogo è essenziale, la comprensione reciproca anche, ma nel rispetto dei rispettivi ruoli. È importante ristabilire rispetto e confini, rivendicando con orgoglio il ruolo del giurista» (p. 840). In merito D. POLETTI, *op. cit.*, p. 8 ss. evidenzia il problema dell'individuazione del potere costituente transnazionale e le condizioni di tale esercizio. Sull'*Internet Bill of Rights* e se un tale atto debba essere basato su *self-regulation* o regole vincolanti cfr. G. DE MINICO, *Towards an Internet Bill of Rights*, in *federalismi.it*, fasc. 5, 2016, pp. 1-33.

bilanciamenti omogenei dei diritti[1288]. Il ruolo di siffatte autorità indipendenti potrebbe essere significativo e incisivo nei confronti dei *big player*: avrebbero il potere e l'indipendenza necessari per esigere trasparenza nelle azioni e nei criteri seguiti dagli algoritmi nel governo dei *big data*[1289]. Potrebbe trattarsi di un'autorità sovraordinata formata dalle competenze delle attuali autorità in un approccio olistico idoneo a rispettare la globalità delle questioni e della necessaria conseguente tutela.

Lo stesso *European Data Protection Supervisor* (EDPS) nel 2015 evidenzia la necessità di un approccio etico condiviso e multidisciplinare tra i diversi regolatori e le diverse autorità, per fornire raccomandazioni e informare la società: istituisce a tal fine un *European Ethics Advisory Board* esterno sulla dimensione etica della protezione dei dati, deputato a esaminare le relazioni tra diritti umani, tecnologia, mercati e modelli di business, attivo dal 2016[1290]. In modo analogo poi, nel 2016, l'*European Data Protection Supervisor* ha suggerito maggior dialogo e più intensa cooperazione tra le autorità e i soggetti che regolamentano i comportamenti nell'ambiente digitale a tutela della protezione dei dati personali, della libertà di espressione, della non discriminazione, della concorrenza e della tutela dei consumatori e ha richiesto, a tal fine, l'istituzione di una struttura di coordinamento digitale, un *Digital Clearing House*, ossia una rete a partecipazione volontaria di organismi di regolamentazione che

---

[1288] A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 141 suggerisce di introdurre obblighi di notificazione in merito alle grandi banche di dati, obbligo che ricorreva nelle prime legislazioni in materia di protezione dei dati personali: secondo l'Autore esiste un'analogia tra l'epoca dei *mainframe* e quella attuale del *cloud computing* e dei *big data*, dal momento che «nuovamente (pur restando un potere informatico distribuito) le grandi risorse informatiche si concentrano in mano a pochi soggetti e risultano anche fisicamente aggregate in enormi *data center*. È dunque nuovamente possibile conoscere chi crea tali grandi basi di dati, chi le gestisce e, quindi, porre in essere le attività di controllo necessarie a garantire la sicurezza delle informazioni inerenti i cittadini». In relazione specificamente alla costruzione del diritto della privacy, secondo R. BIFULCO, *op. cit.*, p. 289 ss. l'indipendenza delle autorità di controllo serve proprio a permettere il più adeguato bilanciamento delle esigenze di tutela dei diritti, ferma restando la possibilità di ricorrere al potere giurisdizionale.

[1289] D. CARDON, *op. cit.*, p. 70 e A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, cit., p. 142.

[1290] In tal senso l'*Opinion* 4/2015 «*Towards a new digital ethics. Data, dignity and technology*» dell'11 settembre 2015.

permetta di condividere informazioni, entro i limiti delle rispettive competenze, circa i possibili abusi nell'ecosistema digitale e il modo più efficace di contrastarli, al fine dell'applicazione delle normative nel settore digitale dell'Unione europea [1291].

Nel futuro si scorge una Dichiarazione dei diritti condivisa, capace di contenere i principi di bilanciamento e il necessario approccio di tutela e idonea a consegnare ai singoli sistemi sovranazionali e ordinamenti giuridici la regolazione di dettaglio e lasciare all'autonomia negoziale, guidata da *policy*, la regolamentazione dei singoli rapporti, ferme restando le eccezioni affidate a tutele collettive che sottraggono al singolo la capacità di disporre della sua autonomia e di incidere sull'intera comunità.

Si delinea un percorso complesso, come lo è del resto la rivoluzione digitale che interessa gli uomini e la società, di cui già si vedono timidi accenni: risulta la via più opportuna per ristabilire il ruolo del diritto e la forza dei diritti, senza essere travolti da macchine e algoritmi, annullati in statistiche e predizioni; il valore della persona deve recuperare la propria dignità e la capacità di incidere nella *data governance*. Altrimenti il sostanziale silenzio del diritto porterà inevitabilmente "il possibile tecnologicamente", il mercato o la prassi agita a dettare le regole, come in parte sta già accadendo.

Il governo dei dati non può essere lasciato all'automatismo della tecnica e all'elaborazione degli algoritmi, ma deve essere disegnato dalla mano dell'uomo e dalle regole del diritto.

Ubi data society, *ibi ius*[1292].

[1291] *Opinion* 8/2016 «*Opinion on coherent enforcement of fundamental rights in the age of big data*» del 23 settembre 2016 dell'*European Data Protection Supervisor* (EDPS).

[1292] Si tratta di un adattamento alla *data society* del brocardo *ubi societas ibi ius, ubi ius ibi societas*, al fine di indicare che l'odierna società e il governo dei dati hanno bisogno di fondarsi sulle regole del diritto, anche per non rendere tutto ciò che è tecnologicamente possibile, solo per questo, giuridicamente legittimo, come suggeriva S. RODOTÀ, *Intervista su privacy e libertà*, cit. Al riguardo V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, cit., p. 683 ss.: «Non solo non si può sfuggire alla millenaria saggezza dell'*ubi societas ibi ius* (e le reti di telecomunicazione sono una parte, molto importante, delle società contemporanee) ma, ancor più importante, occorre evitare di creare nuovi tabù (Internet è al di fuori del diritto) che favoriscono un fenomeno opposto: l'utilizzo da parte degli Stati di pratiche occulte, segrete se non illegali». Sulla teoria del diritto e sul concetto di ordinamento giuridico cfr. S. ROMANO, *L'ordinamento giuridico*, II ed., Sansoni, Firenze, 1945.

Bibliografia

ABELSON H. - LESSIG L. (*et al.*), *Digital identity in cyberspace*. *White paper submitted for 6.805/ Law of Cyberspace: Social Protocols*, *6*, 1998.

ACKERMAN J.M. - SANDOVAL-BALLESTEROS I.E., *The Global Explosion of Freedom of Information Laws*, in *Administrative Law Review*, vol. 58, n. 1, 2006, p. 85 ss.

AGNOLONI T., Linked Open Data *nel dominio giuridico*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 411-430.

AGNOLONI T., *Dall'informazione giuridica agli* open data *giuridici*, in G. PERUGINELLI - M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, Napoli-Roma, 2014, pp. 581-602.

AGRÒ L., *Internet of Humans*, Egea, Milano, 2017.

ALBERTI C., *La disciplina del diritto di accesso nel post Amsterdam tra consacrazione e limitazione*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 1, 2003, pp. 55-97.

ALIPRANDI S., Open licensing *e banche dati*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 25-43.

ALLEGRI M.R., *Riflessioni e ipotesi sulla costituzionalizzazione del diritto di accesso a internet (o al ciberspazio?)*, in *Rivista AIC*, fasc. 1, 2016, pp. 1-31.

ALOVISIO M., *Criticità Privacy nel riuso dei dati pubblici*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 45-64.

AMATO MANGIAMELI A.C., *Diritto e cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Giappichelli, Torino, 2000.

AMATO MANGIAMELI A.C., *Informatica giuridica. Appunti e materiali ad uso di lezioni*, II ed., Giappichelli, Torino, 2015.

AMORETTI F. (a cura di), *Diritti e sfera pubblica nell'era digitale,* numero speciale in *Politica del diritto,* fasc. 3, 2010.

AMORETTI F. - GARGIULO E., *Dall'appartenenza materiale all'appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione*, in *Politica del diritto*, fasc. 3, 2010, pp. 353-389.

ANDREJEVIC M., *The Big Data Divide*, in *International Journal of Communication*, n. 8, 2014, pp. 1673-1689.

ANGELINI F.G., *Pubblica amministrazione digitale, diritto di accesso e privacy*, in L. BOLOGNINI - D. FULCO - P. PAGANINI (a cura di), *Next privacy. Il futuro dei nostri dati nell'era digitale*, Etas, Milano, pp. 249-273.

ARENA G., *Trasparenza amministrativa* (voce), in S. CASSESE (diretto da), in *Dizionario di diritto pubblico*, vol. VI, Giuffrè, Milano, 2006.

ARMAO G., *Considerazioni su amministrazione aperta e protezione dei dati personali*, in *Amministrativ@mente*, fasc. 3-4, 2015, pp. 1-8.

ASHTON K., *That "Internet of Things" Thing*, in *RFID Journal*, 22 giugno 2009.

AUTELITANO F., *La rilevanza delle banche dati nel sistema del "cyberlaw"*, in *I Contratti*, fasc. 10, 1999, pp. 925-935.

AZZARITI G., *Internet e Costituzione,* in *Costituzionalismo.it,* fasc. 2, 2011, pp. 1-6.

BADOCCO F., *Riflessioni sul diritto di accesso a Internet nell'ambito del diritto dell'Unione europea*, in *Informatica e diritto*, fasc. 1, 2009, pp. 153-163.

BANISAR D., *Freedom of Information Around The World 2006*. *A Global Survey of Access to Government Information Laws*, 2006, *www.humanrightsinitiative.org*.

BARONE E., *Diritto d'autore e ICT*, in M. MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Tangram edizioni scientifiche, Trento, 2017, pp. 313-324.

BASSI E., *PSI, protezione dei dati personali, anonimizzazione*, in D. TISCORNIA (a cura di), *Open data e riuso dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 65-83.

BASSINI M., *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quaderni costituzionali*, fasc. 3, 2014, pp. 730-733.

BAUMAN Z. - LYON D., *Sesto potere. La sorveglianza nella modernità liquida*, trad. it., GLF Editori Laterza, Economica, Roma-Bari, 2015.

BAVETTA G., voce *Identità (diritto alla)*, in *Enciclopedia del diritto*, vol. XIX, Milano, 1970, pp. 953-957.

BELISARIO E., *La nuova Pubblica Amministrazione Digitale. Guida al Codice dell'Amministrazione Digitale dopo la Legge n. 69/*2009, Maggioli, Rimini, 2009.

BELISARIO E. - COGO G. - SCANO R., *I siti web delle pubbliche amministrazioni. Norme tecniche e giuridiche dopo le Linee Guida Brunetta*, Maggioli, Rimini, 2011.

BENKLER Y., *La ricchezza della Rete. La produzione sociale trasforma il mercato e aumenta le libertà*, trad. it., Università Bocconi Editore - Egea, Milano, 2007.

BENTHAM J., *Panopticon ovvero la casa d'ispezione*, a cura di M. FOUCAULT - M. PERROT, trad. it., Marsilio, Venezia, 1983.

BERGADANO F. - MANTELERO A. - RUFFO G. - SARTOR G., *Privacy digitale: giuristi e informatici a confronto*, Giappichelli, Torino, 2005.

BETZU M., *Interpretazione e sovra-interpretazione dei diritti costituzionali nel cyberspazio*, in *Rivista AIC*, fasc. 4, 2012, pp. 1-8.

BIANCO C. - RADICETTI F., *Profili normativi e problematici dell'Accesso civico (nota a Cons. Stato, sez. IV, 12 agosto 2016, n. 3631)*, in *Rassegna dell'avvocatura dello Stato*, fasc. 4, 2016, pp. 129-141.

BIASOTTI A., *Il nuovo regolamento europeo sulla protezione dei dati. Una guida pratica alla nuova privacy e ai principali adempimenti del Regolamento UE 2016/679 aggiornata alle più recenti interpretazioni e disposizioni normative*, II ed., EPC editore, Roma, 2017.

BIFULCO R., *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giurisprudenza costituzionale*, fasc. 1, 2016, pp. 289-307.

BOBBIO N., *Il futuro della democrazia*, Einaudi, Torino, 1995.

BOGNI M. - DEFANT A., *Big data: diritti IP e problemi della privacy*, in *Il Diritto industriale*, fasc. 2, 2015, pp. 117-126.

BOLOGNINI L. - FULCO D. - PAGANINI P. (a cura di), *Next privacy. Il futuro dei nostri dati nell'era digitale*, Etas RCS, Milano, 2010.

BOLOGNINI L. - PELINO E. - BISTOLFI C., *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016.

BOMBARDELLI M., *Fra sospetto e partecipazione: la duplice declinazione del principio di trasparenza*, in *Istituzioni del Federalismo*, fasc. 3-4, 2013, pp. 657-685.

BOMBELLI G., *Tecnologia, diritto, antropologia: appunti sull'*Information (Knowledge) Society, in M. MEGALE (a cura di), *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2012, pp. 22-37.

BONOMO A., *Informazione e pubbliche amministrazioni. Dall'accesso ai documenti alla disponibilità delle informazioni*, Cacucci, Bari, 2012.

BORRUSO R., *Computer e diritto*, 2 tomi, Giuffrè, Milano, 1988.

BORRUSO R., voce *Informatica giuridica*, in *Enciclopedia del diritto*, agg., I, Milano, 1997, p. 640 ss.

BORRUSO R. - DI GIORGI R.M. - MATTIOLI L. - RAGONA M. (a cura di), *L'informatica del diritto*, Giuffrè, Milano, 2004.

BORRUSO R. - RUSSO S. - TIBERI C., *L'informatica per il giurista. Dal bit a Internet*, III ed., Giuffrè, Milano, 2009.

BRENNA R., *La protezione dei dati nel Codice della privacy*, in M. MEGALE (a cura di), *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2012, pp. 117-137.

BRIGHI R., *Dati informatici e modelli dei dati. Verso "una nuova dimensione della realtà"*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 281-293.

BRIGHI R. - ZULLO S. (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015.

BUCCOLIERO L., *Il governo elettronico. Modelli, strategie ed elementi di valore per una pubblica amministrazione digitale*, Tecniche nuove, Milano, 2009.

CALIFANO L., *Trasparenza e privacy: la faticosa ricerca di un bilanciamento mobile*, in L. CALIFANO - C. COLAPIETRO (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014, p. 35 ss.

CALIFANO L. - COLAPIETRO C. (a cura di), *Le nuove frontiere della trasparenza nella dimensione costituzionale*, Editoriale scientifica, Napoli, 2014.

CALZOLAIO S., Digital (and privacy) by default. *L'identità costituzionale della amministrazione digitale*, in *Giornale di storia costituzionale*, fasc. 31, 2016, pp. 185-199.

CANALE C., *Internet e le nuove frontiere di tutela della privacy alla luce delle ultime sentenze della Corte di Cassazione e della Corte di Giustizia Europea*, in *Temi romana*, fasc. 2, 2015, pp. 12-24.

CARDARELLI F., *Amministrazione digitale, trasparenza e principio di legalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, pp. 227-273.

CARDON D., *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Mondadori Università, Milano, 2016.

CARLONI E., *La riforma del Codice dell'amministrazione digitale (commento al Decreto legislativo 30 dicembre 2010, n. 235)*, in *Giornale di diritto amministrativo*, fasc. 5, 2011, pp. 469-476.

CARLONI E., *I principi del codice della trasparenza (artt. 1, commi 1 e 2, 2, 6)*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Maggioli, Rimini, 2013, pp. 29-55.

CARLONI E. (a cura di), *L'amministrazione aperta. Regole strumenti e limiti dell'open government*, Maggioli, Rimini, 2014.

CARLONI E., *Le Linee guida del Garante: protezione dei dati e protezione dell'opacità (commento a provv. Autorità garante protezione dati personali 15 maggio 2014)*, in *Giornale di diritto amministrativo*, fasc. 11, 2014, pp. 1113-1121.

CARLONI E., *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Giornale di diritto amministrativo*, fasc. 2, 2015, pp. 148-157.

CARLONI E., *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, in *Rassegna Astrid*, fasc. 4, 2016.

CAROTTI B., *La riforma della pubblica amministrazione - L'amministrazione digitale e la trasparenza amministrativa (commento alla legge 7 agosto 2015, n. 124)*, in *Giornale di diritto amministrativo*, fasc. 5, 2015, pp. 625-629.

CAROTTI B., *L'amministrazione digitale. Le sfide culturali e politiche del nuovo Codice (commento al d.lgs. 26 agosto 2016, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 1, 2017, pp. 7-18.

CARPENTIERI R., *L'Agenda digitale italiana (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 225-233.

CARTA M., *Diritto alla vita privata ed Internet nell'esperienza giuridica europea ed internazionale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2014, pp. 1-19.

CARULLO G., *Big data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Concorrenza e mercato*, 2016, pp. 181-204.

CASINELLI A., *L'e-government (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 234-239.

CASSANO G., *Il diritto all'oblio nell'era digitale*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, pp. 45-59.

CASSANO G. - CONTALDO A., *Diritti della persona, internet e responsabilità dei soggetti intermediari*, in *Il Corriere giuridico*, fasc. 8-allegato 1, 2010, pp. 5-38.

CASSANO G. - GIURDANELLA C. (a cura di), *Il codice della Pubblica Amministrazione digitale. Commentario al D.lgs. n. 82 del 7 marzo 2005*, Giuffrè, Milano, 2005.

CASSANO G. - SCORZA G. - VACIAGO G. (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013.

CASSESE S., *Stato in trasformazione*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 2016, pp. 331-345.

CASTELLS M., *The Information Age: Economy, Society and Culture*, 3 tomi, Blackwell, Cambridge-Oxford, 1996-1998.

CATE F.H. - MAYER-SCHÖNBERGER V., *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, vol. 3, n. 2, 2013, pp. 67-73.

CAVALIERE G.A., *Open Data*, in M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014, pp. 31-52.

CAVALLARO M.C., *Garanzie della trasparenza amministrativa e tutela dei privati*, in *Diritto amministrativo*, fasc. 1, 2015, pp. 121-148.

CAZZANTI R., *Open data e nativi digitali. Per un uso intelligente delle tecnologie,* libreriauniversitaria.it edizioni, Padova, 2016.

COCCAGNA B. - ZICCARDI G., *Open data, trasparenza elettronica e codice aperto*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet giuridica, Milano, 2012, pp. 395-417.

COCUCCIO M.F., *Il diritto all'oblio fra tutela della riservatezza e diritto all'informazione*, in *Il diritto di famiglia e delle persone*, fasc. 2, 2015, pp. 740-758.

COCUCCIO M.F., *Il diritto all'identità personale e all'identità "digitale"*, in *Il diritto di famiglia e delle persone*, fasc. 3, 2016, pp. 949-968.

COLANGELO G., Big data*, piattaforme e antitrust*, in *Mercato Concorrenza Regole*, fasc. 3, 2016, pp. 425-460.

COLAPIETRO C. (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale scientifica, Napoli, 2012.

CONCAS G. - DE PETRA G. - GALLUS G.B. - GINESU G. - MARCHESI M. - MARZANO F., *Contenuti aperti, beni comuni. La tecnologia per diffondere la cultura*, McGraw-Hill, Milano, 2009.

CONTE M., *E-government e privacy*, in L. DE PIETRO (a cura di), *Dieci lezioni per capire e attuare l'e-government*, Marsilio Editori, Venezia, 2011, pp. 171-194.

CORASANITI G., *Diritto e tecnologie dell'informazione. Linee introduttive,* Giuffrè, Milano, 1990.

COSTANZO P., voce *Internet (diritto pubblico)*, in *Digesto delle discipline pubblicistiche*, IV ed., Appendice, Utet, Torino, 2000, p. 347 ss.

COSTANZO P., *Quale partecipazione politica attraverso le nuove tecnologie comunicative in Italia*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2011, pp. 19-46.

COSTANZO P., *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, in *Consulta OnLine*, 2012, pp. 1-14.

COSTANZO P., *Quale tutela del diritto d'autore in internet?*, in *Giurisprudenza Costituzionale*, fasc. 6, 2015, pp. 2343-2357.

CUDIA C., *Appunti su trasparenza amministrativa e diritto alla conoscibilità*, in *GiustAmm.it*, fasc. 12, 2016, pp. 1-10.

CUFFARO V. - D'ORAZIO R. - RICCIUTO V., *Il codice del trattamento dei dati personali*, Giappichelli, Torino, 2007.

CUNEGATTI B., *Le licenze* creative commons, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, pp. 641-663.

CUNIBERTI M. (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, Milano, 2008.

CUNIBERTI M., *La libertà della comunicazione nello scenario della convergenza*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Giuffrè, Milano, 2008, pp. 1-18.

CUNIBERTI M., *Nuove tecnologie della comunicazione e trasformazioni della democrazia*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della*

comunicazione. Profili costituzionali e pubblicistici, Giuffrè, Milano, 2008, pp. 343-383.

CUNIBERTI M., *Tecnologie digitali e libertà politiche*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2015, pp. 275-314.

CUOCOLO L., *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, fasc. 2-3, 2012, pp. 263-287.

D'ACQUISTO G. - NALDI M., *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli, Torino, 2017.

D'AMBROSIO M., *Il c.d. principio dell'*openness *nelle procedure giudiziarie tra oblio e anonimato*, in *Rassegna di diritto civile*, fasc. 1, 2017, pp. 37-56.

D'AMMASSA G., *La legge sul diritto d'autore nell'era multimediale*, in C. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, pp. 379-398.

D'ORLANDO E., *Profili costituzionali dell'amministrazione digitale,* in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2011, pp. 213-229.

D'URGOLO G., *Trasparenza e prevenzione della corruzione nella P.A.: la recente introduzione del Freedom Act of Information (FOIA) nell'ordinamento italiano*, in *GiustAmm.it*, fasc. 3, 2017, pp. 1-14.

DAGA M.C., *Diritto all'oblio: tra diritto alla riservatezza e diritto all'identità personale (nota a Cass., sez. III civ., 26 giugno 2013, n. 16111)*, in *Danno e responsabilità*, fasc. 3, 2014, pp. 274-278.

DEČMAN M. - JUKIĆ T. (a cura di), *Proceedings of the 16th European Conference on e-Government*, ACPI, 2016.

DE MARTIN J.C., *Le evoluzioni delle licenze* Creative Commons, in G. CONCAS - G. DE PETRA - G.B. GALLUS - G. GINESU - M. MARCHESI - F. MARZANO, *Contenuti aperti, beni comuni. La tecnologia per diffondere la cultura*, McGraw-Hill, Milano, 2009, pp. 11-14.

DE MARTIN J.C., *Prefazione*, in L. FLORIDI, *La rivoluzione dell'informazione*, trad. it., Codice edizioni, Torino, 2012, pp. VII-XII.

DE MINICO G., *Diritti, Regole, Internet*, in *Costituzionalismo.it*, fasc. 2, 2011, pp. 1-23.

DE MINICO G., *Internet e le sue fonti*, in *Osservatorio sulle fonti*, fasc. 2, 2013, pp. 1-27.

DE MINICO G., *Gli open data: una politica "costituzionalmente necessaria"?*, in *forumcostituzionale.it*, 2014, pp. 1-6.

DE MINICO G., "*Net neutrality" come diritto fondamentale di chi verrà*, in *Costituzionalismo.it*, fasc. 1, 2016, pp. 1-40.

DE MINICO G., *Towards an Internet Bill of Rights*, in *federalismi.it*, fasc. 5, 2016, pp. 1-33.

DE PASQUALE D., *La linea sottile tra manipolazione della rete e pubblicità*, in *Il Diritto industriale*, fasc. 6, 2012, pp. 552-557.

DE PIETRO L. (a cura di), *Dieci lezioni per capire ed attuare l'e-government*, Marsilio Editori, Venezia, 2011.

DE SANCTIS G., *Le nuove proposte di riforma della Commissione europea in materia di copyright. Analisi dei profili più rilevanti in relazione alle tematiche d'interesse dell'AGCom*, in *GiustAmm.it*, fasc. 2, 2017, pp. 1-13.

DE TULLIO M.F., *La* privacy *e i* big data *verso una dimensione costituzionale collettiva*, in *Politica del diritto*, fasc. 4, 2016, pp. 637-696.

DE VIVO M.C. - POLZONETTI A. - TAPANELLI P., Open Data*,* Business Intelligence *e* Governance *nella Pubblica Amministrazione*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 239-262.

DI CIOMMO F., *La responsabilità civile in Internet: prove di governo dell'anarchia tecnocratica*, in *La Responsabilità Civile*, fasc. 6, 2006, pp. 548-563.

DI COCCO C., *Il diritto d'autore nell'era digitale: la tutela dei beni informatici,* in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli, Torino, 2013, pp. 139-191.

DI COCCO C. - SARTOR G. (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli, Torino, 2013.

DI DONATO F., *Lo stato trasparente. Linked open data e cittadinanza attiva*, Edizioni ETS, Pisa, 2010.

DI FRANCESCO TORREGROSSA M., *La pubblica amministrazione nella società digitale,* Editoriale scientifica, Napoli, 2017.

DI PORTO F. (a cura di), *Big Data e Concorrenza*, in *Concorrenza e mercato*, parte I, 2016.

DI PORTO F., *La rivoluzione* Big Data. *Un'introduzione*, in *Concorrenza e mercato*, 2016, pp. 5-14.

DRAETTA U., *Internet nel diritto internazionale*, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, pp. 3-42.

DURANTE M. - PAGALLO U., *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012.

EINAUDI L., *Prediche inutili. Dispensa 1: Conoscere per deliberare*, Einaudi, Torino, 1956, pp. 3-14.

ERCOLANI S., *Il diritto d'autore e i diritti connessi. La legge 633/1941 dopo l'attuazione della direttiva n. 2001/29/CE*, Giappichelli, Torino, 2004.

FAINI F., *Dati, siti e servizi in rete delle pubbliche amministrazioni: l'evoluzione nel segno della trasparenza del decreto legislativo n. 235 del 2010*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 263-286.

FAINI F., *La strada maestra dell'open government: presupposti, obiettivi, strumenti*, in *Ciberspazio e diritto*, fasc. 2, 2013, pp. 213-238.

FAINI F., *Quale equilibrio fra trasparenza, apertura e privacy nello scenario del d.lgs. 33/2013?*, in *Diritto, Economia e Tecnologie della Privacy*, 2014, pp. 57-103.

FAINI F., *Trasparenza, apertura e controllo democratico dell'amministrazione pubblica,* in *Ciberspazio e diritto*, fasc. 1, 2014, pp. 39-70.

FAINI F., *Diritto all'informazione, diritto d'autore, diritto alla privacy: né vincitori né vinti,* in *Ciberspazio e diritto*, fasc. 2-3, 2014, pp. 147-188.

FAINI F., *L'evoluzione del modello di amministrazione digitale,* in *Rivista elettronica di Diritto, Economia e Management*, n. 1, 2014, pp. 184-210.

FAINI F., *Italian Open Government Strategy in National and Regional Regulation* in A. KŐ - E. FRANCESCONI (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2015*, LNCS 9265, Springer, Cham, 2015, pp. 271-286.

FAINI F., *Informatica e Pubblica Amministrazione*, in G. TADDEI ELMI (a cura di), *Corso di Informatica giuridica*, IV ed., Edizioni Giuridiche Simone, Napoli, 2016, pp. 179-243.

FAINI F., *Diritti digitali. Libertà costituzionali e tecnologie informatiche*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 67-110.

FAINI F., *L'amministrazione digitale e aperta*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 149-194.

FAINI F., Digital age *e diritto dei privati*, in F. FAINI - S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017, pp. 203-223.

FAINI F., *Internet e il diritto a conoscere nei confronti delle pubbliche amministrazioni*, in P. PASSAGLIA - D. POLETTI (a cura di), *Nodi Virtuali, legami informali: Internet alla ricerca di regole*, Pisa University press, 2017, pp. 337-350.

FAINI F. - PALMIRANI M., *The Right to Know Trough the Freedom of Information and Open Data,* in M. DEČMAN - T. JUKIĆ (a cura di), *Proceedings of the 16th European Conference on e-Government*, ACPI, 2016, pp. 54-62.

FAINI F. - PALMIRANI M., *Italian Open and Big Data Strategy,* in A. KŐ - E. FRANCESCONI (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2016*, LNCS 9831, Springer, Cham, 2016, pp. 271-286.

FAINI F. - PIETROPAOLI S., *Scienza giuridica e tecnologie informatiche*, Giappichelli, Torino, 2017.

FALCE V., *La disciplina comunitaria sulle banche dati. Un bilancio a dieci anni dall'adozione*, in *Rivista di diritto industriale*, fasc. 6, 2006, pp. 227-251.

FALCONE M., *Big data e pubbliche amministrazioni: nuove prospettive per la funzione conoscitiva pubblica*, in *Rivista Trimestrale di Diritto Pubblico*, fasc. 3, 2017, pp. 601-639.

FALLETTA P., *Il* freedom of information act *italiano e i rischi della trasparenza digitale*, in *federalismi.it*, fasc. 23, 2016, pp. 1-15.

FALLETTI E., *L'evoluzione del concetto di privacy e della sua tutela giuridica*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, pp. 21-43.

FARINA M., *Fondamenti di diritto dell'informatica*, Experta edizioni, Forlì, 2012.

FARO S. - LETTIERI N., Big Data*: una lettura informatico-giuridica*, in L. LOMBARDI VALLAURI (a cura di), *Scritti per Luigi Lombardi Vallauri*, vol. I, Cedam, Padova, 2016, p. 503 ss.

FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in *Rivista di diritto civile*, fasc. 6, 1990, pp. 801-823.

FINOCCHIARO G., *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2010, pp. 391-404.

FINOCCHIARO G., *Riflessioni su diritto e tecnica*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2012, pp. 831-840.

FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 591-603.

FINOCCHIARO G., *La protezione dei dati personali e la tutela dell'identità*, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, pp. 151-181.

FINOCCHIARO G., *L'equilibrio titolare/*users *nel diritto d'autore dell'Unione europea*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2016, pp. 499-516.

FINOCCHIARO G., *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civili commentate*, fasc. 1, 2017, pp. 1-18.

FINOCCHIARO G. (diretta da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017.

FINOCCHIARO G. - DELFINI F. (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014.

FIORENTINO L. (*et al.*), *Il decreto "crescita 2.0" (commento al d.l. 18 ottobre 2012, n. 179)*, in *Giornale di diritto amministrativo*, fasc. 3, 2013, pp. 223-264.

FLICK C., *Privacy e legge penale nella società dell'informazione e della comunicazione*, in M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici,* Giuffrè editore, Milano, 2008, pp. 243-294.

FLORIDI L., *La rivoluzione dell'informazione*, trad. it., Codice edizioni, Torino, 2012.

FLORIDI L., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. it., Raffaello Cortina Editore, Milano, 2017.

FLORINDI E., *Computer e diritto. L'informatica giuridica nella società dell'informazione e della conoscenza*, Giuffrè, Milano, 2012.

FOCARELLI C., *La privacy. Proteggere i dati personali oggi*, il Mulino, Bologna, 2015.

FROSINI T.E., *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 563-567.

FROSINI T.E., *Liberté, Egalité, Internet*, Editoriale Scientifica, Napoli, 2015.

FROSINI T.E., *Costituzionalismo 2.0*, in *Rassegna parlamentare*, fasc. 4, 2016, pp. 673-692.

FROSINI T.E. - POLLICINO O. - APA E. - BASSINI M. (a cura di), *Diritti e libertà in Internet*, Mondadori education - Le Monnier Università, Milano, 2017.

FROSINI V., *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981.

FROSINI V., *Il diritto dell'informatica negli anni ottanta*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 1984, pp. 390-400.

FROSINI V., *Informatica, diritto e società*, II ed., Giuffrè, Milano, 1992.

FROSINI V., *L'orizzonte giuridico dell'Internet*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2000, pp. 271-280.

FURIOSI E., *L'accesso civico generalizzato, alla luce delle Linee Guida ANAC*, in *GiustAmm.it*, fasc. 4, 2017, pp. 1-21.

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, pp. 1019-1065.

GALETTA D.U., *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *federalismi.it*, fasc. 5, 2016, pp. 1-19.

GALLINO L., *Tecnologia e democrazia. Conoscenze tecniche e scientifiche come beni pubblici*, Einaudi, Torino, 2007.

GAMBINO A.M. - STAZI A., *Diritto dell'informatica e della comunicazione*, II ed., Giappichelli, Torino, 2012.

GARDINI G., *Il codice della trasparenza: un primo passo verso il diritto all'informazione amministrativa?*, in *Giornale di diritto amministrativo*, fasc. 8-9, 2014, pp. 875-891.

GIANNANTONIO E., *Introduzione all'informatica giuridica*, Giuffrè, Milano, 1984.

GIOVANELLA F., *La responsabilità civile degli Internet Service Provider*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, pp. 227-247.

GIOVANNINI E., *Scegliere il futuro. Conoscenza e politica al tempo dei Big Data*, Il Mulino, Bologna, 2014.

GRANDI M., *Far web. Odio, bufale, bullismo. Il lato oscuro dei social*, Rizzoli, Milano, 2017.

GREENWALD G., *Sotto controllo. Edward Snowden e la sorveglianza di massa*, trad. it., Rizzoli, Milano, 2014.

GUERNELLI M., *Il quadro normativo italiano*, in G. FINOCCHIARO - F. DELFINI (a cura di), *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, pp. 109-147.

HÄBERLE P., *Diritto e verità*, ed. it., Einaudi, Torino, 2000.

HAN B.C., *La società della trasparenza,* trad. it, Nottetempo, Roma, 2014.

HUXLEY A., *Il mondo nuovo*, trad. it di L. GIGLI, Mondadori, Milano, 1933.

IASELLI M. (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014.

IRTI N. - SEVERINO E., *Dialogo su diritto e tecnica*, Laterza, Roma-Bari, 2001.

JANNUZZI E. - REGI A., *Diritto all'oblio: finzione o realtà?*, in *Law and Media Working Paper Series*, n. 13, 2016, pp. 1-11.

JORI M., *Elementi di informatica giuridica*, Giappichelli, Torino, 2006.

JORI M. G., *Diritto, nuove tecnologie e comunicazione digitale*, Giuffrè, Milano, 2013.

KATZ D.M. - BOMMARITO M.J. - BLACKMAN J., *Predicting the Behavior of the Supreme Court of the United States: A General Approach*, 2014.

KITCHIN R., *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, Sage, Los Angeles, 2014.

KŐ A. - FRANCESCONI E. (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2014*, LNCS 8650, Springer, Cham, 2014.

KŐ A. - FRANCESCONI E. (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2015*, LNCS 9265, Springer, Cham, 2015.

KŐ A. - FRANCESCONI E. (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2016*, LNCS 9831, Springer, Cham, 2016.

KRANENBORG H. - VOERMANS W., *Access to Information in the European Union. A comparative Analysis of EC and Member State legislation*, Europa Law Publishing, Groningen, 2005.

LA PISCOPIA S., *Italian Freedom of Information Act: approcci interpretativi e dottrinari*, in *Periodico di Diritto e Procedura Penale Militare*, fasc. 5, 2016, pp. 1-22.

LATHROP D. - RUMA L. (a cura di), *Open government: Collaboration, Transparency, and Participation In Practice,* O'Reilly Media, Sebastopol, 2010.

LEONE C., *Il principio "digital first": obblighi e diritti in capo all'amministrazione e a tutela del cittadino. Note a margine dell'art. 1 della legge 124 del 2015*, in *GiustAmm.it*, fasc. 6, 2016, pp. 1-8.

LESSIG L., *The Law of the Horse: What Cyberlaw Might Teach*, in *Harvard Law Review*, vol. 113, 1999, pp. 501-546.

LESSIG L.*, Code and Other Law of Cyberspace*, Basic Books, New York, 1999.

LESSIG L., *Cultura libera: un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale,* trad. it., Apogeo, Milano, 2005.

LÉVY P., *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Feltrinelli, Milano, 1996.

LIMONE D.A., *Politica e Normativa Comunitaria per la Società dell'Informazione (1990-2010)*, in *Rivista elettronica di Diritto, Economia, Management*, n. 1, 2010.

LIPARI N., *Le categorie del diritto civile*, Giuffrè, Milano, 2013.

LOMBARDI VALLAURI L. (a cura di), *Scritti per Luigi Lombardi Vallauri*, vol. I, Cedam, Padova, 2016

LOSANO M.G., *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Einaudi, Torino, 1969.

LOSANO M.G., *Corso di Informatica Giuridica,* 3 tomi, Torino, 1985-1986.

LOSANO M.G., *La "giuscibernetica" dopo quattro decenni*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2005, pp. 727-751.

LUBELLO V., *L'*Open Government *negli Stati Uniti d'America tra il* Freedom of Information Act *e il* bazar, in *Informatica e diritto*, nn. 1-2, 2011, pp. 371-388.

MAESTRI E., Lex informatica *e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars Interpretandi*, fasc. 6, 2017, pp. 15-28.

MAGGIPINTO A., *Amministrazione digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, pp. 283-311.

MAGLIO G., *Identità digitale*, in M. MANCARELLA (a cura di), *Lineamenti di informatica giuridica*, Tangram edizioni scientifiche, Trento, 2017, pp. 58-71.

MANCARELLA M., *Profili negoziali e organizzativi dell'amministrazione digitale*, Tangram Edizioni Scientifiche, Trento, 2009.

MANCARELLA M., *La gestione dell'informazione e il Sistema Pubblico di Connettività*, in G. PREITE (a cura di), *Politica e tecnologie. Spazio pubblico e privato della conoscenza nella società dell'informazione*, Carocci, Roma, 2010, pp. 37-48.

MANCARELLA M., *Il programma triennale per la trasparenza e il sito web dell'ente*, in *Comuni d'Italia*, fasc. 2, 2011, pp. 35-37.

MANCARELLA M. (a cura di), *La Pubblica Amministrazione tra management, eGovernment e federalismo*, Tangram Edizioni Scientifiche, Trento, 2011.

MANCARELLA M. (a cura di), *Lineamenti di informatica giuridica*, Tangram edizioni scientifiche, Trento, 2017.

MANCOSU G., *Trasparenza amministrativa e* open data*: un binomio in fase di rodaggio*, in *federalismi.it*, fasc. 17, 2012, pp. 1-27.

MANTELERO A., *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2012, pp. 135-144.

MANTELERO A., *Privacy digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet giuridica, Torino, 2012, pp. 159-174.

MANTELERO A., *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella* digital economy, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 681-701.

MANTELERO A., *The protection of the right to be forgotten: lessons and perspectives from open data*, in *Contratto e impresa - Europa*, fasc. 2, 2015, pp. 734-743.

MARCHETTI A., *Il diritto di accesso: modelli di enforcement e cause di exemptions nella prospettiva comparata*, in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale Scientifica, Napoli, 2012, pp. 209-242.

MARSOCCI P., *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, in *Rivista AIC*, fasc. 1, 2015, pp. 1-16.

MARTINELLI S., *Diritto all'oblio e motori di ricerca: memoria e privacy nell'era digitale*, Giuffrè, Milano, 2017.

MARTINELLI S., *Il parere dell'EDPS sulla tutela dei diritti fondamentali nell'era dei Big Data*, in *Quotidiano giuridico*, 14 febbraio 2017.

MARTINELLI S., *Le Linee Guida del Consiglio d'Europa per la protezione dei diritti nell'era dei Big Data*, in *Quotidiano giuridico*, 20 marzo 2017.

MARTONI M. - PALMIRANI M., *Internet e identità personale*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 295-308.

MARZANO F., *La trasparenza nella P.A. passa dall'*Open Data *o l'*Open Data *passa dalla trasparenza?*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 287-303.

MASERA A. - SCORZA G., *Internet, i nostri diritti*, Laterza, Roma-Bari, 2016.

MATTELART A., *Storia della società dell'informazione*, trad. it., Einaudi, Torino, 2002.

MAYER-SCHÖNBERGER V., *Delete*, trad. it., Egea, Milano, 2010.

MAYER-SCHÖNBERGER V. - CUKIER K., *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Garzanti, Milano, 2013.

MAZZIOTTI G., *Il copyright digitale*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, pp. 175-199.

MEGALE M. (a cura di), *ICT e diritto nella società dell'informazione*, Giappichelli, Torino, 2012.

MENDEL T., *Freedom of Information: A Comparative Legal Survey*, UNESCO, Parigi, 2008.

MENNELLA M., *Privacy e nuove tecnologie*, in M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Aracne, Roma, 2014, pp. 195-227.

MERLONI F. (a cura di), *La trasparenza amministrativa*, Giuffrè, Milano, 2008.

MERLONI F., *La trasparenza come strumento di lotta alla corruzione tra legge n. 190 del 2012 e d.lgs. n. 33 del 2013*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33*, Maggioli, Rimini, 2013, pp. 17-28.

MEZZANOTTE M., *Il diritto all'oblio. Contributo allo studio della privacy storica*, Edizioni Scientifiche Italiane, Napoli-Roma, 2009.

MINAZZI F., *Il principio dell'*open data by default *nel Codice dell'Amministrazione Digitale: profili interpretativi e questioni metodologiche*, in *federalismi.it*, fasc. 23, 2013, pp. 1-12.

MINIUSSI D., *Il diritto all'oblio: i paradossi del caso Google*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 1, 2015, pp. 209-234.

MODESTI G., *Open data e privacy. La creazione di un programma aziendale per governare il processo di gestione dei dati*, in *Quaderni amministrativi*, fasc. 2-3, 2016, pp. 12-36.

MONDUCCI J., *La tutela della privacy e le misure di sicurezza*, in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli Editore, Torino 2013, pp. 109-137.

MONEA A., *Pubblica amministrazione, vera "casa di vetro"?*, in *Azienditalia - il Personale*, fasc. 6, 2015, p. 311 ss.

MONEA A., *La nuova trasparenza amministrativa alla luce del d.lgs. 97/2016. L'accesso civico*, in *Azienditalia*, fasc. 11, 2016, p. 1040 ss.

MORELLI A., *I diritti e la Rete. Notazioni sulla Bozza di Dichiarazione dei diritti in Internet*, in *federalismi.it*, focus TMT, n. 1, 2015, pp. 1-19.

MORELLI A., *I diritti senza leggi*, in *Consulta online*, fasc. 1, 2015, pp. 1-25.

MORO VISCONTI R., *Valutazione dei* Big data *e impatto su innovazione e* digital branding, in *Il Diritto industriale*, fasc. 1, 2016, pp. 46-53.

MORO VISCONTI R., *Internet delle cose, Networks e plusvalore della connettività*, in *Il Diritto industriale*, fasc. 6, 2016, pp. 536-544.

MORRONE A., *Il* nomos *del segreto di Stato*, in G. ILLUMINATI (a cura di), *Nuovi profili del segreto di Stato e dell'attività di* intelligence, Giappichelli, Torino, 2010, pp. 3-52.

MULA D., *Libertà di manifestazione del pensiero in rete*, in G. CASSANO - G. SCORZA - G. VACIAGO (a cura di), *Diritto dell'internet. Manuale operativo. Casi, legislazione, giurisprudenza*, Cedam, Padova, 2013, p. 1 ss.

NANNIPIERI L., *Costituzione e nuove tecnologie: profili costituzionali dell'accesso ad Internet*, in *www.gruppodipisa.it*, 2013.

NAPOLITANO G., *Le riforme amministrative in Europa all'inizio del ventunesimo secolo*, in *Rivista trimestrale di diritto pubblico*, fasc. 2, 2015, pp. 611-640.

NEGROPONTE N., *Essere digitali,* trad. it., Sperling & Kupfer, Milano, 1995.

NICOTRA I., *La dimensione della trasparenza tra diritto alla accessibilità totale e protezione dei dati personali: alla ricerca di un equilibrio costituzionale*, in *federalismi.it*, fasc. 11, 2015, pp. 1-13.

NINO M., *Il caso "Datagate": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, fasc. 3, 2013, pp. 727-746.

NINO M., *Il rapporto tra libertà di espressione e diritto d'autore: considerazioni critiche alla luce della prassi nazionale e internazionale*, in *Diritti umani e diritto internazionale*, fasc. 3, 2016, pp. 549-585.

NOTO LA DIEGA G., *Il cloud computing. Alla ricerca del diritto perduto nel web 3.0*, in *Europa e diritto privato*, fasc. 2, 2014, pp. 577-658.

NUNZIANTE E., *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *Law and Media Working Paper Series*, n. 6, 2017, pp. 1-13.

OCCHIENA M., *I principi di pubblicità e trasparenza*, in M. RENNA - F. SAITTA, (a cura di), *Studi sui principi di diritto amministrativo*, Giuffrè, Milano, 2012, p. 141 ss.

OREFICE M., *I big data. Regole e concorrenza*, in *Politica del diritto*, fasc. 4, 2016, pp. 697-743.

ORWELL G., *1984*, trad. it. a cura di G. BALDINI, Mondadori, Milano, 1989.

OTRANTO P., *Internet nell'organizzazione amministrativa. Reti di libertà*, Cacucci editore, Bari, 2015.

OXFAM ITALIA (*et al.*) (a cura di), *Realtà virtuale, diritti concreti. Diritti umani nell'Era della Cittadinanza Digitale*, libro-dossier realizzato in occasione del XX Meeting sui diritti umani, 13 dicembre 2016.

PAGALLO U., *La tutela della "privacy" negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008.

PAGALLO U., *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Giappichelli, Torino, 2014.

PAGNANELLI V., *Accesso, accessibilità, Open Data. Il modello italiano di Open Data pubblico nel contesto europeo*, in *Giornale di storia costituzionale*, fasc. 31, 2016, pp. 205-215.

PALMIRANI M. - MARTONI M. - GIRARDI D., *Open Government Data Beyond Transparency*, in A. KŐ - E. FRANCESCONI (a cura di), *Electronic Government and the Information Systems Perspective - EGOVIS 2014*, LNCS 8650, Springer, Cham, 2014, pp. 275-291.

PASCUZZI G. (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016.

PASCUZZI G., *Dematerializzazione*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, pp. 341-344.

PASCUZZI G. - GIOVANELLA F., *Dal diritto alla riservatezza alla computer privacy*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, pp. 43-75.

PASSAGLIA P., *Diritto di accesso a Internet e giustizia costituzionale. Una (preliminare) indagine comparata*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011, pp. 59-88.

PASSAGLIA P., *Internet nella Costituzione italiana: considerazioni introduttive*, in *Consulta OnLine*, 2013, pp. 1-40.

PASSAGLIA P. - POLETTI D. (a cura di), *Nodi Virtuali, legami informali: Internet alla ricerca di regole*, Pisa University press, 2017.

PATRONI GRIFFI F., *La trasparenza della pubblica amministrazione tra accessibilità totale e riservatezza*, in *federalismi.it*, fasc. 8, 2013, pp. 1-12.

PELLERINO G., *I rischi del diritto nella Rete globale*, in *Informatica e diritto*, fasc. 1, 2009, pp. 255-267.

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano, 2007.

PERRI P., *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Giuffrè, Milano, 2007.

PERUGINELLI G. - RAGONA M. (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, Napoli-Roma, 2014.

PIETRANGELO M. (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011.

PIETRANGELO M., *Il diritto e le tecnologie informative: qualche proposta per il nuovo millennio*, in G. PERUGINELLI - M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Edizioni Scientifiche Italiane, Napoli, 2014, pp. 621-633.

PIETROPAOLI S., *Chi deve essere il custode della rete? Considerazioni sul problema dell'esercizio del "diritto all'oblio"*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 545-555.

PIETROPAOLI S., *La rete non dimentica. Una riflessione sul diritto all'oblio*, in *Ars Interpretandi*, fasc. 1, 2017, pp. 67-80.

PINO G., *L'identità personale*, in S. RODOTÀ - M. TALLACCHINI (a cura di), *Ambito e fonti del biodiritto*, vol. I del *Trattato di Biododiritto* diretto da S. RODOTÀ - P. ZATTI, Giuffrè, Milano, 2010, pp. 297-321.

PITRUZZELLA G. - POLLICINO O. - QUINTARELLI S., *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, Milano, 2017.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. I – Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. II – Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016.

POLETTI D., *Il c.d. diritto alla disconnessione nel contesto dei "diritti digitali"*, in *Responsabilità civile e previdenza*, fasc. 1, 2017, pp. 8-26.

POLLICINO O., *Copyright versus freedom of speech nell'era digitale*, in *Giurisprudenza italiana*, fasc. 8-9, 2011, pp. 1944-1953.

POLLICINO O., *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 569-589.

POLLICINO O., *Diritto all'oblio e conservazione dei dati. La Corte di Giustizia a piedi uniti: verso un* digital right to privacy, in *Giurisprudenza costituzionale*, fasc. 3, 2014, pp. 2949-2958.

POLLICINO O., *La rimessione alla Corte della questione di legittimità costituzionale in materia di diritto d'autore sulle reti di comunicazione elettronica*, in *federalismi.it*, n. 3, 2014, pp. 1-5.

POLLICINO O. - BASSINI M., *"Le parole contano", ovvero "tanto rumore per nulla". Sulla (prevista) inammissibilità della questione di legittimità costituzionale della base giuridica del Regolamento AGCOM #ddaonline*, in *medialaws.eu*, 2015.

POLLICINO O. - BERTOLINI E. - LUBELLO V. (a cura di), *Internet: regole e tutela dei diritti fondamentali*, Aracne, Roma, 2013.

PONTI B. (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33. Analisi della normativa, impatti organizzativi ed indicazioni operative*, Maggioli, Rimini, 2013.

PONTI B., *Il regime dei dati oggetto di pubblicazione obbligatoria: i tempi, le modalità ed i limiti della diffusione; l'accesso civico; il diritto di riutilizzo (artt. 4, 5, 7-9, 52 commi 2 e 3, 53)*, in B. PONTI (a cura di), *La trasparenza amministrativa dopo il d.lgs. 14 marzo 2013, n. 33. Analisi della normativa, impatti organizzativi ed indicazioni operative*, Maggioli, Rimini, 2013, pp. 75-124.

PONTI B., *Il codice della trasparenza amministrativa: non solo riordino, ma ridefinizione complessiva del regime della trasparenza on line*, in *neldiritto.it*, 2013.

PONTI B. (a cura di), *Nuova trasparenza amministrativa e libertà di accesso alle informazioni*, Maggioli, Rimini, 2016.

PREITE G. (a cura di), *Politica e tecnologie. Spazio pubblico e privato della conoscenza nella società dell'informazione*, Carocci, Roma, 2010.

RAZZANTE R., *Manuale di diritto dell'informazione e della comunicazione. Privacy, diffamazione e tutela della persona. Libertà e regole nella Rete*, V ed., Cedam, Padova, 2011.

RESTA G., *Identità personale e identità digitale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2007, pp. 511-531.

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4, 2015, pp. 697-718.

RESTA G. - ZENO-ZENCOVICH V. , *Il diritto all'oblio su internet dopo la sentenza Google Spain*, RomaTre Press, Roma, 2015.

RICCIUTO V., *Diritto di rettifica, identità personale e danno patrimoniale all'uomo politico (nota a Trib. Roma, 7-11-1984)*, in *Il diritto dell'informazione e dell'informatica*, 1985, p. 225 ss.

RIFKIN J., *L'era dell'accesso. La rivoluzione della new economy*, trad. it., Mondadori, Milano, 2000.

RIZZO G. - MORANDO F. - DE MARTIN J.C., Open Data: *la piattaforma di dati aperti per il* Linked Data, in *Informatica e diritto*, nn. 1-2, 2011, pp. 493-511.

RIZZUTI M., *Il diritto e l'oblio*, in *Il Corriere giuridico*, fasc. 8-9, 2016, pp. 1077-1082.

RYAN J., *Storia di Internet e il futuro digitale*, trad. it., Einaudi, Torino, 2011.

RODOTÀ S., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997 (nuova ed. 2004).

RODOTÀ S., *Intervista su privacy e libertà*, a cura di P. CONTI, Laterza, Roma-Bari, 2005.

RODOTÀ S., *Una Costituzione per Internet?*, in F. AMORETTI (a cura di), *Diritti e sfera pubblica nell'era digitale,* numero speciale in *Politica del diritto,* fasc. 3, 2010, pp. 337-351.

RODOTÀ S.*, Il diritto di avere diritti,* Laterza, Roma-Bari, 2012.

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014.

RODOTÀ S., *Prefazione*, in A. MASERA - G. SCORZA, *Internet, i nostri diritti*, Editori Laterza, Roma-Bari, 2016, pp. V-XXII.

ROMANO S., *L'ordinamento giuridico*, II ed., Sansoni, Firenze, 1945.

ROMEO F., *Lezioni di logica ed informatica giuridica*, Giappichelli, Torino, 2012.

ROSSETTI A. (a cura di), *Legal Informatics*, Moretti & Vitali editori, Bergamo, 2008.

ROSSETTI A., *È necessario il diritto all'accesso alla rete?*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito*

dell'IGF Italia 2010 (Roma, 30 novembre 2010), Edizioni Scientifiche Italiane, Napoli-Roma, 2011, pp. 89-97.

ROSSI DAL POZZO F., *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Rivista di diritto internazionale*, fasc. 3, 2016, pp. 690-724.

ROVATI A.M., *Prime note su proprietà intellettuale e riutilizzo dei dati pubblici*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 153-184.

SALERNO G.M., *Le ordinanze gemelle sulla disciplina dei provvedimenti interdittivi dell'AGCom: alcune riflessioni*, in *federalismi.it*, n. 3, 2014.

SAMMARCO P., *I nuovi contratti dell'informatica: sistema e prassi*, in F. GALGANO (diretto da), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Cedam, Padova, 2006, p. 177 ss.

SANDULLI M.A., *Il diritto di accesso ai documenti amministrativi: l'attualità di un istituto a vent'anni dalla legge n. 241/1990*, in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale Scientifica, Napoli, 2012, pp. 39-53.

SAPPA C., *Diritti di proprietà intellettuale e dati pubblici nell'ordinamento italiano*, in *Informatica e diritto*, nn. 1-2, 2011, pp. 185-197.

SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Giappichelli, Torino, 2010.

SARTOR G., *Internet e il diritto*, in C. DI COCCO - G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Giappichelli, Torino, 2013, pp. 1-26.

SARTOR G. - VIOLA DE AZEVEDO CUNHA M., *Il caso Google e i rapporti regolatori USA/EU*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2014, pp. 657-680.

SARTORI L., *Open government: what else?*, in *Istituzioni del federalismo*, fasc. 3-4, 2013, pp. 753-775.

SAVINO M., *The Right to Open Public Administrations in Europe: Emerging Legal Standards*, Ocse, Sigma papers, Paris, 2010, pp. 1-40.

SAVINO M., *La nuova disciplina della trasparenza amministrativa*, in *Giornale di diritto amministrativo*, 2013, fasc. 8-9, pp. 795-805.

SAVINO M., *Il Foia italiano. La fine della trasparenza di Bertoldo – il commento (commento a d.lgs. 25 maggio 2016, n. 97)*, in *Giornale di diritto amministrativo*, fasc. 5, 2016, pp. 593-603.

SBARISCIA D., *La tutela attraverso la disciplina del diritto d'autore*, in G. FINOCCHIARO - F. DELFINI, *Diritto dell'informatica*, Utet Giuridica, Torino, 2014, pp. 875-913.

SBRESCIA V.M., *Le comunicazioni elettroniche tra tecnologia e regolazione*, in *Rivista italiana di diritto pubblico comunitario*, fasc. 5, 2011, pp. 1207-1250.

SCORZA G., *Accedo ergo sum,* in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli - Roma, 2011, pp. 125-131.

SGUEO G., *L'amministrazione digitale*, in *Giornale di diritto amministrativo*, fasc. 1, 2016, pp. 114-118.

SICA S. - STANZIONE P. (diretto da), *La nuova disciplina della privacy. Commento al D.Lgs. 30 giugno 2003, n.* 196, Zanichelli, Bologna, 2004.

SOFFIENTINI M., *Il futuro della privacy: dall'Internet of Things ai Big Data*, in *Diritto e Pratica del Lavoro*, n. 13, 2015.

SOLDA KUTZMANN D., *La circolazione dell'informazione del settore pubblico*, in *Digesto delle Discipline Privatistiche,* Utet, Torino, 2007.

STANZIONE M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e diritto privato*, fasc. 4, 2016, pp. 1249-1264.

STAZI A., *La tutela del diritto d'autore in rete: bilanciamento degli interessi, opzioni regolatorie europee e "modello italiano"*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2015, pp. 89-110.

STRADELLA E., *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare e, infine,* cui prodest*?*, in *Rivista AIC*, fasc. 4, 2016, pp. 1-29.

TADDEI ELMI G. (a cura di), *Corso di Informatica giuridica*, IV ed., Edizioni Giuridiche Simone, Napoli, 2016.

TARALLO P. (a cura di), *Digital divide. La nuova frontiera dello sviluppo globale,* FrancoAngeli, Milano, 2003.

TARCHI R., *Il diritto d'accesso nella prospettiva comparata*, in C. COLAPIETRO (a cura di), *Il diritto di accesso e la Commissione per l'accesso ai documenti amministrativi a vent'anni dalla legge n. 241 del 1990*, Editoriale scientifica, Napoli, 2012, pp. 141-207.

TEDESCHI E., *Il diritto di accesso: il nuovo dovere di collaborazione dell'amministrazione (nota a TAR Lazio – Roma, sez. II ter, 15 marzo 2016, n. 3287)*, in *Giornale di diritto amministrativo*, fasc. 6, 2016, pp. 805-814.

TENTONI F., *Trasparenza "Riservata"*, in *Azienditalia - Il Personale,* fasc. 5, 2013, p. 236 ss.

TETI A., *Il futuro dell'Information & Communication Technology. Tecnologie, timori e scenari futuri della "global network revolution"*, Springer, Milano, 2009.

TINCANI P., *Controllo e sorveglianza*, in R. BRIGHI - S. ZULLO (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 19-40.

TISCORNIA D. (a cura di), *Open data e riuso dei dati pubblici,* in *Informatica e diritto*, nn. 1-2, 2011.

TRAVOSTINO M., *Le licenze creative commons*, in M. DURANTE - U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Utet Giuridica, Torino, 2012, pp. 201-218.

TROJANI F., *Il nuovo Codice dell'amministrazione digitale dopo il d.lgs. 179/2016 e il Regolamento eIDAS,* Maggioli, Rimini, 2017.

UBERTAZZI L.C., *I diritti d'autore e connessi. Scritti*, II ed., Giuffrè, Milano, 2003.

UBERTAZZI L.C. (a cura di), *Il regolamento Agcom sul diritto d'autore*, Giappichelli, Torino, 2014.

VACCARI S., *Il difficile bilanciamento tra* favor *per la trasparenza e (necessaria) tutela della riservatezza nel d.lgs. 33/2013*, in *Il diritto dell'economia*, fasc. 1, 2015, pp. 151-178.

VALASTRO A., *Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano*, in M. PIETRANGELO (a cura di), *Il diritto di accesso ad Internet. Atti della Tavola rotonda svolta nell'ambito dell'IGF Italia 2010 (Roma, 30 novembre 2010)*, Edizioni Scientifiche Italiane, Napoli-Roma, 2011, pp. 45-57.

VALENTINO D. (a cura di), *Manuale di diritto dell'informatica*, III ed., Edizioni Scientifiche Italiane, Napoli, 2016.

VIGEVANI G.E., *Diritto all'informazione e privacy nell'ordinamento italiano: regole ed eccezioni*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2016, pp. 473-498.

VILLAMENA S., *Il c.d. FOIA (o accesso civico 2016) ed il suo coordinamento con istituti consimili*, in *federalismi.it*, fasc. 23, 2016, pp. 1-19.

WARREN S.D. - BRANDEIS L.D., *The right to privacy*, in *Harvard Law Review*, vol. 4, n. 5, 15 dicembre 1890, pp. 193-220.

WESSELS B. - FINN R. - SVEINSDOTTIR T. - WADHWA K., *Open Data and the Knowledge Society*, Amsterdam University Press, Amsterdam, 2017.

ZENO-ZENCOVICH V., *Una svolta giurisprudenziale nella tutela della riservatezza*, in *Il diritto dell'informazione e dell'informatica*, vol. 1, 1986, pp. 932-935.

ZENO-ZENCOVICH V., *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, pp. 89-93.

ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2015, pp. 683-695.

ZENO-ZENCOVICH V. - GIANNONE CODIGLIONE G., *Ten legal perspectives on the "Big data revolution"*, in *Concorrenza e mercato*, 2016, pp. 29-57.

ZICCARDI G., *Etica e Informatica. Comportamenti, tecnologie e diritto*, Pearson Addison Wesley, Milano, 2009.

ZICCARDI G., *Informatica giuridica. Tomo I - Controcultura, informatica giuridica, libertà del software e della conoscenza*, II ed., Giuffrè, Milano, 2011.

ZICCARDI G., *Informatica giuridica. Tomo II - Privacy, sicurezza informatica, computer forensics e investigazioni digitali*, II ed., Giuffrè, Milano, 2012.

ZICCARDI G., *Resistance, Liberation Technology and Human Rights in the Digital Age*, Springer, Dordrecht, 2012.

ZICCARDI G., *L'avvocato hacker. Informatica giuridica e uso consapevole (e responsabile) delle tecnologie*, Giuffrè, Milano, 2012.

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

ZICCARDI G., *Il computer e il giurista*, Giuffrè, Milano, 2015.

ZICCARDI G., *L'odio online. Violenza verbale e ossessioni in rete*, Raffaello Cortina, Milano, 2016.

ZICCARDI G., *Il libro digitale dei morti: memoria, lutto, eternità e oblio nell'era dei social network*, Utet, Milano, 2017.

ZICCARDI G. - PERRI P., *Tecnologia e diritto. Fondamenti d'informatica per il giurista*, Giuffrè, Milano, 2017.

ZUANELLI E., *Amministrazione digitale e innovazione tecnologica: analisi, riflessioni, proposte*, Aracne, Roma, 2013.