Raffaella Brighi

La vulnerabilità nel cyberspazio

ABSTRACT

As can be appreciated from the numerous threats to data stored, processed, and sent across cyberspace, digital data are a valuable resource. The most visible threat is cybercrime, but it is the inherently fragile nature of digital data that makes us vulnerable. What exposes people to risk – witness profiling and surveillance, and online reputational damage – is the constant interaction between the virtual and the real, coupled with a lack of computational transparency and the information asymmetry between those who use digital technologies and those who control them. Neutrality and transparency must be protected by law if we are to have inclusive cybersecurity and data protection, making sure that people are secure not only their physical surroundings but also in virtual space.

KEYWORDS

Cyberspace – Vulnerability – Cybersecurity – Transparency – Data Protection.

1. PREMESSA: SPAZIO FISICO E SPAZIO VIRTUALE

La rete Internet, con le sue infrastrutture e i suoi servizi, crea uno spazio per le attività umane, a cui comunemente ci si riferisce con il termine "cyberspazio". Il termine, che ha origini letterarie, sottolinea l'immersione totale dei sensi umani in qualcosa di generato artificialmente, un ambiente virtuale in cui le persone interagiscono tra loro, attraverso le loro rappresentazioni digitali, e con entità create da processi computazionali, quali negozi online, reti sociali, videogiochi o siti. Il cyberspazio è invisibile, intangibile, non territoriale, globale:

> Cyberspace is a place. People live there. They experience all the sorts of things that they expeirence in the real space, there. […] While they are in that place, cyberspace, they are also here. […] They live this life there, while here[1].

1. L. Lessig, 1996, 1403.

Il cyberspazio si fonde con lo spazio fisico. Non solo duplichiamo nel cyberspazio attività che siamo soliti compiere nello spazio fisico, ma Internet sta modificando le modalità nelle quali si svolge ogni tipo di attività, dalla ricerca scientifica, alla produzione, alla socializzazione.

Un'ampia letteratura dimostra come il comportamento umano su Internet sia vincolato prima e più che dal diritto dal "codice", ovvero dai modi in cui operano hardware e software[2]. Nell'era dei *big data*, del *semantic web* e delle ontologie computazionali questo concetto va però inteso in senso più ampio. Non solo il software guida i comportamenti umani al punto che ciò che è possibile o impossibile tecnologicamente si sovrappone alle categorie normative del permesso e dell'obbligo, ma le tecnologie informatiche sono oggi in grado di *costruire* nuovi dati, scoprire relazioni, ridefinire concetti. Tali tecnologie aggregando e combinando (e quindi creando) dati informatici trasformano la realtà e riducono la distinzione tra essa e la sua rappresentazione digitale creando una nuova dimensione della realtà, ovvero una sorta di "realtà aumentata"[3]. Si tratta di qualcosa di più di tecno-regolazione: esse ridefiniscono le categorie ontologiche della realtà trasformando la sua natura intrinseca. Si pensi, ad esempio, alla funzione delle ontologie computazionali in molti sistemi informatici e in particolare nei sistemi per il diritto, in cui attraverso lo sviluppo di ontologie formali si costruisce una comprensione condivisa e comune del dominio, su cui implementare ragionamenti automatici[4]. Non solo non può essere tracciata una linea di demarcazione tra reale e virtuale ma gli artefatti informatici (le strutture dati, le classi, le istanze, gli algoritmi) *costruiscono* in qualche misura la realtà, la stanno "riontologizzando"[5]. Alle tradizionali funzioni *epistemiche*, dove i computer con i processi di elaborazione dell'informazione estendono le capacità cognitive dell'uomo (calcolare, pianificare, ricordare, ricercare ecc.), con i processi di creazione di ambienti e di oggetti virtuali che estendono il mondo fisico, si aggiunge, di fatto, una funzione *ontologica*. L'uso di

2. Sartor introduce il concetto di "regole virtuali" per definire i modi in cui il software può vincolare il comportamento umano (G. Sartor, 2011, 13-7). Tale concetto è anche alla base di molti scritti di Lessig (tra cui L. Lessig, 1999), e si ritrova in Reidenberg (1998), che parla di *lex informatica*.

3. Il rapporto tra strutture della realtà e strutture dati può essere paragonato al rapporto circolare che si crea tra teoria scientifiche e dati sperimentali, ben descritto da B. Van Frassen (1985): «La sperimentazione guida il processo di costruzione della teoria, mentre nello stesso tempo la parte di teoria già costruita guida il progetto di esperimenti che guideranno, a loro volta, la continuazione del processo».

4. Per un inquadramento si rimanda a G. Sartor *et al*., 2011.

5. Il termine è proposto da L. Floridi (2012) che osserva come le ICT (Information and Comunication Technology) stiano modificando la natura intrinseca della realtà, costruendo, in modo nuovo e radicale, «ambienti in cui l'utente è in grado di entrare tramite porte d'accesso (possibilmente amichevoli), sperimentando una sorta di iniziazione».

Internet per le interazioni sociali, per esempio, ha dato luogo ad una realtà sociale, realizzata in digitale, che include ruoli sociali e stati, gruppi e organizzazioni, istituzioni ed eventi sociali[6].

Tuttavia, nel cyberspazio i processi computazionali, legati alla progettazione dei sistemi informatici e alle architetture delle reti, sono spesso occulti, non trasparenti, e quindi potenzialmente indirizzabili da spinte economiche, dai governi o dalla criminalità che vanno a sfruttare le vulnerabilità dei sistemi informatici e dei loro utenti.

2. DATI INFORMATICI, VALORE E VULNERABILITÀ

Nella società della rete i dati informatici generati dalle nostre interazioni online sono una risorsa preziosa[7]. Sono i cosiddetti *big data*, espressione che indica grandi quantità di dati, in costante accumulo, caratterizzati da almeno tre proprietà: il volume di memoria occupata (misurato in Zettabyte – 10^{21} milioni di gigabyte), la velocità intesa come necessità di comprimere i tempi di gestione e di analisi dei dati e la varietà, ovvero eterogeneità, dei formati[8]. La sempre maggiore diffusione di dispositivi mobili, la disponibilità di banda e la semplicità di connessione, uniti agli strumenti tecnologicamente immediati del Web 2.0, hanno moltiplicato le fonti di produzione dei dati informatici. Le applicazioni degli smartphone per facilitare operazioni quotidiane, i social media, la geolocalizzazione e la miriade di servizi offerti dal web (per condividere immagini, documenti e pensieri; per fare acquisti e scambiare informazioni su prodotti; per analizzare spese e consumi; per pianificare viaggi; per calcolare percorsi) sono solo alcuni esempi. Non solo, quando il cosiddetto *Internet of Things* – ossia il dialogo fra sistemi di elaborazione e miliardi di sensori incorporati in oggetti di uso quotidiano, progettati per registrare, elaborare e trasferire dati – sarà più diffuso di quanto non lo sia oggi, si assisterà anche a uno scambio di dati "macchina a macchina" senza l'intermediazione umana, che permetterà di raccogliere e analizzare dati relativi all'ambiente in cui si muove la singola persona.

L'analisi di tali dati – scambiati, integrati e aggregati dai sistemi informatici anche con finalità diverse da quelle per cui sono stati originariamente raccolti – migliora i risultati, i processi e le decisioni; tanto che la scienza informatica è sempre più focalizzata su tecniche di trattamento del dato per estrar-

6. Nell'ambito degli studi sull'interazione uomo-macchina si veda, in particolare, Ph. Brey (2005), in cui l'autore analizza come la realtà sociale e istituzionale possano essere create nel cyberspazio con facilità attraverso l'imposizione collettiva dagli utenti di Internet con appropriate strutture digitali.

7. Sul punto si veda, per esempio, la Comunicazione della Commissione Europea *Verso una florida economia basati sui dati*, COM (2014) 442.

8. Per un'introduzione ai *big data* si veda V. Mayer-Schönberger e K. Cukier, 2013.

ne "valore". Il dato è una risorsa strategica attorno a cui ruotano molti interessi, dagli interessi economici e politici, agli interessi della criminalità.

Nella società della conoscenza, dunque, dato significa *valore*. A conferma di ciò, i più recenti rapporti sulla sicurezza informatica registrano il progressivo aumento di attacchi informatici ad opera del cibercrimine con obiettivo la violazione di dati per le finalità più disparate: dalle frodi e dalle estorsioni informatiche ai furti di identità fino ad arrivare ai casi di spionaggio o sabotaggio[9]. Molte minacce (informatiche e non) sono indirizzate ai dati memorizzati, elaborati e trasmessi dai sistemi informatici. È ormai noto come carte di credito e credenziali di autenticazione (account PayPal, conti bancari, credenziali di accesso a servizi online) siano venduti sul mercato nero della rete per cifre irrisorie[10]. Se il rischio degli attacchi informatici inizia ad essere ben percepito dagli individui – la grande diffusione di *ransomware*[11] che bloccano i dati memorizzati nei dispositivi e chiedono un riscatto ha certamente contribuito a sensibilizzare in tal senso gli utenti della rete –, il rischio connesso ad un uso improprio dei propri dati personali e sensibili è spesso trascurato; il valore dei propri dati non è ancora pienamente compreso dalle persone.

Per sua natura il dato informatico è connotato da alcune caratteristiche specifiche che ne implicano la fragilità. Esso è rappresentato in forma simbolica – a seguito di operazioni di concettualizzazione e di codifica in forma binaria – su supporti fisici di memorizzazione permanente e in memorie volatili, o anche trasmesso attraverso reti di telecomunicazioni. I bit forniscono informazioni solo se correttamente interpretati, ciò comporta che i dati non siano fruibili se non se ne conosce il *senso* e che dati generati da software non più attuali diventino illeggibili; lo stesso accade a causa della rapida obsolescenza a cui è soggetto l'hardware o anche a causa del deterioramento (rottura, perdita) dei dispositivi stessi. La memoria digitale è inoltre vulnerabile a *malware* e attacchi informatici. Ciò che pensiamo di memorizzare in modo permanente, dunque, non è in realtà al sicuro da perdite e danneggiamenti.

D'altro canto il dato digitale è riproducibile in modo fedele un numero infinito di volte, ciò rende la memoria digitale infinita nel tempo. Durante i processi di trasmissione vengono create e memorizzate molte copie degli stessi dati, creando quella che si definisce *stickiness* – viscosità. Concretamente è impossibile eliminare definitivamente un dato dalla memoria della rete e i

9. Oggi è possibile ipotizzare che il mercato sia suddiviso in cyber-professionisti singoli o strutturati in piccoli gruppi (70%), organizzazioni criminali (20%), cyber-terroristi (5%), cyber-criminali assoldati da enti governativi (4%), attivisti (1%). Cfr. R. Baldoni e R. De Nicola, 2015.

10. Intel Security, 2015.

11. I *ransomware* sono software malevoli che infettano computer e dispositivi mobili, veicolati da mail di *phishing* o siti compromessi. Una volta installati, cifrano i contenuti del dispositivo e chiedono un riscatto per consegnare la chiave con cui decifrarli. Tra i più diffusi si segnalano appunto Cryptolocker e TeslaCrypt.

programmi informatici possono ricostruire le numerose tracce lasciate dai dispositivi digitali. La cancellazione dei dati, come è noto, è spesso solo apparente e il dato può essere recuperato facilmente con software specifici (*data carving*)[12]. I dati informatici, inoltre, sono alterabili in maniera (quasi) anonima, fattore che implica gravi ripercussioni sui profili riguardanti l'integrità e la paternità del dato[13].

Un altro aspetto riguarda la *qualità* dei dati[14]. Il grande accumulo di dati informatici non ne agevola il reperimento, l'interpretazione e l'analisi. Il valore dei dati dipende infatti dalla capacità di elaborarli per trarne informazioni. Nel caso dei *big data* ciò si concretizza nell'individuazione di relazioni, all'interno delle informazioni disponibili, anche apparentemente molto distanti, da cui estrarre conoscenza. Svariate sono le operazioni che possono essere svolte sui dati e che hanno quindi ricadute applicative; le principali sono il *clustering*, cioè il raggruppamento di oggetti in categorie dedotte per similitudine, la classificazione, ovvero l'assegnazione di un oggetto a una categoria predefinita e la regressione, che consente di formulare previsioni tramite inferenze a partire da dati noti[15].

Mentre sono ampiamente in corso di sviluppo tali tecniche di analisi massiva, soprattutto sotto la spinta delle grandi *corporations*, ancora poco rilievo è posto alle criticità connesse alla scarsa precisione di tali dati, alla semantica legata spesso al contesto applicativo, alla difficile interoperabilità, alla mancanza di informazioni esplicite e computabili che ne traccino la provenienza e quindi l'affidabilità[16]. L'accessibilità dei dati è oggi legata

12. Lo spostamento di file nel cestino (e il successivo svuotamento) e la formattazione rapida non cancellano effettivamente il dato, ma semplicemente informano il sistema operativo che quello spazio può essere riutilizzato.

13. C. Maioli, 2004.

14. Il problema di ottenere dati qualitativamente validi è complesso e multidisciplinare. Numerosi istituiti di standardizzazione hanno, nel corso degli anni, contribuito alla definizione del concetto di *qualità* di prodotti e servizi e all'individuazione di indicatori e procedure per la misurazione (ad esempio la norma UNI EN ISO 9000:2005). Per un inquadramento C. Batini e M. Scannapieco, 2008.

15. La Big Data Analytics è quell'insieme di tecniche in forte sviluppo che attraverso metodi euristici puntano a identificare regolarità e relazioni all'interno di grandi dataset, integrando informazioni provenienti da fonti diverse.

16. Va rilevato come su questi temi, invece, si stiano da tempo muovendo la comunità scientifica e gli organismi preposti allo sviluppo del web, che operano per promuovere standard e modelli volti ad esprimere in modo formale la semantica dei dati. A partire dal *semantic web* di Tim Berners Lee, dove il fondatore del web ha definito i mattoni per creare un web in cui i dati diventino da *human understandable* a *machine understandable,* molti studi hanno sviluppato il tema della condivisione della conoscenza, coniugato ai principi di apertura e trasparenza del dato. Anche il tema della provenienza del dato è stato ampiamente affrontato, dando come esito nel 2013 l'approvazione del PROV *Framework* del W3C, che favorisce l'interscambio di informazioni sulla provenienza del dato tra sistemi eterogenei con

esclusivamente ai motori di ricerca (se si toglie un dato dall'indice di Google questo viene irrimediabilmente perso) e gli utenti in particolare hanno pochi strumenti per valutare la qualità delle informazioni e implementare su queste analisi e ragionamenti, decidere se fidarsi o meno, e con quale grado di fiducia[17].

Come la fragilità dei dati informatici si rifletta sulla persona, rendendola vulnerabile nel cyberspazio, è efficacemente descritto da Rodotà (2013):

> Ogni intervento sul corpo, ogni operazione di trattamento dei dati personali devono essere considerati come se si riferissero al corpo nel suo insieme […] determinando l'assorbimento nella categoria generale dell'*habeas corpus* di tutte quelle specificazioni con le quali si sono volute accompagnare le innovazioni specifiche e tecnologiche e che, ad esempio, hanno trovato espressione in una formula come *habeas data*.

Molteplici sono i profili. Tra i più discussi, la determinazione dell'identità personale tramite il collegamento dei dati raccolti o prodotti dai diversi servizi di Internet: il nuovo web apre infinite possibilità di costruzione dell'identità personale, che diventa anche comunicazione e rete di collegamenti; le informazioni che la riguardano sono raccolte in profili diversi, ciascuno dei quali riporta frammenti di identità che possono essere aggregati e combinati tra loro per fornire, o meglio "ricostruire", informazioni che non sono esattamente ciò che la persona intendeva dire di sé. Quale legame si instaura tra la persona e le informazioni che variamente la rappresentano nella dimensione digitale?[18] Strettamente legato alla memoria infinita delle rete è, inoltre, il problema della *web reputation*: da un lato la rete può contribuire a far conoscere la fama di una persona o di un'impresa, ma dall'altro vi è il costante pericolo di calunnie e diffamazioni oppure giudizi e feedback negativi, che portano a essere "ricordati" all'infinito solo per fatti, foto o commenti appar-

l'obiettivo di aiutare gli utenti a valutare l'affidabilità dei dati in un ambiente aperto e inclusivo, come il web.

17. Il Report *Evaluating Information: The Cornerstone of Civic Online Reasoning* della Standford Graduate School of Education (2016), che misura e analizza la capacità di discriminazione delle informazioni da parte dei giovani, mostra un'incapacità sconcertante da parte degli studenti di ragionare sulle informazioni che trovano in rete. Gli studenti, per esempio, hanno avuto difficoltà a distinguere tra annunci e articoli di notizie o a identificare la fonte da cui proviene un'informazione.

18. L'interrogativo richiama il concetto di identità personale e come esso si è evoluto nella società dell'informazione. Su questi temi G. Pino, 2003 e 2010; S. Rodotà, 2013; G. Resta, 2007; G. Finocchiaro, 2010. Si veda anche S. Pozzolo e A. Verza, 2015; M. Martoni e M. Palmirani, 2015.

tenenti al passato[19]. Non ultime, le procedure di profilazione[20], generalmente strumentali sia all'offerta di servizi sempre più mirati e conformati sulle specifiche esigenze dell'utente, sia alla fornitura di pubblicità personalizzata, sia allo sfruttamento commerciale dei profili ottenuti, fino ad arrivare all'analisi dei dati informatici come strumento di controllo e sorveglianza delle persone[21].

Le criticità sinteticamente delineate sono senza dubbio accentuate da una scarsa conoscenza delle caratteristiche di funzionamento degli strumenti impiegati, delle loro finalità e delle condizioni d'uso; in questo non aiutano i sistemi moderni che tendono a nascondere come operano gli strumenti per rendere più semplice all'utente ogni operazione.

> Se si entrasse in un negozio, e la guardia giurata alla porta registrasse il nostro nome; se le telecamere tracciassero ogni nostro passo, notando quali oggetti abbiamo guardato e quali ignorato; se un impiegato ci seguisse, calcolando il tempo passato davanti a ogni scaffale; se prima di poter acquistare un oggetto selezionato, il cassiere domandasse che gli si riveli chi siamo – se una, o tutte queste cose, accadessero nello spazio reale ne prenderemmo consapevolezza[22].

La continua interazione reale-virtuale e la scarsa trasparenza degli ambienti virtuali, anticipati in premessa, si coniugano all'inevitabile asimmetria informativa tra chi utilizza le tecnologie e chi le governa, esponendo le persone ai comportamenti descritti. A ciò si aggiunge l'immediatezza con cui le applicazioni consentono, con pochi passaggi o automaticamente, di registrare i propri dati, contrapposta alla difficoltà della cancellazione degli stessi. Anche la gratuità della maggior parte dei servizi, infine, trasforma le persone da clienti o acquirenti in utenti, con una conseguente compressione dei loro diritti[23].

3. DESIGN E PROTEZIONE DEI DATI NELLO SPAZIO VIRTUALE

Le problematiche e le prospettive sollevate dal controllo e dalla regolazione di Internet sono una delle principali sfide a cui è chiamato il paradigma normativo contemporaneo. Quale è il ruolo del diritto in riferimento alla regolazione

19. In questo contesto si inserisce anche l'ampio dibattito sul diritto all'oblio. Per un inquadramento S. Pietropaoli, 2015.

20. Per profilazione si intende l'analisi e l'elaborazione di informazioni relative a utenti o clienti, al fine di suddividere gli interessati in gruppi omogenei per comportamenti o caratteristiche sempre più specifici, con l'obiettivo di pervenire all'identificazione inequivoca del singolo utente o del suo terminale.

21. G. Ziccardi, 2011.

22. L. Lessig, 2015, 80.

23. «Chi riceve un dono non ha diritto di rimostranza o di fare causa. Il regalo toglie potere a chi lo riceve, mentre l'acquisto dà potere a chi lo fa» sostiene Floridi introducendo il concetto di on-life (www.treccani.it/magazine/tecnologia/ Floridi_Benvenuti_nell_era_dell_onlife.html).

di Internet? Dovrebbe essere la legge a cambiare in risposta ai nuovi modelli oppure la legge dovrebbe cercare di cambiare le caratteristiche del cyberspazio per renderlo conforme ad essa?[24]

Il dibattito a tale proposito è molto ampio[25]. Poiché le tecnologie informatiche creano il mondo in cui viviamo, quanto meno, è auspicabile che esse siano progettate in modo da evitare che alcune loro caratteristiche intrinseche le rendano strumenti di compressione dei diritti fondamentali delle persone. Tale prospettiva trova le sue basi nel principio di *neutralità della rete*, che presuppone che il traffico Internet debba essere trattato in condizioni di uguaglianza senza discriminazione, restrizione o interferenza, indipendentemente dal mittente, dal destinatario, dal contenuto, dall'applicazione, dal servizio o dal dispositivo.

Internet nasce come rete *aperta* e *neutrale*, grazie ad alcune scelte tecnologiche di base, e questa è la ragione essenziale del suo successo. I requisiti di neutralità e apertura erano garantiti dalla architettura stessa di Internet che permette ai dati, suddivisi in pacchetti di lunghezza fissa, di viaggiare da un nodo all'altro della rete senza controlli intermedi, con prestazioni influenzate solo dal traffico della rete. Solo quando i pacchetti arrivano al calcolatore di destinazione, le buste digitali sono aperte, i pacchetti riuniti e controllati[26]. Le macchine che smistano i dati in transito (i *routers,* ad esempio) non erano in grado di identificare i diversi tipi di dati, leggerne i contenuti e trattarli diversamente. Oggi non è più così. I dispositivi che governano il passaggio dei dati, gestiti dai prestatori di servizi, possono discriminare i diversi flussi in rete, favorirne alcuni tipi o bloccarne altri, contribuendo a creare nuovi poteri, non solo economici.

Nelle stesse strutture di *governance* della rete – organismi, nati da enti privati o società no profit, che coordinano a livello transnazionale e in autonomia rispetto alle autorità politiche locali il funzionamento e lo sviluppo della rete, in riferimento sia agli aspetti tecnologici sia agli aspetti gestionali – si individuano profili di vulnerabilità[27]. Tra tali strutture ha un ruolo prevalente ICANN (*Internet Corporation for Assigned Names and Numbers*), ente statunitense no profit, che attraverso l'assegnazione degli indirizzi IP, la

24. L. Lessig, 2015.

25. A partire dalla suggestiva dichiarazione di libertà del cyberspazio di Barlow (1996), «*Il Cyberspazio non si trova all'interno dei vostri confini. Non pensate di poterlo edificare, come se fosse un progetto di costruzione pubblica. Non potete. È un atto della natura e cresce da solo grazie alle nostre azioni collettive*», molti si sono interrogati sulla possibilità della sua regolamentazione, tra cui L. Lessig (1999), J. Kang (1999) e G. Sartor (2011). Per un inquadramento, si veda V. Colomba, 2015.

26. Ciò è garantito dal meccanismo di commutazione di pacchetto e dal noto protocollo di comunicazione TCP/IP (V. G. Cerf e R. E. Kahn, 2004).

27. In punto si rimanda, tra gli altri, a A. Odennino (2008).

gestione del sistema dei nomi a dominio[28] nonché la gestione dei *root servers* (i server di riferimento per indirizzare le richieste di navigazione sulla rete), realizza la funzione di coordinamento globale del sistema di identificazione su Internet. Tale regime incide sui diritti dei singoli e il controllo o la manomissione dei meccanismi gestiti da ICANN mette a rischio la libertà della rete[29].

Perché Internet «*da spazio di libertà non diventi spazio di controllo*»[30] si afferma dunque la necessità di una tutela giuridica *ex ante* della neutralità della rete, in quanto garanzia di diritti fondamentali quali la libertà di espressione, la libertà di attività economica, la libertà di accesso alle informazioni. La neutralità della rete non esclude che la trasmissione di certi contenuti sia vietata dal diritto né che certi messaggi siano eliminati al punto d'arrivo. Si intende invece evitare che i dispositivi di rete analizzino i dati in transito, nemmeno per l'attuazione di divieti giuridici, per non legittimare strumenti che possano compromettere i diritti e le libertà fondamentali e avere conseguenze pregiudiziali, ad esempio, per la tutela della privacy.

A tutela della neutralità della rete si segnalano diversi interventi legislativi, dalla proposta della Federal Comunication Commission (USA) del 26 febbraio 2015 – che non solo ribadisce i diritti degli utenti ma prende in esame i rapporti tra *Internet Service Provider* (ISP) e fornitori di servizi (i cosiddetti *peerings*) – al molto discusso Regolamento UE 2015/2120 ("Telecom Single Market") e alle linee guida del Berec, recentemente oggetto di consultazione pubblica[31]. Gli interessi in gioco sono molteplici; gli argomenti pro e contro la neutralità della rete attengono più livelli, tra cui non secondario il piano economico che spinge per l'attuazione di una Internet "a più corsie" che garantisca miglior livelli di servizio e favorisca l'innovazione.

La risposta probabilmente è da cercare in una sintesi delle due posizioni, che utilizzi la tecnologia per sviluppare un modello di rete che sia trasparente

28. In particolar ICANN assegna i nomi di dominio di primo livello (*generic Top-Level Domain* quali .com, .net., .info) e dei *country code Top Level Domain* (che identifica uno specifico territorio, quali .it o .uk).

29. Sul ruolo di ICANN si veda, in particolare, B. Carotti (2007). Dopo anni di dibattito, ICANN si avvia oggi a un modello *multistakholder* di *governance*, volto a garantire maggiore stabilità e sicurezza online, mantenendo Internet aperto ed evitando qualsiasi comportamento che possa essere discriminatorio, al di fuori dell'egemonia degli Stati Uniti.

30. L. Lessig, 2015.

31. Si segnalano inoltre il *Telecomunications Act* (2012) dell'Olanda e gli interventi in materia di Cile, Slovenia, Paesi Bassi. In Italia le principali iniziative si hanno con l'art. 4 della Dichiarazione dei diritti di Internet che, in particolare, recita al comma 2°: «*Il diritto ad un accesso neutrale ad Internet nella sua interezza è condizione necessaria per l'effettività dei diritti fondamentali della persona*» e nella proposta di legge *Disposizioni in materia di fornitura dei servizi della Rete Internet per la tutela della concorrenza e della libertà di accesso degli utenti*, presentata dall'Intergruppo parlamentare per l'innovazione tecnologica nel luglio 2014.

e inclusiva ma che consenta anche di sviluppare nuovi servizi. Quello che è certo è che la neutralità della rete non deve essere posta in una dimensione di contrasto rispetto alla sicurezza informatica, anzi essa è un prerequisito per la protezione dei sistemi; la garanzia che le comunicazioni avvengano su un terreno neutrale e trasparente è il punto di partenza per implementare politiche efficaci per la sicurezza informatica e la protezione dei dati.

La sicurezza informatica entra nel nostro ordinamento, in modo chiaro, con la disciplina per la protezione dei dati personali (*in primis* con il D.P.R. del 28 luglio 1999, n. 318 imposto dalla legge del 31 dicembre 1996, n. 675 e sostituito poi dall'Allegato B del Codice privacy), tuttavia essa non è contemplata solo in riferimento alla privacy ma anche dal Codice per l'amministrazione digitale, relativamente alle firme elettroniche e digitali e alla sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni (art. 50)[32], dal Codice penale in relazione ai crimini informatici (art. 615-*ter* c.p., accesso abusivo a sistema informatico o telematico) e dalla normativa sul diritto d'autore che prevede misure tecnologiche idonee a proteggere le opere dell'ingegno da usi non consentiti dall'autore. Le misure di sicurezza trovano un ruolo di particolare rilievo anche nel recente Regolamento EU relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (n. 2016/679), che oltre ad ampliare i diritti dell'interessato in termini di diritto di rettifica, di portabilità e di oblio, impone al titolare del trattamento l'uso di tecniche di pseudonimizzazione e cifratura e introduce gli obblighi dell'analisi dei rischi e di comunicazione in caso di violazione dei dati personali se questi rappresentano rischi per i diritti e le libertà delle persone fisiche (*data breach*)[33].

In uno scenario di progressivo aumento, quantitativo e qualitativo, delle minacce e degli attacchi informatici la sicurezza informatica ha chiaramente l'obiettivo di salvaguardare i sistemi da potenziali rischi e violazione dei dati, mettendo in atto una serie di misure tecniche e organizzative per prevenire incidenti informatici e per reagire agli stessi in modo da ripristinare tempestivamente il sistema, quantificare i danni e rilevare eventuali responsabilità. La *computer security* è una scienza assai complessa, i sistemi in rapida evoluzione presentano continuamente nuove vulnerabilità, le tecnologie di difesa sono sempre più sofisticate; non è obiettivo di questo lavoro affrontare il tema della vulnerabilità in chiave tecnologica, mentre è opportuno evidenziare alcuni aspetti della sicurezza informatica connessi al "fattore umano".

32. Significativo è il documento *Misure minime di sicurezza ICT per le pubbliche Amministrazioni*, pubblicato il 26 aprile 2016 da AgID, Agenzia per l'Italia digitale.

33. Per un approfondimento si veda P. Perri, 2016.

L'uso non consapevole degli strumenti Internet, come sottolineato, può avere conseguenze concrete sulla persona, in termine di costruzione dell'identità personale, *web reputation*, profilazione. Molti degli attacchi alla rete avvengono sfruttando debolezze interne al sistema stesso, dovute a errori umani e alla scarsa conoscenza delle tecnologie da parte degli operatori. Un'attenzione adeguata deve essere posta dunque *in primis* alla formazione, all'aggiornamento e alla sensibilizzazione, per promuovere quei comportamenti corretti che possano prevenire malfunzionamenti e intrusioni[34]. Molte iniziative sono rivolte inoltre a sviluppare forme di autotutela, educando, soprattutto le generazioni più giovani, a sviluppare un'etica comportamentale nella vita online che consenta di cogliere le ripercussioni reali delle azioni svolte su Internet, con particolare riferimento al valore dei propri dati personali[35]. Il governo dei dati (la data *owernship*) deve poter rimanere in capo all'interessato che stabilisce come i propri dati possano essere utilizzati, ne custodisce la riservatezza o determina la cancellazione.

Tornando alla domanda iniziale, ovvero quanto il diritto possa influire sull'architettura del cyberspazio in particolare per proteggere gli utenti della rete, si rileva come l'approccio di protezione dei dati "by design" e "by default" sia confluito nel citato Regolamento EU (articolo 25, *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita).* Il presupposto è che lo strumento informatico debba essere progettato in modo tale da contenere gli abusi di dati personali e sensibili, attraverso opportune limitazioni d'uso e trattamento, includendo l'utente e la tutela dei suoi diritti.

Secondo il *framework*[36] delineato da Ann Cavoukian già negli anni Novanta e considerato come *global privacy standard* nel 2010 a partire dalla 32nd International Conference of Data Protection and Privacy Commissioners, le regole sulla privacy devono diventare un'impostazione di default ed essere integrate nel design delle infrastrutture tecnologiche, affinché i dati dell'utente siano salvaguardati a priori dai sistemi stessi[37]. La minimizzazione nel tratta-

34. Ad esempio, la corretta gestione delle credenziali di autenticazione, l'attenzione al *phishing* e alle altre tecniche di *social engineering*, la cifratura dei dispositivi, la cancellazione sicura dei dati ecc.

35. In particolare si segnalano le campagne di comunicazione dell'Autorità Garante per la protezione dei dati personali.

36. A. Cavoukian, 2009.

37. Sinteticamente i sette principi fondazionali del suddetto approccio sono: 1. l'essere proattivo non reattivo: la PbD ha come scopo la prevenzione piuttosto che il rimedio; 2. la privacy come impostazione di default, ovvero come regola di base di un sistema IT; 3. la privacy incorporata nella progettazione, cioè integrata nell'architettura dei sistemi informativi; 4. il perseguimento della massima funzionalità, intesa come valore positivo, non valore zero, quindi vantaggioso per tutti; 5. la sicurezza fino alla fine e la piena protezione del ciclo di vita del dato; 6. la visibilità e la trasparenza, dal momento che componenti e operazioni delle tecnologie e delle prassi utilizzate devono sempre essere verificabili; 7. il rispetto per la privacy dell'u-

mento (raccolta, utilizzo, divulgazione e conservazione) dei dati sensibili/identificativi, la separazione tra identificazione e contenuto dei dati personali, l'uso di pseudonimi e di tecniche di anonimizzazione nonché la cancellazione dei dati personali in tempi brevi sono modalità attraverso cui attuare veri e propri meccanismi di prevenzione.

Una considerazione per finire. Attraverso il codice si definiscono le possibilità; il diritto può affidare la tutela dei dati agli strumenti informatici stessi, intervenendo sul design, anche in considerazione della tendenza delle persone a una sovraesposizione "volontaria", e in questo modo contribuire alla costruzione della consapevolezza sociale del grande valore insito nei nostri dati. Per utilizzare ancora una volta le parole di Lessig «*[Il] codice può cambiare perché evolve in modo diverso o perché il governo o il mondo delle imprese lo spingono a evolvere in modo particolare*». D'altra parte la breve analisi delle vulnerabilità dei dati in rete che abbiamo qui proposto rivela che dal codice stesso provengono minacce per la persona; è la "dittatura dell'algoritmo" come sostiene Rodotà, il codice che in maniera sempre più pervasiva e occulta ridefinisce le categorie della realtà e determina la ridistribuzione dei poteri. In questo senso, *trasparenza*, *neutralità* e *apertura* dei dati, del codice, delle architetture – promossi da gran parte della comunità scientifica – sono requisiti importanti anche per la sicurezza informatica, che non può essere garantita dalla segretezza bensì dalla robustezza delle procedure (secondo la metafora della cassaforte trasparente), a tutela delle persone vulnerabili nello spazio virtuale.

RIFERIMENTI BIBLIOGRAFICI

Baldoni Roberto, De Nicola Rocco, a cura di, 2015, *Il Futuro della Cyber Security in Italia, Un libro bianco per raccontare le principali sfide che il nostro Paese dovrà affrontare nei prossimi cinque anni*. Laboratorio Nazionale di Cyber Security, Consorzio Interuniversitario Nazionale per l'Informatica.

Barlow John Perry, 1996, *A Declaration of the Independence of Cyberspace*, in https://www.eff.org/it/cyberspace-independence.

Batini Carlo, Scannapieco Monica, 2008, *La qualità dei dati. Concetti, metodi e tecniche*. Springer-Verlag, Milan.

Brey Philp, 2005, «The Epistemology and Ontology of Human-Computer Interaction». *Minds and Machines*, 15, Springer: 383-98.

Carotti Bruno, 2007, «L'icann e la governance di internet». *Rivista trimestrale di diritto pubblico*, 3: 681-721.

Cavoukian Ann, 2009, *Privacy by Design: Take the Challenge*, in http://www.ipc.

tente e la centralità dell'utente, potenziate seguendo un approccio *user-centred* (Cavoukian, 2010).

on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=856.

Id., 2010, *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*, in http://www.privacybydesign.ca/index.php/paper/implementation-andmapping-of-fair-information-practices/.

Cerf Vinton G., Kahn Robert E., 2004, «A Protocol for Packet Network Intercommunication». In *ieee Transactions on Communications*, Vol. Com-22, 5, May 1974: 638-48.

Colomba Vittorio, 2015, *I diritti nel cyberspazio. Architetture e modelli di regolamentazione*, con un saggio di Lawrence Lessig. Diabasis, Parma.

Finocchiaro Giusella, 2010, «Identità personale (diritto alla)». In *Digesto delle Discipline Privatistiche*, 721-38. Utet, Torino.

Floridi Luciano, 2012, *La rivoluzione dell'informazione*. Codice Edizioni, Torino.

Intel Security, 2015, *The Hidden Data Economy*, in http://www.mcafee.com/us/-resources/reports/rp-hidden-data-economy.pdf.

Kang Jonathan,1999, «Developments in the Law – The law of Cyberspace». *Harvard Law Review*, 112.

Lessig Lawrence, 1996, «The Zones of Cyberspace». *Stanford Law Review*, 48, 5: 1403-11.

Id., 1999, «The Law of the Horse: What Cyberlaw Might Teach». *Harvard Law Review*, 113: 501-46.

Id., ed., 2015, «Il diritto del cavallo». In V. Colomba, *I diritti nel cyberspazio. Architetture e modelli di regolamentazione*. Diabasis, Parma.

Maioli Cesare, 2004, «Introduzione all'informatica forense". In P. Pozzi (a cura di), *La sicurezza preventiva dell'informazione e della comunicazione. Sicurezza delle informazioni*. Franco Angeli, Milano.

Martoni Michele, Palmirani Monica, 2015, «Internet e identità personale». In R. Brighi, S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, 295-308. Aracne, Roma.

Mayer-Schönberger Victor, Cukier Kenneth, 2013, *Big Data*. Hartcourt Publishing Company, New York.

Oddenino Alberto, 2008, *La governance di Internet fra autoregolazione, sovranità statale e diritto internazionale*. Giappichelli, Torino.

Perri Pierluigi, 2016, «Sicurezza giuridica e sicurezza informatica dal D.Lgs. 196/03 al Regolamento generale sulla protezione dei dati». In L. Pelliccioli (a cura di), *La privacy nell'età dell'informazione. Concetti e problemi.* L'ornitorinco, Milano.

Pietropaoli Stefano, 2015, «Chi deve essere il custode della rete? Considerazioni sul problema dell'esercizio del "diritto all'oblio"». In R. Brighi, S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, 545-55. Aracne, Roma.

Pino Giorgio, 2003, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*. Il Mulino, Bologna.

Id., 2010, «L'identità personale». In S. Rodotà, M. Tallachini (a cura di), «Ambiti e fonti del diritto». In *Trattato di Biodiritto*, I: 297-321. Giuffrè, Milano.

Pozzolo Susanna, Verza Annalisa, 2015, *A proposito di identità. Contributi per una riflessione*. Il Mulino, Bologna.
Reidenberg Joel R., 1998, «Lex Informatica: The Formulation of Information Policy Rules Throuhg Technology». *Texas Law Review*, 76: 553.
Resta Giorgio, 2007, «Identità personale e identità digitale». *Il Diritto dell'Informazione e dell'Informatica*, 3: 511-31.
Rodotà Stefano, 2013, *Il diritto di avere diritti*. Laterza, Roma-Bari.
Sartor Giovanni, 2011, «Internet e il diritto». In *Temi di diritto dell'informatica*. Giappichelli, Torino.
Sartor Giovanni *et al.*, a cura di, 2011, *Approaches to Legal Ontologies: Theories, Domains, Methodologies*. Springer, Netherlands.
Van Frassen Baas C., 1985, *L'immagine scientifica*. clueb, Bologna.
Ziccardi Giovanni, 2011, *Hacker. Il richiamo della libertà*. Marsilio, Venezia.