Big Data e profili di responsabilità civile e vicaria

Salvatore Sica - Virgilio D'Antonio - Giorgio Giannone Codiglione - Giovanni Sciancalepore

1. Il completo assorbimento dell'azione umana nel paradigma tecnologico e l'avvento di un sistema di circolazione sincronica e delocalizzata delle informazioni, oggi, sta radicalmente mutando il paradigma di riferimento di ogni metodo che possa definirsi scientifico.

La tecnica, strumento nato per accompagnare l'uomo nel cammino dell'innovazione, ovvero nella sfida rappresentata dalla replicazione del presente e la comprensione del futuro, ha raggiunto espressioni così complesse ed autonomiche da spingere gli studiosi ad affermarne il definitivo predominio sulla volontà umana, o ancora, a fissarne l'immagine come di una forza parallela e contrapposta ad ogni forma di regolazione[1].

In particolare, nell'ultima decade del nuovo millennio si è assistito all'avvento di tre fenomeni legati all'evoluzione tecnologica: *a*) l'introduzione su larga scala di entità capaci di agire in maniera autonoma rispetto alla volontà dell'uomo, o di sostituirne funzionalmente (o implementarne) parti vitali; *b*)

[1] È quanto ad esempio emerso dal confronto tra N. Irti-E. Severino, *Dialogo tra diritto e tecnica*, Roma-Bari, 2001 e, ancora in N. Irti, *L'uso giuridico della natura*, cit., spec. p. 90 ss. Per una più ampia riflessione sul problema della regolazione della tecnica e della preservazione dei valori fondamentali e fondativi della società moderna v. tra gli altri J. Ellul, *La technique ou l'enjeu du siècle*, Paris, 1954, trad. it. a cura di C. Pesce, Milano, 1969; Id., *Le système technicien*, Paris, 1977, trad. it. a cura di G. Carbonelli, Foligno, 2009; Id., *Le bluff technologique*, Paris, 1988; S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; Id., *La vita e le regole*, Milano, 2009, spec. pp. 9-72; Id., *Diritto, scienza, tecnologia: modelli e tecniche di regolamentazione*, in *Riv. crit. dir. priv*., 2004, pp. 357-375; A. Supiot, *Homo juridicus*, Milano, 2006, spec. p. 139 ss.

 ISSN 2704-8179

la massiccia attività di estrazione, accumulo ed elaborazione di qualsivoglia informazione attinente alla persona umana e all'ambiente che la circonda (c.d. *Big Data*); *c*) l'utilizzo di Internet come tessuto connettivo sensibile capace di captare, diffondere e processare le informazioni coordinando ed influenzando i rapporti tra il paradigma umano/senziente e quello automatizzato/predittivo.

Questi tre «filoni aurei» dell'innovazione contemporanea, all'apparenza accomunati soltanto da istanze sociali tradizionalmente collegate allo sviluppo della tecnica, quali il benessere collettivo (economico, biologico, ecologico) o la sicurezza statale (declinata ad esempio come prevenzione del rischio e tutela della pace[2]), possono essere invero riletti ed interpretati sotto differenti prospettive:

nella stessa maniera in cui, nella prima era delle comunicazioni elettroniche, le informazioni relative agli utenti hanno subito un processo di dematerializzazione[3], oggi il rilevamento di un fatto naturalistico, di un comportamento umano, dell'interazione tra uomo e cosa è attuato in maniera sempre più uniforme e standardizzata attraverso la captazione automatica e digitalizzata. Satelliti, sensori, etichette radio intelligenti (RFID), dispositivi video sono progettati, messi in commercio o azionati per favorire il costante monitoraggio e la messa a disposizione dei risultati in un formato neutro ed intellegibile a tutti.

L'informazione digitalizzata circola in rete con facilità e viene immagazzinata e gestita dai soggetti che approntano i servizi fruibili attraverso la rete, nonché dalle imprese che fabbricano e commercializzano dispositivi tecnologici disegnati per catturare l'ambiente esterno e gli avvenimenti che ne scandiscono la quotidianità; il «dato» non si presta ad un'applicazione unica e fissa nel tempo, ma permane e transita nella disponibilità dei soggetti che lo detengono poiché non è mai possibile conoscere in anticipo quale sia lo *scopo finale* per cui esso è stato raccolto e se ne esista uno soltanto.

[2] Sul tema, per tutti si veda il quadro di sintesi offerto da W. Sofsky, *Rischio e sicurezza*, Torino, 2005, passim.

[3] Il riferimento va alla «società dell'informazione» nata tra la fine del XX secolo e la prima decade del nuovo millennio: per una ricognizione cfr. F. Cairncross, *The death of distance: how the communication revolution is changing our lives*, Boston, 2ª ed., 2002; J. Rifkin, *The Age of Access. The New Culture of Hypercapitalism, Where All of Life is a Paid-for Experience*, New York, 2000; J. Ryan, *Storia di Internet e il futuro digitale*, Torino 2011, passim e sotto profilo precipuamente giuridico si rimanda agli imprescindibili (e per certi versi profetici) studi di V. Frosini, *Cibernetica diritto e società*, Milano, 1968; Id., *Il diritto nella società tecnologica*, Milano, 1981.

 ISSN 2037-5662

Partendo da queste premesse, è facile rilevare come non si sia mai avuta nella storia dell'umanità una così vasta, dettagliata ed eterogenea disponibilità di informazioni intellegibili in maniera uniforme[4] e combinabili informaticamente nelle più disparate maniere.

Dall'approccio eziologico, che studia un determinato evento per ricollegarlo in maniera univoca ad un altro, si staglia nella sua elementare immediatezza un diverso schema operazionale che fa capo alla nozione di correlazione.

Per correlazione si intende il risultato ottenuto dall'analisi e dalla sovrapposizione di un indefinito numero di informazioni, dal contenuto variabile (posizione geografica, temperatura del suolo, densità dell'aria, dinamiche di interazione telefonica o su Internet, preferenze di consumo, informazioni personali, sensibili, anonime, pseudonime ecc.) e non necessariamente organizzato secondo criteri e standard prestabiliti, che disveli l'esistenza di rapporti biunivoci tra uno o più elementi (o valori) tali da potere constatare, sulla base di criteri statistico/percentuali, un certo grado di influenza reciproca.

In altre parole, l'approccio correlativo mira a fornire indicazioni *nuove* agli umani (o ancora ad entità non umane programmate per attuare ordini o elaborare schemi d'azione), formulate sulla base di un certo grado di «parentela» e coerenza tra determinate informazioni, che risultino *utili* nel senso di suggerire o confermare un risultato o un postulato, predire un determinato fenomeno o produrre inferenze orientando le attitudini e le capacità di scelta e comportamento nello spazio e nel tempo[5].

[4] Poiché fornite attraverso uno standard uniforme di lettura, quale il codice binario.

[5] Secondo il pluricitato volume di V. Mayer-Schönberger-K. Cukier, *Big Data*, Milano, 2013, p. 76, la correlazione rappresenta una «relazione statistica tra i valori di due dati». La nozione di correlazione in generale si sviluppa sia nelle scienze sociali (come quelle economico/statistiche, la sociologia o, ancora, la linguistica) che nelle scienze di base o naturali (ad es. la fisica). In entrambi campi si tratta di ricercare un rapporto di interdipendenza tra due elementi, caratteristiche o valori, per cui uno può variare in un certo modo in funzione dell'altro. In argomento cfr. anche R. Kitchin, *Big Data, new epistemologies and paradigm shifts*, in *Big Data and Society*, 2014, pp. 1-12; M.L. Ambrose, *Lessons from the Avalanche of Numbers: Big Data in Historical Perspective*, in 11 *ISJLP* 201 (2015) e V. Zeno-Zencovich-G. Giannone Codiglione, *Ten Legal Perspectives on the «Big Data Revolution»*, in *Conc. merc.*, 23, 2016, pp. 29-57. Sui concetti di «causalità» e «correlazione» nella letteratura scientifica si v. ad es. G.U. Yule, *On The Methods Of Measuring Association Between Two. Attributes*, in 75 *Journal of the Royal Statistical Society* 579 (1912); K. Pearson, *Notes on the History of Correlation*, in *Biometrika*, 1920, p. 1 ss.; A. Graziani, *Correlazioni e causalità nei fatti economici*, in *Giorn. econ.*, 1907, pp. 1029-1040; V. Capecchi, *Causalità e correlazione nella problematica sociologica*, in *Studi di Sociologia*, 3, 1964, pp. 229-274; M.C.

 ISSN 2037-5662

Negli ultimi anni, sono state intraprese diverse esperienze empiriche o di ricerca basate su metodi computazionali e funzioni precipuamente predittive[6]: grazie alla lettura incrociata di enormi data-set, frutto dell'afflusso di molteplici punti di raccolta, è possibile ad esempio ricostruire le interazioni che avvengono in un dato luogo geografico con una precisione pari quasi ad una scala di 1 a 1, raggiungendo una definizione elevata non solo con riguardo alla mera rappresentazione grafica. In questo modo, appare più agevole comprendere quale percorso stradale possa risultare maggiormente scorrevole al fine di raggiungere una determinata meta, quale elemento ambientale o comportamentale spinga uno o più soggetti ad agire per il perseguimento di un determinato scopo di consumo, o, ancora è possibile favorire l'elaborazione automatica di ordini e schemi comportamentali di un robot o di una protesi bionica innestata nel corpo umano, raggiungendo gradi di precisione tali da proclamarne l'autonomia o, comunque, favorendo la perfetta integrazione di una «cosa» nella sfera biologica della persona che ha subìto l'impianto. Entrambi gli approcci descritti (eziologico e correlativo), constano pur sempre di un filtro cognitivo che è ideato e interposto dall'uomo, con l'unica differenza che mai come oggi la «legge» scientifica, animata e inglobata nella tecnica, si muove (nella) e influenza (la) realtà prescindendo dalla volontà umana.

Gli sforzi profusi dai governi occidentali per avviare ed implementare un modello sociale totalmente immerso nell'informazione come quello rappre-

Galavotti, *Causalità, leggi, spiegazione*, in *Quad. storia econ. pol*., 5/6, 1987/1988, pp. 121-133; A. Marradi, *Linee guida per l'analisi bivariata dei dati nelle scienze sociali*, Milano, 1997, passim; F. Viole-D.N. Nawrocki, *Causation*, in *SSRN* (http://ssrn.com/abstract=2273756), giugno 2013.

[6] L'approccio computazionale, imperniato sull'avvento dei *Big Data* viene considerato un modello di ricerca interdisciplinare tra scienze sociali, scienze informatiche e scienze complesse passibile di poter incidere in maniera netta sul generale metodo di studio della biologia e della fisica. Si vedano D. Lazer-A. Pentland-L. Adamic-S. Aral-A.L. Barabási-D. Brewer-N. Christakis-N. Contractor-J. Fowler-M. Gutmann-T. Jebara-G. King-M. Macy-D. Roy-M. Vanalstyne, *Computational Social Science*, in *Science*, 323, 2009, n. 5915, pp. 721-723; R. Conte-N. Gilbert-G. Bonelli-C. Cioffi-Revilla-G. Deffuant-J. Kertesz-V. Loreto-S. Moat-J.P. Nadal-A. Sanchez-A. Nowak-A. Flache-M. San Miguel-D. Helbing, *Manifesto of Computational Social Science*, in 214 *EPJ* 325 (2012); S. Faro-N. Lettieri, *Walking Finelines between Law and Computational Social Science*, in *Inf. e dir*., 1, 2013, pp. 9-24 (num. monografico); J. Lin, *Perspectives on Computational Social Science: On Building Better Mousetraps and Understanding the Human Condition: Reflections on Big Data in the Social Sciences*, in 659 *Annals* 33 (2015); M. Hindman, *Perspectives on Computational Social Science: Building Better Models: Prediction, Replication, and Machine Learning in the Social Sciences*, ivi, p. 48 ss.

 ISSN 2037-5662

sentato dall'Internet delle cose (*Internet of Things* o IoT) – fusione dei tre fenomeni descritti in precedenza («cose intelligenti», *Big Data*, Internet) in un assetto globale integrato – apre numerose questioni di matrice etica, politica, sociologica, regolamentare: ogni istanza ad esse collegata influenza in una certa misura le altre, dando vita ad un inestricabile intreccio di rapporti biunivoci[7].

L'*Internet of things* consiste nel collegamento continuo, ininterrotto, interoperabile ed interattivo tra dispositivi, oggetti, sensori e macchine apprestato dall'accesso a reti a banda larga e/o senza fili per mezzo di protocolli di indirizzi logici e fisici[8]: i rapporti comunicativi tra utenti o macchine già possibili grazie ad Internet (U2U – U2M) si estendono ad oggetti inanimati ma dotati di sensore (U2C o C2C) e a macchine capaci di compiere determinate azioni (M2M, M2C)[9].

In questa sede ci si propone di studiare l'assetto vigente nei comparti maggiormente coinvolti nell'avvento dei *Big Data*, al fine di leggere le soluzioni adottate in una prospettiva operazionale, cioè guardando all'impatto sortito da questo fitto schema di interrelazioni tra autonomi sistemi tecnologicamente avanzati sull'assetto tripartito della società attuale (stato-mercato-persona).

2. Come è noto, Internet rappresenta una struttura di comunicazione tra più punti di accesso (nodi) attraverso un medesimo linguaggio (il c.d. protocollo TCP/IP). L'approccio centrifugo teorizzato per la prima volta da Paul Baran coincideva appunto nell'assunto libertario e paritario di garantire un sistema di connessione tra centri di trasmissione «diversi» che riuscisse a trasportare, nel modo più veloce possibile, un certo pacchetto di dati da un punto all'altro anche in presenza di condizioni di turbativa dell'equi-

[7] Cfr. per il momento N.M. Richards-J.H. King, *Big Data Ethics*, in 49 *Wake Forest L. Rev*. 393 (2014) e V. Zeno-Zencovich-G. Giannone Codiglione, *Ten Legal Perspectives on the «Big Data Revolution»*, cit., p. 53 ss.

[8] Commissione UE, 29 settembre 2009, *Comunicazione sull'internet e sulle reti del futuro*, COM(2008) 594 def., p. 5.

[9] Cfr. Commissione UE, 18 giugno 2009, *L'internet degli oggetti – Un piano d'azione per l'Europa*, COM(2009) 278 def., p. 2 s.; Parlamento UE, *Risoluzione del 15 giugno 2010 sull'internet degli oggetti*, (2009/2224(INI)), in *GUUE*, 12 agosto 2011, C 236 E/25, per cui «(…) "internet degli oggetti" si riferisce al concetto generale di oggetti (sia artefatti elettronici sia oggetti di uso quotidiano) leggibili, riconoscibili, indirizzabili, localizzabili e/o controllabili a distanza tramite internet (…)».

 ISSN 2037-5662

librio precostituito[10]. Ancora oggi la rete incarna appieno questo disegno, con la differenza che essa viene utilizzata su scala globale per ogni tipologia di attività svolta dall'uomo. L'utente non solo trasmette, ma produce autonomamente (e cede) informazioni in maniera consapevole o implicita; enti pubblici ed imprese gestiscono l'infrastruttura e forniscono a pagamento o (apparentemente) in assenza di un corrispettivo economico l'accesso ai servizi di connettività o alle molteplici tipologie di prestazione ad essa associati[11].

L'Open Internet order emesso dalla *Federal Communication Commission*[12] e il regolamento n. 2120/2015 «che stabilisce misure riguardanti l'accesso a un'Internet aperta»[13], consolidano e introducono principî ordinatori e regole sulla c.d. net neutrality[14], indirizzate al mantenimento e alla promozione di una rete veloce, imparziale e aperta (*fast, fair and open network*).

L'ordine del 26 febbraio 2015 segue la sentenza *Verizon v. FCC*[15], con cui la Corte d'Appello per il Secondo Circuito ha accolto il ricorso di alcuni tra i maggiori fornitori di accesso statunitensi (c.d. broadband providers), privando di validità alcune parti del precedente Open Internet order del 2010.

La nuova regolamentazione, recependo le indicazioni della Corte d'Appello, estende il proprio ambito d'applicazione ad ogni tipo di servizio di

[10] Il fattore scatenante fu, come è noto, il timore di un attacco nucleare da parte della Russia e il possibile, sostanziale, collasso della rete telefonica analogica, costruita attorno ad un sistema di tipo verticale e centralizzato. Cfr. P. Baran, *On distributed communication networks*, (memorandum RM-3420-PR, Santa Monica, 1964, reperibile all'URL: http://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf/; J.C.R. Licklider, *Memorandun for members and affiliates of the intergalactic computer network*, 23 aprile 1966, reperibile all'URL: http://www.packet.cc/files/memo.html/. Per una chiara ricostruzione storica sugli inizi di quella particolare esperienza di ricerca che coinvolse alcuni istituti di ricerca militari (e poi universitari), v. J. Ryan, *Storia di Internet e il futuro digitale*, Torino, 2011, p. 31 e ss.

[11] Potendo distinguersi, in via meramente esemplificativa, in *backbone networks*, le compagnie che approntano grandi reti in fibra in tutto il mondo; *broadband* provider, le imprese che forniscono servizi dati di tipo domestico, professionale o individuale ed *edge* provider, i prestatori di servizi accessibili una volta connessi alla rete.

[12] FCC, *In the Matter of Protecting and Promoting the Open Internet*, Docket No. 14-28, 12 marzo 2015. Un interessante studio dell'order è stato svolto e reso pubblico da un gruppo di esperti coordinato dal prof. M. Dècina, in seno al MISE, nel corso della discussione del Regolamento europeo al Consiglio d'Europa: Aa.Vv., *Riflessioni sull'Open Internet Order della FCC*, reperibile all'URL: http://www.sviluppoeconomico.gov.it/images/stories/documenti/Open_internet.pdf/.

[13] Pubblicato in *GUUE*, 26 novembre 2015, L 310/1.

[14] T. Wu, *Network Neutrality, Broadband Discrimination* in 2 *J. on Telecomm. & High Tech. L.*, 141 (2003).

[15] *Verizon v. Federal Communications Commission*, 740 F.3d 623 (D.C. Cir. 2014).

 ISSN 2037-5662

rete (banda larga, mobile o fisso) e riclassifica l'accesso ad Internet come servizio di telecomunicazione e non più come mero servizio informativo, equiparandolo ad un bene di utilità primaria a rilevanza pubblica come il telefono (c.d. *common carrier*)[16].

Le disposizioni dell'Open Internet order (cc. dd. *bright line rules*) vietano al gestore della rete di bloccare l'accesso a contenuti leciti, applicazioni, servizi, o dispositivi non dannosi (*no blocking*), di ridurre o degradare il traffico Internet legale sulla base di contenuti, applicazioni, servizi o dispositivi non dannosi (*no throtthling*) e, infine, di offrire servizi di traffico Internet a pagamento che possano creare disparità di connessione alla Rete attraverso l'offerta di *fast lanes* (*no paid priorization*)[17].

Il principio di non discriminazione con riguardo all'accesso o la prestazione di servizi è inoltre rafforzato dall'affermazione della regola di «*no unreasonable interference or disadvantage to consumers or edge providers*», che modula l'azione regolatoria più in generale attorno agli interessi dell'utente e dei prestatori di servizi web. Seppur si ammetta in astratto che anche l'*edge* provider (ovvero il prestatore di servizi diversi dall'accesso, quale un *social network*) possa offrire ai propri utenti prestazioni differenziate e *premium* dietro corrispettivo, l'ordine impone che tali attività non debbano causare una irragionevole interferenza o svantaggio nei confronti di tutti gli altri consumatori o prestatori concorrenti[18].

La nozione comunitaria di neutralità tecnologica, sintesi dei concetti di accesso, interconnessione ed interoperabilità, è frutto della riforma in tema comunicazioni elettroniche e converganza avviata con il pacchetto di diret-

[16] Il richiamo è al Title II del *Communications Act* e ancora alla sec. 706 del *Telecommunications Act of* 1996. La medesima Corte d'Appello ha poi confermato la validità del testo normativo a seguito di un nuovo ricorso proposto dalle società di comunicazione statunitensi: la questione potrebbe essere in via definitiva posta all'attenzione della Supreme Court. V. *United States Telecom Association v. Federal Communications Commission*, dock. No. 15-1063, (D.C. Cir. 2016).

[17] L'order impone altresì uno standard di condotta univoco e chiaro, implementa gli obblighi di trasparenza, attraverso la previsione di un *duty to disclose* posto in capo agli operatori con più abbonati avente per oggetto ogni limitazione di carattere tecnico ed economico che possa in qualche modo compromettere o limitare il servizio offerto. Inoltre viene indicato un formato standard di divulgazione di tali informazioni, che agisce come una sorta di *safe harbor* per i prestatori e, infine si fa salva la possibilità di adottare ragionevoli forme di gestione per fini non commerciali di alcuni tipi di rete (es. reti Wi-Fi senza licenza).

[18] FCC, *In the Matter of Protecting and Promoting the Open Internet*, cit., §8.11, pp. 9, 60 s. e 285.

 ISSN 2037-5662

tive del 2002 e proseguita con gli interventi di modifica del 2006 e 2009[19]. In questo quadro, il regolamento «Internet aperta» ricalca le previsioni adottate oltreoceano adattandole al quadro normativo previgente.

L'art. 3, n. 1 afferma il diritto per gli utenti di «accedere a informazioni e contenuti e di diffonderli, nonché di utilizzare e fornire applicazioni e servizi, e utilizzare apparecchiature terminali di loro scelta, indipendentemente dalla sede dell'utente finale o del fornitore o dalla localizzazione, dall'origine o dalla destinazione delle informazioni, dei contenuti, delle applicazioni o del servizio, tramite il servizio di accesso a Internet»[20].

L'art. 3, n. 3, primo periodo impone dall'altra parte che i fornitori di servizi di accesso a Internet debbano trattare «tutto il traffico allo stesso modo, senza discriminazioni, restrizioni o interferenze, e a prescindere dalla fonte e dalla destinazione, dai contenuti cui si è avuto accesso o che sono stati diffusi, dalle applicazioni o dai servizi utilizzati o forniti, o dalle apparecchiature terminali utilizzate».

Il principio procompetitivo di «non irragionevole interferenza o svantaggio di matrice statunitense viene poi diversamente declinato con riguardo alle diverse figure implicate nell'offerta di servizi in rete:

i) il prestatore di contenuti è libero di offrire servizi qualitativamente migliori, a patto che essi non vadano a discapito della disponibilità o la qualità generale dei servizi di accesso a internet per gli altri utenti (art. 3, n. 5);

ii) ai sensi dell'eccezione di cui all'art. 3, n. 3, secondo periodo e ss., il fornitore di accesso è invece autorizzato ad attuare misure ragionevoli di implementazione del traffico a patto che esse siano trasparenti, non discriminatorie, proporzionate e non si basino su considerazioni di tipo commer-

[19] In Italia, ad esempio, l'art. 4 del d.lgs. 259 /2003 (c.d. Codice delle comunicazioni elettroniche), al comma 3, lett. *b*), fissa tra gli obiettivi della disciplina delle reti e dei servizi di comunicazione elettronica quello di garantire la neutralità tecnologica, intesa come la «non discriminazione tra particolari tecnologie, non imposizione dell'uso di una particolare tecnologia rispetto alle altre e possibilità di adottare provvedimenti ragionevoli al fine di promuovere taluni servizi indipendentemente dalla tecnologia utilizzata».

[20] L'articolo ricalca per grandi linee la nozione apprestata dall'art. 4, n. 1 della Dichiarazione dei diritti in Internet, redatta dalla Commissione per i diritti e i doveri in Internet istituita in seno alla Camera dei deputati e presieduta dal prof. S. Rodotà, per cui «Ogni persona ha il diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone». In argomento si cfr. inoltre i considerando nn. 3, 6 e 7 del regolamento.

 ISSN 2037-5662

ciale, ma sull'oggettiva differente qualità tecnica dei requisiti di servizio di specifiche categorie di traffico. Tali misure inoltre non dovranno monitorare lo specifico contenuto né durare più a lungo del necessario.

In maniera analoga rispetto a quanto affermato dalle *bright line rules*[21], il regolamento impone poi al fornitore di accesso di non bloccare, rallentare, modificare, limitare, interferire, degradare o discriminare specifici contenuti, applicazioni o servizi, ad eccezione di quanto necessario e solo per il tempo necessario al fine di: *a*) attuare una norma o un ordine giudiziario comunitario; *b*) preservare l'integrità e la sicurezza della rete, dei servizi apprestati e del terminale utente; *c*) prevenire la congestione della rete o mitigarne gli effetti[22].

In sostanza, volendo assestarci su un primo livello di comprensione del fenomeno, il contenuto dei due atti normativi coincide per larghe linee, favorendo un modello di implementazione e gestione di Internet basato su tre assunti: *i*) le informazioni possono circolare liberamente e senza subire sostanziali rallentamenti ed accelerazioni rispetto agli altri flussi, eccetto nei casi di eccessiva congestione del traffico, motivi di sicurezza, esecuzione di ordini giudiziari; *ii*) la connettività ad un punto finale della rete è libero sia per gli utenti che per qualsivoglia tipo di entità tecnica progettata ed idonea ad accedere al flusso comunicativo[23]; *iii*) la prestazione di servizi in Internet deve essere svolta in maniera tale da non cagionare agli altri un irragionevole interferenza o svantaggio o, discutendo in termini comunitari, deve rispettare i principi di proporzionalità e non discriminazione.

3. Poste queste basi comuni, il regolamento europeo sull'Internet aperta si esprime in maniera maggiormente specifica riguardo al ruolo svolto dagli

[21] FCC, *In the Matter of Protecting and Promoting the Open Internet*, cit., § 8.2 (f), p. 284.

[22] Art. 3, terzo comma e v. anche il considerando n. 9 del regolamento Internet aperta.

[23] L'art. 2 del regolamento Internet aperta definisce il servizio di accesso ad Internet come «un servizio di comunicazione elettronica a disposizione del pubblico che fornisce accesso a Internet, ovvero connettività *a praticamente tutti i punti finali di Internet, a prescindere dalla tecnologia di rete e dalle apparecchiature terminali utilizzate*» (corsivo aggiunto). Specularmente, anche il § 8.2 (a) dell'order: «A mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, *including any capabilities that are incidental to and enable the operation of the communications service*, but excluding dial-up Internet access service. This term also encompasses any service that the Commission finds to be providing a functional equivalent of the service described in the previous sentence, or that is used to evade the protections set forth in this Part».

 ISSN 2037-5662

intermediari, ammettendo in astratto che i prestatori diversi dai fornitori di accesso, nell'ipotesi di servizi di interesse pubblico o ancora di «alcuni nuovi servizi di comunicazione da macchina a macchina»[24], possano offrire contenuti, applicazioni, servizi o loro combinazioni garantendo diversi ed elevati standard qualitativi, a patto che tale offerta non degradi la disponibilità e la qualità generale dei servizi di accesso a Internet per gli utenti finali[25].

Tale assunto, come si è visto ripreso dall'art. 3, n. 5 del regolamento e in generale riconducibile al divieto di produrre un'irragionevole interferenza o svantaggio di cui al § 8. 11 del FCC order, apre in maniera specifica l'analisi al secondo livello di gestione dell'IoT, concernente le imprese e/o le entità chiamate a ricoprire in vario modo la mediazione tra «reale», umano e rete di comunicazione.

A tal fine sembra opportuno suddividere lo studio avendo riguardo per due sotto-categorie soggettive: *a*) le imprese preposte all'intermediazione delle informazioni nella rete; *b*) le imprese e/o le entità che adoperano i servizi offerti dalle prime o, ancora, sfruttano la connettività alla rete come intermediario «puro», in un certo senso operando alla stregua di un utente che accede ad un punto finale attraverso un terminale (soggetti questi che potrebbero essere agevolmente ricompresi entro la definizione fornita dal considerando n. 16 del regolamento Internet aperta).

[24] Cfr. il considerando n. 16 del regolamento Internet aperta: «I fornitori di contenuti, applicazioni e servizi chiedono di poter fornire servizi di comunicazione elettronica diversi da quelli di accesso a Internet, per cui sono necessari livelli specifici di qualità del servizio che non sono garantiti da servizi di accesso a Internet. Tali livelli specifici di qualità sono richiesti, ad esempio, da alcuni servizi che rispondono a un interesse pubblico o da alcuni nuovi servizi di comunicazione da macchina a macchina. I fornitori di comunicazioni elettroniche al pubblico, compresi i fornitori di servizi di accesso a Internet, e i fornitori di contenuti, applicazioni e servizi dovrebbero pertanto essere liberi di offrire servizi diversi dai servizi di accesso a Internet ottimizzati per specifici contenuti, applicazioni o servizi o loro combinazioni, nei casi in cui l'ottimizzazione sia necessaria per soddisfare i requisiti relativi a contenuti, applicazioni o servizi per un livello specifico di qualità. Le autorità nazionali di regolamentazione dovrebbero verificare se e in quale misura una tale ottimizzazione sia oggettivamente necessaria per garantire una o più caratteristiche specifiche e fondamentali di contenuti, applicazioni o servizi e per consentire una garanzia di qualità corrispondente agli utenti finali, piuttosto che accordare semplicemente una priorità generale rispetto a contenuti, applicazioni o servizi analoghi disponibili tramite il servizio di accesso a Internet ed eludere in tal modo le disposizioni in materia di misure di gestione del traffico applicabili ai servizi di accesso a Internet».

[25] Si legga anche il considerando n. 17.

 ISSN 2037-5662

Con riferimento alla prima categoria, le norme civilistiche, penalistiche e/o autoregolamentari vigenti in Europa fanno capo alla direttiva 2000/31/CE sul commercio elettronico, concorrendo a tracciare per le tre categorie di provider individuati (fornitori di accesso, temporanea e permanente memorizzazione di informazioni) una generale immunità per i contenuti o le condotte illecite poste in essere in rete utilizzando i propri servizi, nonchè, in parallelo, un divieto di monitorare o vagliare in via preventiva le comunicazioni elettroniche[26].

La direttiva incarna due principali obiettivi di politica del diritto: non gravare oltremodo sulla sostenibilità economica delle attività di impresa attuate dai provider e non limitare la libera circolazione delle informazioni.

In subordine, anche a seguito di una costante rilettura della materia offerta dal formante giurisprudenziale, si afferma in capo ai prestatori un onere di immediata reazione al momento della venuta a conoscenza dell'esistenza di un'informazione o di un'attività illecita. La segnalazione, proveniente da un'autorità giurisdizionale o ancora da un privato titolare di un interesse negativamente coinvolto, darà luogo alla rimozione dell'informazione dal bacino di dati messi a disposizione del pubblico o, ancora, a causa dell'impossibilità tecnica di attuarne una completa eradicazione (ad es. l'ubicazione extra-UE dei server) e della proporzionalità della misura rispetto al complesso degli interessi coinvolti, il prestatore dispone la disabilitazione dell'accesso all'informazione, in *abstracto* privando l'utente della facoltà di poterne fruire ed accedervi[27].

Tale quadro regolamentare, frutto della commistione tra precetti normativi e prassi applicative nello spettro della tutela e del bilanciamento dei diritti fondamentali, è ricalcato sulla disciplina statutaria entrata in vigore negli Stati Uniti alla fine degli anni novanta dello scorso secolo, con la marcata differenza che oltreoceano la regola generale si frammenta a seconda del tipo di illecito (violazione del copyright, perseguita con il *Digital Millennium*

[26] In uno sconfinato apporto della letteratura sul tema si rimanda a G.M Riccio, *La responsabilità civile degli internet providers*, Torino, 2001; T. Verbiest – G. Spindler - G.M. Riccio, *Study on the liability of internet intermediaries*, 2007, Markt/2006/09/E, rintracciabile all'URL:http://ec.europa.eu/internal_market/ecommerce/docs/study/liability/final_report_en.pdf/.

[27] Per tutti, si vedano, con riguardo alla giurisprudenza comunitaria CGE Grande sez., 13 maggio 2014, causa C-131/12, *Google Spain, Google Inc.* c. *AEPD, Costeja González*, in *Dir. inf.*, pp. 535 – 562 (diritto alla cancellazione e all'oblio sui motori di ricerca); CGE, sent. 27 marzo 2014, causa C-314/12, *Telekabel Wien c. Constantin film e Wega*, in www.curia.europa.eu/ (tutela del diritto d'autore e disabilitazione dell'accesso da parte del mere conduit provider).

 ISSN 2037-5662

Copyright Act del 1998 e tutela della personalità dell'utente, attraverso il *Communication Decency Act* of 1996) e, ancora, che grazie alle prescrizioni in tema di copyright, la rimozione del contenuto illecito sovente avviene in una fase precedente a quella giudiziaria, grazie all'imposizione per via statutaria di un procedimento facilitativo di tipo autoregolamentare (c.d. *notice and take down*)[28].

Calando queste regole nell'architettura dell'Internet delle Cose, il prestatore di servizi, inteso come il soggetto operante per scopi di lucro che fornisce l'accesso e, ancora, garantisce la produzione e la disseminazione dell'informazione da un punto all'altro della rete, sia in maniera permanente che temporanea, è obbligato a facilitare il flusso informazionale senza doverne modificare o influenzare il percorso, attivando altresì forme di intervento tempestivo a tutela di soggetti diversi da coloro che hanno dato vita e/o immesso l'informazione illecita nel circolo comunicativo (poiché inesatta, non conforme, contraria a precetti normativi).

Dall'altra parte, la progressiva importanza ricoperta da entità sostanzialmente diverse dai meri prestatori di servizi o dagli utenti, conduce a concentrare la rassegna sugli obblighi e le responsabilità ad essi imputabili.

L'apporto di macchine dotate di intelligenza artificiale, o comunque capaci di porre in essere azioni senza il diretto intervento dell'uomo è stata oggetto di riflessioni e speculazioni teoriche sin dall'avvento dei primi studi sull'impatto della cibernetica e dell'informatica nella società e rispetto allo svolgersi della regola giuridica[29].

Oggi, diversamente dal passato, tali entità non operano soltanto seguendo programmi rigorosamente predeterminati (come lo stesso etimo della parola 'programma' indica) ed attingendo esclusivamente alla propria «espe-

[28] 17 U.S.C. § 512 (c). Sul punto sia consentito rimandare a G. Giannone Codiglione, *Illeciti su Internet e rimedi nel diritto d'autore* (Tesi di dottorato), Università di Salerno, 2014, spec. 99 ss. e 158 ss., nonché a . Ginsburg, *Il «Digital Millennium copyright Act» ed il «Sonny Bono copyright term extension Act»: due novità dagli Stati Uniti*, in *Riv. dir. comm.*, 7-8, 1999, pp. 625 e ss.; G.M Riccio, *La responsabilità civile degli internet providers*, cit., pp. 171 e ss.

[29] Senza pretesa di esaustività si rimanda alle pionieristiche riflessioni di V. Frosini, *Cibernetica diritto e società*, Milano, 1968, spec. pp. 111 ss., il quale si interrogava sull'opportunità di considerare un robot dotato di intelligenza artificiale come un soggetto morale, in un conflitto tra coscienza interna (propria dell'uomo come essere che nasce da ζωή) e coscienza esterna (potenziamento della prima, frutto della tecnica); M.G. Losano - C. Ciampi (a cura di), *Artificial intelligence and legal information systems*, Amsterdam-Tokyo 1982; G. Sartor, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano 1990.

 ISSN 2037-5662

rienza», ma sono chiamati a sfruttare ed implementare il bacino indefinito di informazioni che fluisce nell'IoT, apparendo così capaci di potenziare in maniera indefinita le proprie capacità di base senza necessariamente dover emulare o sviluppare forme intuitive (cioè basate su meccanismi cognitivi causali induttivo-deduttivi) di coscienza[30].

La capacità di autoapprendimento e i sensori connessi alla rete installati su macchine ed oggetti chiamati a operare nell'ambito dell'IoT[31] permette già, anche se su scala ridotta e in via sperimentale, ad autovetture senza conducente di viaggiare affrontando con attenzione e riflessi maggiori degli umani gli imprevisti di una comune strada cittadina, a droni volanti di effettuare consegne a domicilio, a frigoriferi semi-vuoti di coordinare l'approvvigionamento corretto delle derrate alimentari dialogando con il supermercato, a termostati intelligenti di ridurre la produzione di calore in un edificio e stornarla su un altro edificio, a pizzaioli e avvocati robot di sostituire l'uomo nell'esercizio di attività professionali tradizionalmente connotate da un elevato grado di qualificazione[32].

Rispetto a tali problemi, gli ordinamenti giuridici si pongono tradizionalmente attuando due differenti approcci: *a*) imputare la responsabilità al soggetto che ne è proprietario o che, in qualche modo, ne detiene la custodia o è ad esso legato da un vincolo giuridico (responsabilità per colpa aggravata o semi-oggettiva)[33]; *b*) allocare il rischio scaturente dall'attività svolta da en-

[30] M.G. Losano, *Informatica per le scienze sociali*, Torino,1985, pp. 38 e ss.; B. Latour, *Politics of Nature: How to Bring the Sciences Into Democracy, Harvard,* 2004; E. Mazzarella, *L'androide Philip Dick. Identità umana e artificio. Idee per una libertà sostenibile*, in P. Barcellona – F. Ciaramelli – R. Fai (a cura di), *Apocalisse e postumano. Il crepuscolo della modernità*, Bari, 2007, pp. 415 e ss.

[31] Si veda, ad es. con riferimento al c.d. wearable computing E. Germani – L. Ferola, *Il wearable computing e gli orizzonti futuri della privacy*, in *Dir. inf*., 1, 2014, pp. 75 e ss.; A. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, in 21 *Rich. J.L. & Tech.* 6 (2015).

[32] Sono notizie recenti l'assunzione da parte della Law Firm globale Baker & Hostetler di Ross, robot fallimentarista progettato da IBM e capace di adempiere le mansioni di cinquanta avvocati umani (ulteriori informazioni all'URL: http://www.rossintelligence.com/) e, ancora della creazione da parte del laboratorio di ricerca Prisma Lab dell'Università Federico II di Napoli di RoDyMan, un robot di servizio capace di replicare con destrezza e mobilità alcune particolare tipologie di attività umana (http://www.rodyman.eu/).

[33] Seguendo il principio *agency – respondeat superior*, per cui – analogamente a quanto avvenuto nel periodo feudale tra landlords e tennants – il proprietario di un'attività (*employer*) viene chiamato a rispondere dei danni causati dai suoi dipendenti (*employees*) nell'esercizio di un'attività riconducibile al proprio beneficio ed interesse economico. Sul punto si rimanda a P.S. Atiyah,

 ISSN 2037-5662

tità non umane alle società produttrici, ove l'errore o il danno cagionato sia riconducibile ad un difetto di fabbricazione o, ancora, all'estensione temporale dell'efficacia della garanzia (*strict liability*)[34].

Tali indizi portano chiaramente verso la negazione di un'effettiva autonomia al paradigma «post-umano» (nel senso di un mancato riconoscimento alla macchina dotata di intelligenza artificiale di una propria personalità giuridica)[35], al massimo investita per via legislativa o giudiziale di un rapporto proprietario, di custodia o ancora di consumo tale da imporre determinati oneri di controllo o responsabilità a soggetti o enti che ne fruiscono direttamente o ancora che ne hanno sviluppato la produzione e la commercializzazione seriale[36].

Vicarious Liability in the Law of Torts, London, 1967, pp. 12 e ss. Per una rassegna di alcuni casi riguardanti la responsabilità per danno (o morte) sul luogo di lavoro cagionato da robot v. *Miller v. Rubbermaid Inc.*, 2007 Ohio App. LEXIS 2672 (Jun. 13, 2007); *State ex rel. Scott Fetzer Co. v. Industrial Comm'n of Ohio*, 692 N.Ed 2d 195 (Ohio 1998) (per curiam); *Edens v. Loris Bellini, S.p.a.*, 597 S.E.2d 863 (S.C. Ct. App. 2004), dalla lettura dei quali si evidenzia come soltanto in un caso sia stata concessa la ultracompensazione del danno (*Scott Fetzer Co.*) per l'omissione delle necessarie misure di sicurezza da parte dell'*employer*.

[34] Si veda, nel case-law statunitense *Jones v. W + M Automation, Inc.*, 818 N.Y.S.2d 396 (App. Div. 2006), *appeal denied*, 862 N.E.2d 790 (N.Y. 2007) in cui si è affermata la responsabilità del produttore per il danno causalmente riconducibile ad un difetto dell'automa presente sin dal momento dell'acquisto. V. anche *Payne v. ABB Flexible Automation, Inc.*, 1997 U.S. App. LEXIS 13571 (8th Cir. Jun. 9, 1997); *Provenzano v. Pearlman, Apat & Futterman, LLP*, 2008 U.S. Dist. LEXIS 86098 (E.D.N.Y. Oct 24, 2008). Nella dottrina italiana si vedano G. Alpa – M. Bin – P. Cendon (a cura di), *La responsabilità del produttore*, in F. Galgano (dir. da), *Trattato di diritto commerciale*, diretto da Galgano, XIII, Padova, 1990; S. Sica – V. D'Antonio, *La responsabilità per danno da prodotti difettosi*, in P. Stanzione – A. Musio (a cura di) *La tutela del consumatore*, Torino, 2009, pp. 595-670; G. Alpa – M. Bessone (a cura di), *Danno da prodotti e responsabilità dell'impresa. Diritto italiano ed esperienze straniere*, Milano, 1980; G. Ponzanelli, *La responsabilità del produttore negli Stati Uniti d'America*, in *Danno e resp.*, 1999, p. 1066 ss..

[35] L.B. Solum, *Legal Personhood for Artificial Intelligences*, in 70 *N. C. L. Rev*. 1231 (1992); G. Teubner, *Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law*, Max Weber Lecture No. 2007/04; P. Stanzione, *Biodiritto, postumano e diritti fondamentali*, in *Comp. e dir. civ*., 2010, spec p. 11 s.; S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, 2012, spec. pp. 312 e ss., 341 e ss.

[36] È quanto ad esempio emerge dal documento finale pubblicato nell'ambito del progetto RoboLaw, coordinato dalla Scuola Superiore Sant'Anna di Pisa e finanziato dall'Unione Europea: Aa.Vv., *D6.2 Guidelines on Regulating Robotics*, 2014, spec. pp. 185. In questo senso viene in parte confermato l'assunto deducibile da una lettura combinata delle tre leggi ideate dallo scrittore Isaac Asimov, per cui l'uomo risponderebbe dei danni cagionati ai suoi simili solo nel caso in cui siano riconducibili ad un proprio ordine. I. Asimov, *Visioni di robot*, Milano, 2010, p. 37. Di là delle suggestioni letterarie, si tratterebbe pertanto di una forma di allocazione del rischio mitigabile caso

 ISSN 2037-5662

Le «cose» connesse all'IoT opererebbero pertanto come appendice della sfera giuridica del privato-utente che ne fruisce o, anche in parallelo, quale strumento utilizzato dal produttore o gestore al fine di garantire un servizio migliore e tecnologicamente più avanzato[37].

4. Differentemente dalle ipotesi poc'anzi esaminate – in cui il robot agisce e modifica la natura in base ad un ordine e/o alla percezione «soggettiva» che trae dalla realtà – ciò che svolge un ruolo preponderante nell'azione (e dunque anche nell'eventuale errore) dell'oggetto o della macchina intelligente, come più generalmente nella dinamica di funzionamento dell'IoT (con le sue influenze sul comportamento umano), è il potenziale orientativo-predittivo posseduto dall'informazione (intesa come dato veicolato nella rete), verso cui convergono tutti i comparti sino ad adesso presi in esame (*data-driven architecture*)[38].

per caso attraverso l'assolvimento di appositi oneri probatori (si pensi a quanto richiesto alternativamente nel nostro ordinamento dagli artt. 2049, 2050, 2051 o 2053 cod. civ.) o, indirettamente con l'inserimento per via contrattuale di clausole di esonero dalla responsabilità e/o il ricorso al sistema assicurativo facoltativo o obbligatorio. Sul punto cfr. M. Wolf, *Schuldnerhaftung bei Automatenversagen*, in *JuS*, 1989, pp. 899 e ss.; M. Nagenborg - R. Capurro - J. Weber - C. Pingel, *Ethical Regulations on Robotics in Europe*, in 22 *AI & Society*, 349 (2008); P. Asaro, *Robots and Responsibility from a Legal Perspective*, in *IEEE ICRA'07 Workshop on Roboethics*, Roma, 14 aprile 2007; S. Wu, *Unmanned Vehicles and US Product Liability Law*, in 21 *J. L. Info. & Sci.* 234 (2012); A. Bertolini, *Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules*, in 5(2) *Law Innovation and Technology*, 2013, pp. 214-247; F.P. Hubbard, *'Sophisticated Robots': Balancing Liability, Regulation, and Innovation*, in 66 *Fla. L. Rev.* 1803 (2014); A. Bertolini – P. Salvini – T. Pagliai – A. Morachioli – G. Acerbi – L. Trieste – F. Cavallo – G. Turchetti – P. Dario, *On Robots and Insurance*, in *Int. J. of Soc. Robotics*, (pubbl. on line il 3 marzo 2016). Ciò ovviamente con esclusivo riguardo ai casi di responsabilità extracontrattuale: U. Pagallo, *Robotica*, in M. Durante – U. Pagallo, *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, spec. p. 146 e ss., nell'analizzare il problema promuove, nell'ambito di ipotesi di contrattazione automatica perfezionata da robot (o tra robot) un'equiparazione tra robot e schiavi dell'antica Roma richiamando l'istituto del *peculium*, in cui lo schiavo o il figlio non emancipato, seppur non dotato di libertà ed autonomia patrimoniale poteva ricevere dal *pater familias* somme di denaro o proprietà, di cui era direttamente responsabile. Sulla specifica questione v. anche V. Dhar, *Should You Trust Your Money to a Robot?*, in 3 *Big Data* 55 (2015).

[37] Per una rassegna civilistica sulla nozione di «cosa» cfr. S. Pugliatti, *Beni e cose in senso giuridico*, Milano, 1962, pp. 12 e ss.; V. Zeno-Zencovich, voce *Cosa*, in *Dig. disc. priv*., sez. civ., Torino, 1988, III, pp. 438 e ss., ma ancora, in prospettiva filosofica e tecnologicamente avanzata R. Esposito, *Le persone e le cose*, Torino, 2014, *passim*.

[38] In argomento, per un primo approfondimento sul potenziale innovativo dei *Big Data* e sulle conseguenze della nuova disciplina comunitaria sulla privacy v. V. Mayer-Schönberger – Y. Pa-

 ISSN 2037-5662

È dunque il *valore* attribuito all'informazione, esplicitamente o implicitamente, prima della creazione, durante o dopo il suo utilizzo, a incidere sulla funzionalità dell'intero sistema, influenzando e conformando le regole giuridiche ad esso sottese e i molteplici obiettivi di tutela che coinvolgono questa innovativa rappresentazione dinamica del mondo filtrata dalla rete Internet[39].

L'informazione riferita all'uomo o all'ambiente che lo circonda entra nel circuito comunicativo in maniera volontaria (ad es. registrazione e sottoscrizione di un contratto di utilizzo di un social network; ricerca on line e non attivazione nel browser di dispositivi anti tracciamento) o tacita (sensori ambientali, gps, apparecchi di videosorveglianza, rilevatori di targa e velocità degli autoveicoli): in questa prima fase, trasposta in formato binario, essa diviene «dato» avente preciso contenuto, cui è riconosciuto dall'ordinamento un determinato valore giuridico e, quindi, specifica tutela.

Ad esempio le condizioni generali di contratto dei maggiori social network attribuiscono all'utente registrato un diritto di proprietà sulle informazioni aventi caratteri di proteggibilità sotto il profilo autoriale: nel caso di immagini e contenuti in astratto coperti da diritti di proprietà intellettuale, la prestazione del consenso attraverso l'iscrizione riconosce automaticamente al prestatore una licenza d'uso gratuita e trasferibile a terzi, che viene meno formalmente solo all'atto della cancellazione dell'utente dalla piattaforma. L'atto della pubblicazione di un contenuto sulla propria bacheca dà altresì vita ad una manifestazione di consenso espressa che autorizza qualsiasi terzo, iscritto e non alla piattaforma, di accedere ed utilizzare il suddetto contenuto. Allo stesso modo, la prestazione dei dati personali dell'utente è rimessa all'accettazione delle privacy policies (con i relativi strumenti di *private enforcement*), integrate dalla normativa vigente in tema di protezione dei dati personali.

DOVA, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, in 17 *Colum. Sci. & Tech. L. Rev.* 315 (2016).

[39] V. ad es. E.W. KITCH, *The Law and Economics of rights in valuable information*, in 9 *J. Legal Stud*. 683 (1980); J. LITMAN, *Information Privacy/Information Property*, in 52 *Stan. L. Rev*. 1283 (2000); S. RODOTÀ,*Tecnologie e diritti*, Bologna, 1995, pp. 52 e ss.; K.J. ARROW, *Il benessere economico e l'allocazione delle risorse per l'attività inventiva*, cit., pp. 117 - 139, spec. p. 124 s.; R. PARDOLESI – C. MOTTI, *«L'idea è mia!»: lusinghe e misfatti dell'*economics of information, in *Dir. inf*., 1990, pp. 345 e ss.; ID., *L'informazione come bene*, in G. DE NOVA (a cura di), *Dalle* res *alla* new properties, Milano, 1991, p. 37 e ss.; V. ZENO-ZENCOVICH – G.B. SCANDICCHI, *L'economia della conoscenza e i suoi riflessi giuridici*, in *Dir. inf*., 2002, 6, p. 971 ss.

 ISSN 2037-5662

Nel nuovo contesto dei *Big Data*, la medesima informazione può però venire utilizzata una o più volte per un preciso scopo, ma poi essere stoccata e divenire oggetto di duplicazioni (si pensi ancora alla licenza d'uso di un contenuto IP) modifiche, divisioni, accorpamenti, o ancora può rimanere inalterata e pronta per un nuovo utilizzo, ove esso non sia stato oggetto di autonoma rimozione, aggiornamento, istanza di cancellazione[40].

É possibile dunque affermare che grazie all'avvento del principio di correlazione e all'implementazione delle capacità tecnologica di raccolta e stoccaggio di dati, sia possibile attuare un uso sincronico ed infinito di qualunque tipo di informazione per una varietà di scopi non meglio precisati: ciò dipenderà dall'intrinseco valore d'uso attribuito ad esso dal sistema e dalla modalità di combinazione attuata.

Seguendo questo tentativo di ricomposizione del sistema, è opportuno ricercare quali possano essere gli «statuti» dell'informazione che discendono dall'interazione tra natura, cose, rete e duomo[41], cogliendo i rapporti sussistenti tra *qualità* e *quantità* dei dati e analizzando le due macro-tendenze normative riscontrabili nei maggiori centri nevralgici della Internet *policy* occidentale (UE-USA).

In ambito europeo, il nuovo Regolamento generale sulla protezione dei dati personali (d'ora in poi, il Regolamento), traccia alcune specifiche linee d'intervento proprio con riguardo alle attività di raccolta ed elaborazione dei dati che comporterà l'IoT.

Sotto un profilo qualitativo, si estende la nozione di dato personale a tutte le informazioni relative ad una persona fisica, anche nelle ipotesi di un trattamento multiplo che conduca a una combinazione tra dati provenienti anche da dispositivi o terminali di accesso in Rete di per sé non identificativi[42].

[40] Cfr. Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, WP 223, 16 settembre 2014, p. 7.

[41] Si interroga con profondità e chiarezza sul problema dell'afasia immanente alla ricerca di una dommatica del bene giuridico «informazione» E. Resta, *Il tempo e lo spazio del giurista*, in G. Comandè – G. Ponzanelli, *Scienza e diritto nel prisma del diritto comparato*, Torino, 2003, pp. 253 e ss., spec. 255 s.

[42] L'art. 4, n. 1), afferma che deve intendersi come dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

 ISSN 2037-5662

L'art. 4, n. 1) del Regolamento in tal senso esclude dall'obiettivo di protezione i soli dati anonimi e quelli trattati in maniera tale da garantire un accettabile livello di pseudonimizzazione. In questo comparto si installa poi il divieto di trattamento automatizzato di dati personali per scopi analitico-predittivi del comportamento o di altre caratteristiche di una persona fisica (c.d. profilazione), eccetto nei casi in cui esso sia stato esplicitamente ammesso dagli Stati membri (previa l'introduzione di specifiche garanzie), consentito dall'interessato o ancora necessario per la conclusione di un contratto tra quest'ultimo e il titolare (art. 22)[43].

Gli obblighi relativi al trattamento corrispondono allo schema tracciato dalla direttiva del 1995, rafforzando i principi sull'acquisizione, l'integrità e la revoca del consenso[44], la liceità, la correttezza del trattamento e la trasparenza[45].

Quanto al trattamento ammesso (poiché lecito) anche in assenza di consenso, il Regolamento immunizza tutte le informazioni trattate per il perseguimento di rilevanti scopi di interesse pubblico o interessi vitali dell'interessato o di altra persona fisica (art. 1, n. 1, lett. *d*), quali il monitoraggio dell'evoluzione e la diffusione o la prevenzione di catastrofi naturali o derivanti dall'azione dell'uomo, prevedendo altresì delle limitazioni ai diritti ri-

[43] Considerando n. 71: «L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona (…). Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. (…)».

[44] Il considerando n. 32 e l'art. 7 del Regolamento affermano come il consenso debba essere libero ed inequivocabile ed applicarsi a tutte le attività di trattamento svolta per una o più finalità, non avendo dall'altra rilevanza il silenzio, l'inattività, la preselezione di caselle .

[45] Nel senso di informazione dell'interessato in maniera chiara e trasparente sulle attività svolte con i dati raccolti e sull'esercizio dei poteri e le libertà positive riconosciute dall'ordinamento (considerando n. 39, artt. 12-15).

 ISSN 2037-5662

conosciuti all'interessato[46]. Il principio di «stretta necessità» del trattamento rispetto agli scopi previamente dichiarati ed oggetto di consenso da parte dell'interessato (art. 6, n. 1, lett. c), dir. 95/46/CE), viene poi «diluito» attraverso la previsione di limiti e obblighi in relazione ai trattamenti svolti per finalità diverse da quelle per cui sono stati raccolti. Tali tipologie di trattamento sono essere oggetto di un obbligo di valutazione preventiva da parte del titolare, il quale dovrà vagliarne i rischi e le conseguenze in rapporto alle finalità del trattamento primario, al contesto in cui è avvenuta la raccolta, alla natura dei dati e all'esistenza di misure di temperamento quali la pseudonimizzazione o la cifratura (art. 6, n. 4)[47].

La conservazione dei dati da parte del titolare, effettuata secondo criteri di sicurezza e riservatezza, deve essere sempre limitata al tempo necessario a perseguire le finalità del trattamento: il titolare è quindi tenuto a prevedere un tempo massimo di conservazione o, ancora, può disporre periodicamente la verifica della correttezza e l'eventuale rettifica delle informazioni detenute.

Come si è avuto modo di rilevare in altra sede[48], l'obbligo di valutazione d'impatto e la consultazione preventiva di cui all'art. 35, si applica ai trattamenti che comportano la sorveglianza sistematica su larga scala e il trattamento globale, automatizzato e sistematico di informazioni riguardanti aspetti personali volto ad incidere sulla capacità decisionale di detti soggetti, producendo effetti significativi sul piano giuridico o personale.

L'informazione riferita o riferibile ad una persona fisica è pertanto immessa in uno schema di elaborazione e condivisione progettato in modo tale da fornire all'interessato un controllo a distanza, nel senso di una costante informazione sui trattamenti effettuati e del libero esercizio dei diritti ad esso riconosciuti (accesso, revoca del consenso, opposizione, portabilità, ret-

[46] Cfr. i considerando nn. 52, 73, nonché n. 46, per cui «Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana».

[47] V. anche il considerando n. 50.

[48] Per informazioni di maggior dettaglio sull'argomento si veda *supra*, Risk-based approach *e trattamento dei dati personali*.

 ISSN 2037-5662

tifica, cancellazione, limitazione). L'agevole passaggio delle informazioni da un titolare all'altro e la ricorrenza di ulteriori attività di trattamento correlate alla prima, paiono però limitare la portata di tale principio solo ad un primo stadio vitale dei dati raccolti.

La possibilità che l'informazione, a seguito della sua agglomerazione e rielaborazione, possa essere utilizzata ai fini predittivi e in generale per incidere sull'apparato decisionale della popolazione è difatti contemplata ed ammessa dalla normativa in commento, seppur sottoposta ad un complesso procedimento di vaglio preliminare e costante monitoraggio da parte del prestatore e dell'autorità di controllo.

La tendenza pare pertanto quella di una progressiva frammentazione della nozione giuridica di dato personale che segue due direzioni.

Una è collegata alla logica protettiva del rapporto tra interessato e valore identificativo dell'informazione: le nuove norme seguono il flusso del dato personale nei limiti del consenso dell'interessato, del trattamento per scopi di rilevante interesse pubblico o, ancora, ove esso astrattamente possa condurre all'identificazione di una persona fisica.

L'approccio *by design* e soprattutto gli obblighi di prevenzione del rischio previsti in relazione al trattamento, sembrano poi indicare una chiara volontà legislativa di modellare le strategie imprenditoriali dei prestatori di servizi (e dei produttori di oggetti e macchine) verso il consolidamento di meccanismi di minimizzazione del trattamento, filtraggio e destrutturazione in forma anonima o pseudonima dei dati[49], favorendo così attività successive di compressione e stoccaggio che rimangono estranee alla portata applicativa del Regolamento, a meno che non sia possibile dimostrare che una loro combinazione possa condurre all'identificazione di una persona fisica[50].

Come è noto, dall'altra parte dell'oceano l'informazione colta nel suo flusso circolatorio viene protetta con un approccio in maggior misura orientato al c.d. *consumer welfare*. Le leggi federali non contemplano una protezione globale della privacy, occupandosi di disciplinare direttamente o in-

[49] La spinta normativa verso l'attuazione di un'organizzazione protesa verso la valutazione del rischio dei trattamenti e l'adozione di misure preventive è chiara. Il considerando n. 28, ad esempio, afferma che «l'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati» puntualizzando poi come l'introduzione esplicita della «pseudonimizzazione» nel regolamento non sia intesa a precludere altre misure di protezione dei dati.

[50] V. ad. es. l'art. 32 sulla sicurezza del trattamento e, ancora l'art. 25, nn. 1 e 2 del regolamento.

 ISSN 2037-5662

direttamente la tutela di precise attività o figure soggettive[51]. Nell'assenza di un organico approccio, la tutela trova maggiore estensione grazie all'apporto del formante giurisprudenziale[52], agli sforzi legislativi di carattere integrativo o sostitutivo profusi dalla maggioranza degli stati federali e, infine, alla cruciale attività di vigilanza svolta dalla *Federal Trade Commission*[53].

Ad esempio, nel corso degli ultimi cinque anni, la Commissione Federale per il commercio ha emanato numerosi ordini nei confronti dei principali prestatori di servizi della società dell'informazione[54]. I provvedimenti rafforzano i concetti di trasparenza, consenso e sicurezza delle informazioni trattate con riguardo a tutte le tipologie di dati personali raccolte dai prestatori (c.d. *covered information*). In questo senso, le misure comminate dalla FTC attraverso un approccio *case-by-case* hanno concorso a richiamare l'attenzione in maniera vincolante sulla corretta ottemperanza ad alcuni principi-chiave della tutela di stampo comunitario: a conferma di ciò, gli ultimi tre ordini vietano espressamente ogni forma di violazione e *misrepresentation*

[51] Volendo effettuare una breve ricognizione, seguendo un ordine cronologico e senza pretesa di esaustività è possibile rintracciare: il *Fair Credit Reporting Act* (1970), volto alla tutela dei dati riferiti ai rapporti di credito; il *Privacy Act* (1974), che mutua i principi-cardine tracciati nel documento programmatico denominato *Code of Fair Information Practices* (il quale peraltro ispirerà la Raccomandazione dell'OCSE del 1980), ma con esclusivo riferimento ai rapporti tra cittadino ed uffici governativi; il *Family Educational Rights and Privacy Act* (1974); il *Financial Privacy Act* (1978); il *Cable Communications Policy Act* (1984); il *Video Privacy Protection Act* (1988); *Driver's Privacy Protection Act* (1994); il *Portability and Accountability Act* (1996); il *Children's Online Privacy Protection Act* (1998); il *Gramm-Leach-Bliley Act* (1999); il *Telephone Records and Privacy Protection Act* (2006) ed il *Genetic Information Nondiscrimination Act* (2008).

[52] V. ad es. ai recenti casi *United States v. Jones*, 132 S. Ct. 945 (2012) e *Riley v. California*, 134 S. Ct. 2473 (2014).

[53] Sul punto v. A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974; R.A. Posner, *Privacy, Secrecy, and Reputation*, in 28 *Buffalo Law Rev.* 1 (1979); C. Bennet, *Regulating Privacy*, New York, 1992; B. Markesinis – G. Alpa, *Il diritto alla «privacy» nell'esperienza di «common law» e nell'esperienza italiana*, in *Riv. trim. dir. proc. civ*., 1997, pp. 417-454; V. Zeno-Zencovich, *Una lettura comparatistica della legge n. 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. proc. civ.*, 1998, p. 733 ss.; F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict And Cooperation*, in 78 *Law & Contemp. Probs*. 231 (2015).

[54] *FTC v. Twitter Inc*., 2 marzo 2011, docket no. C-4316; *FTC v. Google Inc*., 13 ottobre 2011, docket no. C-4336; *FTC v. Facebook Inc*., 27 luglio 2012, docket no. C-4365; *FTC v. My Space LLC*., 30 agosto 2012, docket no. C-4369. Per una più approfondita analisi dei provvedimenti si rimanda a S. Sica – V. D'Antonio, *I* Safe Harbour Privacy principles: *genesi, contenuto, criticità*, in *Dir. inf*., 4/5, 2015, spec. pp. 819 e ss.; A. Hasty, *Treating Consumer Data Like Oil: How Re-framing Digital Interactions Might Bolster the Federal Trade Commission's New Privacy Framework*, in 67 *Fed. Comm. L.J*. 293 (2015).

 ISSN 2037-5662

concernente accordi o programmi governativi volti a proteggere la privacy dei consumatori.

Con particolare riguardo all'IoT e ai *Big Data*, la *Federal Trade Commission* ha di recente emanato due raccomandazioni[55], in cui in sostanza vengono riprese le strategie comunitarie, indicando la necessità di valorizzare i principi di informazione e scelta consapevole del consumatore-utente, incentivare la progettazione e produzione di *device* che garantiscono elevati standard di sicurezza e, infine, di attuare pratiche di minimizzazione del trattamento dei dati personali. In quest'ultimo comparto, i documenti della Commissione assegnano all'impresa la libertà di scegliere la pratica di prevenzione del rischio maggiormente confacente al proprio modello di business, optando ad esempio per l'assoluta astensione dalla raccolta di dati, per l'applicazione di limiti temporali o qualitativi al trattamento e conservazione, sino all'attuazione di pratiche di de-identificazione dei dati[56].

5. Nella sostanziale omogeneità delle tendenze regolatorie, appare possibile apprestare un primo tentativo di rilettura degli elementi sin ora raccolti.

Inquadrando dall'alto lo scenario di comunicazione e interazione collaborativa aperto dall'avvento dell'Internet delle Cose, pare affermarsi una nuova espressione del principio di solidarietà in ambito digitale, data non solo dal generale obbligo di favorire il passaggio delle informazioni da un punto all'altro della rete (neutralità), ma anche dalla necessità per ogni soggetto/oggetto implicato nel flusso informazionale di fornire attivamente il proprio apporto implementando ed arricchendone la portata descrittiva, al fine di apprestare una computazione (e ricostruzione) della realtà quanto più precisa ed efficiente possibile[57].

[55] FTC Staff Report, *Internet of Things. Privacy and Security in a Connected World*, Gennaio 2015; Id., *Big Data: a toolf for exclusion or inclusion?*, Gennaio 2016.

[56] FTC Staff Report, *Internet of Things. Privacy and Security in a Connected World*, cit., p. 12 e ss. Sul punto, nella dottrina più recente v. S.R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, in 93 *Tex. L. Rev*. 85 (2014); J. Brill, *The Internet Of Things: Building Trust And Maximizing Benefits Through Consumer Control*, in 83 *Fordham L. Rev*. 205 (2014); T. M. Lenard – P. H. Rubin, *Big Data, Privacy and the Familiar Solutions*, in 11 *J.L. Econ. & Pol'y* 1(2015).

[57] Si accosterebbe così, ad un'accezione inclusiva della solidarietà digitale, riconducibile al diritto di accedere e comunicare in rete, anche una diversa declinazione dell'attitudine cooperativa. In questi termini, accanto alla «libertà informatica» sintetizzata da alcuna dottrina si potrebbe accostare un diverso concetto di «solidarietà informatica», per cui il transito di informazioni lecite

 ISSN 2037-5662

Questa ripartizione laterale dei compiti comporta l'attribuzione sincronica di diverse tipologie di responsabilità ad ogni soggetto che fornisce il proprio contributo al funzionamento dell'IoT: non sarebbe in tal senso possibile imputare univocamente il danno ad uno solo tra i soggetti coinvolti nel flusso poichè esso andrebbe valutato seguendo il grado di influenza (o il tipo di combinazione) impresso all'informazione da un livello all'altro della struttura e rispetto al risultato (o scopo) apprestato e perseguito dal sistema[58].

Si pensi all'accostamento di informazioni afferenti da più *device* e effettuata da molteplici prestatori di servizi attraverso algoritmi differenziati: potrebbe discutersi di forme di responsabilità solidale e/o oggettiva regolate preventivamente per via legislativa o lasciate ad una maggiore discrezionalità interpretativa da parte del formante giurisprudenziale, senza dimenticare la possibilità di un massiccio ricorso a forme di assicurazione obbligatoria.

Ciò che però più rileva in questo contesto è che il predetto scenario condurrebbe ad un ridimensionamento delle funzioni tradizionalmente ricondotte alla responsabilità civile, con un ritorno, paventato recentemente da alcuna autorevole dottrina, ad una valorizzazione del profilo privatistico dell'istituto, quindi inteso non più in maggior parte come strumento di conformazione del comportamento di una società, ma come tecnica di compensazione dei danni che discendono dal suo «ordine spontaneo» e, ancor prima, di sanzione e mitigazione (o ancora eliminazione) della pericolosità intrinseca alla natura umana[59].

da un punto all'altro della rete comporta l'arricchimento del valore complessivo del sistema e, dunque della propria funzionalità e degli effetti benefici che può apportare alla vita di una società. Cfr. V. Frosini, *1984. L'Informatica nella società contemporanea*, in *Inf. e dir*., 1984, p. 7 e ss.; Id., *L'orizzonte giuridico dell'Internet*, in *Dir. inf*., p. 271 ss.; S. Rodotà, *Solidarietà*, Roma-Bari, 2014, spec. p. 115 s.

[58] Come pare peraltro venire indicato, con solo riguardo all'attività di trattamento dei dati personali, nell'o*pinion* resa dall'Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, cit., p. 11.

[59] Per una recente ricostruzione della questione v. P.G. Monateri, *La materia del 'politico' e il 'problema' della responsabilità civile*, in G. Alpa – V. Roppo, *La vocazione civile del giurista*, Bari-Roma, 2013, pp. 243-252. Sulle «funzioni» della r.c. si veda, in una lettura sconfinata, S. Rodotà, *Modelli e funzioni della responsabilità civile*, in *Riv. crit. dir. priv*., 1984, pp. 596 e ss.; R. Keeton, *Creative Continuity in the Law of Torts*, in 75 *Harv. L. Rev*. 473 (1962); F.C. Zacharias, *The Politics of Torts*, in 95 *Yale L.J*. 698 (1986); P.G. Monateri, *La responsabilità civile*, cit., pp. 19-28; G. Alpa, *La responsabilità civile*, cit., p. 131 ss.; C. Salvi, *La responsabilità civile*, cit., p. 38; S. Sica, *Note in tema di sistema e funzioni della regola aquiliana*, in *Danno e resp*., 2002, 8-9, pp. 911 e ss.

 ISSN 2037-5662

Ribaltando la prospettiva, in una società *data-driven*, la pericolosità umana è fortemente influenzata dall'infrastruttura che ne orienta il comportamento e dal progressivo processo di spersonalizzazione delle informazioni che ne determinano a loro volta il funzionamento.

Il dato, raccolto ed elaborato in maniera tale da non poter incidere o produrre rischi sul regime di protezione garantito alla persona cui è riferito[60], tenderebbe a venire accumulato e agglomerato dai prestatori sottoforma di *res nullius*, risorsa neutra liberamente appropriabile ed utilizzabile[61]. L'informazione riferita ad una persona fisica mantiene un valore in termini di riservatezza e potere di controllo dell'interessato (si pensi al diritto alla portabilità, recentemente introdotto dal Regolamento[62]), ma al momento dell'immissione nel circuito comunicativo tende sempre di più a riprodursi mutando forma e ricoprendo un ruolo di bene economico a carattere marcatamente proprietario[63].

Il ruolo dei prestatori di servizi e dei produttori di oggetti e macchine intelligenti – in astratto riconducibili tutti entro la nozione di «titolare o responsabile del trattamento» e in buona parte sottoposti anche alla direttiva sul commercio elettronico – intesi come accumulatori ed agglomeratori di dati (personali, anonimi o pseudonimizzati) paventa il rischio della configurazione di posizioni dominanti con ricadute sulla crescita e la gestione

[60] Si veda ad es. quanto affermato in precedenza dall'Article 29 Data Protection Working Party, *Parere 05/2014 sulle tecniche di anonimizzazione*, WP216, 10 aprile 2014, p. 11, per cui «nei casi in cui un insieme di dati sottoposto a una tecnica di anonimizzazione (anonimizzato e reso pubblico dal responsabile del trattamento originario) sia oggetto di trattamento da parte di terzi, questi ultimi possono procedere in modo legittimo senza necessariamente tener conto dei requisiti in materia di protezione dei dati, a condizione che non possano (direttamente o indirettamente) identificare le persone interessate nell'insieme di dati originario».

[61] Venendo così equiparati alle informazioni e ai rilievi dei fenomeni naturali, non riferibili ad una persona in particolare e sottoposti ad un regime di «non protezione» come quello riconosciuto dal regolamento comunitario per gli elementi atti a stabilire risultati predittivi utili alla prevenzione di gravi rischi per la popolazione. Inoltre, lo «statuto» riservato a tale tipologia di informazioni dimostra un grado ancor maggiore di volatilità e neutralità rispetto al contenuto protetto ad esempio da diritti d'autore o proprietà intellettuale, che pur nella loro infinita ed agevole duplicabilità trovano nell'integrità dell'espressione creativa originaria e nel collegamento «paternalistico» tra autore e opera dell'ingegno (seppur nelle differenti declinazioni apprestate nelle tradizioni di *civil* e *common law*) i principali elementi di valore e tutela.

[62] Si vedano l'art. 20 e il considerando n. 68.

[63] Sul problema v. seppur collocandosi in una prima fase di sviluppo dei *Big Data*, M. Scott Boone, *Ubiquitous Computing, Virtual Worlds, and the Displacement of Property Rights*, in 4 *ISJLP* 91 (2008) e già S. Rodotà, *Tecnopolitica*, 2ª ed., Roma-Bari, 2004, spec. pp. 155 e ss.

 ISSN 2037-5662

complessiva dell'*Internet of things*. Infatti, come dimostrano le vicende relative al passaggio dalla prima alla seconda «rivoluzione» di Internet (dalla diffusione su scala globale come rete «civile» al c.d. web 2.0), la crescita del potenziale innovativo della rete è direttamente proporzionale al mantenimento della libera circolazione dell'informazione (ove essa sia lecita).

L'avvento di un nuovo movimento di *enclosure* che si concentri sulla accumulazione del «dato» come declinazione futuristica di un nuovo «capitale»[64], accostata alle barriere in entrata già attive con riguardo alle architetture software ed hardware di combinazione e custodia delle informazioni (si pensi alle questioni di tutela proprietaria degli algoritmi[65] e quelle attinenti lo «sbloccaggio» dei dispositivi mobili per ragioni di sicurezza nazionale[66]), è foriera in astratto di cagionare effetti *lato sensu* anticompetitivi[67] e di incidere sulla distribuzione diffusa e paritaria dei criteri di gestione della rete, quindi sull'esercizio dei poteri pubblicistici riconosciuti agli Stati sovrani[68].

[64] Sulla nozione di «capitale» in politica dell'economia si rimanda, in una sconfinata e discordante messe di opinioni, ad es. a J. Eaton, *Economia Politica*, Torino, 1971, passim. Il tema è stato esplorato con riguardo all'attuale assetto economico, sociale e tecnologico da A. Gorz, *L'immateriale. Conoscenza, valore e capitale*, ed. it., Torino, 2003, spec. pp. 24 e ss.

[65] Cfr. R. Pardolesi, *«Gooooglaw». Del ricorso alla disciplina antitrust per colpire il tiranno benevolente*, in *Foro it*., 2013, V, 18 e M. Lao, *«Neutral» Search As A Basis for Antitrust Action?*, in *Harv. J. of L. & Tech.Occasional Paper Series — July 2013*.

[66] Con riguardo alla vicenda che ha coinvolto il Federal Bureau of Investigation americano e la celebre azienda di Cupertino v. *In re Matter of the Search Warrant of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, n. ED 15-0451M, (U.S. D.C., Centr. D. Ca., Feb. 16, 2016).

[67] Un primo tentativo di riflessione sul tema è rintracciabile in G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Dir. inf*., 4/5, 2015, pp. 909 e ss., ma si vedano anche A. Mantelero, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, ivi, 2012, pp. 135 e ss.; Commissione europea, *Strategia per il mercato unico digitale in Europa*, 6 maggio 2015, COM(2015) 192 final; European Data Protection Supervisor, *Privacy and competitiveness in the age of big data, Bruxelles*, 5/2014; European Parliament - Directorate General For Internal Policies Policy Department A: Economic And Scientific Policy, *Challenges for competition policy in a Digitalised Economy*, IP/A/ECON/2014-12, Bruxelles, 7/2015, spec. pp. 25 e ss.; P. Jones Harbour, *The Transatlantic Perspective: Data Protection and Competition Law*, in H. Hijmans – H. Kranenborg (a cura di), *Data Protection anno 2014: How to Restore Trust?: Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Bruxelles, 2014, p. 25 e ss.; A.P. Grunes, *Another Look at Privacy*, in 20 *Geo. Mason L. Rev.* 1107 (2013); N. Newman, *Search, Antitrust, and the Economics of the Control of User Data*, in 31 *Yale J. on Reg.* 401 (2014).

[68] Sul punto si v. recentemente e da diverse prospettive, V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems; La sorveglianza digitale e il governo internazione delle reti di telecomu-*

 ISSN 2037-5662

Il valore predittivo dei dati e la portata che tale funzione sortirà sul comportamento di tutta la popolazione, infatti, coinvolge sincronicamente l'insieme dei diritti e dei valori fondamentali dell'uomo, con la necessità di approntare forme di tutela multilivello avverso il controllo, l'uniformazione e l'omologazione acausalistica dei comportamenti.

L'esaltazione di logiche egualitarie[69] o di strategie protettive basate sulla preventiva valutazione del rischio (si pensi al dato frammentato o anonimizzato), possono al contempo condurre alla sistematica lesione della dignità umana e del principio di non discriminazione[70], espressioni più elevate delle diversità di una società, poste a garanzia della libertà di pensiero, di scelta e d'azione in maniera difforme e non massificata[71]. In questo quadro, un

nicazione, in *Dir. inf*., 4/5, 2015, pp. 683-696; F. Musiani, *Governance by algorithms*, in 2 *Internet Policy Review* (2013); N. Kim – J. Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, in 80 *Mo. L. Rev*. 723 (2015).

[69] Nel senso di estensione indiscriminata dell'accesso a uomini e macchine, con la conseguente, concreta, impossibilità per i primi di poter decidere di effettuare un completo «opt-out» dal sistema di captazione automatica della realtà esteriore approntato dall'Internet delle Cose. V. M. Bailey, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things*, in 94 *Tex. L. Rev*. 1023 (2016).

[70] In questo senso contemplando un'accezione del principio di non discriminazione concentrato sulla tutela delle diversità di scelta e comportamento e non considerando in questa sede le altre argomentazioni prodotte da alcuna dottrina sugli effetti stigmatizzanti e discriminatori in danno di gruppi sociali vulnerabili potenzialmente sortiti dall'utilizzo diffuso di algoritmi e modelli predittivi associati alla raccolta di dati sensibili: v. D. Hirsch, *That's Unfair! Or is it? Big Data, Discrimination and the FTC's Unfairness Authority*, in 103 *Ky. L.J*. 345 (2015). In argomento, lo stesso considerando n. 71 del regolamento generale sulla protezione dei dati afferma che «(…) al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni».

[71] Si pensi a quanto in maniera attuale ed incisiva afferma l'art. 2, primo comma del d.lgs. 196/2003, prescrivendo che il trattamento dei dati personali si debba svolgere «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». In generale sul

 ISSN 2037-5662

importante appiglio normativo pare risiedere – seppur nelle differenti formulazioni proposte in Europa e Stati Uniti – nel neonato principio di 'non irragionevole interferenza o svantaggio ad utenti e prestatori', da declinare oltre l'ambito strettamente consumeristico come generale garanzia di tutela della persona umana nell'ambito della diffusione e dello sviluppo di *Big Data* ed Internet delle Cose.

rapporto tra principio di dignità e sistema dei diritti fondamentali nelle moderne società di mercato v. S. Rodotà, *Il diritto di avere diritti*, cit., p. 179 e ss.; G. Resta, *Dignità, persone, mercati*, Torino, 2014, spec. pp. 3 e ss.

 ISSN 2037-5662