"Annali online della Didattica e della Formazione Docente"
Vol. 9, n. 13/2017, pp. 7-25 – ISSN 2038-1034

# *Il minore come persona digitale. Regole, tutele e privacy dei minori sul Web*

**Enrico Maestri**

**Abstract** – *The purpose of this work is to discuss and investigate the following theses: 1. the code, that is to say the software and the hardware cyberspace is made of, imposes a normative set-up both on Web collective and individual conduct. By that, law's regulative task on Web can't be denied; for instance, think about sanctions imposed by laws about copyright, contracts, slander and obscenity. Yet Internet represents a universe made of flows and frictions, unwilling to whatever top-down governance alien to its users. Code is performative: "what it says, it does"; 2. cyberspace is an ambivalent place, where many activities are laid on top of real world's ones and many others are peculiar to it, showing its own plasticity. Technological innovation's growth rate is still increasing, together with new insidious forms of invasion of people's private life. It is still strong the temptation to waive one's own rights only to enjoy the technological paradise we are offered. A new entity – digital person – makes its appearance on digital ecosystem, as technological outcome of classical person concept's reconfiguration; 3. the development of 2.0 applications allows to put into connection people and their digital identities: individuals get involved in a digital swarm, forming links free from any territorial and simultaneous physical presence's chains. Our privacy (in particular, that of the minors, born in the digital era) is progressively eaten away by our rising indulgency, apathy, unconcern and explicit support to measures, shown us as necessary and harmless. If it is yet untimely to say that privacy is almost death, new generations, whether they like it or not, are playing a leading role in a cultural praxis and in a primary socialization which is far from the concept of privacy; 4. the fourth thesis, summing up this note, investigates if it is yet possible or not to give space to new effective forms of governance, appointed to defend the digital person: its rights to dignity, habeas data and personal data privacy.*

**Riassunto** – *Nel corso di questo lavoro ho inteso approfondire e discutere le seguenti tesi: 1. il code, ossia il software e l'hardware che costituiscono il cyberspazio, impone un assetto normativo sul comportamento individuale e collettivo nel Web. Con ciò non si nega la funzione regolativa del diritto sul cyberspazio; si pensi ad esempio alle sanzioni previste dalle leggi sul copyright, sul diritto contrattuale, sulla diffamazione e sull'oscenità. Pur tuttavia, Internet rappresenta un universo di flussi e di attriti restio all'imposizione top-down di qualsivoglia governance estranea ai propri utenti. Il code è performativo: "ciò che dice fa"; 2. il cyberspazio è un luogo ambivalente, ove molte attività si sovrappongono alle attività del mondo reale e molte attività gli sono peculiari, denotando la plasticità che gli è propria. Il tasso di crescita dell'innovazione tecnologica continua ad aumentare ed è accompagnato da nuove insidiose forme di invasione della sfera privata delle persone. È forte la tentazione di rinunciare ai propri diritti per godere del paradiso tecnologico che ci viene offerto. Nell'ecosistema digitale compare una nuova entità – la persona digitale – quale esito tecnologico della riconfigurazione della nozione classica di persona; 3. lo sviluppo delle applicazioni 2.0 permette la connessione tra persone e loro corrispondenti identità digitali: soggetti che formano legami senza vincoli di spazio e di compresenza fisica diventano parte di uno sciame digitale. La nostra privacy (e in particolar modo quella dei minori, nativi digitali) è progressivamente erosa dalla nostra crescente accondiscendenza, apatia, indifferenza o supporto esplicito a misure che ci sono presentate come indispensabili o innocue. Se è ancora prematuro affermare che la privacy è ormai morta, le giovani generazioni sono protagoniste, volenti o no, di una prassi culturale e di una socializzazione primaria lontane dal concetto di privacy; 4. la quarta tesi, con cui concludo questo contributo, approfondisce la questione se si possono*

*ancora ricavare spazi per forme di governance efficaci a tutelare la persona digitale: il suo diritto alla dignità, all'habeas data e alla riservatezza dei dati personali in Internet.*

**Keywords** – Lex informatica, internet governance, digital person, offensive internet, privacy

**Parole chiave** – Lex informatica, governance di internet, persona digitale, offensività online, riservatezza

**Enrico Maestri** è Professore associato di *Filosofia del diritto* presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Ferrara, dove attualmente insegna *Teoria generale del diritto* e *Metodologia e logica giuridica*. È autore di numerosi saggi su temi di biodiritto, di bioetica, di diritto delle nuove tecnologie e di giustizia ecologica. Tra le sue più recenti pubblicazioni: *Lex Informatica. Diritto, persona e potere nell'età del cyberspazio* (Napoli, Edizioni Scientifiche Italiane, 2015); *Giustizia ecologica. Un confronto tra la teoria di Rawls e la teoria di Nussbaum* (in "Diritto e questioni pubbliche", 2016); *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio* (in "Ars interpretandi", 2017).

"Anche le brave persone diventano pirati in un mondo in cui le regole appaiono assurde".

(L. Lessig, *Making Art and Commerce Thrive in the Hybrid Economy*, New York, Penguin Press, 2008; tr. it. *Il futuro del copyright (e delle nuove generazioni)*, Milano, Etas, 2009)

## 1. Modalità di regolazione di internet tra cyberlibertarianism e cyberpaternalism

Nonostante risulti difficile individuare un corretto inquadramento della natura giuridica del cyberspazio, secondo i sostenitori dell'approccio giuspositivistico il diritto continua a disciplinare compiutamente le attività digitali di ogni cybernauta. Internet rinvia all'immagine di uno spazio virtuale, in cui la difficoltà risiede tanto nel definire le relazioni tra spazio reale e virtuale quanto nello stabilire come predisporre un diritto della Rete; esso, infatti, non può essere ancorato a uno spazio territoriale. Conseguentemente, occorre individuare linee di confine non più fisiche, ma inevitabilmente logiche. Ciononostante, è pur vero che dagli inizi degli anni Novanta ogni azione compiuta in Rete ha una disciplina di riferimento, spesso corredata da sanzioni anche gravi.

Non solo in Italia, ma anche nel resto del mondo l'evoluzione del diritto sulle nuove tecnologie ha via via normato tutti gli aspetti della vita digitale e dei comportamenti online, arrivando a toccare qualsiasi ambito.

Dunque, secondo i giuristi di diritto positivo, ogni attività che si svolge in Rete è disciplinata da una norma cui occorre prestare attenzione, perché "la Rete è un luogo profondamente concreto e capace di accogliere nel suo seno, nel bene e nel male, le più umane esigenze"[1].

[1] P. Costanzo, voce *Internet*, in *Digesto delle Discipline Pubblicistiche*, Torino, Utet, 2000, p. 349.

Internet è, perciò, sia un insieme di norme sia una struttura dalla logica interna fondata su regole tecniche. Dal punto di vista giuridico, Internet non è un soggetto; la realizzazione dei vari rapporti telematici in Rete richiama l'immagine di un *luogo* dove si instaurano relazioni commerciali, personali o in cui vengono commessi atti illeciti.

In che misura *effettivamente* il diritto regoli il comportamento nel cyberspazio è una questione a sé. Il diritto, comunque sia, "continues to threaten an expected return. Legislatures enact, prosecutors threaten, courts convict"[2].

Il cyberspazio è di per sé uno spazio del mondo reale, non solo perché da quest'ultimo può essere regolato, ma soprattutto perché gli utenti del cyberspazio vivono nella realtà: "Cyberspace is not, and never could be, the kingdom of mind; minds are attached to bodies, and bodies exist in the space of the world. And Cyberspace as such as does not preexist its users"[3]. L'unicità del paradigma del *cyberspace as place* risiede nella particolare interazione che esso realizza tra potere normativo e progettazione tecnica (elemento qualificante di questo spazio, che va continuamente esaminata). È solo traducendo queste specificità in leggi e in politiche mirate che potrà avviarsi un progetto di regolazione del cyberspazio, ancorato a un approccio di carattere pragmatico[4].

In contrapposizione a questa prospettiva (il diritto "doma" il *code*[5]*),* la corrente *cyberlibertaria* ha rivendicato la natura libertaria della Rete, qualificandola come un unico spazio virtuale che potesse e dovesse restare scevro da qualsiasi tipo di regolazione (*a-regulation or self-regulation*), specie se statale. John Perry Barlow, nella sua ormai mitica *A Cyberspace Independence Declaration* (9 febbraio 1996), declama: "Governi del Mondo, stanchi giganti di carne ed 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".

Le condotte sfuggono al controllo del governo in ragione dell'anonimità e della multigiurisdizionalità che connotano il cyberspazio: è la stessa natura dello spazio digitale a rendere *irregolamentabile* il comportamento.

In tal senso sono rivelatrici le riflessioni di Johnson e Post, secondo i quali: "Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of on line behaviour on individuals and things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-

[2] L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, in "Harvard Law Review", 501, 1999, p. 508.

[3] J. E. Cohen, *Cyberspace as/and places*, in "Columbia Law Review", 107, 2007, p. 218.

[4] T. Wu, *Cyberspace sovereignty? – Internet and the International System*, in "Harvard Journal Law & Technology", 3, 1997, p. 256.

[5] Per *code* (o *Lex informatica*) s'intende l'insieme dei protocolli informatici, del software, dell'hardware, degli algoritmi e del codice binario con cui i programmatori informatici strutturano ed architettano la Rete, stabilendo i vari modi d'uso delle tecnologie informatiche.

making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules"[6].

Il cyberspazio non sarebbe dunque uno spazio senza regole, bensì uno spazio distinto e diverso in cui le ormai delegittimate autorità pubbliche dei luoghi reali sono sostituite dagli utenti della Rete, che dettano per se stessi regole atte a realizzare i loro desideri e bisogni. Entrare nel cyberspazio, del resto, è un atto di volontà ben preciso che determina l'accettazione delle regole di Internet: "No one accidentally strays across the border into cyberspace. To be sure, Cyberspace is not a homogenous place. Crossing into Cyberspace is a meaningful act that would make application of a distinct law of Cyberspace' fair to those who pass over the electronic boundary"[7].

Ad avviso dei sostenitori del *cyberlibertarianism*, la *governance* del cyberspazio si costruisce dal basso (*bottom-up*): a dettare le regole sono gli stessi utenti, legittimati proprio dall'utilizzo della Rete. La legge, infatti, intesa come "thoughtful group conversation about core values"[8] persisterà, ma non potrà – e d'altro canto, nemmeno potrebbe – essere quella stessa applicabile a territori fisici e geograficamente definiti.

Presumere che l'architettura della Rete sarebbe fissata *by default* e il governo sarebbe incapace di adottare misure efficaci in grado di modificarla, rende in parte errata la credenza relativa all'architettura ontologica e normativa del cyberspazio.

Inoltre, a fronte di un approccio particolarmente attento alla struttura della Rete, essa non considera seriamente l'evidente ricaduta di tutte le attività che si svolgono *online* nel mondo reale.

Quando si visita il *cyberspace,* non si viaggia verso un luogo: anche nello spazio virtuale un comportamento antisociale è vietato e il soggetto che lo compie, ancorché *online*, resta soggetto alla diretta regolazione dello Stato di residenza[9].

Pur tuttavia, bisogna ammettere che il *self-regulation approach* del cyberspazio coglie una questione reale: la fonte primaria dello spazio in Rete rimane pur sempre un processo decentralizzato di adozione *volontaria* di standard tecnici da parte di operatori di rete (*Internet Service Providers*), piattaforme Web (*Website Platforms*) e comunità degli utenti (*Virtual Communities*). L'esistenza di differenti sotto-comunità di utenti determina l'eterogeneità delle regole applicabili, tra loro antinomiche. Tali antinomie normative sono superabili mediante l'accesso ad altre e diverse aree della Rete da parte di coloro che non dovessero condividere un determinato corpo di regole vigente in un determinato Stato.

In accordo con l'approccio teorico-giuridico di Lawrence Lessig, io ritengo che l'architettura del cyberspazio non sia fissata *by default*, bensì in funzione del *design* (*rectius:* del suo *code*). Il *code* è mutevole: potrebbero essere il governo o il mondo delle multinazionali a determinarne una particolare evoluzione. L'architettura del cyberspazio è neutrale. Laddove le architetture del *code* incidono sui vincoli giuridici, finiscono per soppiantare anche i valori del diritto. Nel

[6] D. R. Johnson, D. Post, *Law and Borders. The Rise of Law in Cyberspace*, in "Standford Law Review", 48, 1996, p. 1370.

[7] *Ivi*, p. 1379.

[8] *Ivi*, p. 1402.

[9] A. Murray, *Information Technology Law. The law and society*, Oxford, Oxford University Press, 2013, p. 56.

caso della proprietà intellettuale, ad esempio, il *code* appare *sovrainclusivo* rispetto alla legge: quest'ultima favorisce un'implementazione architettonica del *code* tale da favorire i detentori di cospicue percentuali di proprietà intellettuale, così esentando le multinazionali delle telecomunicazioni dalle responsabilità di servizio universale e condivisione delle reti. Nel campo del *copyright* l'architettura digitale, cioè il modo con cui le tecnologie disegnano *ex ante* lo spazio di comportamento degli utenti, ha progressivamente ristretto i margini di libertà (*fair use*) delle scelte individuali.

La società post-Internet determina un'intensificazione della normativa sul *copyright* digitale, posta a sostegno delle grandi imprese produttrici di contenuti digitali: la legge, infatti, inizia a disciplinare minuziosamente i comportamenti dell'utente-cittadino-consumatore (c.d. *netizen*). Il diritto interagisce col *code* (*co-regulation*), vietando sia l'aggiramento delle protezioni tecnologiche sia la produzione di tecnologie finalizzate all'elusione delle protezioni medesime[10]. L'architettura, rappresentata dal sistema numerico binario, è diventata un vincolo fortissimo per l'individuo, massimamente invasiva delle sue capacità di azione: la proprietà digitale diviene proprietà mimetica dell'architettura (ogni utilizzo di un'opera creativa si trasforma automaticamente in una copia) e pone ora controlli e regole, influendo su legge e mercato[11]. Ad avviso di Lessig, d'ora in poi i controlli sull'accesso ai contenuti non saranno ratificati dai tribunali, ma verranno inseriti dai programmatori tramite il *code*. Diversamente dai controlli introdotti per legge, quelli inseriti dalla tecnologia non formano oggetto di verifica giudiziale[12]. D'altronde, mentre la regola legislativa risulta verificabile e contestabile, altrettanto non può dirsi per la regola tecnologica[13].

Al fine di bilanciare i limiti e le possibilità del comportamento nel cyberspazio, la sfida normativa consiste dunque nel realizzare una continua interazione tra regolazione statuale o sovranazionale e l'architettura del *code*.

In questo senso e contrariamente a quanto esaminato in materia di *copyright* dei beni intangibili, la natura preventiva del *code* potrebbe seguire un percorso inverso, cioè quello dell'incorporazione nelle regole informatiche di valori giuridici condivisi.

In questo modo, il *code* è *sottoinclusivo* rispetto alla legge: essa può incidere sull'uso generale di quelle tecnologie digitali (ad esempio, i *Censor Software* o i *Kids-Mode Browsing*) deputate alla realizzazione di un set di valori condivisi (tutela dei soggetti più vulnerabili, libertà di espressione, parità di accesso alle forme di informazione e comunicazione tecnologica,

[10] R. Caso, *L'"immoralità" delle regole tecnologiche: un commento alle teorie degli studiosi Burk e Gillespie*, in G. Ziccardi (a cura di), *Nuove tecnologie e diritti di libertà nelle teorie nordamericane*, Modena, Mucchi Editore, 2007, p. 38.

[11] Ad esempio, il sistema delineato dal *Digital Rights Management* (DRM) impone di fatto clausole contrattuali e condizioni d'uso restrittive dell'utilizzo del bene digitale. Attraverso un controllo pervasivo ed invasivo della privacy del consumatore, è il titolare del contenuto, prima e più del legislatore, ad impostare i termini dell'equilibrio tra interesse economico proprietario e fruizione del contenuto.

[12] L. Lessig, *Cultura libera: un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale*, Milano, Apogeo, 2007, pp. 124 ss.

[13] R. Caso, *L'"immoralità" delle regole tecnologiche: un commento alle teorie degli studiosi Burk e Gillespie*, cit., p. 43.

promozione del controllo democratico nella progettazione tecnologica, garanzia di riservatezza dei dati personali).

Lessig propone due esempi in cui il *code* appare la soluzione a problemi di informazione, rispettando un approccio *value-centered design*.

Il primo problema impone di chiedersi se la delimitazione di zone (*zoning*) dell'espressione digitale, avente contenuti adatti ai soli adulti, sia in grado di tenere i minori lontani dalla pornografia.

Il secondo problema, invece, induce a domandarsi se nel cyberspazio sia davvero possibile decidere se partecipare o acconsentire alla nostra sorveglianza e rinunciare, di conseguenza, alla nostra privacy.

La risposta a questi due problemi – nel primo caso, delimitare una zona per la pornografia e, nel secondo caso, scegliere di tutelare una privacy protetta – dipende dall'architettura intrinseca del cyberspazio. La risposta è lasciata alla discrezionalità dei regolatori: dare regole per il cambiamento dell'assetto tecnico del *code* o lasciare il cyberspazio com'è e accettare che finalità condivise siano lasciate al loro destino, quali la salvaguardia della privacy dei minori a non essere esposti a contenuti indecenti o offensivi?

Siamo di fronte a quello che filosoficamente viene indicato come un vero e proprio "dilemma giuridico": da un lato, si promuove sempre più la progettazione di infrastrutture informatiche che vincolino a comportamenti corretti e conformi alle norme giuridiche (si pensi, ad esempio, ai principi della *privacy by design*); dall'altro lato, il radicamento e la costante applicazione del *code* stabilito dal software e dall'hardware potrebbe diventare una prassi e contribuire a generare nelle persone la convinzione che i comportamenti tenuti in Internet siano corretti *by default*[14].

## 2. La persona tra identità digitale e biografia digitale

Dave Eggers ambienta uno dei suoi ultimi romanzi, *Il Cerchio* (Milano, Mondadori, 2014), nel campus di una grande azienda (il *Cerchio*). La giovane protagonista, Mae Holland, è e rimane sola, senza alcun orizzonte di azione collettiva e di solidarietà di classe. Lo scopo dell'azienda (che non produce beni materiali) è mettere in connessione il maggior numero di persone possibile, ma, al contempo, renderle trasparenti, indurle a rinunciare ad ogni forma di privacy. In un futuro distopico ciascuno si muoverà con addosso una serie di apparecchi che lo renderanno visibile e *partecipato* da decine di milioni di altri individui. Pur di far parte della comunità degli eletti del *Cerchio*, Mae Holland non esita a rinunciare alla propria privacy per un regime di trasparenza assoluta, che richiede di condividere sul Web qualsiasi esperienza personale e di trasmettere in *live streaming* la propria vita. Dentro il *Cerchio* ogni cosa è perfetta: le persone migliori hanno creato i sistemi migliori e i sistemi migliori hanno creato il po-

[14] R. Brighi, *Dati informatici e modelli dei dati. Verso "una nuova dimensione della realtà"*, in S. Zullo, R. Brighi (a cura di), *Filosofia del diritto e nuove tecnologie*, Roma, Aracne, 2015, p. 290.

sto più bello del mondo. Tuttavia, per poter usufruire delle comodità offerte dal *Cerchio*, le persone devono rinunciare totalmente alla loro privacy[15].

L'individuo diventa una miniera da cui estrarre le preziose informazioni che porta con sé; cedendo i propri dati volontariamente, egli si rende protagonista attivo della cancellazione della propria privacy.

Se i dati personali si trasformano in merce, è chiaro che, al momento del loro ingresso nella Rete, i diritti riconosciuti nel mondo reale diventano più fragili e più sfumati. Essi sono sottoposti alla pressione di soggetti privati sovranazionali che, per aggirare determinati vincoli giuridici, scelgono la giurisdizione più vantaggiosa al fine di mettere in atto un vero e proprio *Forum Shopping by Plaintiffs* dello spazio regolativo. L'habitat ideale per chiunque voglia esercitare una sorveglianza globale sui *corpi digitali*[16] è creato dal connubio fra questa capacità giuridica, la capacità digitale di raccolta dati che lo sviluppo impetuoso delle tecnologie informatiche offre, la capillare diffusione di Internet e, infine, la creazione di *Big Data*[17]. Essi sono analizzati e gestiti con il processo del *Data Mining,* ossia con un insieme di tecniche (raccolta di dati, applicazione di algoritmi, esame e interpretazione dei risultati, applicazione del profilo) che, sulla base dei dati raccolti, genera nuove informazioni al fine di prevedere dei risultati prima del loro verificarsi[18].

Sebbene la persona abbia dato il consenso alla registrazione dei dati (si pensi, ad esempio, alle informazioni RIFD conservate nelle *Oyster Cards* usate per il trasporto pubblico a Londra), non sempre immagina che da questi dati possono essere elaborati profili utilizzabili a scopo di marketing. L'opacità stessa del processo di profilazione allontana ogni possibilità di assoggettare a controllo l'uso dei dati raccolti.

Grazie alle categorizzazioni su cui la profilazione si basa, la vita della società contemporanea ruota attorno ad un unico perno: l'informazione. Al contempo, però, queste tecniche si pongono in continua tensione con il diritto alla privacy, con il diritto alla protezione dei dati personali e con il diritto alla non discriminazione.

[15] Come spesso accade, la realtà ha ormai superato la fantasia. Dai primi mesi del 2016 Facebook ha lanciato la piattaforma *Facebook Live*, un nuovo servizio per trasmettere video in streaming in diretta e alcune altre novità che rendono più facile per tutti creare, trasmettere o solo guardare video su Facebook. Con *Facebook Live* è possibile fare con lo smartphone una diretta streaming di quello che si ha di fronte: quando si aprirà la casella per pubblicare uno status, comparirà l'icona "Live Video", oltre a quelle "Aggiungi foto/video" e "Crea album fotografico" e si potrà aggiungere una breve descrizione sulla diretta che si sta per fare e selezionare quali fra gli amici potranno vederla; durante la diretta si potrà vedere il numero di amici che la stanno seguendo, i loro nomi e i loro commenti allo streaming. Ebbene, da recenti notizie di cronaca, la funzione *live* di Facebook ha permesso di trasmettere in diretta l'omicidio di un passante di 74 anni e l'impiccagione in diretta perpetrata dal padre, poi suicidatosi, sulla figlia undicenne. In entrambi i casi, prima che l'algoritmo di Facebook rimediasse rimuovendo i video, questi ultimi ormai erano già stati condivisi da centinaia di migliaia di visualizzazioni, postate su YouTube e su altre piattaforme web di *video sharing*.

[16] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, Feltrinelli, 2002, pp. 138-141.

[17] Sull'impatto dei *Big Data* nella società contemporanea, cfr. V. Mayer-Shönberger, N. K. Cukier*, Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013.

[18] T. Z. Zarsky, *Governmental Data Mining and its Alternatives*, in "Penn State Law Review", 11, 2011, pp. 285-330.

Nella vita quotidiana vengono offerte ai cittadini soluzioni sempre più rapide e semplici per effettuare acquisti attraverso pagamenti elettronici, per utilizzare servizi di *socialità digitale* tramite l'iscrizione a siti di social network, per effettuare in modo veloce ricerche di contenuti con un motore di ricerca. I servizi disponibili sugli smartphone o qualsiasi altro *wearable device* sono innumerevoli: ad esempio, i *fitness tracker* sono i dispositivi che hanno raggiunto la maggiore diffusione ed il miglior successo nel mercato.

Il dato personale non s'identifica più con il dato anagrafico: esso va inteso come qualsiasi *informazione biografica* che si riferisce ad un soggetto; rientrano in questa categoria tutte le informazioni che descrivono un elemento biologico, economico, sociale e finanziario della persona. Ogni transazione di dati che si svolge su Internet viene immagazzinata nei *Big Data* per poi essere analizzata dal *provider* del servizio oppure da un'azienda terza, che ne acquisisce i dati sul mercato. I dati personali memorizzati rimarranno per sempre nei *Big Data*, sfuggendo definitivamente al controllo del legittimo proprietario, ossia del soggetto cui si riferiscono.

Per meglio focalizzarci sul problema in questione, immaginiamo un banale esperimento mentale: cosa accadrebbe se un soggetto, pubblico o privato, fosse in grado di accedere ai database gestiti dalle 30 *corporations* che controllano il 90% del traffico mondiale della Rete e che contengono i dati digitali personali sensibili e sensibilissimi di un individuo?

Si riuscirebbe a ricostruire in modo pressoché perfetto, minuzioso e dettagliato[19] tanto il profilo della vita digitale quanto il profilo della vita reale di questa persona[20], dando persino conto dei suoi dati biologici e genetici.

Il processo di *profilazione* rende trasparente la vita di qualsiasi individuo, esponendolo alle discipline *minutissime* ed ipertecniche del potere[21]. Nasce dunque la necessità di tutelare i diritti di una nuova entità – la *persona digitale* – che si muove nel cyberspazio, dove i limiti temporali e spaziali sono stati abbattuti[22] e dove domina chi dispone delle più adeguate conoscenze e dei migliori mezzi tecnologici.

La *persona digitale* transita continuamente tra due mondi interconnessi da piattaforme, veri e propri veicoli di trasmissione, memorizzazione e manipolazione di tutte le informazioni; questo *nonluogo*[23] digitale e globale è il *World Wide Web*, una tecnologia che, a partire dal 1991, ha profondamente modificato la visione del mondo dell'uomo contemporaneo, trasformandone usi e costumi quotidiani.

In questo ambiente, in cui le barriere sono abbattute e le regole sembrano non esistere, l'utente si sente partecipe di un grande gioco virtuale dove tutto gli è permesso: egli non deve preoccuparsi delle conseguenze sociali e giuridiche delle sue *azioni digitali*.

I siti di socializzazione (*social networking sites*), tra i quali il più diffuso è Facebook, incentivano ed esaltano quest'atteggiamento. Sul social network il soggetto si sente quasi in dovere

[19] Si pensi ad esempio ai dati biometrici sensibilissimi come le impronte digitali utilizzate quali password per l'accesso al dispositivo dall'ultima generazione di smarthphone.

[20] M. Hildebrandt, S. Gutwirth (Eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, New York, Springer, 2008, pp. 47-63.

[21] M. Foucault, *Sorvegliare e punire. La nascita della prigione*, Torino, Einaudi, 2014, pp. 214-247.

[22] D. Lyon, *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, cit., pp. 22-25.

[23] M. Augè, *Nonluoghi. Introduzione a un'antropologia della surmodernità,* Milano, Elèuthera, 2009.

di condividere informazioni personali, foto e video che lo ritraggono; esse, una volta rese pubbliche in Rete, rimangono nella piena disponibilità di Facebook, che le conserva e può legittimamente utilizzarle, poiché sono state raccolte con il consenso informato ed esplicito dei suoi utenti.

La rete Internet si è manifestata una tecnologia in grado di modificare la configurazione dei rapporti sociali ad ogni livello (dai rapporti tra individui ai rapporti tra potere pubblico e cittadino), assumendo dimensioni globali.

Per avere una visione pragmatica di Internet, oltre che più aderente alla realtà sociale, occorre individuare le possibili tutele della *persona digitale*, intesa come figura diversa e nuova, la cui fenomenologia dei rapporti umani subisce un mutamento per effetto del nuovo ambiente in cui viene ad esprimersi.

Una persona reale e un'intelligenza artificiale (un *informational organism* o *inforg*[24]) non si possono porre sullo stesso piano, sebbene entrambe agiscano in un ambiente digitale. Da un punto di vista tecnico il confronto regge perfettamente, perché – si sostiene – non conta se l'informazione è data da un'entità vivente o da un'entità artificiale. Tuttavia, si corre il rischio di perdere di vista i caratteri propri del genere umano, come il valore della dignità e il senso morale dell'appartenenza alla propria specie.

La *persona digitale* è costituita da tutte le informazioni inserite dall'individuo nella Rete: ogni azione immagazzinata in *files* (tracce digitali lasciate dalla sua navigazione e documenti prodotti dall'interazione con l'ambiente Web in cui si trova) rappresenta la personalità di qualsiasi individuo espressa nel *nonluogo* Internet, costituendone l'identità digitale[25].

La panoplia di innovazioni digitali e l'uso massivo delle tecnologie *smart* trasforma la persona (intesa classicamente quale identità soggettiva e integrità psico-fisica) in *persona digitale*, cioè in un *cluster* di dati[26] in cui la corporeità, anziché scomparire, viene trasfigurata *socialmente* e disciplinata *tecnologicamente*.

Tanto nel mondo reale come nel mondo digitale la persona si riconosce attraverso i suoi ricordi, le sue esperienze e i suoi interessi, ossia attraverso i frammenti di memoria che contribuiscono a creare l'immagine del Sé e la propria biografia[27], costituita da tutti i file (foto, video, documenti), le informazioni e le azioni prodotte dalla persona durante la sua permanenza nella Rete: essi concorrono, cioè, a ricostruire l'immagine di sé che l'individuo, mediante lo strumento del Web, intende proiettare all'esterno. La biografia rappresenta il legame tra le due persone, quella fisica e quella digitale, secondo due modalità diverse: per la *persona fisica* è la capacità di auto-riconoscersi e di avere consapevolezza del proprio piano di vita; per la *persona digitale*, invece, è costituita da una sequenza di frammenti della propria immagine. Quale proiezione *disincarnata* di un corpo fisico, la *persona digitale* acquista i diritti e recepisce i valori dei quali la persona fisica è titolare e portatrice nel mondo reale.

[24] L. Floridi, *La rivoluzione dell'informazione,* Torino, Codice, 2012.
[25] C. Sullivan, *Digital Identity*, Adelaide, University of Adelaide Press, 2011, pp. 5-10.
[26] M. Castells, *La nascita della società in rete*, Milano, UBE, 2002, p. 22.
[27] S. Rodotà, *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012, pp. 273-276.

L'importanza della tutela dei dati personali su Internet (e la loro trasformazione in informazioni) si spiega in ragione del ruolo determinante che essi assumono nel definire la personalità dell'individuo sul Web.

Tuttavia, si deve tenere presente che l'identità, sia nel mondo reale sia nel mondo digitale, non è un dato statico ma dinamico e mutevole nel tempo. La *persona digitale* è intimamente legata alle informazioni di cui è composta: ogni addizione o sottrazione di informazione può incidere sensibilmente sulla sua struttura ontologica digitale e, di conseguenza, sull'immagine proiettata all'esterno.

L'immagine della *persona digitale* nella sua *integrità* è nota solo al suo proprietario, cioè a colui che l'ha plasmata con la propria volontà[28]; la conoscenza che i terzi ne hanno è circoscritta, invece, agli unici dati con i quali vengono in contatto, ossia la *scia* dei frammenti digitali lasciati nel Web.

In questo senso la *persona digitale* è un'entità polimorfica, che varia in base al contesto ed alla natura dei dati.

Dunque, l'*identità digitale* è un concetto diverso da quello di *persona digitale*: la prima denota un processo di validazione dell'utente connesso al Web, che accede ai servizi informatici (piattaforme social, pagamenti elettronici, ecc.) dove le rappresentazioni di sé sono tante quanti sono i differenti profili che si possono creare; la seconda, invece, indica la rappresentazione dell'immagine virtuale che si può ottenere dai dati, successivamente trasformati in informazioni, che il soggetto immette nella Rete e che garantiscono una *virtualizzazione infinita* delle proprie pratiche sociali.

La difficoltà nel controllo e nella gestione delle informazioni personali, una volta pubblicate sul Web, rappresenta la maggior criticità della *persona digitale* e della sua vita su Internet, soprattutto in ragione del numero di connessioni che ogni individuo collegato alla Rete intrattiene, nonché della loro potenziale vastità.

Ciò comporta una vera e propria mutazione genetica del trattamento dei dati e della loro concezione: passando da componente fondamentale per la costruzione della *personalità digitale* dell'individuo a valore immateriale di scambio, essi entrano a fare parte di quell'immensa rete di calcolo che è Internet.

## 3. I minori nella Rete tra obscenity e privacy

Ad avviso di Levmore e Nussbaum, Internet viene banalmente descritto come un luogo virtuale dove l'uomo è in grado di esercitare la libertà al massimo grado. Le sofisticate tecnologie con basse barriere all'accesso dei contenuti digitali incantano sia i libertari sia i comunitaristi, poiché consentono la divulgazione istantanea di informazioni a milioni di utenti. I regolatori, al fine di garantire sempre più la libertà di parola, promulgano leggi come il *Communications Decency Act*, che limita *de facto* la responsabilità giuridica dei *service providers* di Internet nell'attività di divulgazione delle informazioni immesse in Rete, qualsiasi contenuto esse ab-

[28] *Ivi*, p. 318.

biano. Tuttavia, un Internet non regolamentato è un terreno fertile per la diffusione e l'agevolazione di comportamenti illeciti: gli abusi perpetrati attraverso la comunicazione di contenuti indecenti ed offensivi sono frutto di scelte sociali, tecnologiche e giuridiche[29].

Nell'ambito giuridico statunitense, laddove sia in gioco la tutela dei minori, qualunque tipo di discorso, ritenuto accettabile in normali circostanze, potrebbe essere vietato. La Corte Suprema ha infatti evidenziato il forte interesse pubblico nella tutela del benessere fisico e psicologico dei minori. Qualunque restrizione in materia, però, dev'essere compiuta "by narrowly drawn regulations without unnecessarily interfering with First Amendment freedoms"[30]; ciò significa che si devono sempre tenere presenti le libertà garantite dal Primo Emendamento, evitando di interferire con esse quando non sia strettamente necessario. È lecito, pertanto, vietare la vendita ai minori di materiale potenzialmente dannoso, benché inoffensivo laddove destinato ad un adulto. Allo stesso modo, durante le ore del giorno in cui è possibile che i bambini siano parte dell'audience, è lecito proibire la diffusione via radio o televisione di contenuti trasmessi con linguaggio indecente. Tuttavia, la capacità del Governo di vietare contenuti per la protezione dei minori non è illimitata; dimostrazione ne è il caso *Reno v. American Civil Liberties Union*[31]. In quell'occasione la Corte Suprema aveva dichiarato incostituzionali due articoli del *Communications Decency Act* (CDA), provvedimento del 1996 del Congresso sulla regolamentazione di materiale pornografico in Internet, che proibiva la comunicazione di materiale indecente con i minori tramite Internet. La Corte aveva messo in luce che gli articoli in questione penalizzavano esageratamente gli adulti, affermando che l'interesse del Governo nella tutela del minore non avrebbe dovuto giustificare la soppressione della libertà di espressione degli adulti. Pertanto, in sostituzione del *Communications Decency Act,* nel 1998 il Congresso aveva promulgato il *Child Online Protection Act* (COPA). Esso tiene maggiormente in considerazione la differenza tra materiale dannoso per i minori e materiale oggettivamente indecente, vietando espressamente la comunicazione ai minori di materiale del primo tipo e consentendo agli adulti la libera visione del materiale del secondo tipo.

In ambedue le regolazioni il Congresso statunitense ha fallito due volte: nel primo caso, un'eccessiva regolamentazione ha finito per sfociare nella censura della Corte Suprema per infrazione del Primo Emendamento sulla libertà di espressione; nel secondo caso, nel tentativo di porvi rimedio, ha gravato gli adulti di una responsabilità eccessiva.

Ciò dimostra che nel cyberspazio tutte le forme tradizionali di "limitazione preventiva" risultano inapplicabili: per la sua stessa struttura di progettazione, nonché per le sue dimensioni e la sua mutevolezza, è praticamente impossibile pensare ad Internet come ad uno strumento in qualche modo censurabile.

Sul piano del diritto, infatti, l'incertezza circa l'applicabilità analogica a Internet delle discipline giuridiche relative ai media tradizionali rappresenta il problema di partenza; quindi, posto

[29] S. Levmore, M. C. Nussbaum (Eds.), *The Offensive Internet. Speech, Privacy, and Reputation,* Harvard, Harvard University Press, 2011.

[30] Cfr. Corte Suprema degli Stati Uniti, citata in K.A. Ruane, *Freedom of Speech and Press: Exceptions to the First Amendment*. Congressional Research Service, p. 22, in https://www.fas.org/sgp/crs/misc/95-815.pdf, consultato in data 10/04/2017.

[31] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

che ciò che è illegale offline lo è anche online, spesso la reale applicazione delle norme si scontra con la difficoltà di sussumere le fattispecie concrete di Internet all'interno di quelle astratte previste dalla normativa tradizionale.

La delocalizzazione (che pone problemi d'identificabilità dei soggetti oltre che di giurisdizione[32]), le grandi possibilità d'anonimato concesse agli utenti, le modalità peculiari di pubblicazione dei materiali: sono tutte particolarità di Internet che rendono estremamente difficile l'applicazione della normativa riferita ai mass-media tradizionali.

A rivelarsi inefficaci sono stati anche i recenti tentativi di estendere online la responsabilità giuridica da fatto illecito civile e penale agli *Internet Service Provider*, vera e propria spina dorsale della Rete. Al riguardo, la pressione che i *content and access providers* hanno esercitato sugli organi regolatori ha mostrato la loro volontà di prediligere un indirizzo di autogestione e di autoregolamentazione, a totale detrimento di un'efficiente forma statale e sovranazionale di controllo giuridico[33].

Gli Stati, nel tentativo di riaffermare la propria sovranità digitale, cercano disperatamente di monitorare, filtrare o proteggere i flussi digitali; tuttavia, i dati di Internet sono replicabili all'infinito ed esistono contemporaneamente in molteplici luoghi. Essi possono essere illegalmente reindirizzati o inoltrati a determinati destinatari, mentre i riceventi hanno la possibilità di eluderli, come pure di accedervi[34].

È forse il *code* che potrebbe intervenire a vicariare la parziale insufficienza dell'*enforcement* giuridico nel cyberspazio?

Relativamente ai contenuti offensivi e pornografici, la risposta dei tribunali è "vedere ed aspettare". Nella convinzione che il sistema di Internet non esisterebbe prima delle azioni e dei comportamenti degli uomini ("*cyberspace is not extraterritorial*"[35]), tribunali e legislatori ri-

[32] Su questo punto, cfr. ad esempio la sentenza Cassazione Sez. V Penale, 4741/2000, 17 Novembre 2000.

[33] Oggi la norma di riferimento è la Direttiva dell'8 giugno del 2000 ("*Direttiva sul commercio elettronico"*, 2000/31/CE; recepita dal D. Lgs. n. 70 del 2003), che ha sancito l'assenza di un obbligo generale di sorveglianza per gli ISP (art. 15, 2000/31/CE). Più nel dettaglio possiamo dire che i Provider, in linea di massima, non sono responsabili quando svolgono servizi di c.d. *mere conduit* (art. 12)*, caching* (art. 13) *e hosting* (art. 14).

[34] Occorre sottolineare che sia la direttiva 2004/48/ce in materia di *copyright enforcements* sia le Convenzioni e le linee-guide linea in materia di *cybercrime*, le quali hanno implementato gli strumenti in materia di *data protection* e di *data retention*, intimano agli *Internet Service Provider* di comunicare l'IP dei soggetti coinvolti per procedere alla loro identificazione. Ciò sia prima sia dopo la direttiva 2006/24/ce sulla conservazione dei dati, dichiarata invalida nel 2014 dalla Corte di Giustizia dell'Unione Europea per violazione dei diritti fondamentali della vita privata e della protezione dei dati personali. Eppure, quest'insieme di norme giuridiche deve confrontarsi con difficoltà di natura tecnica, le quali rischiano di indirizzare le indagini della Polizia giudiziaria e le relative misure verso soggetti sbagliati. Ogni secondo, infatti, si collegano ad Internet milioni di persone e gli *Internet Service Provider* conservano tutte le informazioni di accesso di attività svolta dagli utenti: l'autorità che effettua una richiesta errando sull'orario anche di un solo secondo potrebbe perseguire l'utente sbagliato, magari collegatosi un secondo prima ed, eventualmente, condannarlo come autore dell'illecito telematico. Oltre al noto utilizzo dei *proxy servers*, esistono strumenti tecnici che rendono anonima la navigazione, come gli *anonymous remailers*, server che ricevono messaggi di posta elettronica e li inviano nuovamente senza rivelare la loro provenienza originaria.

[35] A. Etzioni, *The Limits of Privacy*, New York, Basic Books, 1999, pp. 96-99.

tengono che si debba attendere per osservare lo sviluppo del network in molti contesti differenti quali la pornografia, la privacy e la tassazione.

Si tratta di un errore fatale: organi giurisdizionali e legislativi dimostrano di non aver compreso che il sistema tecnico ha invaso la totalità del vissuto e l'intera pratica sociale; difatti, la relazione con il sistema tecnico è immediata (o de-medializzata). Ormai i *pattern* culturali sono divenuti semplici riflessi dell'ambiente tecnico: è ciò che McLuhan intese esprimere con la celebre formula: "The medium is the message"[36].

L'erroneità di una tale impostazione si appalesa anche con riguardo ad una seconda questione, più peculiare dell'ecosistema digitale, consistente nella già poc'anzi esposta osservazione: "code is law". Ciò significa che le architetture di Internet già contengono codici e linguaggi normativi di auto-organizzazione in grado di stabilire e influenzare l'uso delle informazioni disponibili in Rete.

Anziché scandalizzarsi e criminalizzare i comportamenti tenuti dai minori navigando in Rete[37], occorre programmare le tecnologie affinché siano funzionali ad un controllo portato all'interno dell'infrastruttura[38].

Laddove i regolatori pubblici decidessero di progettare *policy* di controllo solo *ex post*, lasciando ai privati produttori dei codici informatici il controllo delle possibilità connesse a Internet, a venire compromesse sarebbero la privacy, la libera circolazione delle idee e altri importanti valori sociali, quali la dignità, la reputazione e il rispetto delle persone; a questo punto, non potremmo dolerci del fatto che i giovani sono diventati protagonisti e vittime di una *shitstorm* in cui l'interazione è fortemente connotata in senso negativo e, talvolta, violento. Grazie a impostazioni predefinite relative alla privacy, l'architettura informatica dei blog, Snapchat, Twitter, Instagram e Facebook determina una de-medializzazione della comunicazione: ciascuno produce e diffonde informazioni, sicché soggetto e oggetto si confondono e ognuno sfrutta se stesso. Incoraggiati dal medium digitale, i giovani diventano loro malgrado i protagonisti di una dilagante cultura dell'indiscrezione e della mancanza di rispetto[39]. Ogni click viene registrato e usato per generare feedback performativi (nella stessa misura degli "I like"); essi, infatti, incentivano ulteriori azioni che annullano il confine tra privacy e sorveglianza, tra auto-illuminazione e reputazione. Sul Web i giovani si esprimono in modo anonimo, pur avendo un profilo che cercano senza posa di ottimizzare: anziché essere "nessuno", si espongono insistentemente e ambiscono ad essere "qualcuno". Non vogliono essere anonimi, ma lo spazio digitale li trasforma in "qualcuno anonimo". Manca loro la spiritualità del riunirsi; d'altronde, il Web non glielo permette: sono individui isolati, *hikikomori* e auto-segreganti che vivono davanti al display[40]. Paradossalmente, ancora una volta, il Web li costringe ad una forma di auto-illuminazione che riduce la distanza tra il pubblico e il privato. Quest'assenza di distanza,

[36] J. Ellul, *Il sistema tecnico. La gabbia delle società contemporanee*, Milano, Jaca Book, 2004, p. 59.
[37] L. Lessig, *Remix. Il futuro del copyright (e delle nuove generazioni)*, Milano, ETAS, 2009, pp. 218-222.
[38] C. Sunstein, *Republic.com. Cittadini informati o consumatori di informazioni?*, Bologna, il Mulino, 2003.
[39] B. C. Han, *Nello Sciame. Visioni del digitale*, Roma, nottetempo, 2015, pp. 26-30.
[40] *Ibidem*, p. 24.

indotta dalla comunicazione digitale, privilegia di fatto un'esibizione pornografica dell'intimità e della sfera privata[41].

Solo intervenendo sulle architetture della rete e imponendo un mutamento del *code* si potrà affrontare la questione della protezione dei minori dalle forme di espressione destinate agli adulti nella Rete (oscene, indecenti, pornografiche, violente); infatti, nessuna forma di regolamentazione sarà efficace se non controllerà dall'interno, *by design*, le architetture che consentono o strutturano le nostre azioni sul Web.

Ad esempio, l'uso generale delle tecnologie d'identificazione su Internet accrescerebbe la regolabilità del comportamento nel cyberspazio: quest'opzione tecnica, implementabile dai governi, renderebbe impossibile qualsiasi raccolta e trasmissione di dati personali d'identificazione sull'utente di un browser *Kids-mode*.

Finché i regolatori pubblici continueranno a immaginare una perfetta simmetria tra azioni *offline* e azioni *online,* nessuna normazione preventiva risulterà efficace: il confine tra *offline* e *online* potrà risultare netto solo agendo sulle scelte di *design* degli spazi virtuali su Internet[42].

La pornografia nello spazio reale è tenuta fuori dalla portata dei minori: per essi è comunque difficile (anche se non impossibile) acquistare materiale pornografico sia a causa delle leggi, che proibiscono la vendita di pornografia; sia a causa delle norme sociali, che impongono di evitare coloro che vendono pornografia ai minori; infine, a causa del mercato, perché la pornografia è costosa[43].

Le regole dello spazio reale – qui sta il punto decisivo della questione – dipendono da certe caratteristiche di *design*. Nello spazio reale l'età è un fatto immediatamente conoscibile: ovviamente un ragazzo potrebbe cercare di dissimularla, ma generalmente ciò non accade; infatti, all'adulto che vende o tratta pornografia è nota la minore età del ragazzo. Nello spazio reale l'autenticazione di sé consente facilmente di creare zone che rendono *off-limits* i contenuti osceni dell'espressione[44].

Nel cyberspazio, invece, l'età non è immediatamente conoscibile. Quand'anche le stesse restrizioni di mercato, nonché le stesse leggi e norme sociali, trovassero applicazione al cyberspazio, ogni tentativo di istituire delle zone *off-limits* per la pornografia si scontrerebbe con la difficoltà concreta di accertare l'età. Per un sito che accetta il traffico utente, ogni richiesta è identica alle altre: l'architettura fondamentale del cyberspazio garantisce l'invisibilità alle caratteristiche dell'utente.

L'unica soluzione che consenta di identificare l'età parrebbe essere la modifica del *code* della Rete per consentire la trasmissibilità delle informazioni relative all'età *dell'user* e per rendere tracciabile l'anonimato. È pur vero che, allo stato attuale, non c'è un rapporto necessario tra un terminale (avente un dato indirizzo IP) e la persona; i governi, però, potrebbero intervenire per facilitare l'uso delle tecnologie di identificazione e di autenticazione degli utenti sul Web.

[41] *Ibidem*, pp. 88-89.

[42] D. J. Solove, *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*, New Haven, Yale University Press, 2007, p. 190.

[43] L. Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, cit., p. 504.

[44] *Ibidem*.

Tutelare i minori sul Web è dunque possibile, a patto, però, d'imporre un giudizio relativo ai soggetti che dovrebbero avere accesso a determinati contenuti, cui verrebbero sottoposti anche coloro che compongono il *code* informatico; in tal modo, anche le architetture del cyberpazio sarebbero disegnate in conformità alle regole statali.

## 4. La persona digitale tra habeas corpus e habeas data

L'esigenza di proteggere la segretezza dell'informazione è sempre stata presente nella storia dell'umanità. Il potere ha sempre percepito il valore del segreto e dell'*asimmetria informativa,* soprattutto in contesti di sorveglianza della popolazione o di conflitto sociale interno. Idem dicasi per i singoli che considerano la tutela del segreto dei propri dati sensibili come una garanzia fondamentale per la loro libertà individuale e per la loro piena espressione nella società.

Senza soffermarsi sulle molteplici definizioni di privacy[45] e sui rapporti con la protezione dei dati personali[46], qui interessa rammentare che tanto il diritto alla privacy quanto la protezione dei dati personali sono riconosciuti nelle Costituzioni nazionali e nelle Carte europee e internazionali dei diritti fondamentali.

Negli Stati Uniti la Costituzione non contempla il diritto alla privacy: esso viene indirettamente tutelato dal Quarto Emendamento, relativo al divieto delle perquisizioni irragionevoli da parte dell'autorità giudiziaria. Tuttavia, è proprio in seno al dibattito dottrinale statunitense che si formulerà la prima definizione di privacy.

Poiché negli Stati Uniti la diffusione dei giornali e lo sviluppo del giornalismo nel XIX secolo avevano favorito la circolazione di false notizie (*fake news*), la dottrina e la giurisprudenza dovettero interessarsi al problema della tutela della privacy dagli abusi provocati dalla circolazione di informazioni non veritiere.

Samuel D. Warren e Louis D. Brandeis furono i primi giuristi a definire e a sistematizzare il diritto alla privacy[47].

Nel loro saggio esso è definito come un diritto negativo, un *right to be let alone*, poiché tutela il soggetto che pretende di mantenere segrete le informazioni afferenti la sua sfera intima, ideologica, familiare e sessuale.

Un diritto così definito implica il divieto a qualsiasi soggetto pubblico o privato di sorvegliare l'individuo e di interferire nella sua sfera privata, tranne che nei casi tassativamente previsti dalla legge. Il diritto alla privacy, reso estremamente dinamico e mutevole dall'evoluzione tecnologica, coinvolge nuovi aspetti della vita e richiede l'introduzione di nuove forme di tutela.

[45] D. J. Solove, *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*, cit., pp. 170 ss.

[46] F. Pizzetti, *Il prisma del diritto all'oblio*, in Id. (a cura di), *Il caso del diritto all'oblio*, Torino, Giappichelli, 2013, pp. 21-63.

[47] S. D. Warren, L. D. Brandeis, *The right to Privacy*, in "Harvard Law Review", 5, 1890, pp. 193-220.

Non si tratta solo di difendere i dati personali dalla violazione del segreto e dalla pubblicazione indebita da parte di terzi[48], ma anche dal rischio di manipolazione cui sono esposti dopo l'immissione in sistemi di comunicazione e di diffusione difficilmente controllabili.

In forza di questa evoluzione, per rispondere alle esigenze progressivamente e incessantemente espresse dalla *socialità digitale,* oggi il nucleo originario del diritto alla privacy è arricchito da nuove circostanze. Tra di esse rientrano il diritto al controllo dell'uso, da parte di terzi, delle informazioni riguardanti una persona[49] e il diritto a non vedere le proprie informazioni alterate. Successivamente, il riconoscimento del diritto alla difesa delle proprie scelte di vita[50] ha reso la privacy un aspetto fondamentale ed una precondizione al pieno godimento del diritto all'autodeterminazione; infine, si ricordi il diritto alla costruzione della propria identità ed all'adozione di tutte le misure "che impediscono a ciascuno di essere semplificato, oggettivato e valutato fuori contesto"[51].

La privacy gode dunque di una duplice valenza. Verso l'esterno, tale diritto protegge le informazioni personali dal controllo di terzi; verso l'interno, esso è orientato alla tutela dell'autodeterminazione del proprio piano di vita, elemento costitutivo della sfera privata[52] di ciascuno, che ne è proprietario. In definitiva, l'espansione dei significati e delle tutele ricondotte all'interno della privacy sono indirizzate alla tutela dell'integrità e della dignità personale.

La tutela dei dati personali non può limitarsi agli organi di informazione di massa, come stampa e televisione (già oggetto di una disciplina *ad hoc*), ma deve estendersi alla rete Internet, capillarmente diffusa in ogni settore della società.

Chi controlla il mercato della produzione e della distribuzione dell'informazione stabilisce quali merci verranno prese in considerazione e, quindi, a quali informazioni sarà ufficialmente consentito di accedere nel "mercato dei dati personali".

I dati di cui le *corporations* informatiche entrano in possesso sono di diversa natura: orientamento ideologico, orientamento religioso, preferenze sessuali, transazioni economiche, tipologia dei consumi, dati biometrici (impronte digitali, scansione della retina) e dati genetici[53].

A ben vedere, si tratta di dati che nel loro insieme rivelano gli interessi critici e gli interessi esperienziali della vita di una persona, fino a svelarne la sua essenza ontologica[54].

Si è proposto di potenziare la criptazione dei dati contenuti nelle memorie dei dispositivi per proteggere la privacy del proprietario delle informazioni afferenti a dati di natura biologica. Tuttavia, è paradossale che i dati non contraffabili, come le impronte digitali, siano così preziosi da rendere vana una qualsiasi *policy* di bilanciamento tra protezione dei dati sensibilis-

[48] P. Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, in "California Law Review", 87, 1999, pp. 751-766.

[49] Livello di tutela introdotto da A. Westin, *Privacy and Freedom*, New York, Athaeneum, 1970.

[50] L. Friedman, *The Republic of Choice. Law, Authority and Culture,* London, Harvard University Press, 1990, p. 184.

[51] J. Rosen, *The Unwanted Gaze. The Destruction of Privacy in America*, New York, Random House, 2000, p. 20.

[52] S. Rodotà, *Tecnologie e diritti*, Bologna, il Mulino, 1995, p. 122.

[53] R. Wacks, *Privacy. A Very Short Introduction*, Oxford, Oxford University Press, 2010, pp. 10-12.

[54] *Ivi,* pp. 21-22.

simi e il loro uso legittimo; in materia di consenso informato, infatti, è ormai consolidata tra le *data and biobanking corporations* la prassi dell'utilizzo del *out-put system*.

In questo senso, i metodi di sicurezza informatica basati su parametri biometrici permetterebbero all'azienda di disporre, in linea del tutto teorica, di un archivio costituito dalle impronte digitali dei suoi clienti, ponendo in essere una vera e propria schedatura di dubbia legalità.

In un contesto di questo tipo, l'oggetto di tutela si espande notevolmente: oltre alla protezione della diffusione di notizie riguardanti l'immagine pubblica dell'individuo, esso viene ad includere l'astensione da parte di soggetti terzi alla conservazione e manipolazione di dati, che, nella maggior parte dei casi, sono tracce digitali impossibili da cancellare; nonostante i dati personali siano stati sottoposti a un processo di anonimizzazione, rimane pur sempre possibile l'applicazione del processo inverso di re-identificazione.

Poiché gran parte dei processi computazionali opera in modo nascosto per l'utente, l'accezione contemporanea di privacy deve necessariamente indicare la protezione dei dati appartenenti all'individuo e afferenti alla sua personalità, indipendentemente dal luogo nel quale essa si esprime.

Ad esempio, attraverso la tecnologia del *cloud computing* l'utente trasferisce la sua attività informatica in un ambiente virtuale accessibile tramite browser, sfruttando in questo modo lo spazio di memoria offerto dal provider solo mediante connessione ad Internet. Il trasferimento dei dati avviene su un supporto di memorizzazione (Dropbox, Google Drive, OneDrive, ecc.) che sfugge al controllo del creatore e proprietario dei file. Quest'operazione avviene legalmente: è lo stesso utente che accetta e sottoscrive le condizioni del contratto di *clouding*, ma l'azienda fornitrice del servizio non garantisce sufficienti informazioni relative all'utilizzo che farà dei dati acquisiti e al trattamento cui andrà a sottoporli.

La *persona digitale* è il risultato dei dati prodotti dalla persona fisica, orpello elettronico, corpo-informazione, corpo-password; essa è, in definitiva, il ricettacolo di dati e di informazioni raccolti e processati che formano la *biografia digitale* della persona[55].

Ma, si badi, nella *persona digitale* non viene smarrita la corporeità del soggetto: questi non si distacca dalla sua materialità, ma viene socialmente mutato e tecnologicamente disciplinato, al punto tale che i sistemi informatici potrebbero indurlo a tenere scientemente comportamenti *contra legem*.

Rimane il fatto che la *persona,* seppur trasmutata da un punto di vista sia genetico (*cyborg*) sia cibernetico (*inforg*), mantiene intatto il diritto alla dignità e alla scelta delle informazioni conoscibili dalla società tramite il Web.

Come l'integrità fisica viene protetta dal potere pubblico tramite l'*habeas corpus*, così nel contesto digitale il corpo della *persona digitale* viene protetto tramite l'*habeas data*[56]; esso prevede l'intangibilità dell'immagine pubblica prodotta dai dati immessi nella Rete e la tutela dalla manipolazione indebita, da parte di terzi, dei propri dati.

[55] F. Cristofari, *Gli algoritmi dell'identità: il corpo umano*, in S. Amato, F. Cristofari, S. Raciti, *Biometria. I codici a barre del corpo*, Torino, Giappichelli, 2013, pp. 43-45.

[56] S. Rodotà, *Il mondo nella rete. Quali diritti, quali i vincoli*, Roma-Bari, Laterza, 2012, pp. 27-32.

L'*habeas data* rappresenta il diritto della *persona digitale* di non vedere manipolato il proprio corpo virtuale da agenti esterni, dal suo stesso consenso o da un'autorità competente non autorizzata. Questa nuova forma di sovranità sui dati personali digitali costituisce il fondamento della tutela della sfera di riservatezza individuale e del nuovo concetto di privacy.

Con l'*habeas data* non si vuole limitare la diffusione dei dati personali, ma si vuole proteggere l'immagine complessiva nella quale il soggetto si riconosce e con la quale desidera proiettarsi all'esterno, senza l'interferenza di alcun soggetto terzo che la manipoli o la alteri. L'*habeas data* protegge il diritto alla dignità e all'autodeterminazione della *persona digitale* sia nel Web sia nel mondo reale.

Una visione di Internet più aderente alla realtà deve individuare le tutele effettive dell'*habeas data* di cui è titolare la *persona digitale*, intesa quale figura nuova e quale esito di una nuova fenomenologia dei rapporti umani consolidatasi nell'ecosistema digitale: trovare le contromisure giuridiche alla fenomenologia del "mi piace" è una questione che può essere risolta solo a patto che i regolatori pubblici prendano sul serio la possibilità di incidere *by design* sul *code* e sulle architetture del sistema computazionale.

## 5. Bibliografia di riferimento

Oltre ai saggi già riportati in nota, si vedano i seguenti per ulteriori approfondimenti:

Akdeniz Y., *Internet Child Pornography and the Law: National and International Responses*, London, Routledge, 2008.

Betzu M., *Regolare Internet. Le libertà di informazione e di comunicazione nell'era digitale*, Torino, Giappichelli, 2012.

Buckingham D., Willett R., *Digital Generations: Children, Young People, and the New Media*, London, Routledge, 2006.

Bygrave L. A., *Data Privacy Law: An International Perspective*, New York, Oxford University Press, 2014.

Land R., Bayne S. (Eds.), *Education in Cyberspace*, London, Routledge, 2005.

Lessig L., *Code Version 2.0*, New York, Basic Books, 2006.

MacDougall R. C., *Digination. Identity, Organization and Public Life in the Age of Small Digital Devices and Big Digital Domains*, Lanham, Fairleigh Dickinson University Press, 2012.

Marsden C. T., *Internet Co-Regulation. European Law, Regulatory Governance, and Legitimacy in Cyberspace*, Cambridge, Cambridge University Press, 2011.

Murray A., *The Regulation of Cyberspace: Control in the Online Environment*, London, Routledge, 2006.

Perrit H. H., *Jurisdiction in Cyberspace*, in "Villanova Law Review", 1, 1996, pp. 1-64.

Preston C. B., *Zoning the Internet: A New Approach to Protecting Children Online*, in "Brigham Young University Law Review", 6, 2007, pp. 1417-1467.

Radin M.J., *Proprietà e cyberspazio*, in "Rivista critica di diritto privato", 1, 1997, pp. 89-111.

Reed C., *Making Laws for Cyberspace*, Oxford, Oxford University Press, 2012.

Reidenberg J., *Lex informatica: the Formulation of Information Policy Rules through Technology,* in "Texas Law Review", 76, 3, 1998, pp. 553-593.

Rogers A., *Protecting Children on Internet: Mission Impossible?*, in "Baylor Law Review", 61, 2009, pp. 323-356.

Solove D. J., *The Digital Person. Technology and Privacy in the Information Age*, New York, New York University Press, 2004.

van der Hof S., van der Berg B., Schermer B. (Eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety*, La Hague, Asser Press, 2014.

Ziccardi G., *L'odio online. Violenza verbale e ossessioni in rete*, Milano, Raffaello Cortina, 2016.

**Received May 8, 2017**
**Revision received May 14, 2017 / May 19, 2017**
**Accepted May 23, 2017**