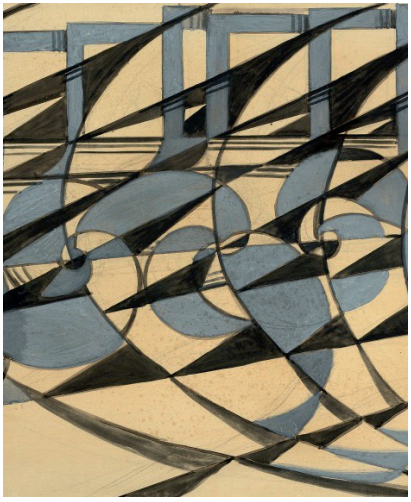
RECTA RATIO
Testi e Studi di Filosofia del Diritto



Agata C. Amato Mangiameli
Maria Novella Campagnoli

Strategie digitali

#diritto_educazione_tecnologie

G. Giappichelli Editore

Recta Ratio

Testi e Studi di Filosofia del Diritto

collana diretta da
Francesco D'Agostino, Francesco Viola
Salvatore Amato e Isabel Trujillo

Settima serie – 134

Procedure di valutazione

Le procedure per la valutazione dei testi ai fini della pubblicazione nella collana "Recta Ratio. Testi e Studi di Filosofia del diritto" si ispirano ai princìpi di trasparenza, autonomia e competenza dei revisori.

I testi presentati devono soddisfare i criteri di rilevanza scientifica del tema, originalità ed innovatività della trattazione, conoscenza della letteratura rilevante, rigore metodologico, approccio critico. La revisione, che dovrà esprimersi su ognuno dei suddetti punti, si conclude con un giudizio complessivo del revisore, che dovrà dichiarare se a suo parere il testo è accettato, accettato previa revisione (da indicare espressamente), non accettato.

Gli autori che desiderano inserire un lavoro in "Recta Ratio" devono inviarne copia ad ambedue i direttori. Questi, con l'ausilio del Comitato scientifico, preliminarmente giudicano dell'ammissibilità del volume proposto per la pubblicazione nella Collana. Se la valutazione è positiva, si procede alla revisione tra pari (*peer review*) secondo il sistema del doppio cieco. Le revisioni devono essere due.

L'assegnazione della revisione è compiuta dai direttori di comune accordo sulla base della competenza nella materia trattata. Almeno una delle due revisioni deve essere effettuata da un competente del settore scientifico degli insegnamenti propri della "filosofia del diritto".

Il volume sarà accettato per la pubblicazione solo se il parere di entrambi i relatori è positivo. Nel caso di discordanza netta sull'accettazione si procederà ad una terza revisione. Nel caso che uno dei revisori sia per l'accettazione senza condizioni e l'altro sia per l'accettazione con modifiche, prevarrà il parere di quest'ultimo. Nel caso che uno dei revisori sia per l'accettazione con modifiche e l'altro per la non accettazione, si procederà ad una terza revisione.

Qualora i revisori richiedano modifiche, i direttori valuteranno se le modifiche richieste siano state adeguatamente recepite.

"Bisogna che sia determinata qual è la retta ragione
e qual è la misura che la definisce"
(Aristotele, *Etica Nicomachea*, 1138b).

Il principio della *recta ratio* ha attraversato la storia del pensiero umano, suscitando reazioni contrastanti. Da criterio di verità delle azioni umane per Aristotele a criterio puramente soggettivo e inesistente in *rerum natura* per Hobbes. In ogni caso, la problematica che esso solleva non può essere elusa o sottovalutata, poiché chiama in causa due dimensioni fondamentali della esperienza umana che costituiscono il nucleo essenziale di riflessione di ogni filosofia pratica.

Innanzi tutto si tratta di sapere quale criterio di misura debba avere l'azione dell'uomo: come si possa distinguere una scelta o una decisione razionale dal mero arbitrio. Se si vuole salvare la comunicazione intersoggettiva e con essa la convivenza sociale, è necessario che vi sia una qualche misura comune della condotta umana, una misura che valga per ogni uomo.

La *recta ratio* non è solo criterio di azione, ma è anche disposizione interiore: è il criterio in rapporto al quale ogni uomo costruisce (o distrugge) la sua identità. Nella tradizione classica, essa, come tale, veniva infatti collegata alla virtù. Anche chi non ama riconoscersi in tale tradizione non può non ammettere che la ragion pratica esige comunque un'attenzione anche per i singoli soggetti e per le situazioni particolari che essi sperimentano. Quali sono le virtù che devono caratterizzare nel mondo di oggi non solo l'operare del giudice e del giurista, ma anche quello del cittadino?

Attraverso indagini scientifiche e materiali didattici, questa collana si propone pertanto di contribuire a rinnovare l'inesauribile ricerca di questa misura comune e di questa disposizione interiore nell'ambito delle regole e delle azioni giuridiche.

In copertina:

G. Balla, *Automobile in corsa* (particolare), 1925.

Agata C. Amato Mangiameli
Maria Novella Campagnoli

Strategie digitali

#diritto_educazione_tecnologie

G. Giappichelli Editore – Torino

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-8833-4

Pubblicato nel mese di aprile 2020
presso la G. Giappichelli Editore – Torino

Indice

pag.

III
Qualche nuovo s/oggetto. Tra algoritmi, intelligenza artificiale, big data

IV
Alcune nuove tecniche di regolazione

pag.

V
Nuove condotte penalmente rilevanti. *La tecnologia alimenta il crimine!*

pag.

PARTE II

EDUCARE *CON* LE NUOVE TECNOLOGIE

Maria Novella Campagnoli

pag.

Materiali normativi

Premessa

Viviamo in quella che viene definita come la quarta rivoluzione della comunicazione: device e app di ogni genere accompagnano e facilitano le nostre attività quotidiane (non solo quelle personali ma anche quelle professionali), nuove piattaforme e nuovi network ci permettono di sviluppare inedite forme di socialità e di condivisione e, nel frattempo, i nostri dati vengono profilati, trattati e ricombinati di continuo.

Nuove opportunità si dischiudono e nuovi rischi emergono, minacciando i diritti (fra tutti quello alla privacy) e sollecitando più efficaci garanzie, anche e soprattutto a tutela dei più giovani, i c.d. nativi digitali, che, pur, familiarizzando facilmente con le diverse tecnologie, non sempre ne comprendono appieno le implicazioni giuridiche.

Di qui, la necessità e l'urgenza di riflettere sul complesso rapporto fra diritto, educazione e tecnologia, nella consapevolezza che, se, da un lato, è opportuno educare *alle* nuove tecnologie, favorendone un uso sicuro, da un altro lato, è opportuno educare *con* le nuove tecnologie, avvalendosi di tecniche multimediali e di supporti interattivi.

Alternando contributi inediti e altri già pubblicati ma comunque aggiornati e rivisitati, *Strategie digitali. #diritto_educazione_tecnologie* risponde proprio a questa duplice esigenza: quella di promuovere un approccio critico alle nuove tecnologie e, al contempo, quella di incentivarne la diffusione a sostegno della didattica, anche alla luce di quanto è stato recentemente stabilito dal *Piano Nazionale Scuola Digitale* e dal decreto n. 616 del 10 agosto 2017 recante *Modalità acquisizione dei crediti formativi universitari e accademici di cui all'art. 5 del decreto legislativo 13 aprile 2017 n. 59*.

In sintonia con quel campo di studi, ricerche e insegnamenti nati dall'unione di discipline umanistiche e informatiche (*Huma-*

nities Computing o *Digital Humanities*), il volume offre agli studenti universitari, agli specializzandi, ai futuri docenti – e in generale a chiunque si occupi a vario titolo di informatica, diritto e scienze sociali – una lettura del digitale e di quel cyberspace, che, a suo modo, ripropone la metafora delle tre sedie: *una per la solitudine, due per l'amicizia, tre per la compagnia*.

Agata C. Amato Mangiameli
Maria Novella Campagnoli

Roma "Tor Vergata", 21 novembre 2019

PARTE I

EDUCARE *ALLE* NUOVE TECNOLOGIE

Agata C. Amato Mangiameli

I

UN NUOVO SPAZIO. IL CYBERSPACE

Sommario

1. De-territorializzazione, de-centralizzazione, data-veglianza

L'attuale invenzione tecnica non si limita a produrre artefatti (strumenti) in grado di far risparmiare tempo e energia, ma va oltre: elabora finalità inedite fortemente segnate dai nuovi spazi dell'informazione, sempre più virtuali. Partecipa dunque della creazione di nuovi scopi e raggiunge lo stadio retorico, che, in quanto tale, schiude il virtuale come mondo autonomo e favorisce differenti modalità di conoscenza, con propri stili, criteri di valutazione e valori.

I processi in atto sono ampiamente noti: per un verso, de-territorializzazione e de-centralizzazzione, per l'altro, data-veglianza.

1.1. De-territorializzazione anziché territorializzazione. Il moderno ritrova nel *bodenhafter Urgrund* la radice di ogni diritto ed è il territorio l'elemento caratterizzante – accanto agli altri (popolo e sovranità) – dello Stato [1]. Il contemporaneo, invece, riduce dra-

[1] L'occupazione di terra costituisce all'esterno (nei confronti di altri popoli) e all'interno (rispetto all'ordinamento del suolo e della proprietà en-

sticamente l'importanza dell'elemento geografico. La comunità è senza un luogo di riferimento stabile [2], l'uomo, d'altra parte, è il nomade che vive assumendo sulla terra il nome di *microcosmos*, sul territorio quello di *micropolis*, nello spazio commerciale quello di *micro oikos*, e

"nello Spazio del sapere – scrive Lévy – l'umano si restringe ancora di più: è solo un cervello. Anche il suo corpo diventa un sistema cognitivo. Il cervello entra in contatto e si unisce ad altri cervelli, attraverso sistemi di segni, linguaggi e tecnologie intellettuali, partecipa a comunità pensanti che esplorano e creano mondi plurali. Allora il cervello dell'*homo sapiens sapiens* si trasforma, mostra il proprio volto e si converte in policosmo" [3].

Più in particolare, nel *cyberspace*, diversamente da quel che accade nell'ordinamento spaziale concreto, la paradossale dialettica del rapporto inclusione-esclusione-reclusione [4] non si dà, sia perché il virtuale rende fluida ogni differenza e sposta i problemi in non-luoghi globali, sia perché esso irradia una forza che abbraccia tutto, in modo che *everyone and everything is on the net* [5]. Ogni differenza precostituita è superata, ogni limite predeterminato è risolto, ogni prigione in quanto circoscrizione è abbattuta.

---

tro un territorio) "l'archetipo di un processo giuridico costitutivo". È quindi a presupposto non solo del "diritto territoriale e successione nel territorio", dell'"esercito e milizia territoriale", ma anche della stessa dicotomia diritto privato-diritto pubblico. Lo Stato moderno, poi, rispetto ad altre unità politiche "forma sulle fondamenta dell'unità politica interna da esso realizzata una superficie territoriale conchiusa, delimitata verso l'esterno da confini precisi e capace di regolare in modo specifico i rapporti esterni con altri ordinamenti territoriali similmente organizzati" (C. SCHMITT, *Il nomos della terra. Nel diritto internazionale dello "jus publicum europaeum"*, trad. it., Milano, Adelphi, 1991, in part. pp. 24-26 e p. 145).

[2] Ogni fenomeno di virtualizzazione conduce – secondo Michel SERRES – a un "fuori dal *ci*" che, tuttavia, non impedisce affatto di *esistere*: *Atlas*, Paris, Éditions Julliard, 1994.

[3] *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milano, Feltrinelli, 1996, p. 159.

[4] Sulla cattiva tendenza a escludere v. le importanti note di J. KRISTEVA, *Stranieri a se stessi*, trad. it., Milano, Feltrinelli, 1990.

[5] W.R. JOHNSON, *Anything, anywhere, anytime: The future of networking*, in D. LEEBAERT (ed.), *Technology 2001: The future of computing and communications*, Cambridge (Mass.), MIT Press, 1992, p. 150 ss.

Ma è proprio vero che nel mondo cibernetico, grazie a nuovi concetti e alle nuove dinamiche filtrate dalla matrice informatica, non si dà esclusione alcuna e che, anzi, in Rete è garantita a tutti la stessa libertà?

A ben vedere, il problema non è costituito tanto dal rischio che Internet divida il mondo in caste e generi tecno-esclusione [6], quanto dalle stesse implicazioni della de-territorializzazione. Infatti, l'annullamento delle distanze spazio-temporali emancipa alcuni dai vincoli territoriali, liberandoli dagli ostacoli di carattere fisico. Altri, all'opposto, restano relegati in un territorio che ha ormai perso di significato e che non è in grado di attribuire alcuna identità. Se le distanze non significano più nulla, le località rimaste sono anch'esse senza senso e chi vi abita è condannato all'insignificanza:

"l'unica località che gli appartiene e (abita) gli sta sparendo di sotto i piedi" [7].

Al di là della questione, è necessario sottolineare che la quarta rivoluzione della comunicazione, diversamente dalle altre [8], ha un *feedback* particolare, non giunge a noi da un nostro simile, bensì da una macchina o tramite una macchina che opera sostanziali trasformazioni sui messaggi umani [9].

---

[6] Può pure accadere e tuttavia non è detto che la tecno-esclusione non possa essere superata nel futuro. Le condizioni sono che si insegni a scuola "a programmare, e non soltanto a utilizzare i programmi" e che il cittadino della società globale segua il modello San Paolo: "nato in Turchia da una famiglia ebrea di lingua greca, leggeva la Torah in ebraico; poi è vissuto a Gerusalemme, dove parlava l'aramaico. A chi gli chiedeva il passaporto, rispondeva in latino *civis romanus sum*" (attuali le considerazioni di U. ECO, *La cultura corre on line chi non si adegua è perduto. "Come evitare che Internet divida il mondo in caste"*, in *La Repubblica*, 8 gennaio 2000, p. 13).

[7] Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, trad. it., Roma-Bari, Laterza, 1999, in part. p. 22.

[8] Lo sviluppo del *linguaggio*, l'affermarsi della *scrittura*, l'invenzione della *stampa*: si veda l'ormai classico E.A. HAVELOCK, *Cultura orale e civiltà della scrittura. Da Omero a Platone*, trad. it., Roma-Bari, Laterza, 1999; e E. EISENSTEIN, *Rivoluzione inavvertita. La stampa come fattore di mutamento*, trad. it., Bologna, Il Mulino, 1986.

[9] Come evidenzia Tibor VAMOS, *Epistemologia del computer. Le possibilità dell'impossibile. Vecchie idee mescolate a nuove*, trad. it., Milano, Sperling & Kupfer, 1993.

1.2. De-centralizzazione piuttosto che centralizzazione. La caratteristica prima della Rete [10] è l'essere senza un centro e una periferia. Altrimenti detto, il flusso digitale non conosce gerarchie e in un certo senso neppure centri di supervisione (diretta, come quella esercitata nei luoghi di lavoro, nelle scuole, negli ospedali, nelle caserme, nelle prigioni, o indiretta, ovvero quella che si compie tramite l'accumulazione di informazioni codificate) [11].

L'ipertesto, ad esempio, non rinvia a gerarchie di significati, emerge anzi da pertinenze locali ed è il punto d'incontro di un piano semiotico de-territorializzato con una "direttrice di efficacia o di piacere". Così, anziché

> "essere interessato a cosa abbia pensato un autore introvabile, chiedo al testo di far pensare me [...]. La virtualità del testo alimenta la mia intelligenza in atto" [12],

la Rete potenzia il mio pensiero, qui e ora, e con esso svuota di contenuto qualsiasi schema gerarchico, generatore come si usa dire di potere e di controllo. Del resto, se tutto è centro (e/o tutto è periferia), non ha senso chiedersi dove si trovi la sede deputata a gestire i flussi comunicativi, né domandarsi chi coordini gerarchicamente l'uso dei database.

Hypertest Web è la più importante espressione per indicare condivisione, collaborazione, socialità, tra pari: una innovazione sociale, quindi, e non mera innovazione tecnica. Il fine è chiaro,

---

[10] La "rete infinita, dove ogni punto può connettersi a ogni altro punto e la successione delle connessioni non ha termine teorico, perché non vi è un esterno e un interno: in altri termini, il rizoma può proliferare all'infinito" (così scriveva U. ECO nella *Prefazione* a P. SANTARCANGELI, *Il libro dei labirinti. Storia di un mito e di un simbolo*, Milano, Sperling & Kupfer, 1984, X). Sul rizoma ovvio il rinvio a G. DELEUZE, F. GUATTARI, *L'anti-Edipo*, trad. it., Torino, Einaudi, 1975; *Rizoma*, trad. it., Parma-Lucca, Pratiche, 1977; *Millepiani: capitalismo e schizofrenia*, trad. it., Roma, Istituto Enciclopedia Italiana, 1987.

[11] La sorveglianza, quale supervisione sulle attività della popolazione, è una delle dimensioni caratterizzanti la prima modernità, modernità che, in A. GIDDENS, si radicalizza e produce disaggregazione (*disembedding*), diventa cioè una tarda-modernità (piuttosto che *post*-) dei sistemi esperti (*Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo*, trad. it., Bologna, Il Mulino, 1994).

[12] P. LÉVY, *Il virtuale*, trad. it., Milano, Raffaello Cortina, 1997, in part. pp. 39-40.

altrettanto chiaro è il terreno di scontro. Per Tim Berners-Lee [13] del *World Wide Web* si tratta di un nuovo sistema che permette il collegamento tra sistemi esistenti senza alcun controllo o coordinamento centrale. Non è detto, però, che la de-centralizzazione sia reale, assai spesso è un mito, visto che le norme sono imposte da qualche autorità (globale) e i protocolli IP sono definiti in una *Request for comments*. Di qui la necessità del Web semantico, che si ottiene eliminando i concetti centralizzati di verità assoluta e ponendosi nell'ottica e con il fine di una conoscenza limitata, anziché conoscenza e verificabilità totali [14]. Il fine è nobile: il libero scambio dei meta-dati fra le parti; l'auspicio è condivisibile: il Web libero da vincoli di un'autorità centrale; la realizzazione è però quanto mai ardua: lo straordinario rovesciamento delle parti (ad esempio, autore/lettore, attore/spettatore), la significativa mescolanza di esperti e profani, la sorprendente ricchezza di meta-dati, non è detto che rendano gli utenti autonomi nella navigazione e liberi di decidere quale tipo di informazione sia più appropriata e opportuna.

1.3. Data-veglianza piuttosto che sorveglianza. Ora il controllo è continuo, automatico, involontario: caratteri questi normalmente riferibili a sistemi astratti, a sistemi con capacità auto-rafforzante e ubiquitaria [15]. La data-veglianza è più forte e diretta, poiché si tratta del

"*systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*" [16].

Lo sviluppo degli algoritmi predittivi è legato a doppio filo con la data-veglianza, individuale o di massa. Si pensi all'analisi predittiva in criminologia. C'è un software, CRUSH (*Criminal Re-*

---

[13] *The World Wide Web – Past, present and future* (1996) – (https:// journals.tdl.org/jodi/index.php/jodi/article/ view/3 /3#past).

[14] T. BERNERS-LEE, *L'architettura del nuovo web. Dall'inventore della rete il progetto di una comunicazione democratica, interattiva e intercreativa*, Milano, Feltrinelli, 2001.

[15] J. ELLUL, *La tecnica rischio del secolo*, trad. it., Milano, Giuffrè, 1969.

[16] L'espressione e la definizione risalgono a R. CLARKE, *Information technology and dataveillance*, in *Communications of the ACM*, 31, 5, 1988 (http:// www.rogerclarke.com/DV/CACM88.html).

duction Utilizing Statistical History), in grado di predire l'azione criminale, combinando analisi statistiche, profili, atteggiamenti, precedenti, luoghi, e ancora tanto altro. È già usato in alcuni Stati e con effetti di riduzione dei crimini soprattutto violenti. Si pensi all'analisi dei comportamenti sociali e alle tecniche della scienza sociale computazionale. Ci sono a tal riguardo algoritmi di vario tipo. Soltanto alcuni: *PageRank*, ovvero serie di calcoli matematici che selezionano le pagine che devono essere mostrate per prime nella ricerca su Google; *Adwords*, algoritmo che decide quali annunci pubblicare in base a scansioni delle e-mail, delle pagine visitate, dei propri interessi, dei servizi più utilizzati; l'algoritmo del *News Feed* di Facebook che gestisce i flussi delle storie infinite classificando le condivisioni più importanti/meno importanti e che è in continuo aggiornamento (con il consueto annuncio: *Building a Better News Feed for You*), pare proprio contro il *clickbait*, e cioè la condivisione ingannevole.

Diversamente dalle metafore del Panopticon e del Grande Fratello – che hanno come referente un potere coercitivo centrale –, l'odierna sorveglianza prende forma nei c.d. non-luoghi informatici, all'interno dei quali le informazioni, di continuo introdotte, diventano la contingente misura di tutte le cose. Si tratta di non-luoghi in cui i dati automaticamente assemblati vincolano tutti e tutto, dove i risultati mutano involontariamente le entità, i significati e le vite su scala globale. I non-luoghi informatici non offrono riparo da chi ci osserva, né un bastione attorno al quale organizzare una possibile linea di difesa.

Al Panopticon si sostituisce il *Synopticon*:

"l'atto di guardare svincola chi guarda dalla propria localizzazione, e lo trasporta almeno spiritualmente nel ciberspazio, dove la distanza non conta più, anche se, fisicamente, non ci si è mossi. Non conta più se gli oggetti del Synopticon, trasformati ora da guardati in guardanti, si muovono o stanno fermi. Dovunque siano e dovunque vadano, essi possono collegarsi – e lo fanno – alla Rete extraterritoriale che permette ai molti di guardare i pochi. Il Panopticon costringeva la gente a una posizione in cui poteva essere guardata. Il Synopticon non ha bisogno di costringere nessuno, seduce la gente perché guardi" [17].

[17] Così Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, cit., pp. 59-60.

Nel cyberspace si producono delle dinamiche inedite, frutto di ricordi che si estendono nel tempo e nello spazio [18], di linee di confine che si riorganizzano casualmente e di continue trasformazioni secondo criteri non gerarchici. Nel cyberspace la gente è invitata a osservare e a spiare dalla sua postazione, trasformandosi da sorvegliato in sorvegliante.

È certo un'idea di sorveglianza riveduta e corretta in base ai mezzi adoperati [19], che pone diversi interrogativi e richiede criteri di resistenza. Le contemporanee pratiche di sorveglianza si avvalgono di sistemi parecchio sofisticati, in grado di mettere insieme in tempo reale le tantissime tracce che per qualche motivo si ritrovano nelle schede di alcuni computer e al contempo di incrociare la mole di dati provenienti da varie fonti e raccolti per i più disparati motivi e per una serie di ragioni più o meno importanti [20].

Anche nei luoghi di lavoro la sorveglianza è (può essere) potenziata. Grazie ai (o a causa dei) sistemi informatici, si pensi alle varie forme di pedinamento elettronico, il lavoratore può diventare per dir così trasparente. L'ufficio centrale comunica online per tutta la durata dell'attività lavorativa: interagisce così con le unità periferiche, invia direttive, istruzioni, e al contempo vigila che i tempi siano rispettati, che il lavoratore sia collegato e che soprattutto non sia distratto da eventi diversi ed esterni. L'interazione apre nuove e importanti prospettive, e quel che più conta coglie ogni irregolarità. Il controllo si trasforma: da eventuale in strutturale.

---

[18] Come notava già diverso tempo fa G.T. MARX, *Undercover: Police surveillance in America*, Berkeley, University of California Press, 1989; si veda pure ID., *The case of the omniscient organization*, in *Harward business review*, marzo-aprile 1990, p. 4 ss.

[19] Una sorveglianza comunque affinata dalla macchina ultra-intelligente, verso cui KELLY invitava a non fare alcuna battaglia di retroguardia: la tecnologia compirà un grande passo, quello cioè di produrre macchine capaci di auto-adattarsi e di evolvere secondo una propria direzione, senza alcuna supervisione umana. Dare quindi alle macchine la 'libertà' è l'unico modo per noi di esercitare un 'controllo intelligente'. Il poco tempo che ci rimane in questo secolo deve essere allora un tempo di preparazione al principale compito psicologico che ci rimane nel XXI secolo: quello di lasciare perdere con dignità (*Out of control: The new biology of machines, social systems and the economic world*, Reading (Mass.), Addison Wesley, 1994).

[20] Cfr. D. LYON, *L'occhio elettronico. Privacy e filosofia della sorveglianza*, trad. it., Milano, Feltrinelli, 1997.

2. Intermezzo: cyberspace e ordine spontaneo

Con cyberspace si intende l'ambiente virtuale interattivo generato dal computer. Navigare in Internet significa soprattutto frequentare il ciberspazio, la cui natura è comunicativa e non-territoriale. Lo dimostra già l'analogia con l'oceano: l'assenza dell'elemento territoriale fa sì che vi siano naviganti (*net-surfer*) e che solo il *surfing*, cioè la navigazione senza una meta ben precisa, si adatti alle esigenze della Rete. Navigare il World Wide Web significa utilizzare un ipertesto spostandosi (grazie a *browser*: Google Chrome, Mozilla Firefox, Microsoft Internet Explorer, Apple Safari, Opera, Microsoft Edge, Maxthon, Flock, Avant, Deepnet Explorer, Phase Out) da un sito virtuale all'altro, semplicemente cliccando su icone o su parole (*hot spots*).

Il cibernauta dispone di una serie di scatole cinesi informatiche, tendenzialmente infinite, perché senza limiti è la realtà oltre lo schermo, la realtà di questo nuovo universo parallelo creato e alimentato dalle reti globali di comunicazione via computer; e per entrarvi esistono varie società (*provider*), distinte dal tipo d'offerta: qualche volta offrono la sola connettività (*access provider*), altre volte anche servizi (*service provider*). Ma il cibernauta dispone soprattutto di nuove velocità, che non hanno a che vedere con il tempo lento e differito che il territorio porta con sé. Se, infatti, lo spazio-territorio ha inaugurato un tempo-prima e un tempo-dopo la fondazione, la delimitazione, la recinzione, il confine tra esterno e interno; nello spazio-movimento del ciberspazio, il tempo è scandito dall'accelerazione e dall'ubiquità dei contatti, ormai tutti all'interno dei circuiti propri dello spazio virtuale.

La Rete crea contatti istantanei e sorvola ogni confine. È tutt'uno con l'immediatezza che piccoli o grandi mezzi (dalle postazioni elettroniche di vario tipo ai *wearable computer*) generano, intensificano, perpetuano. Entità mobili all'interno di altre combinano le loro velocità, si scambiano i messaggi e le informazioni, si intersecano in uno spazio mobile, in cui tutto cambia rispetto a tutto e in cui la distanza non è niente e la velocità è tutto.

2.1. De-territorializzazione, de-centralizzazione e accelerazione richiamano l'idea di ordine spontaneo. Nel cyberspace, infatti, l'ordine può avere origine solo endogene, e non esogene, si auto-genera, non è creato né diretto dall'alto, è dunque spontaneo.

È indispensabile così capire la differenza che passa tra l'ordine costruito e l'ordine spontaneo, poiché soltanto allora, comprendendo cioè le regole che governano un ordine spontaneo, è possibile individuare le regole di tutti i sistemi che si auto-organizzano e auto-generano.

Il rinvio all'opera di Friedrich August von Hayek è qui ovvio. Diversamente dall'ordine costruito (*taxis*), l'ordine formatosi spontaneamente (*cosmos*) può possedere qualsiasi grado di complessità, può essere fondato su relazioni puramente astratte, può anche non avere alcuno scopo. Questo significa innanzitutto: il potere di controllo esercitato su un ordine esteso e più complesso è minore rispetto al grado di controllo che si può avere su un ordine deliberatamente costruito. Molti aspetti dell'ordine spontaneo sfuggono al controllo e quando si interviene si provocano delle interferenze, e persino degli ostacoli, nel gioco delle forze che producono l'ordine spontaneo medesimo. Il tipo di potere che possediamo

"sopra una sistemazione concreta, o *taxis*, non lo possediamo sopra un ordine spontaneo, di cui conosciamo, e siamo in grado di influenzare, solo gli aspetti astratti" [21].

In secondo luogo, si deve osservare che l'ordine spontaneo – in quanto astratto – può continuare ad esistere anche quando mutano tutti gli elementi particolari che lo costituiscono. Tutto quel che si richiede, per preservare l'ordine astratto, è che sia mantenuta una certa struttura di relazioni, o che elementi di un certo tipo continuino a essere correlati in un certo modo. Per il fatto, poi, che l'ordine è spontaneo – e quindi non è creato da un ente esterno –, esso può anche non avere alcuno scopo particolare, sebbene la consapevolezza della sua esistenza può essere estremamente importante rispetto alla grande varietà di scopi che noi intendiamo perseguire. Detto altrimenti: l'ordine spontaneo può tornare molto utile agli individui che agiscono al suo interno, e ciò implica che gli individui con le loro azioni siano interessati al mantenimento dell'ordine medesimo, nonostante non

[21] *Legge, legislazione e libertà. Una nuova enunciazione dei principi liberali della giustizia e della economia politica*, trad. it., Milano, Il Saggiatore, 1986, p. 57.

siano in grado di padroneggiarlo intellettualmente o di sistemarlo deliberatamente. Degli ordini spontanei, infatti, si conoscono soltanto alcune regole alle quali obbediscono gli elementi di vario genere e non si conoscono invece tutti gli elementi individuali e tutte le circostanze particolari che concorrono alla formazione dell'ordine. In breve:

"la nostra conoscenza sarà ristretta al carattere generale dell'ordine che ne risulterà [...] [e] saremo in grado di influenzare solo il carattere generale, e non anche i dettagli, dell'ordine che ne risulta" [22].

Questo significa che le regole generali di diritto, su cui si basa un ordine spontaneo, tendono verso un ordine astratto, il cui contenuto particolare o concreto non è conosciuto o previsto da alcuno. Si tratta di regole e non di comandi: regole che devono essere indipendenti da un qualsiasi scopo, che devono essere indirizzate a intere classi di membri non individualmente designati, e che non da ultimo devono essere applicabili a un numero ignoto e indeterminato di persone e di situazioni.

Significativa è a tal proposito la struttura della società moderna. Le regole che hanno reso possibile la sua crescita non furono progettate all'inizio con l'intento di raggiungere tale risultato, giacché è tipico dell'ordine spontaneo il fatto di non essere pianificato deliberatamente e di non perseguire fini individuati da particolari comandi. Ciò che distingue l'ordine formatosi spontaneamente dall'ordine costruito, cioè dall'organizzazione, è il fatto che il primo può preservarsi soltanto in modo indiretto, e cioè rafforzando e implementando le regole che conducono alla formazione di un ordine spontaneo, piuttosto che attraverso il metodo di dirigerne i membri. Il tentativo di utilizzare gli elementi dell'organizzazione, e con essi i possibili interventi (interferenze) nell'ordine spontaneo, oltre a basarsi su un totale fraintendimento, non può mai considerarsi razionale. Scrive von Hayek:

"mentre è possibile far intervenire delle regole sussidiarie in appoggio ai comandi che determinano un'organizzazione, e utilizzare le organizzazioni come elementi di un ordine spontaneo, non può mai essere van-

[22] *Ivi*, pp. 53 e 56.

taggioso integrare le regole che governano un ordine spontaneo mediante dei comandi isolati e sussidiari concernenti quelle attività in cui le azioni sono guidate da regole generali di condotta" [23].

Ora, al di là della ricostruzione di von Hayek, anche il cyberspace costituisce, a suo modo, un ordine spontaneo e come tutti gli ordini formatisi spontaneamente necessita di regole, anziché di comandi. Necessita quindi di regole, alle quali gli individui – pur nel perseguimento dei loro fini temporanei, particolari e qualche volta ancora sconosciuti – sono soggetti, perché preservano permanentemente l'ordine astratto e rappresentano i 'valori ultimi comuni' [24].

Sotto questo profilo, il cyberspace può costituire l'input per una rinnovata ricerca del diritto e proprio a partire dalle distinzioni ordine spontaneo(*cosmos*)/ordine creato(*taxis*), regole di condotta generali ed astratte (del primo)/comandi particolari (del secondo). D'altra parte, se il cyberspace è *cosmos*, il diritto non può essere ridotto all'insieme di leggi prodotte dalla libera volontà di un legislatore. Per di più

"il diritto è esistito per molte epoche prima che all'uomo venisse in mente di poterlo creare o modificare" [25].

E nel ciberspazio mal si adeguano le interpretazioni e applicazioni delle regole da parte di giuristi diventati

"in quanto al servizio di una concezione generale che essi stessi non hanno creato, gli strumenti non di principi di giustizia, ma di un apparato in cui l'individuo deve servire i fini dei suoi legislatori" [26].

---

[23] *Ivi*, pp. 65-66.

[24] *Ivi*, in part. pp. 200-202.

[25] *Ivi*, p. 95.

[26] *Ivi*, in part. p. 87.

3. Cyberspace e identità. Una macchina *per l'intimità* e un nuovo totem

Il cyberspace, nei cui corridoi si esalta la libertà fisica puramente spettacolare, cinesteticamente eccitante, e che dà le vertigini [27], riconfigura identità individuali e collettive.

Si ricorre, infatti, sempre più spesso al computer per esperienze e avventure che interagiscono con il nostro modo di pensare (e di esprimersi), modificano le nostre emozioni, influenzano le nostre vite sociali. Ormai si usa dire: diventato una 'macchina per l'intimità' [28], in luogo del semplice motore analitico di Charles Babbage [29], il computer non fa più qualcosa *per* noi, bensì lo fa *a* noi. L'ego, i ruoli e le funzioni hanno nelle comunità virtuali una nuova esistenza [30].

Nella nascente cultura della simulazione, e più in particolare nei MUD (*Multi-User Domains*) e nelle BBS (*Bulletin Board System*) [31], le persone scoprono la vita mentale che esiste oltre la fisicità. Si avventurano in giochi di ruolo o in mondi della fantasia, incontrando amici e amanti virtuali, solo attraverso l'interazione con la tecnologia [32].

Non può quindi sorprendere se il tempo trascorso *con il* e *nel* computer offra un nuovo campo di creatività, di apertura sul mondo, di identità. Devono così essere rinegoziati i confini tra natura e tecnologia, tra reale e virtuale, tra animato e inanimato, tra

---

[27] Così D. TOMAS, *The technophilic body: on technicity in William Gibson's cyborg culture*, in *New Formations*, 8, primavera 1989, p. 113 ss.

[28] Sul punto v. S. TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, trad. it., Milano, Apogeo, 1997.

[29] Col potere di combinare insieme simboli generici, in successioni di tipi e dimensioni illimitate (A. LOVELACE, *Sketch of the analytical engine invented by Charles Babbage*, in P. MORRISON, E. MORRISON (eds.), *Charles Babbage and his calculating engines*, New York, Dover Publications, 1961, in part. p. 252).

[30] F. DI SPIRITO, P. ORTOLEVA, C. OTTAVIANO (a cura di), *Lo strabismo telematico: contraddizioni e tendenze della società dell'informazione*, Torino, Utet, 1996.

[31] B. MARTENS, B. WISER, *GBBS Pro Bulletin Board System*, Hardcover, Lulu.com, 2017; L.M. SURHONE, M.T. TIMPLEDON, S.F. MARSEKEN (eds.), *Waffle (BBS Software): Bulletin Board System, Soylent Communications, DOS, UNIX, UUCP, Usenet, Fidonet*, Beau Bassin, Betascript Publishing, 2010.

[32] Vedi J.W. DECEW, *In pursuit of privacy. Law, Ethics and the Rise of Technology*, London, Cornoll University Press, 1997.

io unitario e io multiplo. E persino i corpi [33], disincarnati e poi reincarnati nel personaggio policromo e sfaccettato del 'cowboy della consolle' [34], subiscono processi di trasposizione nella nuova economia delle personificazioni artificiali [35].

Al di là delle rappresentazioni fantascientifiche della letteratura cyberpunk, è certamente pensabile un uso dell'ambiente virtuale interattivo del ciberspazio come spazio per la crescita dell'identità, sia individuale che collettiva.

La prima, infatti, nel passaggio dal reale al virtuale e poi di nuovo dal virtuale al reale, risulterebbe meglio attrezzata per capire gli artifici e per guarire della propria incompletezza [36]. Se l'io del virtuale è flessibile e molteplice, se dietro lo schermo del computer si scoprono *molti sé*, una comprensione profonda dell'identità nella vita reale passa anche attraverso il sé (i molti sé) online.

La seconda, l'identità collettiva per l'appunto, goderebbe dei risultati che la civiltà telematica apporta sulle modalità di partecipazione e rappresentanza politica. Con slogan ad effetto si dice: né masse, né élite; né cittadini, né stranieri. Il villaggio globale destrutturerebbe costruzioni storicamente opprimenti, per

---

[33] Basti pensare ai corpi virtuali della diagnostica e della chirurgia medica, o al nuovo e più complesso rapporto naturale-artificiale. Utili indicazioni in P.L. CAPUCCI (a cura di), *Il corpo tecnologico. L'influenza delle tecnologie sul corpo e sulle sue facoltà*, Bologna, Baskerville, 1993. Più in particolare, su virtualizzazione e moltiplicazione del corpo, v. F. DAGOGNET, *Le corps multiple et un*, Le Plessis-Robinson, Synthélabo, 1992, e *La peau découverte*, Le Plessis-Robinson, Synthélabo, 1993. Sull'opzione artificialista e sull'identificazione io/cyborg, cfr. innanzitutto D.J. HARAWAY, *Manifesto Cyborg. Donne, tecnologie e biopolitiche del corpo*, trad. it., Milano, Feltrinelli, 1995.

[34] V. SOBCHACK, *Screening Space: The american science fiction film*, New York, Rutgers Unuversity Press, 1987; cfr. pure ID., *The scene of the screen: toward a phenomenology of cinematic and electronic "presence"*, in H.V. GUMBRECT, L.K. PFEIFFER (Hrsg.), *Materialität der Kommunikation*, Frankfurt a. M., Suhrkamp, 1988.

[35] Così, ad esempio, sesso e desiderio vengono a loro volta riconfigurati in termini di larghezza di banda e di differenza interna. Altrimenti detto: il cibernauta, sollevato dalla prigione del corpo, "deride la carne" e i segreti recessi delle carezze si trasformano in "lampi guizzanti" che proiettano "ombre abbracciate sul muro del bunker" (questa la conclusione di W. GIBSON nel romanzo *Neuromante*, trad. it., Milano, Nord Edizioni, 1991).

[36] Sugli effetti soggettivi della presenza del computer ne accennava già nel 1984 S. TURKLE: *Il secondo io. Il computer e l'uomo: convivere, amarsi, capirsi*, trad. it., Milano, Frassinelli, 1985.

rimpiazzarle con nuovi modelli più attenti alla molteplicità e varietà. In altri termini: più attenti alla democrazia e assolutamente distanti dal dispotismo del sistema della 'delega'.

Le comunità della Rete rivitalizzano per dir così la piazza ateniese. Se in Rete, se attraverso l'interfaccia grafica, ciascuno discute di ogni argomento, tutti deliberano e tutti votano a colpi di mouse, non ha più senso proprio l'intermediazione rappresentativa dello Stato-nazione. Peraltro, il diritto di cittadinanza nella comune telematica non soffre delle limitazioni, a volte intollerabili, della nazionalità, della razza, del genere e della religione.

Si aprono quindi nuove e insospettate prospettive, che con energia mettono in crisi una parte considerevole dei tradizionali modelli culturali e dei rapporti sociali. Basti qui rinviare alla mescolanza pubblico e privato – o come si usa ormai dire alla creazione di 'menti collettive' e alla 'individualizzazione di spazi pubblici di informazione' [37] – per poter intuire come le descrizioni e interpretazioni del piccolo mondo pre-digitale e quelle della globalizzazione digitale si incrocino, si sovrappongano e assai spesso entrino in aperto contrasto.

3.1. Non stupiscano gli accostamenti qui di seguito: il reale evoca il *faccia a faccia*, il virtuale, al contrario, esalta l'*interfaccia*. Lì è il volto (i volti), dai contorni netti. Qui sono le immagini, le *quasi-presenze*, dai confini sempre labili. E se il volto, prima ancora di ogni forma di conoscenza e di rapporto, si manifesta quale centro di alterità [38], il corpo virtuale invece è sempre un continuo divenire altro, dove altro è solo reinventato, reincarnato, moltiplicato, vettorializzato e deterritorializzato.

L'identità e l'alterità per così dire tradizionali sono messe a dura prova. Pensate a partire da definizioni e determinazioni, inclusioni ed esclusioni, devono ora aprirsi ai nuovi ambiti di interazione, alle inedite cronologie e a limiti mai tracciati in modo

---

[37] P. LÉVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, cit.

[38] Basti pensare alle suggestive meditazioni di LEVINAS (*Totalità e infinito. Saggio sull'esteriorità*, trad. it., Milano, Jaca Book, 1982, in part. p. 191 ss.) sul volto da guardare, da rispettare, da accarezzare. Sull'etica dei volti, sull'esteriorizzazione dell'uomo e sulla scelta tecnologica, v. le lucide osservazioni di I. MANCINI, *L'uomo è ancora di moda?*, in AA.VV., *La vicenda uomo tra coscienza e computer*, Assisi, Cittadella Editrice, 1985, p. 39 ss.

definito. I limiti, ad esempio, tra l'eterogenesi e l'alienazione, tra l'attualizzazione e la reificazione, tra la virtualizzazione e l'amputazione.

La virtualizzazione proprio perché tale sposta l'accento ontologico dalla soluzione al problema. L'entità virtuale trova la propria consistenza essenziale in un campo problematico, dove i confini non sono più ovvi, i luoghi e i tempi si mescolano, e tra interno ed esterno vi è un incessante passaggio. Altrimenti detto, la virtualizzazione

"fluidifica le differenze istituite, aumenta i gradi di libertà, fa del vuoto che scava un elemento motore" [39].

Per persuadersi di quanto problematica sia, ad esempio, l'identità nel mondo delle nuove tecnologie, è sufficiente qui rinviare alla psicologia delle c.d. amicizie digitali. I legami stretti peregrinando da un sito all'altro subiscono delle accelerazioni turbo ed evitano le tante possibili censure.

Nel buio del ciberspazio, affrancati dal quotidiano e da condotte convenzionali, ognuno diventa audace. Le colonie elettroniche riuniscono *intimi sconosciuti* [40] che condividono stesse passioni e stessi interessi, e che – proprio perché sconosciuti, se non anche travestiti – si sentono liberi di esprimere le proprie opinioni, di non tacere le proprie passioni, di abbandonarsi ad emozioni altrimenti ritenute ardue. La realtà virtuale ci dà l'occasione di sperimentare nuove forme di libertà, facendo del vuoto che scava intorno all'*io* un elemento motore.

Chi viaggia, infatti, nel ciberspazio è separato e isolato. È un individuo immerso nel vuoto di un contesto finzionale. E lo è, non tanto perché seduto dinanzi uno schermo è per forza di cose da solo, ma in quanto il perdurare del gioco telematico – proprio perché gioco – dipende da un mero atto di volontà: si entra e si esce dai *Multi-users dungeons and dragons* a proprio piacimento. Si visita un sito, si è sedotti dal tema, si ha qualcosa da dire perché anonimi, e se qualcosa irrita, oppure se il *sé nascosto* delude, si abbandona semplicemente il sito.

---

[39] P. LÉVY, *Il virtuale*, cit., in part. p. 8.

[40] Sulla tematica attuali le osservazioni di R. STAGLIANÒ, *Circo Internet. Manuale critico per il nuovo millennio*, Milano, Feltrinelli, 1997, p. 15 ss.

Grazie all'interazione a distanza, ci si connette ad altri, scambiando la propria identità, usurpandola, fantasticando su un diverso e falso io, oppure mantenendo il vero io, del quale però l'altro non può mai essere certo. Comunicazione e condivisione vengono così inseriti in un gioco dei travestimenti, del quale si può legittimamente supporre che sia emotivamente soddisfacente. Ma si può altresì ipotizzare una comunicazione e una condivisione *sui generis*.

Se l'illusione sarà così potente da non permettere la distinzione tra ciò che è reale e ciò che non lo è, se il gioco diventerà imperioso mescolando sempre più essere e apparenza, l'identità dipenderà dall'identità virtuale e la comunicazione dalla comunicazione online. In altre parole, si corre il rischio che il gioco dei travestimenti

"finisca di essere giocato e diventi qualcosa d'inquietante: una tenebrosa, per niente ludica, comunità di spettri" [41].

L'analisi dei *role-playing games* è significativa. Su Internet, e in particolare nell'Internet Relay Chat (IRC) o in una comunità MUD, le conversazioni online e i giochi diventano dei veri e propri laboratori dove si costruisce l'identità. L'io può essere completamente ridefinito: può cambiare sesso, ruolo, carattere, professione, nazionalità, e altro ancora. Scontento del reale e disilluso, l'individuo – protetto dall'anonimato – sperimenta quel che è rimasto inesplorato della propria soggettività.

'Io sono molti', giacché nella situazione ludica, possono essere interpretati al contempo ruoli diversi e create vite parallele [42].

---

[41] "Non altro sarebbe una comunità i cui membri sono tutti, chi più chi meno, persuasi che le loro identità posticce siano le loro vere identità" (T. MALDONADO, *Critica della ragione informatica*, Milano, Feltrinelli, 1997, pp. 63-64).

[42] Gli esempi di Giulia e di June – riportati diverso tempo fa da Allucquere Rosanne STONE (*A proposito del corpo reale: storie di frontiera sulle culture virtuali*, in M. BENEDIKT (a cura di), *Cyberspace. Primi passi nella realtà virtuale*, trad. it., Padova, Muzzio, 1993, in part. pp. 89-90) e da Sherry TURKLE (*La vita sullo schermo*, cit., p. 386) – restano emblematici: Giulia è uno psichiatra di mezza età che, affascinato dalle conversazioni femminili, mette a punto la personalità di una donna anziana, sola e disabile, per partecipare a *computer conference*. In pochi anni conquista parecchie ammiratrici, finché una delle sue più devote, decidendo di incontrarla, lo sma-

'Io sono molti', poiché nei luoghi d'incontro elettronici: *i*) si genera una facile intimità. Isolati nel mondo del virtuale i partecipanti stabiliscono rapporti rapidamente sempre più intensi. Il cyberspace velocizza tutto, anche i rapporti amicali; *ii*) si incoraggiano la proiezione e lo sviluppo di un transfert. In mancanza qualche volta di indizi visivi e in compagnia quasi sempre di una tastiera, è favorita la proiezione: il mondo virtuale può condurre a facili idealizzazioni, come pure a rapide demonizzazioni; *iii*) si crea dipendenza. Il mondo virtuale è via via considerato appagante, rispetto a un mondo reale sempre più deludente.

In particolare, nei luoghi d'incontro elettronici, le linee di demarcazione fra sé e gioco (e inoltre: sé e ruolo, sé e simulazione) restano opache e si confondono [43]. La scoperta di molti sé interiori, l'induzione a falsi io, le personalità apocrife, permettono di indossare e interpretare varie maschere. Ciò naturalmente è frequente nella vita quotidiana e nonostante tutto assume nella vita virtuale una diversa valenza se *il gioco finisce d'esser giocato*. Qui, infatti, i molti sé, ovvero i sé frammentati,

> trascinano in una miriade di direzioni, invitandoci a giocare una varietà di ruoli fino al punto che il concetto di *sé autentico* finisce per sparire [44].

3.2. I risvolti della personalità, qui appena accennati, sono particolarmente interessanti se collegati con la proposta, da più parti avanzata, di democrazia diretta in Rete.

---

schera. La notizia si diffonde presto sulla Rete ed è accompagnata ora da accettazione divertita, ora da rabbia cieca, la rabbia di quelle donne che avevano confidato a Giulia i sentimenti più intimi; June è, invece, una undicenne che, entrando nei MUD, vive nel corso di un anno di vita reale in tre famiglie diverse: quella della madre biologica e del patrigno, del padre biologico e della matrigna, e quella di un primo patrigno molto amato che è stato il secondo marito di sua madre. In ognuna delle tre famiglie vigono delle regole diverse, e così la personalità di June muta di volta in volta.

[43] Sugli effetti della rivoluzione digitale e sull'uso di computer, smartphone e ogni altro device tecnologico, per i più diversi scopi (conversare, giocare, ecc.), si vedano sempre di Sherry TURKLE, *Insieme ma soli. Perché ci aspettiamo sempre più dalla tecnologia e sempre meno dagli altri*, trad. it., Torino, Codice, 2012, e *La conversazione necessaria. La forza del dialogo nell'era digitale*, trad. it., Torino, Einaudi, 2016.

[44] Così K.J. GERGEN, *The saturated self. Dilemmas of identity in contemporary life*, New York, Basic Books, 1991, p. 7.

I falsi io, i molti sé, le personalità apocrife, si prestano a essere così definiti perché, appartato dinanzi alla sua tastiera, vi è essenzialmente una sorta di navigatore solitario. Il cibernauta si domanda e si risponde, è potenzialmente emittente e ricevente, autore e lettore, costretto solo da un minimo di materia, pochi grani di sabbia di silicio, e dal *bit*, DNA dell'informazione. Anche il cibernauta delle c.d. piattaforme sociali è a un tempo spettatore e protagonista, governato e governante, appartiene alla massa (degli utenti) e al contempo all'élite, è chiamato nello stesso tempo all'ascolto e alla decisione.

Si dice: la Rete è un formidabile mezzo di informazione e quindi uno strumento dalle enormi potenzialità (intellettuali, sociali, economiche e soprattutto politiche). La distribuzione di notizie utili a tutti fa sì che ogni cittadino diventi protagonista della politica. E così per chi ne è stato sinora escluso, la Rete rappresenta il miglior terreno di gioco, dove sperimentare forme diverse di comunicazione, di autorappresentazione e di autorganizzazione politica.

Com'è intuitivo, la Rete è un formidabile strumento per lo stesso potere (economico, finanziario, politico), capace di censurare il dibattito, di mettere il 'tassametro' e di rivendere più o meno tutto [45]. Anche nella Rete si ritrovano le élite, schiere di professionisti,

"che sanno compiere le scelte più 'economiche' nel proprio settore e nei confronti delle quali il non appartenente a quel gruppo deve tributare un'inevitabile deferenza" [46].

Nella disputa tra populismo ed elitismo, il navigatore-cittadino deve dare conto di un'affermazione pressoché ovvia: non è affatto necessario che tutte le istanze siano risolte dal popolo, poiché alcune, e in special modo quelle che attengono ai dettagli della legislazione, possono benissimo (devono) essere trattate e decise solo da pochi [47].

---

[45] H. RHEINGOLD, *Comunità virtuali. Parlare, incontrarsi, vivere nel ciberspazio*, trad. it., Milano, Sperling & Kupfer, 1994, p. 6.

[46] Così R. STAGLIANÒ, *Circo Internet*, cit., in part. p. 41.

[47] "È evidente – scriveva STUART MILL – che solo il governo basato sulla partecipazione di tutto il popolo soddisfa pienamente le esigenze della vita

Al di là della *querelle* massa-élite, è opportuno sottolineare due aspetti del populismo in Rete. Il primo riguarda la gente che si avventura nei corridoi del ciberspazio e che inscena nuovi comportamenti e nuove rappresentazioni collettive; il secondo è colto a partire dalle caratterizzazioni psicologiche del populista della Rete. Entrambi gli aspetti, seppur trattati separatamente, alimentano i rituali digitali e interagiscono tra loro.

Quello in Rete, com'è naturale, è l'erede del vecchio populismo. Pur in forma diversa, ne preserva il messaggio, così articolato: *a*) chiunque è in grado di decidere; *b*) la correttezza della decisione è garantita dall'essere presa da tutti, piuttosto che dai professionisti della politica; *c*) questi ultimi, decidendo della vita altrui, non possono non errare e comunque le loro scelte sono sempre di parte.

Intorno a questo nucleo essenziale, la società digitale, grazie alle sue caratteristiche, aggiunge qualcosa di suo. L'interconnessione generalizzata di tutti i terminali determina

"l'avvento di una cultura transnazionale, sradicata, mondiale, che prende dalla metafora dell'elettrone il proprio carattere libero ed incoglibile" [48].

Le piccole comunità virtuali costituiscono una conferma. Nonostante la loro palese diversità e i differenti fini cui si richiamano, esse esistono come *granelli di farina in una pagnotta che sta lievitando* [49], poiché fanno già parte di una cultura sempre più estesa, in un certo qual modo a-temporale ed a-topica. La gente che si avventura nei corridoi del cyberspace, che naviga in simulazioni sullo schermo, parla, s'incontra e vive, immersa in un sistema che azzera il tempo della circolazione dei messaggi ed è palesemente senza luogo.

Dietro il villaggio globale vi è in realtà solo un *cocooning* elet-

---

sociale. Ogni partecipazione è utile anche se riguarda solo la più infima delle funzioni pubbliche. Comunque la partecipazione deve essere grande quanto lo consenta il grado di civiltà raggiunto dalla comunità. Quanto di meno vi è di desiderabile è l'ammissione di tutti ad una parte del potere sovrano dello Stato" (*Considerazioni sul governo rappresentativo*, trad. it., Roma, Editori Riuniti, 1997, pp. 58-59).

[48] Così L. SCHEER, *La democrazia virtuale*, trad. it., Genova, Costa & Nolan, 1997, in part. p. 37.

[49] H. RHEINGOLD, *Comunità virtuali*, cit., p. 11.

tronico. E in questo bozzolo la gente si barrica, al riparo da stress, aggressioni e malattie. Qui, diversamente dalla piazza pubblica, la gente può giocare tutto, senza alcun rischio; le aggressioni insopportabili del mondo esterno vengono neutralizzate e filtrate, rese quindi vivibili e praticabili. Il *tele-cittadino* è a questo proposito emblematico:

"se ristabilisse la pena di morte [...] potrebbe assistervi dal suo schermo senza avere la sensazione di essere stato spostato in un ordine barbaro e senza che per lui sia importante sapere se ciò che vede sullo schermo appartiene al reale o al virtuale" [50].

Non deve sorprendere quanto sin qui detto. Proprio perché vi è uno schermo tra l'individuo e l'altro individuo, tra la stessa gente di una comunità virtuale, o ancora tra le genti delle diverse comunità elettroniche, la realtà viene filtrata e il mondo può funzionare come illusione. Schermo è, infatti, ciò che impedisce di vedere: di vedere l'altro e di essere visti dall'altro.

L'io e l'altro, allora, possono essere reali o virtuali, possono pagare di persona oppure soltanto nell'ordine simbolico. E se chiusi nel bozzolo, si collegano tra loro solo perché penetrano il muro elettronico dei segni. Così, l'aggregazione collettiva, che si fonda sulla circolarità reale-virtuale, non è il frutto di 'comuni destini', bensì l'effetto di un utilizzo collettivo del digitale.

La comunità virtuale può essere perciò voluta e disvoluta, si fa, si disfa e si rifà, secondo le avventure e le mode dell'universo incantato del virtuale. Un universo questo incantato perché si apre su paradisi artificiali senza rischi: sessualità senza Aids, allucinazione senza overdose, violenza senza vittime. E che incanta, giacché qui libertà, eguaglianza e fraternità

"sono dati in sovrappiù, come il *free money*. Sono i valori 'gratuiti' del nuovo ordine politico, quelli per cui non è più necessario pagare e che non chiedono più che si muoia per loro" [51].

Questa possibilità di diffondere le idee di libertà, eguaglianza e fraternità, fra grandi masse di persone, va innanzitutto ri-

---

[50] L. SCHEER, *La democrazia virtuale*, cit., p. 44.

[51] *Ivi*, p. 83.

collegata alle enormi capacità dei computer, memorie artificiali, sterminate e inerranti. Memorizzano infatti tutto e trasmettono di continuo informazioni, stabiliscono collegamenti diretti e ottengono immediati riscontri.

Va altresì ricollegata alla caratteristica prima dei membri delle comunità elettroniche: animati da passioni e da progetti, hanno temi e intese comuni, e tuttavia vivono senza un luogo di riferimento stabile e senza i vincoli che il luogo detta. Di qui, la libertà, l'eguaglianza e, se si vuole, la fratellanza dei membri erratici delle comunità virtuali. La virtualizzazione

"reinventa una cultura nomade, non con un ritorno al Paleolitico, né alle antiche civiltà di pastori, ma facendo emergere uno spazio di interazioni sociali in cui le relazioni si riconfigurano con un'inerzia minima" [52].

Le divisioni territoriali, le sovranità assolute degli Stati-nazione, e poi ancora le differenze sociali ed economiche tra Stati e Stati, tra individui e individui, possono essere considerate già in sé, un ostacolo al villaggio globale; la cultura nomade, al contrario, si sottrae a qualsiasi tipo di confine, di vincolo, e può considerarsi una delle strade maestre della globalizzazione.

3.3. I membri erratici delle comunità virtuali sono tra loro legati da un tema, da una passione, da un interesse comune. Ma sono altresì separati: dai cibernauti di altre comunità virtuali e dalla gente *tout court*.

Le singole comunità nel cyberspace sembrano scimmiottare gli americani di Tocqueville:

"si dividono [...] con grande cura in piccole associazioni molto distinte per gustare a parte le gioie della vita privata. Ognuno di essi vede con piacere che i suoi concittadini gli sono uguali, ma ne ammette solo un numero molto limitato fra i suoi amici e ospiti. [...] io credo che i cittadini delle nuove società, invece di vivere in comune, finiranno per formare solo piccoli gruppi [...] moltissime classificazioni artificiali e arbitrarie, per mezzo delle quali ognuno cerca di distinguersi per timore di essere trascinato contro voglia nella massa" [53].

---

[52] P. LÉVY, *Il virtuale*, cit., in part. p. 10.

[53] *La democrazia in America*, trad. it., Milano, Rizzoli, 1994, pp. 633-634.

Piuttosto che un villaggio globale, i membri delle diverse comunità virtuali finiscono col creare delle tribù postmoderne [54]. Anziché, attorno a un totem, si siedono – stavolta da soli – davanti ad un computer. E a loro si rivolge il populista della Rete. Anche lui, come gli altri, in un cocooning elettronico, al riparo dal reale e dai suoi limiti, è essenzialmente intimista. Non cerca raduni di piazza, né contatti diretti. Com'è ovvio, invoca la gente: ma, rispetto alla sua gente, aggregata intorno ad un tema come se fosse un totem, non porta responsabilità alcuna. Né potrebbe. Ogni contesto virtuale è residuale e rudimentale, ogni intesa è una replica simulata temporanea.

Allo stesso modo delle folle (residuali) e delle tribù (rudimentali), le formazioni postmoderne sono mono-tematiche. Oggetto della loro attenzione è solo un argomento, per di più relativamente semplice, tale cioè da poter essere compreso da ogni membro della comunità virtuale, collocato ora qui ora lì. Specializzate in un solo compito, in un unico tipo di azione, in un solo gruppo di simboli, le tribù postmoderne hanno una aspettativa di vita straordinariamente bassa. Le ragioni di ciò sono molte, tra queste, la stessa efficienza della Rete mondiale delle comunicazioni e l'immediatezza dell'informazione.

Si pensi ai modelli proposti dai media, grazie all'espediente della replica simulata dell'azione in luoghi molto distanti tra loro, tali modelli:

"reggono alla prova di 'folle' smisurate [...] Ma il fatto che i modelli siano diffusi dai *media* e non dispongano di altri mezzi di diffusione o fonti di credibilità determina anche la brevità della loro esistenza" [55].

La temporaneità, poi, delle tribù postmoderne può essere meglio colta grazie alle metafore del vagabondo e del turista. L'uno e l'altro sanno di non rimanere a lungo nel luogo dove sono arrivati. Entrambi sono per dir così extraterritoriali: attraversano spazi in cui vivono altre persone, hanno incontri brevissimi e superficiali (non-incontri), sono dispensati da ogni responsabilità.

Il vagabondo sogna la libertà: e per continuare a sognare

---

[54] Cfr. Z. BAUMAN, *Le sfide dell'etica*, trad. it., Milano, Feltrinelli, 1996, in part. p. 145 ss.

[55] *Ivi*, in part. pp. 147-148.

"struttura lo spazio che gli capita di occupare nel momento in cui lo occupa, solo per distruggere di nuovo quella struttura nel momento in cui se ne va".

Il turista paga la libertà: e pagando sperimenta emozioni esotiche, occupa temporaneamente spazi estetici.

"Il mondo è lì per essere piacevolmente vissuto e quindi dotato di significato. Nella maggior parte dei casi il significato estetico è il solo di cui abbia bisogno e che possa avere" [56].

Il cibernauta e il populista della Rete hanno lo *status* del vagabondo e del turista. Come questi, il primo e il secondo attraversano non-luoghi, usano l'arte del non-incontrarsi, si avventurano tra loro episodicamente. Entrambi sono esonerati dalla responsabilità degli altri: la vicinanza nel cyberspace e l'interfaccia tra il populista e la sua gente non si traducono in una esperienza del *noi*.

Se, infatti, la prossimità morale è il risultato del vivere con altri, lì dove l'arte del non-incontrarsi diventa particolarmente raffinata, lì dove la *perdita del volto* [57] diventa condizione necessaria d'ogni avventura nei corridoi del ciberspazio, l'*urbanitas computerizzata* subisce il fascino di una pseudo-vicinanza senza prossimità morale e con essa perde l'opportunità di acquisire l'esperienza del noi. Allo stesso modo della folla urbana, l'*urbanitas* computerizzata non è un insieme di individui, bensì un aggregato mobile, eterogeneo e informe. Qui le unità senza volto possono essere eliminate, dissolte e sostituite, e quanto avviene non modifica alcunché ed è del tutto indifferente anche ai fini delle possibili fonti di coinvolgimento sociale [58].

---

[56] *Ivi*, pp. 245-246.

[57] H. PLESSNER, *Al di qua dell'utopia. Saggi di sociologia della cultura*, trad. it., Torino, Marietti, 1974.

[58] Z. BAUMAN, *Le sfide dell'etica*, cit., 160.

4. In luogo di una conclusione: modello Cnosso e labirinto digitale

Perché il ciberspazio promuova l'intelligenza collettiva, ancora soffocata da mille tensioni, è necessario che esso segua il modello Cnosso, anziché quello di Micene.

Cnosso, come si sa, non ha cinte fortificate, sorge su alture vicino al mare con un succedersi di terrazze e gradinate. Nel palazzo cretese l'architettura aperta e funzionale, le immagini dalle tinte chiare e luminose entro contorni stilizzati e ritmici, rispecchiano una società che ha raggiunto stabilità ed equilibrio, in una parola la pace. Micene, di contro, è annidata sul monte e cinta da mura ciclopiche, essa è reggia e al contempo fortezza. Il tetro palazzo degli atridi è la degna cornice di fosche vicende familiari e dinastiche cantate nelle tragedie, e lascia intravedere una civiltà basata sul culto della forza e sulla gloria militare. Qui, assume un'importanza di primo piano il potere e la separazione di interno ed esterno; lì, nei palazzi di Cnosso, la raffinatezza degli ori, la gioiosa rappresentazione dei riti e dei giochi, la libera raffigurazione della donna, rivelano una civiltà affacciata sul mondo e molto vicina alla natura. I dettagli architettonici, infatti, testimoniano soprattutto la continuità di ambienti e di ambiti. Continuità tra palazzo e altri palazzi, tra palazzo e case private, tra ambienti di rappresentanza e laboratori artigiani, continuità ancora d'interno ed esterno, perché sia nel palazzo, che nei palazzi e nelle case, si possa godere il più possibile e liberamente della natura.

Ora, perché il mondo contemporaneo superi scandalose contraddizioni e miserie insopportabili, bisogna raffinare il ciberspazio che, come Cnosso, è infinitamente complesso: tutto coesiste e nulla gli è estraneo, senza interno e senza esterno si trova circondato da luminose forme geometriche che rappresentano i dati, per l'appunto il labirinto digitale. Ma perché proprio il misterioso labirinto di Cnosso dovrebbe rafforzare e raffinare l'architettura del ciberspazio? Se è vero che la civiltà minoica era essenzialmente pacifica e che non conosceva la schiavitù, è altrettanto vero che il mito del labirinto è un tutt'uno con la leggenda del Minotauro, quel mostro orrendo che ogni nove anni esigeva il tributo di sette giovinetti e di sette fanciulle ateniesi e che fu ucciso da Teseo.

Com'è noto, le interpretazioni del mito, come pure della civiltà minoica nei suoi diversi periodi, sono molteplici e per certi versi tra loro in contraddizione. Da un lato, vi è chi sottolinea l'unicità di questa cultura, nella quale il potere non significava affatto dominio, distruzione e oppressione, e Minosse era tra i re mortali il più regale e regnava su gran parte dei popoli confinanti con lo scettro di Zeus! Dall'altro, vi è chi ritiene che nella società minoica, divisa certamente in classi, fossero comunque presenti discriminazione, disuguaglianza e forse anche schiavitù.

Al di là delle distinzioni e delle interpretazioni: Minosse *e* il Minotauro/Minosse *è* il Minotauro, resta comunque misterioso il simbolo di questa civiltà irenica. E per alcuni interpreti resta misterioso proprio perché la sua danza [59]

"danzò la sua felicità, danzò la sua dualità, danzò la sua liberazione, danzò il tramonto del labirinto, lo sprofondare fragoroso di pareti e specchi nella terra, danzò l'amicizia fra i minotauri, animali, uomini e dèi",

ben difficilmente può essere compresa da popoli guerrieri. L'ibrido uomo-toro si esibisce all'aperto, leggero, aggraziato, su uno spiazzo inondato di luce, ma i greci guerrieri non ne colgono il senso. Il palazzo pieno di luce, il labirinto bianco che è traccia architettonica della bellezza, della gioia e della leggerezza sovrane, si trasforma dinanzi a guerrieri nel labirinto nero, abitato da un mostro divoratore di uomini. E forse il mito può essere letto proprio così: l'uccisione del mostro quale rimozione definitiva della cultura di pace.

Certo, anche i cretesi hanno armi. Le loro daghe, ad esempio, sono splendidamente decorate e di notevole qualità tecnica. E con ogni probabilità, proprio l'aumento della guerra e della pirateria nel Mediterraneo, fa sì che pure Creta intraprenda delle battaglie, sia per difendere il suo vasto commercio marittimo che per proteggere le sue coste. Ma a differenza di altre civiltà, non vi è traccia di contese tra le città-Stato dell'isola, né vi sono indizi di guerre di conquista e di uno stato di guerra cronico, che altrove invece costituisce la regola. Così, l'inesistenza di città fortificate e militarizzate, come pure l'assenza di protezione di palazzi e

[59] Così nel racconto di F. DÜRRENMATT, *Minotauro, una ballata*, trad. it., Milano, Marcos Y Marcos, 1997.

ville, sono conferme di una possibile coesistenza pacifica tra gli uomini e tra le società.

Si tratta allora di decifrare, o piuttosto inventare, la lineare A, scrittura adoperata a Creta insieme all'ideografica e alla lineare B, perché lì risiede l'enigma della pace e quindi la fondamentale differenza tra Cnosso e Micene. Inventarla naturalmente alla luce ora del labirinto digitale, che è in grado di ridisegnare ogni relazione – persino il nostro rapporto con l'oblio –, di recuperare tutto ovunque sia immagazzinato, e che analogamente alla biblioteca di Babele non conosce problemi locali o globali la cui eloquente soluzione non sia reperibile in un qualche esagono.

II

UN NUOVO BENE: L'INFORMAZIONE

Sommario

1. "Ciò che vien meno nell'epoca della riproducibilità tecnica"

"Ciò che vien meno nell'epoca della riproducibilità tecnica è l"aura' dell'opera d'arte. Il processo è sintomatico; il suo significato rimanda al di là dell'ambito artistico. La tecnica della riproduzione, così si potrebbe formulare la cosa, sottrae il riprodotto all'ambito della tradizione. Moltiplicando la riproduzione, essa pone al posto di un evento unico una serie quantitativa di eventi. E permettendo alla riproduzione di venire incontro a colui che ne fruisce nella sua particolare situazione, attualizza il riprodotto. Entrambi i processi portano a un violento rivolgimento che investe ciò che viene tramandato – a un rivolgimento della tradizione, che è l'altra faccia della crisi attuale e dell'attuale rinnovamento dell'umanità".

La tesi di Walter Benjamin è nota [1]. Le sempre più sofisticate e diverse tecniche di riproduzione, con il loro carattere di mas-

[1] *L'opera d'arte nell'epoca della sua riproducibilità tecnica*, trad. it., Torino, Einaudi, 1991, p. 10.

sa, agiscono sull'arte nella sua forma tradizionale e modificano la sua funzione. Vacilla infatti l'autorità della cosa e viene meno l'*hic et nunc* dell'opera, e cioè il concetto di autenticità. Diversamente dalla riproduzione manuale, dove l'autentico mantiene la sua piena autorità e il falso resta falso, nel caso della riproduzione tecnica (ad esempio, la fotografia) l'originale riprodotto rivela aspetti (dell'originale) solo grazie al mezzo (all'obiettivo) e si presenta in contesti all'originale stesso inaccessibili.

Si pensi alla scena ripresa nello studio cinematografico: essa è il risultato di uno speciale procedimento, ossia della ripresa con la macchina disposta in un certo modo e del montaggio delle riprese tra loro. Accade così che l'aspetto della realtà sottratto all'apparecchio diventi l'aspetto più artificioso e la vista sulla realtà immediata una chimera nel paese della tecnica. Si pensi, poi, alla fotografia e al disco. Con l'una, la cattedrale abbandona la sua ubicazione per essere accolta in uno studio di un amatore d'arte e, con l'altro, il concerto eseguito in teatro è ascoltato in una camera. In entrambi i casi, la creazione artistica, grazie alla riproduzione in sede impropria, va incontro al fruitore e soddisfa l'esigenza tipica della società contemporanea, la richiesta delle masse di beni culturali che giocoforza diventano merce.

Al di là della posizione di Benjamin, secondo il quale riproducibilità ed esponibilità pongono finalmente fine ad una concezione aristocratica dell'arte, trasformano l'intera sua funzione, instaurano la fondazione su un'altra prassi, vale a dire il suo fondarsi ora sulla politica piuttosto che nel rituale, questa ricostruzione costituisce lo spunto per trattare della centralità della tecnica, quale elemento determinante della produzione ed elaborazione di idee, teorie, significati del mondo.

Se già infatti la fotografia, considerata da Baudelaire una tecnica [2], è stata in grado di mettere in discussione la nozione stessa di arte, poiché per la prima volta il valore espositivo mostra la sua superiorità sul valore cultuale, è agevole constatare che l'attuale sviluppo tecnologico, con la messa a punto di macchine intelligenti per il trattamento delle informazioni, crea possibilità ra-

[2] E insieme umile serva delle scienze e delle arti, allo stesso modo della stampa e della stenografia (*Le public moderne et la photographie*, in *Études photographiques*, n. 6 Mai 1999, *journals.openedition.org*).

dicalmente nuove e muta profondamente convinzioni e confini. Si tratta anzi di una trasformazione generale, in cui nulla resta così come è, in cui tutto conquista significati nuovi. Se infatti si estende la natura e la portata delle nostre percezioni, se la continuità visiva rimpiazza la contiguità territoriale, invertendo le nozioni abituali di interno ed esterno [3], se sono in gioco per dir così un nuovo modo di essere e delle nuove velocità di fuga [4], è chiaro che anche il nostro rapporto con il mondo, e in particolare con lo spazio e il tempo, subisce una tale modifica da rendere impossibile stabilire se a essere trasformato sia il mondo umano medesimo o semplicemente il nostro modo di percepirlo.

2. Il sapere, il virtuale e le nuove domande

Lungi dall'essere una qualsiasi conquista, l'attuale tecno-scienza plasma a tal punto il mondo da far mutare non solo assetti costituiti (sociali, economici, politici), ma da erodere anche diversi confini. Ai nostri fini è sufficiente ripensare, con Lyotard [5], alla vicenda del sapere nelle società informatizzate. L'egemonia informatica impone che la conoscenza sia traducibile in linguaggio-macchina e che i 'produttori' dell'informazione, come pure i suoi utenti, dispongano dei mezzi necessari per tradurre in tale linguaggio. Se così è, c'è da aspettarsi l'abbandono dell'antico principio secondo il quale acquisizione del sapere e formazione dello spirito (e anche della personalità) sono inscindibili. Rispetto al 'sapiente', il sapere subisce una radicale esteriorizzazione, e d'altra parte il rapporto tra conoscenza, suoi fornitori e suoi utenti, tende sempre più a rivestire la forma valore, tipica del rapporto che intercorre tra la merce e i suoi produttori e consumatori. In altri termini, il sapere, prodotto per essere venduto, e consumato per essere valorizzato in un nuovo tipo di produzione, cessa di essere fine a se stesso e perde il proprio valore

[3] *La scorza è rovesciata*, per dirla con Paul VIRILIO di *La bomba informatica*, trad. it., Milano, Cortina, 1999.

[4] M. DERY, *Velocità di fuga. Cyberculture a fine millennio*, trad. it., Milano, Feltrinelli, 1997.

[5] *La condizione postmoderna. Rapporto sul sapere*, trad. it., Milano, Feltrinelli, 2002.

formativo. Le conoscenze(-informazioni), così, circolano via via negli stessi circuiti della moneta e si adeguano all'opposizione che definisce la moneta: conoscenza dei mezzi di pagamento/conoscenza dei mezzi di investimento. Sono pertanto definite, non più dall'opposizione sapere/ignorare, bensì da conoscenze scambiate nell'ambito della riproduzione quotidiana *versus* credito di conoscenza per ottimizzare le prestazioni di un programma.

Già queste brevi considerazioni di Lyotard, che com'è noto risalgono al 1979, inducono a ritenere che l'attuale invenzione tecnica sia di così vasta portata da non consentire di confinare i nuovi strumenti (per calcolare, scrivere, archiviare, progettare, comunicare, educare) nel puro e semplice regno dei mezzi. Detto altrimenti, i nuovi strumenti (e dispositivi) oltrepassano la dialettica dei mezzi per raggiungere lo stadio retorico degli scopi.

2.1. Se la parola è all'inizio indissociabile dalla *presenza* (qui e ora), la scrittura – quale 'grammatizzazione della parola'[6] – separa il messaggio dal referente corporeo e dalla situazione contingente. La stampa, poi, con il suo carattere mobile (svincolato da situazioni concrete, riproducibile e circolante), standardizza la grafia e stacca il testo letto dalla traccia diretta di una prestazione muscolare: prosegue dunque il processo di grammatizzazione. L'informatica, infine, accelera il movimento avviato dalla scrittura. Con la riduzione di ogni messaggio a combinazioni di due simboli elementari – zero e uno –, sempre identici e decodificabili da qualsiasi computer, l'informatica è la tecnica maggiormente virtualizzante, perché è quella che maggiormente grammatizza.

Sin qui, si tratterebbe dunque solo di nuovi strumenti che, seppure meglio degli altri, continuano l'opera di grammatizzazione, ottenendo dalle presenze (qui ed ora) e dalle relazioni (o situazioni specifiche) quegli elementi convenzionali (o normalizzati) che come atomi astratti sono autonomi, trasferibili, indipendenti (da contesti viventi). Tali atomi astratti costituiscono già lo stadio minimo del virtuale, giacché ciascuno di essi può attualizzarsi in una varietà indefinita di circostanze, tutte qualitativamente diverse e tutte sempre riconoscibili quali esemplari dello

[6] Per dirla con Pierre LÉVY, *Il virtuale*, trad. it., Milano, Raffaello Cortina, 1997.

stesso elemento virtuale. La grammatizzazione non ha a che fare con atomi reali e sostanziali, bensì con particelle virtuali. Proprio per la loro proprietà di non significazione, è possibile il loro reimpiego: un insieme limitato di componenti elementari, liberi e staccabili, può costruire una quantità infinita di sequenze, di assemblaggi e di composti significanti. Il che vuol dire altresì che il significato delle sequenze (degli assemblaggi e dei composti) non è deducibile a priori dalla somma dei suoi elementi, ma è piuttosto un'attualizzazione creatrice nel contesto.

2.2. Per la retorica degli scopi, e cioè per lo schiudersi del virtuale come mondo autonomo, è da sottolineare il costituirsi di un contenuto normativo della tecnologia medesima. Detto altrimenti, la tecnologia si fa essa stessa regola e da quest'ultima discendono tutte le altre. A tal proposito si è significativamente osservato che

"lo sviluppo della tecnica assurge da materia regolata a principio regolatore, si tramuta da oggetto in soggetto di normazione. Non c'è più luogo a distinguere tra regola e regolato: abbiamo dinanzi l'onnipotente unità del dispiegamento tecnologico [...] Cioè, la tecnica si eleva – o 'salta' – dall'indefinita pluralità delle singole 'operazioni', tutte particolari e specialistiche, a principio ordinatore, a supremo dover essere, in cui ogni norma trova la propria genesi" [7].

E nel diventare principio regolatore, la tecnologia propone visioni e prospettive inedite. Del resto, se ad un primo livello il computer è senz'altro uno strumento, col quale scriviamo, teniamo aggiornata la nostra contabilità, comunichiamo con gli altri, oltre questo primo livello, scopriamo che il computer è più di uno strumento, poiché ci offre nuovi modelli mentali.

Se poi si considera che con il computer la tradizionale distanza tra persone e macchine è diventata in un certo qual senso più difficile da mantenere, perché si sperimenta una continua riduzione delle differenze tra l'uomo e la macchina, è necessario ammettere che grazie alla tecnologia le distinzioni tra ciò che è specificamente umano, pensante, vivo, e ciò che è specificamente

---

[7] Così N. IRTI, *Atto secondo*, in N. I., E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, Laterza, 2001, p. 51 ss.

tecnologico, logico, inanimato (e tuttavia interattivo) devono essere rivisti e devono essere rinegoziati i vecchi confini.

Una conseguenza di tale rinegoziazione è che nuove domande sorgono e si è spinti verso nuovi discorsi. Si pensi ad esempio alla domanda morale iniziale – prima cioè che la scienza moderna partorisse le tecnologie in grado di rendere reali e concreti i suoi sistemi altrimenti astratti –, essa era del tipo: 'come e in che modo si possono conoscere doveri e responsabilità dell'uomo?', ed era così perché i sistemi di pensiero che definivano la posizione dell'uomo nel mondo erano fondamentalmente giuridici. Una volta però che la scienza moderna si insinua nelle costruzioni immaginarie della realtà da parte dell'uomo e pretende di fare affermazioni sulle esperienze dell'uomo, quella stessa domanda si trasforma in un'altra 'di qual genere tecnologico l'uomo è una specie?' e si completa infine con altre del tipo: 'cosa significa essere vivi?' 'può l'artefatto, oggetto biologico, essere considerato un essere vivente?' [8].

3. Il primo attuale motore dell'economia

Il settore dell'informatica mette a disposizione dell'economia le cosiddette ICT (Internet, ampia banda e wireless, applicazioni multimediali, corporate TV), grazie alle quali anche il modo di fare impresa muta. Si tratta infatti ormai di un insieme di attività orizzontali e connesse, attente al cliente e alle sue aspettative, decisamente più tempestive, competitive e reattive al cambiamento. E così, ad esempio, le imprese conquistano una maggiore specializzazione e competenza, sperimentano approcci di marketing che pongono il consumatore (*co-producer*) al centro dei processi di creazione di valore, offrono prodotti e servizi sempre all'avanguardia.

L'economia, d'altra parte, diventa economia del virtuale. In stretta simbiosi con le Reti e le tecnologie a supporto digitale, si assiste non solo a una riorganizzazione dei cicli produttivi, ma

[8] Per ulteriori considerazioni e implicazioni si riveda quanto evidenziato da Joseph WEIZENBAUM, uno dei padri della *Computer Science*, nel suo *Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale*, trad. it., Torino, Gruppo Abele, 1987.

anche a un ripensamento delle strategie e a una espansione di ben precisi settori economici, quali per l'appunto il turismo, lo sport, lo spettacolo, la finanza. Più in particolare, proprio la c.d. densità delle connessioni, e cioè la facilità, la rapidità e l'economicità dei collegamenti tra numerosi operatori oltre i vincoli posti dallo spazio e dal tempo, fa sì che l'informazione svolga un ruolo centrale all'interno dell'assetto socio-economico.

Si potrebbe pensare che sia stato sempre così: il contadino, l'artigiano, il commerciante, infatti, dovevano comunque acquisire specifiche competenze e tenersi al contempo informati. In realtà, però, il nostro rapporto con la conoscenza è mutato. Si è passati dai saperi stabili alla formazione permanente, e cioè il sapere che prediligeva il versante della contemplazione e della durata, oggi si è fatto flusso e nutrimento di azioni operative, esso stesso un'operazione, e non riguarda più soltanto una casta di specialisti, ma a ognuno di noi, nella propria quotidianità, è richiesto di acquisire, produrre e trasmettere informazioni-conoscenze in modo cooperativo [9].

Al di là della possibile contrapposizione tra virtualizzazione (conoscenza e informazione necessitano pur sempre di supporti fisici, di luoghi d'iscrizione materiali, e quindi non di beni immateriali si tratterebbe, bensì di beni de-territorializzati, ossia svincolati da un qui e ora specifici) e smaterializzazione (la Rete moltiplica le fonti di diffusione cognitiva e sposta l'attenzione dal materiale all'immateriale. Tutto ciò che è immateriale diventa ora fondamentale per l'economia [10]), quel che è certo è che le informazioni e le conoscenze, diversamente dal passato, diventano oltre che beni economici primari, anche la fonte e la condizione determinante per tutte le altre forme di ricchezza.

Per la retorica degli scopi, allora, le considerazioni sin qui svolte devono necessariamente essere sviluppate. Ed infatti, se l'informazione-conoscenza(-comunicazione) diventa il primo motore dell'economia, ovvero la principale fonte di produzione di ricchezza, è chiaro che molti schemi e molte teorie possono considerarsi decisamente superati. Si pensi ad esempio alla teoria eco-

---

[9] In tal senso, cfr. P. LÉVY, *Il virtuale*, cit., in part. p. 47.

[10] C. GOLDFINGER, *L'utile e il futile. Per un'economia dell'immateriale*, trad. it., Torino, Utet, 1996.

nomica classica: essa poggia sul postulato della rarità dei beni, sul carattere irreversibile del processo economico (usura, spesa, trasformazione, consumo) e sulla natura esclusiva (o privativa) della cessione e dell'acquisizione. Tutto ciò naturalmente non accade nel caso dell'informazione: essa infatti non la si perde e neppure, facendone uso, la si distrugge.

Consideriamo in particolare il software, essenza dell'immaterialità. Si tratta innanzitutto di un bene non-rivale, nel senso che è possibile cedere una copia senza comunque privarsi e perciò stesso senza che sia ridotto il proprio benessere. È inoltre un bene riproducibile innumerevoli volte e con costi pressoché nulli: e una tale caratteristica è certo nuova, nel senso che con i mezzi di diffusione dell'informazione e del sapere tradizionali (libri, riviste cartacee, ecc.) ciò non è possibile. Ne consegue che per i c.d. beni non-rivali il problema della scarsità non si dà e che quindi, sempre per questi beni, mal si adattano le teorie economiche ereditate dal periodo precedente, come pure quelle norme tradizionalmente legate alla scarsità e alla natura esclusiva (o privativa) della cessione e dell'acquisizione. Il software, poi, alla stessa stregua della informazione-conoscenza, è cumulativo e modulare: nuove componenti possono di continuo aggiungersi al preesistente, per addizioni e miglioramenti, e solo se non è soggetto a regole, a procedure e in generale a limitazioni, è possibile che quella sua natura, cumulativa e modulare, sia effettivamente garantita. Di qui, probabilmente, la netta superiorità tecnica del *free software* rispetto al software proprietario. Se così è, inutile dire che le forme giuridiche, e più specificamente i diritti di proprietà (ben definiti e tutelati), finiscono col limitare l'innovazione stessa. Non è a caso che proprio negli ultimi anni i conflitti sulla proprietà intellettuale hanno raggiunto una inedita intensità, vi è una radicale messa in discussione di termini quali liberismo e protezionismo, e l'industria (del software) è agitata da guerre commerciali che degenerano in crociate ideologiche, come quella per l'appunto tra Microsoft, nel ruolo di rappresentante del *software proprietario*, e IBM, nel ruolo di campione del *software open source* [11].

---

[11] Vd. C. FORMENTI, *Mercanti di futuro*, Torino, Einaudi, 2002; ID., *Not economy. Economia digitale e paradossi della proprietà intellettuale*, Milano, Etas, 2003. Inoltre, per un interessante approfondimento anche degli aspetti tecnici, cfr., fra gli altri, D. QUINTERO, F. MARTINIS, E.L. CERDAS MOYA, R.

Le brevi considerazioni sin qui svolte confermano che anche nell'ambito economico, visto l'affermarsi della nuova economia dell'abbondanza e del virtuale, vi è bisogno che i sistemi di misura e di valorizzazione del reale e del potenziale fondati su risorse limitate, e perciò non più adeguati, siano sostituiti da nuovi sistemi e nuove teorie in grado di gestire la dialettica virtuale-attuale. Se è infatti l'informazione a costituire oggi il bene primario per eccellenza, è necessario allora muovere dalla considerazione che l'informazione nel cyberspace: *i*) può assumere significati (e funzioni) diversi (ed anche imprevedibili) a seconda dell'ipertesto in cui è inserita; *ii*) ciò che è in gioco è la sua attualizzazione, la lettura, ovvero il significato che può assumere nel contesto; *iii*) la sua riproduzione (la sua copia) non costa praticamente niente, se non il costo generale del mantenimento del cyberspace.

Ora, la necessità di un ripensamento dell'economia è resa ancor più urgente se si considera con Rheingold che, quando si mettono insieme aspetti della tecnologia ed economia,

"il risultato è un'infrastruttura che rende possibili certe azioni umane che prima non erano realizzabili. Le *killer applications* dell'industria delle comunicazioni mobili di domani non saranno gli apparecchi o i software, ma il loro uso sociale. I cambiamenti più radicali verranno, come spesso accade, dal tipo di rapporti tra imprese, comunità e mercati che tali infrastrutture renderanno possibili" [12].

4. L'opulenza e/o l'indigenza dell'informazione

L'odierno rapporto con l'informazione è, senza dubbio, carico di novità radicali, ma anche di parecchie problematiche.

Per un verso, grazie alle nuove tecnologie, l'informazione è immediatamente accessibile. E se tutti sono informati, ognuno è in grado di prendere le decisioni più opportune richieste dalle diverse circostanze. Il cittadino democratico ideale sembrerebbe

---

CAMARDA SILVA FOLCO, *IBM Open Platform DBaaS on IBM Power Systems*, Milano, RedBooks, 2018.

[12] *Smart mobs. Tecnologie senza fili, la rivoluzione sociale prossima ventura*, trad. it., Milano, Raffaello Cortina, 2003. In particolare, sulle killer applications, ancora attuale, R. BROIDA, D. JOHNSON, *101 Killer Apps for Your Pocket PC*, New York, McGraw Hill Professional, 2004.

identificarsi con il cittadino totalmente informato. D'altra parte, l'informazione è, in ogni caso, strumento di arricchimento e veicolo formidabile di quella cittadinanza democratica che è una delle principali conquiste della modernità.

Per un altro verso, però, non si può non sottolineare il fatto che laddove manchi un approccio critico, quelle stesse tecnologie interattive e multimediali che consentono la diffusione di continui flussi di informazioni e notizie, possono sovrapporre le narrazioni ai fatti, la fantasia alla realtà, la verità alla menzogna [13], danneggiando, così, non soltanto l'effettiva conoscenza e la piena comprensione degli accadimenti e dei fenomeni, ma, talvolta, persino la stessa democrazia.

Si ripropongono, dunque, alcune domande fondamentali: *è possibile che le élite si avvalgano delle ICT per condizionare il pubblico e per orientarlo secondo quelli che, di volta in volta, sono i loro scopi (economici e/o finanziari e/o politici)? Non c'è il rischio che le élite si tramutino in custodi egemonici delle ICT e, con esse, pure dell'informazione-comunicazione?* [14].

Quesiti, quanto mai attuali, soprattutto se si considera il modo in cui – a seguito di scelte tutt'altro che casuali e neutre – ad alcune informazioni particolarmente scomode non viene dato il giusto rilievo e il necessario approfondimento, quasi per tentare di indurne la dimenticanza, quasi che l'assenza di seguito (e di informazione) valga a *negare* l'esistenza stessa del fatto [15].

A questa dinamica che, incidendo sulla notizia, manipola il consenso, s'accompagna anche la ridondanza delle informazioni che, superata

---

[13] Alle più note e discusse fake news, si aggiungono le *clickbait* (storie deliberatamente inventate per ottenere più visitatori nel sito web e aumentare le entrate della pubblicità) e le *hate news* (che – oltre a costituire un falso – promuovono il razzismo, la misoginia, l'omofobia e altre forme di discriminazione).

[14] Riprendo, qui, le domande che – già alcuni anni fa – si poneva R.A. DAHL (*La democrazia e i suoi critici*, trad. it., Roma, Editori Riuniti, 2005, in part. p. 462).

[15] Cosa che, ad esempio, si è verificata nel mese di novembre di quest'anno, in occasione della scelta di uno studente francese di darsi fuoco in segno di protesta politica. In quel caso, infatti, il silenzio mediatico che ha accompagnato la triste vicenda, sembrava, in una qualche misura, volerla negare.

"[…] una determinata soglia critica, porta alla noia percettiva [...] [ossia all'] apatia, come rigetto, e persino come disgusto di fronte a messaggi troppo ripetuti. […] [cosa che, per altro, si verifica] anche quando i messaggi sono troppi e scarsamente differenziati. In situazioni di questo genere […] [infatti] i messaggi non vengono più percepiti come figure contrapposte a un fondo. [Ragion per cui] tutto diventa fondo [o, meglio, tutto diventa indistintamente] rumore di fondo" [16].

Altrimenti detto e in breve – immersa in un brusio diffuso – ogni notizia diventa residuale, rudimentale, quasi si trattasse di una replica simulata, contingente e temporanea: un dato accessorio, trascurabile, inutile.

5. Sulla chiacchiera informatica

Di solito le conversazioni telematiche sono dagli addetti ai lavori tradotte con il termine chiacchiera (chat). E non è a caso. Il termine è anzitutto sinonimo di notizia senza fondamento, di voce falsa o malevola, di pettegolezzo o diceria; in genere, poi, rinvia ad una conversazione condotta per passatempo o come sfogo a considerazioni (e pensieri) frivoli o malevoli. A contatto col cyber, il termine per dir così non viene affatto emendato. Anzi, nell'immenso *bla-bla* digitale si accentuano la natura e lo scopo.

Il linguaggio informatico evoca continuamente – nonostante la serietà di molti temi, di molte opinioni e ipotesi – la chiacchiera, se non addirittura il chiacchiericcio. La causa di questo costante rinvio è da attribuirsi, con molta probabilità, a quella che a ben vedere è la specialità e la specificità di questo particolare tipo di comunicazione. Del resto, l'intrattenimento informatico si svolge in un territorio *sui generis*. Non conosce né luogo, né tempo, né misura. Essendo tale, al suo interno, possono insinuarsi solo quelle dinamiche che non deroghino alla sua natura: la chiacchiera avanza irriverente, perché innanzitutto sul proprio terreno non conosce delimitazioni, né pietre di confine; perché, in secondo luogo, non ha un rapporto temporale determinato, se non *ex post* e solo per l'avvicendarsi di una nuova

[16] T. MALDONADO, *Critica della ragione informatica*, Milano, Feltrinelli, 1997, p. 88 ss.

notizia (voce, pettegolezzo, diceria); perché, infine, le idee di misura e di forma le sono davvero estranee. Si perde in chiacchiere chi rinuncia al tentativo di elaborare notizie vere, per dar sfogo a passatempi e a pensieri leggeri.

In generale, l'Internet relay chat, i club online, le comunità virtuali, i forum, offrono all'utente che si connette la possibilità di affrontare argomenti più o meno seri. In particolare, i *bulletin board sistems* consentono lo scambio di informazioni – affisse in bacheca – più o meno importanti. Nel *Whole earth 'lectronic link* le persone, con poco o molto impegno, partecipano a dibattiti pubblici e si scambiano messaggi privati. Nei *Multi-user simulation environment* chiunque abbia immaginazione e curiosità s'incontra virtualmente con altri secondo linguaggi più o meno bizzarri. Nuove e singolari forme di comunicazione, di condivisione e – per certi versi – anche di socialità, sono rese possibili grazie a software gratuiti (MyBulletinBoard, phpBB, FluxBB, Simple Machines Forum) o anche a pagamento (vBulletin, Invision Power Board).

Una breve raccolta di chiacchiere informatiche nelle comunità virtuali permette di giustapporre il *rumores differre* [17] al *communicare* (o *consociare*), dove si mette in comune la parola con il suo senso e dove l'incontro non si rassegna a essere episodico (il non-incontro di Martin Buber), perché risultato di una vicinanza, di un destino comune, oltre l'infinito e nomade navigare (da un sito all'altro).

Ecco qualche chiacchiera all'interno di Usenet [18]:

Chiacchiera n. 1)

Newsgroup: rec.crafts.texitiles,alt.seving.

---

[17] E la "vertigine di poter dire la propria opinione davanti ad una platea potenziale di decine di milioni di persone" (così R. STAGLIANÒ, *Circo Internet, Manuale critico per il nuovo millennio*, Milano, Feltrinelli, 1997, in part. pp. 132-133.

[18] Una Rete mondiale, nata negli anni '80 formata da migliaia di server interconnessi che raccolgono articoli, news, messaggi e post, che riguardano varie tematiche (topic), a cui – tramite la Rete – chiunque può avere accesso. In particolare, grazie ad Usenet, gli utenti possono *a*) esprimere la propria opinione e confrontarsi con altri su argomenti di loro interesse; *b*) ricevere informazioni e aggiornamenti su un determinato tema e/o settore; *c*) richiedere delucidazioni specifiche.

Percorso:well!uunet!fatech!utkcs2!athena.cas.vanderbilt.edu!vus1.

Da:vus l @athena.cas.vanderbilt.edu (Biblioteca scientifica VU)
Argomento: storia sociale del cucito.

Organizzazione: Matematica, Vanderbilt University, Nashville.

Mi interessa la storia della tessitura. Ho visto vari libri sull'aspetto dei vestiti di vari periodi. Ho visto modelli che cercano di riprodurli.

Ma quello che più mi interessa è più una storia sociale del cucito. Il mio campo di interesse sono gli anni dal 1066 al 1500. Chi faceva i vestiti delle dame del castello? Che aghi usavano? Quando è stato inventato il bottone ...

Grazie
Carlin
sappen@ctrvax.vanderbilt.edu

Chiacchiera n. 2)

Newsgroup: uiowa.forsale,misc.forsale,rec,pets,rec.pets.herp
Da: bbreffle@icaen.uiowa.edu (Barry Ronald Breffle)
Argomento: Pitoni birmani in vendita
Organizzazione: Iowa Computer Aided Engineering Network, University of Iowa
VENDESI

Ho da vendere vari pitoni birmani. Discendono da pitoni in cattività da molte generazioni. I pitoni birmani sono belli e salutari. Mangiano tutti bene...

Posta elettronica: bbreffle@icaen.uiowa.edu.

Ecco due esempi di FAQ [19] in tema di aviazione e di cupon:

Faq n. 1)

Q1: Com'è organizzata l'aviazione?
Q2: Vorrei imparare a volare. Come si fa?
Q3: Vorrei comprare una cuffia. Quale compro?
Q4: Che ne pensate di un aviofono portatile?

[19] *Frequently Asked Questions*: elenco di domande poste frequentemente nei newsgroup e di risposte organizzate in una sorta di codice elettronico per principianti.

Q5: Parlatemi delle ordinazioni per corrispondenza.
Q6: Sono un pilota privato. Come faccio a registrare l'ora?
Q7: Parlatemi delle informazioni meteo online DUATS.
Q8: Parlatemi dell'accesso a BITNET.

Faq n. 2)

Q1: Che cosa è un cupon?
Q2: Come si ottiene un cupon?
Q3: Come si utilizza il cupon?
Q4: Posso utilizzare più cupon alla volta?
Q5: Il cupon ha una scadenza?
Q6: Il cupon è nominativo?

Ecco ancora qualche chiacchiera sviluppata nell'ambito dei MUD [20]: ovvero di quegli spazi della fantasia, all'interno dei quali ci si diverte e si dà, per così dire, via libera al/ai proprio/i sé nascosto/i.

Chiacchiera n. 1)

Io e un mio amico siamo stati rimproverati per quello che abbiamo fatto in un MUD ... Ci siamo limitati a usare il comando *emote* in questo modo ... "<suo nome> tiene ferma <nome della vittima> mentre <mio nome> la violenta" ...

Un'azione riprovevole, che però qui avviene in un contesto libero, senza significato specifico. Non lo facciamo per vittimizzare le persone ..., ma per divertirci. D'accordo è roba da perversi, ma non è questo il punto... La vittima in realtà non se ne è curata, ritenendolo uno scherzo. Bè, ecco allora arrivare GOD e affermare che "violentare il personaggio di un partecipante è come violentare il partecipante stesso".

IDIOZIE

Questo è un GIOCO, nulla di più. Questo GOD deve darsi una calmata e smetterla di essere così serio. I MUD sono fatti per divertirsi, non per fare i seriosi. Non tornerò mai più su quel MUD

[20] Acronimo di *Multi-User Dungeon*, videogiochi di ruolo eseguiti su Internet attraverso il computer da più utenti. Giochi testuali, dove i giocatori interagiscono con il mondo e gli altri utenti digitando dei comandi sulla tastiera. Fra i più noti: *Equilibrium, Clessidra Mud, Tuch of Glory, Rda Mud, Isylea, Nebbie Arcane, Silmaril Mud, The Gate Mud.*

di mia spontanea volontà. Abbiamo fatto lo stesso in altri MUD e, anche se la vittima non ha gradito, i GOD della situazione le hanno detto "niente di grave; non ti hanno mica ucciso" [21].

Chiacchiera n. 2)

Sfida a duello La Furia *vs* Cloud

Caro mio vecchio Cloud, volevo proporti una sfida a duello per farla finita!

Il tuo astio e la tua cattiveria sono inutili!

Ormai il tuo potere e la tua supremazia è solo un lontano ricordo! Il migliore sono io!

In caso di vittoria il perdente consegna tutto il bottino.

Cloud, accetti?

Muori!

Accetto ovviamente!

Duelliamo… Dai … e vediamo chi tra me e te ha davvero il superpotere!

Non vi è dubbio che queste sono soltanto alcune delle tantissime chiacchiere disponibili in Rete. Oggi più che mai, infatti, ognuno di noi (non solo privati cittadini, ma anche figure e autorità istituzionali, politiche, religiose, e così via) ricorrono con frequenza alla comunicazione online. Di qui, il continuo sovrapporsi (e la continua confusione) fra quelli che sono i c.d. discorsi seri e le informazioni affidabili, con le opinioni personali, le dicerie e, persino, con le fake news. Basti perlustrare, ad esempio, *The Hate Page of the Week*: ritroviamo in generale un mercato vitale di idee politiche e in particolare una comunicazione informale sui fondamenti della società democratica. Naturalmente gli interessi e i temi sono i più vari: dagli annunci del Ku Klux Man, agli appelli dell'Aryan Nation, ai racconti dal Chiapas, oppure, alle vicende aggiornate dei Tupac Amaru, oppure al reclutamento dei foreign fighters e altro ancora.

Al di là dei tanti possibili esempi, però, ciò che qui è importante sottolineare è che esiste una stretta relazione tra i discorsi in-

[21] Per ulteriori considerazioni sullo stupro all'interno di un MUD, sul significato del comando *emote* e sull'affettività della vita postmoderna, S. TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, trad. it., Milano, Apogeo, 1997, p. 373 ss.

formali che si svolgono nelle comunità virtuali e il carattere estraniante della chiacchiera. In particolare, sono le modalità dell'incontro – già dette nelle comunità virtuali – a determinare una tale stretta relazione.

In tal senso, appare inevitabile il rinvio alle parole di Heidegger. Benché di per se stessa non abbia sempre una valenza negativa, la chiacchiera comunque si moltiplica insinuandosi in cerchie sempre più ampie. Le cose stanno così perché così si dice! E nel frattempo che si alimenta e cresce, non solo esime da una comprensione autentica, ma concorre anche a diffondere un approccio acritico e assolutamente indifferente. Persino il discorso pubblico può così tramutarsi in chiacchiera col rischio

"di non tener più aperto l'essere-nel-mondo in una comprensione articolata, anzi di chiuderlo e di coprire così l'ente intramondano [...]. La chiacchiera non è un prodotto dell'essere-assieme [...]. L'aver tutto visto e tutto compreso [...] la sicurezza di sé e la disinvoltura del Si, creano un'indifferenza crescente verso la comprensione emotiva autentica [...]. L'Esserci è spinto in un'estraniazione in cui nasconde a se stesso il suo più proprio poter-essere" [22].

[22] *Essere e tempo*, trad. it., Milano, Longanesi, 1970, p. 261 ss.

III

QUALCHE NUOVO S/OGGETTO. TRA ALGORITMI, INTELLIGENZA ARTIFICIALE, BIG DATA

Sommario

I

1. Dalla storia dei desideri e dei simulacri umani

La storia delle *macchine pensanti* è decisamente datata e articolata, come sono tutte quelle storie che hanno origine in bisogni e presupposti umani fondamentali e che si presentano come costanti universali. Reali o sognate, vere o imbrogli, le figure antropomorfe, questi doppi e simulacri umani di cui è ricca la storia [1], qualche volta tradiscono il desiderio dell'uomo di appropriarsi delle capacità divine di creare (e togliere) la vita.

[1] Le statue di Anubis, le macchine dell'imperatore Chin, le ancelle della fucina di Vulcano, le teste parlanti di papa Silvestro II e di Alberto Magno, e poi ancora il flautista e il tamburino di Vaucanson, le bambole perfette dei Jaquet-Droz, lo scacchista di von Kempelen, e tantissimo altro. Si veda

In particolare, l'idea delle macchine pensanti nasce dall'intensa fiducia nel potere creativo della mente, fiducia che fa esclamare ad Amleto:

"oh Dio! Io potrei viver confinato in un guscio di noce, e tuttavia ritenermi signore d'uno spazio sconfinato, non fossero i miei sogni" [2].

Nasce altresì da quell'insopportabile paura della solitudine che affligge l'uomo, così che da sempre si accompagna con immaginari compagni di gioco, automi, demoni, bambole meccaniche:

"può ben darsi – notava Nataniele – che a voi, gente fredda e prosaica, Olimpia faccia paura. Soltanto all'anima poetica si schiude l'anima gemella! […] Lo sguardo del suo occhio divino dice più che qualsiasi linguaggio" [3].

Nasce ancora dalla smania di immortalità e dall'antico desiderio di dare la scintilla della vita, secondo il mito di Prometeo:

"io non conosco al mondo / nulla di più meschino di voi, o dèi / […] Io renderti onore? E perché? / Hai mai lenito i dolori / di me ch'ero afflitto? / Hai mai calmato le lacrime / di me ch'ero in angoscia? / […] Io sto qui e creo uomini / a mia immagine e somiglianza, / una stirpe simile a me, / fatta per soffrire e per piangere, / per godere e gioire / e non curarsi di te, / come me!" [4]

---

in particolare M.G. LOSANO, *Storie di automi. Dalla Grecia classica alla Belle Époque*, Milano, Einaudi, 1990, e *Automi d'Oriente. "Ingegnosi meccanismi" del XIII secolo*, Milano, Edizioni Medusa, 2003.

[2] Atto II, scena II.

[3] Si tratta dell'attrazione che Nataniele prova verso la bella Olimpia, automa meccanico costruito dal professore Spallanzani e a cui Cornelius-Coppola ha inserito gli occhi – com'è noto narrata nel 1816 da Ernst HOFFMANN (*L'uomo della sabbia*, trad. it., Milano, Rizzoli, 2005, in part. pp. 40-41) e che ispirò nel 1880 il primo atto dell'opera di OFFENBACH, *I racconti di Hoffmann*, e nel 1919 suscitò il vivo interesse di FREUD nel saggio *Il perturbante* (in *Opere 1905-1921*, Roma, Newton, 2004, p. 1049 ss.). Qui, secondo il padre della psicanalisi, l'automa non è altro che la materializzazione dell'atteggiamento femminile avuto, nell'infanzia, da Nataniele verso suo padre: "Olimpia è un complesso dissociato di Nataniele, che gli appare sotto l'aspetto di individuo distinto, mentre l'asservimento di Nataniele a tale complesso si estrinseca nel suo amore insensato e ossessivo per Olimpia. Un amore di questo genere può a buon diritto essere definito narcisistico" (p. 1057).

[4] GOETHE, *Prometeo*, vv. 13-14, 38-42, 52-58.

Sin qui la narrazione artistica della vicenda umana che, fra tragedie, inni e racconti fantastici, ricomprende le storie di congegni e nature inorganiche, nel segno qualche volta dell'affinità, assai spesso delle pulsioni e dei bisogni segreti.

2. …ai moderni meccanismi

Altro approccio, altri legami: la storia delle macchine pensanti è anche la storia di grandi rivolgimenti e riorganizzazioni. Prima ancora che si potesse progettare, costruire e programmare il calcolatore intelligente, per avviare gli studi sull'Intelligenza artificiale [5] è stata necessaria la c.d. invenzione della mente [6], in particolare: *a*) la visione moderna dell'essere umano come entità distinta dal mondo, scandita dalla ri-concettualizzazione della ragione come strumento per l'esame delle parole (Hobbes), delle idee (Locke), delle rappresentazioni (Leibniz); *b*) l'affermarsi della nuova matematica e la ricerca di regole logiche che vengono espresse mediante il linguaggio, quali le verità di ragione di Leibniz, le leggi del pensiero di Boole, fino al calcolo dei predicati di Frege, Russell e Whitehead; *c*) lo sviluppo, dapprima, delle macchine da calcolo meccaniche (oltre all'orologio calcolatore di Schickard, la scatola di Pascal e il calcolatore di Leibniz), in seguito, il progetto della macchina alle differenze (di Babbage) e la costruzione del calcolatore differenziale (di Scheutz), sino poi ai calcolatori automatici elettronici [7].

Sono così costruiti meccanismi che riproducono singole funzioni intelligenti, dapprima i semplici regolatori e selettori automatici e poi i diversi dispositivi atti a memorizzare, apprendere, riconoscere forme. Dagli analizzatori differenziali ai sistemi di tabulazione elettronica, dal calcolatore a relè per numeri complessi ai calcolatori giganti e, inoltre, all'automa degli scacchi, dal-

---

[5] Si veda P. MCCORDUCK, *Storia dell'intelligenza artificiale*, trad. it., Padova, Muzzio, 1987.

[6] L'espressione è di R. RORTY, *La filosofia e lo specchio della natura*, trad. it., Milano, Bompiani, 1988.

[7] Si vedano: H.H. GOLDSTINE, *Il computer da Pascal a Von Neumann. Le radici americane dell'elaboratore moderno*, trad. it., Milano, Etas, 1981; V. PRATT, *Macchine pensanti. L'evoluzione dell'intelligenza artificiale*, trad. it., Bologna, Il Mulino, 1990.

l'Univac I [8] al Powerbook di Negroponte [9], quel che più rileva è il passaggio dalla semplice automazione

"delle primordiali macchine per tabelle alla sua attuale condizione di versatile macchina informatica, [...] la potenza del computer [...] [viene] proiettata sull'ordito già elaborato dalla ricerca operativa e dall'analisi dei sistemi" [10].

Quanto più lo sviluppo scientifico e tecnico avvicina la macchina al pensiero artificiale [11], tanto più l'elaboratore si trasforma da calcolatrice in calcolatore. La prima svolge funzioni aritmetiche, il secondo funzioni logiche di confronto. Nella prima è l'uomo a inserire i dati operandi, a determinare la sequenza delle operazioni, a valutarne il risultato; nel secondo è un'altra macchina, cioè l'unità di governo, che durante lo svolgimento delle operazioni necessarie e grazie alla memoria centrale di volta in volta controlla, archivia, trasforma.

E intanto che si costruiscono dispositivi sempre più raffinati, si attiva un dibattito sull'intelligenza del calcolatore – si pensi al dialogo radiofonico tra il filosofo della scienza Richard Braithwaite, il matematico Max Newman, il neurochirurgo Geoffrey Jefferson e il logico Alan Turing [12] –, e via via si modifica l'immagine

---

[8] Si tratta del primo calcolatore elettronico messo in commercio e acquistato nel 1951 dall'ufficio del censo degli Stati Uniti, che rinnovò le tecniche di elaborazione dati e più in particolare automatizzò la produzione di tabelle che avveniva nelle cosiddette *tab rooms*.

[9] *Essere digitali*, trad. it., Milano, Sperling & Kupfer, 1996, p. 1.

[10] Così J. WEIZENBAUM, *Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale*, trad. it., Torino, Gruppo Abele, 1987, p. 48.

[11] E oggi al pensiero *tout court*, a sentire le riflessioni sul futuro di Ray KURZWEIL. Grazie ad una crescita esponenziale *esplosiva*, molto presto i supercalcolatori di nuova generazione, e cioè i *cluster* (insiemi di processori a basso costo, uguali a quelli dei comuni PC, collegati tra loro per spartirsi il carico di lavoro), saranno in grado di simulare il funzionamento del cervello e le sue funzioni neuronali di apprendimento. Ed entro qualche decennio, le tecnologie informatiche includeranno tutte le conoscenze e competenze umane, comprese le tecniche di *pattern recognition*, come pure le capacità di risolvere problemi e di rispondere appropriatamente alle emozioni (la cosiddetta intelligenza emotiva, tipica del cervello umano) (*La singolarità è vicina*, trad. it., Milano, Apogeo, 2008).

[12] Alla Bbc il 14 gennaio 1952, pubblicato in *Sistemi intelligenti*, aprile 1998.

che noi abbiamo della macchina: dapprima 'conduttore e trasmettitore di *potenza*', ora 'trasformatore di *informazione*' [13].

3. ...alle moderne intuizioni

Quella dell'Intelligenza artificiale è la storia di grandi intuizioni. Nel saggio *Computing machinery and intelligence* [14], Turing si chiede se sia possibile per ciò che è meccanico manifestare un comportamento intelligente. La risposta è nota: la macchina universale, equivalente logico di una macchina a stati finiti, è equiparabile al cervello e può dunque essere programmata in modo da imitare il funzionamento cerebrale [15]. Ciò che infatti è rilevante, sia del cervello che della macchina universale, è soltanto lo schema logico degli stati discreti, lettura e scrittura. Non è invece rilevante la chimica o la fisica, poiché qualsiasi cosa faccia un cervello, esso lo fa in virtù della sua struttura in quanto sistema logico e non già perché posto nella testa di una persona o perché tessuto spugnoso costituito da un tipo particolare di formazione biologica cellulare. E se questo è vero, se cioè la descrizione dei processi mentali è indipendente dal corpo:

"ci proponiamo […] di vedere cosa possa essere fatto con un 'cervello' che sia, più o meno, senza un corpo, provvisto al massimo di organi di vista, parola e udito" [16],

allora la struttura logica del cervello può essere rappresentata altrettanto bene in qualche altro elemento, incorporata in qualche altra macchina fisica.

Oltrepassando, per un verso, l'idea secondo cui solo l'intelligenza umana sarebbe capace di trovare metodi per superare gli errori, e per l'altro, l'idea secondo cui l'intelligenza della macchina sarebbe nulla più che un riflesso dell'intelligenza del suo creatore, è aperta la strada per la costruzione di macchine con ri-

---

[13] J. WEIZENBAUM, *Il potere del computer e la ragione umana*, cit., pp. 54-55.

[14] Pubblicato in *Mind*, 59, 1950, pp. 433-460.

[15] Si veda in particolare *Macchine intelligenti*, in A. TURING, *Intelligenza meccanica*, trad. it., Torino, Bollati Boringhieri, 1994, p. 88 ss.

[16] *Ivi*, p. 103.

sorse analoghe a quelle di un operatore umano. In primo luogo, la memoria: deposito di informazioni, alla stregua della carta sulla quale l'operatore umano scrive i suoi calcoli o alla quale si richiama quale libro delle regole. In secondo luogo, l'unità operativa: parte dove sono compiute le varie operazioni singole che un calcolo comporta (e quali siano queste singole operazioni dipende dalle diverse macchine). In terzo luogo, il governo o controllo: nella macchina il libro delle regole dell'operatore umano è sostituito dalla tavola delle istruzioni presente in una parte della memoria. È compito quindi del governo verificare che le istruzioni siano eseguite correttamente e nell'ordine giusto. Va da sé che il libro delle regole, appena accennato, è una comoda immagine, giacché il calcolatore umano si ricorda di ciò che deve fare. E tuttavia, se si vuole che una macchina riproduca in modo fedele il comportamento di un calcolatore umano nello svolgimento di una serie di operazioni, è necessario chiedere all'uomo come andrebbero risolte quelle operazioni e la sua risposta deve essere tradotta nella forma di una tavola di istruzioni. Inserire tavole di istruzioni in una macchina significa dunque programmare una macchina in modo che compia l'operazione X [17].

La macchina di Turing costituisce un sistema formale automatico. In particolare, il sistema formale è come un gioco nel quale i segni (i pezzi, le occorrenze [18]) sono manipolati in accordo con delle regole, al fine di vedere quali configurazioni possono essere ottenute. E come in ogni gioco, bisogna specificare che cosa sono i segni, qual è la posizione iniziale e quali mosse sono permesse in ogni posizione data. Vanno subito notate tre caratteristiche (del gioco o sistema formale): *1*) il sistema è interamente auto-contenuto, nel senso che solamente i pezzi con le loro mosse contribuiscono a mutarlo; *2*) è perfettamente definito, ovvero non vi sono ambiguità, approssimazioni, casi intermedi, per de-

---

[17] V. di TURING sia la *Proposta per lo sviluppo nella divisione matematica di una macchina calcolatrice elettronica (ACE). Parte I: presentazione descrittiva* e sia *Macchine calcolatrici e intelligenza*, in *Intelligenza meccanica*, cit., p. 29 ss. e p. 125 ss.

[18] "Le *posizioni* di un sistema formale possono funzionare come *occorrenze* in un altro sistema (di 'livello superiore') […]. Ogni occorrenza del gioco dell'algebra è una posizione valida in un altro gioco, che potremmo chiamare il 'gioco delle formule ben formate'" (così J. HAUGELAND, *Introduzione*, in J. H. (a cura di), *Progettare la mente. Filosofia, psicologia, intelligenza artificiale*, trad. it., Bologna, Il Mulino, 1989, pp. 15-16).

terminare una certa posizione o la correttezza della mossa; *3*) è controllabile entro un lasso finito di tempo, ossia per valutare la validità della mossa in una posizione deve essere verificato solo un numero finito di cose [19]. Il sistema formale automatico, poi, non è altro che un congegno fisico, una macchina,

"che manipola automaticamente le occorrenze di un qualche sistema formale in accordo con le regole di quel sistema. È come una partita di scacchi che muove e gioca *da sola* […], o come un sistema assiomatico che scrive le proprie dimostrazioni e teoremi senza nessun aiuto da parte di un matematico" [20].

Pertanto nel costruire un sistema formale automatico è necessario risolvere due problemi di fondo. Da un lato, far sì che il congegno obbedisca alle regole, dall'altro, automatizzare il meccanismo per decidere tra diverse opzioni valide quale mossa eseguire. E la macchina di Turing [21], con un numero illimitato di caselle di memoria, con un numero finito di unità di esecuzione e con un indicatore di unità, fa sì che i due problemi (cioè quello dell'obbedienza alle regole e del controllo) vengano risolti.

4. …e al dilemma: intelligenza e/o coscienza artificiale?

Non è detto che giocare contro una tale macchina dia la precisa sensazione di stare scontrandosi contro qualcosa di vivo [22], quel che però è certo è che la macchina diventerà sempre più intelligente. L'11 maggio 1997 è una data importante: il calcolatore Ibm Rs/6000, Deep Blue, batte Garry Kasparov, campione del

---

[19] Il che equivale a dire: "un gioco o un sistema che ha tutte e tre le proprietà è *digitale*. In questo senso tutti i sistemi formali sono digitali. La proprietà di essere digitali ha, per ciò che riguarda i sistemi formali, le seguenti importanti conseguenze: due sistemi che sembrano essere assai differenti possono, nonostante ciò, essere essenzialmente il medesimo sistema" (*ivi*, p. 13).

[20] *Ivi*, p. 17.

[21] Nel 1936 lo scienziato dimostrò come costruire una macchina secondo i suoi principi: *On computable numbers, with an application to the* Entscheidungsproblem, in *Prooceedings of the London Mathematical Society*, serie II, 42, 1936, p. 230 ss.

[22] Come invece sosteneva TURING, *Macchine intelligenti*, cit., in part. pp. 91 e 97.

mondo di scacchi. Nel febbraio del 2011 Watson della Ibm batte alcuni campioni nel gioco televisivo Jeopardy e nel 2015-2016 il sistema AlphaGo batte due dei giocatori di dama più forti al mondo, nel gennaio del 2019, i campioni di Starcraft sono stati battuti dall'intelligenza artificiale di DeepMind.

Queste sfide mettono in evidenza gli importanti livelli raggiunti dalle macchine, ormai in grado di gestire simboli e predisporre mosse, così da vincere. Non annulla però la diversità che esiste tra l'esperienza di giocare, attributo tipico dell'essere umano, e lo stesso comportamento intelligente, che l'umano può condividere con diversi programmi e vari sistemi. Nonostante gli sviluppi resta perciò inattuata quella storia della narrativa fantastica e della fantascienza popolata da esseri artificiali dotati di coscienza: Frankenstein di Mary Shelley, i robot di Karel Čapek, Robbie di Isaac Asimov, come pure HAL di Stanley Kubrick che, diverso dagli altri citati, è privo del corpo. Resta inattuata poiché è indubbio che il tema della coscienza è di approccio particolarmente complesso, poteva non suscitare immediato interesse dal punto di vista ingegneristico, anche se ormai si assiste all'affermarsi della disciplina *Artificial Consciousness* (riecheggia l'altra: *Artificial Intelligence*) e al diffondersi di convegni sulla Scienza della coscienza (si pensi alle tante edizioni che hanno luogo a Tucson in Arizona), convegni e centri che riuniscono diversi studiosi con approcci e ragioni differenti (filosofi e scienziati, farmacologi e fisici, neuro-scienziati e neuropsicologi, ecc.).

Di qui l'attenzione per i tanti significati che l'espressione coscienza comunica e per i diversi fenomeni che le scienze cognitive tentano di spiegare, dai più o meno semplici (ad esempio, le capacità di integrare le informazioni, di reagire agli stimoli, di controllare i comportamenti) ai più complessi, quale può essere la spiegazione scientifica del perché sentiamo dolore, gioia, angoscia. Si tratta di un interrogativo fondamentale, anche alla luce degli attuali sviluppi tecnici e dei progressi nel campo delle neuroscienze, sempre più attente alla coscienza, ai suoi contenuti e alla sua interazione con l'ambiente. C'è in gioco la grande questione della decisione (libera) che distingue l'essere umano da ogni altro ente, ma che via via sembra poter essere spiegata da considerazioni che sottolineano l'*errore di Cartesio*[23], ovvero la

[23] V. A. Damasio, *L'errore di Cartesio. Emozioni, ragione e cervello umano*, trad. it., Milano, Adelphi, 1995.

separazione tra la razionalità e la regolazione biologica, tra la decisione e l'emozione.

Quanto accennato ha delle particolari ricadute. L'attenzione verso i processi mentali, prima descritti indipendentemente dal corpo, si rivolge ora a tutte quelle dimensioni che concorrono a prendere le decisioni e a determinare i comportamenti. D'altra parte, come nel caso della macchia nera il nostro cervello integra l'informazione visiva a nostra insaputa e grazie al combinarsi di altri dati [24], le nostre scelte e le nostre azioni dipendono da una serie di circostanze e dai marcatori somatici, esempi questi di

"*sentimenti generati a partire dalle emozioni secondarie*. Quelle emozioni e sentimenti *sono stati connessi, tramite l'apprendimento, a previsti esiti futuri di certi scenari*. Quando un marcatore somatico negativo è giustapposto a un particolare esito futuro, la combinazione funziona come un campanello d'allarme; quando invece interviene un marcatore positivo, esso diviene un segnalatore di incentivo" [25].

Se così, una svolta si rende necessaria: gli studi sull'IA devono potere essere integrati da tutte quelle ricerche per meglio comprendere il formarsi della coscienza, ormai oggetto di studio scientifico visto che essa può essere letta come quell'aspetto ausiliare della nostra dotazione biologica di adattamento all'ambiente. Ancora una volta, altro approdo e altra riorganizzazione: non più la mente distinta dal corpo, bensì l'organismo che partecipa dell'esperienza cosciente. Il che vuol dire, dal punto di vista tecnologico, la previsione che si sia in grado di intervenire nei suoi meccanismi e che questi stessi possano essere riprodotti.

---

[24] Si tratta della c.d. macchia cieca nel nostro campo visivo, corrispondente all'innesto del nervo ottico nella retina. In quella zona dovremmo vedere una macchia nera, eppure il nostro campo visivo è privo di interruzioni (per le prime considerazioni sull'argomento si veda in http://www.fondazionepatriziopaoletti.it/news/816/rubrica_human_nature_come_l_acqua_per_i_pesci_.html).

[25] Così A. DAMASIO, *L'errore di Cartesio*, cit., pp. 245-246.

II

1. A partire dalle reti neurali artificiali

Il presente è il risultato di vecchie e nuove riorganizzazioni e intuizioni. Nel presente gli studi su algoritmi, software, app, si moltiplicano e si rafforzano. Intanto mutano le velocità e si assiste a cambi di paradigma. Pochi anni per fare quel che si è fatto in secoli: è sufficiente qui considerare il tempo trascorso tra la rivoluzione della stampa e quella informatica, tra quest'ultima e la rivoluzione dei big data (cioè dati di varia natura, generati da algoritmi in tempo reale e il cui volume è impressionante). D'altra parte, anche le teorie dei 6/12 gradi di separazione per entrare in relazione sono oggi – nell'era della connessione – sostituite da quella secondo la quale ogni persona sarebbe collegata a qualunque altra grazie a soli 3/4 contatti. Inoltre, nell'era della crescita esponenziale di dati, il paradigma logico-deduttivo cede il passo all'approccio statistico, che tra i vari scopi (ad esempio: fare previsioni, verificare delle ipotesi e suggerirne di nuove, facilitare l'analisi dei dati e ridurre la loro mole) ha quello fondamentale di raggruppare gli oggetti in classi, il più possibile omogenee, e di determinare il numero e le caratteristiche delle classi.

Algoritmi, intelligenza artificiale, big data, tre espressioni-chiave attorno alle quali ruota l'odierno sviluppo tecno-scientifico che prosegue sulla via dell'evoluzione delle reti neurali, avendo come riferimento quelle biologiche, e che utilizza i c.d. algoritmi di apprendimento: ora algoritmi di apprendimento supervisionato (a partire da un insieme di input ai quali corrispondono output noti, la Rete apprende il nesso che li unisce e impara a generalizzare, ossia a calcolare nuove associazioni corrette input-output processando input esterni al *training set*), talaltra di apprendimento non supervisionato (a partire da un insieme di variabili di input, la Rete crea dei cluster rappresentativi per categorizzarle), ora algoritmi di apprendimento per rinforzo (è dall'interazione con l'ambiente che i circuiti neurali imparano ed eseguono una serie di azioni, delle quali quelle che si avvicinano al risultato sono considerate di rinforzo, mentre le altre sono eliminate perché foriere di errore). Le reti neurali artificiali presentano diversi vantaggi, di qui la loro diffusione nei più disparati settori laddove sono richiesti *data mining*, elaborazione di

modelli predittivi e simulativi, classificazione ecc. Con queste, infatti, si possono processare senza particolare dispendio di tempo ed energie una gran mole di dati, si può operare assai spesso in modo corretto nonostante input imprecisi o incompleti, e quando invece sono ben implementate sono in grado di autoaggiornarsi in presenza di modifiche ambientali. Com'è intuitivo, le reti neurali artificiali presentano pure dei limiti, ad esempio la loro computazione non è analizzabile in modo completo, gli output somministrati non rappresentano assai spesso la soluzione perfetta, non sono idonee per il momento a risolvere determinate categorie di problemi.

Al di là dei vantaggi e dei limiti delle reti neurali artificiali, le tre espressioni chiave ricordate propongono una domanda fondamentale: l'attività svolta dai sempre più sofisticati software può considerarsi neutrale, ovvero, quell'insieme di algoritmi e di big data, entro la cornice di una intelligenza artificiale capace di riconoscere, classificare, ragionare, diagnosticare, agire, può essere ritenuto di per sé in ogni caso obiettivo?

2. Algoritmi e non-neutralità

Gli esseri umani scrivono gli algoritmi, analizzando innanzitutto il problema, descrivendo la specifica funzionale, come pure i passi da eseguire per giungere al risultato, traducendo infine il diagramma di flusso in programma. Ipotesi di partenza, parametri, dati, funzioni, di un programma possono essere di volta in volta diversi: non c'è quindi un unico modo di produrre un algoritmo e d'altra parte una variazione anche semplice di un parametro o di un dato conduce a risultati diversi. Alcune volte, poi, l'algoritmo può persino muovere da pregiudizi: basti pensare a quello di Google Photo che ha catalogato sotto il termine 'gorilla' l'immagine di due persone di colore, altre volte l'algoritmo serve a raccogliere dati sui (bravi/cattivi) cittadini, come ad esempio il programma Sesame Credit del governo cinese.

In *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia* Cathy O'Neill [26]

[26] Trad. it., Milano, Bompiani, 2017.

mette in guardia dall'affidabilità e oggettività degli algoritmi, poiché questi possono esprimere pregiudizi a causa di una programmazione che si presenta sotto il segno della superficialità, possono altresì essere ricondotti a previsioni alquanto singolari (si pensi al software di predizione della criminalità PredPol della polizia di Los Angeles) o essere utili per vere e proprie truffe (si pensi al software che ha consentito alla Volkswagen di alterare le rilevazioni delle emissioni inquinanti).

Oltre a Cathy O'Neill, anche Dominique Cardon [27], Wolfie Christl e Sarah Spiekermann [28], e molti altri ancora mettono in guardia dagli algoritmi. Dietro formule e modelli matematici, dietro diagrammi e procedimenti formali, si celano meccanismi di alterazione dell'informazione e di condizionamento dell'azione. Ad esempio: il successo commerciale può dipendere dall'ordine con cui Google posiziona i risultati delle ricerche; il like dipende dalla selezione predisposta dagli algoritmi del social network, per cui solo alcuni messaggi possono essere marcati dal 'mi piace'; il prezzo di un biglietto aereo dipende dal profilo del viaggiatore ricostruibile attraverso l'uso di un certo dispositivo, l'orario d'accesso, le ricerche già effettuate; l'accesso al prestito e i tassi di rientro dipendono da formule matematiche i cui parametri non sono riconducibili soltanto alla capacità finanziaria; anche il destino politico di un paese, o di più paesi, può dipendere dal software e da chi possiede i dati sugli elettori.

Già questi pochi esempi confermano gli aspetti critici, ovvero: l'asimmetria informativa tra una società che offre un servizio e l'utente, l'assenza di trasparenza relativa ai princìpi e ai parametri alla base del funzionamento dell'algoritmo, la creazione di una sorta di *filter bubble*, così che siano mostrate all'utente soltanto quelle informazioni che l'algoritmo ha calcolato gli possano interessare, o al contrario, che ha ritenuto per varie ragioni di non dovere fornire. Di qui, l'inesistenza di algoritmi neutrali, di algoritmi che si limitano a riflettere la realtà, essi anzi propongono una loro versione fatta dalle formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato. E intanto aumentano in modo esponenziale i

---

[27] *Che cosa sognano gli algoritmi*, trad. it., Milano, Mondadori, 2016.

[28] *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*, Paperback, Autflage, 2016.

dati, ogni soggetto è classificabile e ogni nuovo dispositivo raccoglie dati [29], dal like si risale con margini d'errore minimi al colore della pelle, all'orientamento sessuale, all'appartenenza politica, come pure al quoziente intellettivo, alla religione e a tanto altro ancora, accade così che gli algoritmi generino sempre più messaggi personalizzati e stratagemmi per orientare la condotta.

3. Intelligenza artificiale e big data

Di grande rilievo, in quest'ambito, è l'ormai acquisita capacità di auto-apprendimento delle macchine, grazie all'applicazione delle citate reti neurali artificiali. I computer capaci di apprendere in modo automatico costituiscono la vera grande svolta e con essa evidenziano il possibile rischio di un sistema non controllato, tale da richiedere una sorta di *Algorithm Liberation Front* per rendere trasparenti i criteri decisionali alla base dei diversi strumenti.

L'Intelligenza artificiale opera in vario modo, quel che però va innanzitutto sottolineato è l'importanza che essa riveste in tutte quelle attività che richiedono decisioni a partire da enormi quantità di dati. A tal proposito si consideri Google Street View e in particolare l'elaborazione dei dati qui raccolti da parte dei sistemi di IA. Le informazioni ricavabili, anche dal c.d. rumore, sono certo interessanti per lo studio delle città e delle persone che le abitano.

Significativa è stata la ricerca di un team della Stanford University: a partire da più di 50 milioni di immagini su 200 città mappate da Google Street View, immagini elaborate con una tecnica di riconoscimento degli oggetti così da permettere al software di individuare le auto (ben 22 milioni) e di classificarle (secondo la marca, il modello, l'anno), il team è stato in grado di fornire alcune indicazioni demoscopiche. Per la ricerca si è usato un algoritmo a rete neurale *convoluzionale* (*convolutional neural network*, *ConvNet*) in grado di processare 50 milioni di immagine

[29] V. in tal senso Michal KOSINSKI, esperto di psicometria, branca della psicologia fondata sull'analisi delle tracce digitali, e in particolare studioso dei profili psico-demografici degli utenti di Facebook. È uno dei principali protagonisti della vicenda Cambridge Analytica.

in due settimane, contro i circa quindici anni dell'intelligenza umana, e con la caratteristica essenziale di ricavare dati reali, poiché in due settimane i 22 milioni di veicoli individuati restano indicativi del patrimonio di veicoli circolanti in quelle città.

Muovendo da questa grande mole di dati, i ricercatori hanno utilizzato queste informazioni al fine di capire le inclinazioni politiche, hanno così osservato come con più pick-up l'area urbana aveva una probabilità dell'82% di votare repubblicano, e invece con più berline c'era l'88% di possibilità che il quartiere votasse democratico. In questo caso, l'algoritmo usato è quello tipico del *machine learning*, e cioè l'analisi della regressione con la quale si stima un'eventuale relazione funzionale tra la variabile dipendente e le variabili indipendenti. Simile tecnica fornisce delle informazioni parecchio accurate, non limitate naturalmente alle foto di auto e alle previsioni di voto, di qui l'importanza di questi nuovi strumenti (in questo caso, la rete neurale in grado di gestire al meglio le immagini) per gli scienziati sociali e per le loro previsioni.

Intelligenza artificiale e big data, ovvero database che raccolgono enormi quantità di informazione di vario tipo (dalle immagini ai video, dai testi all'audio, dai like su Facebook alle transazioni monetarie) e che richiedono l'utilizzo di calcolatori di grande potenza per la raccolta di questi dati eterogenei e sterminati, come pure per l'individuazione di relazioni (collegamenti, connessioni) e per l'estrapolazione di previsioni. Si tratta di una nuova era, nella quale il paradigma dei big data riporterebbe il discorso sul piano dell'oggettività, visto che sarebbero gli stessi dati, senza alcuna pregiudiziale e senza essere condizionati dall'orizzonte di attese dell'osservatore, a dirci del benchmark, del modello, e della correlazione significativa fra un numero tendenzialmente infinito di variabili. Tutto ciò sarebbe reso possibile, oltre che dalla straordinaria potenza di calcolo, dal tipo di apprendimento che in quanto statistico non richiederebbe una reale comprensione dei fenomeni.

Per il vero, i dati non sono oggettivi e i modelli statistici rappresentano la realtà modificandola, e cioè orientando i comportamenti. Secondo Dominique Cardon [30], le misurazioni statisti-

[30] *Che cosa sognano gli algoritmi*, cit.

che servono a fabbricare il futuro, poiché la società si orienta secondo le informazioni che le sono prospettate. D'altra parte, è da sottolineare come i big data non siano a disposizione di chiunque, bensì di pochi, che detengono e organizzano i dati sulla spinta di interessi commerciali, e che le caratteristiche degli algoritmi in uso (ad esempio, di Google, Facebook, Amazon) restano per lo più ignoti [31].

4. Ci vuole una regola! Una Carta dei diritti 4.0!

Tim Berners-Lee, inventore del World Wide Web, ritiene ormai necessaria una Costituzione che protegga l'indipendenza di Internet e i diritti dei suoi utenti. Di qui la campagna *The web we want*, volta a sollecitare la redazione di una carta dei diritti digitale in ciascun paese, dal momento che se non si ha

"un internet libero [...] non possiamo avere un governo libero, una buona democrazia, un buon sistema sanitario, comunità connesse e diversità di culture [...] è ingenuo pensare di poter rimanere a braccia conserte e ottenerlo [...] I nostri diritti vengono violati sempre più da ogni parte e il pericolo è che ci si possa abituare a tutto questo. Per questo voglio usare il 25esimo compleanno perché ci si impegni tutti a riportare nelle nostre mani il web e a stabilire quale rete vogliamo per i prossimi 25 anni".

Nonostante resti un ottimista [32], Berners-Lee sottolinea in molteplici occasioni come il Web sia ormai popolato da guardiani digitali sempre più potenti, le cui armi sono algoritmi in grado di manipolare le persone e di limitarne la libertà.

"*The system is failing. The way ad revenue works with clickbait is not fulfilling the goal of helping humanity promote truth and democracy. So I am concerned*" [33].

---

[31] Cfr. F. PASQUALE, *The black box society: The secret algorithms that control money and information*, Cambridge, Harvard University Press, 2015.

[32] "*I'm still an optimist, but an optimist standing at the top of the hill with a nasty storm blowing in my face, hanging on to a fence*" (T. BERNERS-LEE, *Tim Berners-Lee on the future of the web: 'The system is failing'*, in *The Guardian*,15 novembre 2017).

[33] *Ivi*.

Di qui la richiesta della regolamentazione della pubblicità politica online, così da evitare usi impropri e eticamente non giustificati.

"We urgently need to close the 'internet blind spot'in the regulation of political campaigning" [34].

Riportare quindi il Web, quale spazio aperto e luogo delle opportunità, lontano da quel che effettivamente lo minaccia, e cioè la perdita di controllo dei dati personali, la diffusione di disinformazione e di *fake news*, la sinuosa pubblicità politica. La via è in parte obbligata. Si tratta di garantire in senso proprio il consenso informato, che in molti casi manca, specie in quelli in cui, in cambio di contenuti o servizi gratuiti, si cedono dati personali; si tratta inoltre di rendere trasparenti gli algoritmi, così da capire come si formano le informazioni (e le disinformazioni), come si determinano al contempo gli orientamenti degli attori sociali.

L'odierna quantità di dati è realmente abnorme, una raccolta questa che utilizza dispositivi di vario tipo e nei più diversi ambiti: dalla televisione ai telefoni e ai computer, dalle carte di credito alle smart card, dai sensori delle case alle infrastrutture intelligenti delle città. Il flusso è continuo, l'ordine dei byte segna record incredibili, ma quel che lascia per certi versi stupiti è la capacità di usare ogni singola informazione di questa quantità indicibile per analizzare, elaborare, suggerire e orientare modelli di interpretazione e di azione. La rivoluzione big data consiste proprio in ciò: trattare le tante variabili in poco tempo e con poche risorse computazionali, e questo è ovviamente importante in ogni settore. Si pensi per il marketing ai c.d. metodi di raccomandazione (Netflix, Amazon) per indurre all'acquisto di un bene o un servizio, metodi questi che muovono dai dati provenienti dalla navigazione dell'utente (pagine visitate, prodotti ricercati, acquisti) e ne individuano il profilo, lo status, la condizione, l'attendibilità, ecc. Si pensi inoltre per la sfera pubblica alle statistiche di rilevanza penale, che muovono ormai da una enorme quanti-

[34] Così si legge in occasione del 28 anniversario della sua invenzione (T. BERNERS-LEE, *Three challenges for the web, according to its inventor*, in *Web Foundation*, 12 marzo 2017).

tà di dati e connessioni anche inusuali e che possono essere usate per prevedere il verificarsi dei reati e per dispiegare le forze di polizia. Si pensi ancora al rilievo che i dati hanno in medicina e all'apporto dei big data che, se condivisi, potrebbero ad esempio realizzare sistemi in grado di analizzare e combattere tempestivamente focolai epidemici, ma anche di predirli e prevenirli.

5. Dal Regolamento europeo sul trattamento e la libera circolazione dei dati personali

Diventa allora necessario avere delle regole, una dichiarazione di principi da osservare, al momento della raccolta, della classificazione, dell'analisi, della sintesi dei dati.

Nel 2016 il Parlamento europeo e il Consiglio hanno adottato il regolamento 679 che si applica al trattamento interamente o parzialmente automatizzato di dati personali, come pure al trattamento non automatizzato di dati personali contenuti in archivi o destinati a figurarvi (art. 2). Qui è l'art. 6 a prevedere la presenza di almeno una delle seguenti condizioni quale fondamento di liceità del trattamento, e cioè che (*a*) l'interessato abbia espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; che (*b*) il trattamento sia necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; che (*c*) il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; che (*d*) il trattamento si renda necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; che (*e*) il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; che (*f*) il trattamento sia essenziale per il conseguimento del legittimo interesse del titolare del trattamento o di terzi, ove non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Il regolamento prevede innanzitutto una idonea richiesta del consenso, in particolare tale richiesta deve contenere le informazioni relative al titolare del trattamento, agli eventuali destinatari

e alle finalità (natura e durata) che ci si propone con la raccolta e l'uso dei dati. Per una raccolta e un uso dei dati improntati alla correttezza e alla trasparenza, la richiesta dovrà inoltre contenere le informazioni circa i diritti dell'interessato di intervenire sull'uso e sul periodo di conservazione dei dati. Pur variando a secondo dell'utilizzo o meno di strumenti elettronici, e a secondo del servizio che si intende offrire, formule e informazioni utilizzate per chiedere il consenso devono essere espresse in modo comprensibile, semplice e chiaro, oltre che distinguibili da altre richieste rivolte all'interessato per ulteriori questioni (art. 7.2). All'idonea richiesta del consenso segue la volontaria accettazione al trattamento dei dati. Il consenso deve, infatti, essere espresso attraverso un atto positivo libero, specifico, inequivocabile e informato, non è ammesso il consenso tacito o presunto, può essere comunicato sia per iscritto o oralmente, sia mediante mezzi elettronici.

Poiché i dati personali rappresentano il cittadino, prima, durante e dopo il trattamento, bisogna in base all'art. 5 che siano osservati i seguenti principi, ovvero: *a*) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ('liceità, correttezza e trasparenza'); *b*) raccolti per finalità determinate, esplicite e legittime, e trattati in maniera che non sia incompatibile con tali finalità ('limitazione della finalità'); *c*) proposti perché adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ('minimizzazione dei dati'); *d*) considerati esatti rispetto alle finalità per le quali vengono trattati e, quindi, corretti se necessario ('esattezza'); *e*) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ('limitazione della conservazione'); *f*) trattati in modo da garantire una adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti, e dalla perdita, dalla distruzione o dal danno accidentali ('integrità e riservatezza'). A questi diversi e importanti principi va aggiunto quello di 'responsabilizzazione' del titolare del trattamento, proprio in quanto competente e in grado di comprovare il rispetto dei principi ricordati.

Quanto ai diritti, ai c.d. *diritti tecnologici*, l'interessato ha il diritto (art. 7.3) di revocare il proprio consenso in qualsiasi momento e con la stessa facilità con la quale lo ha prestato. Ciò non pregiudica la liceità del trattamento (basata sul consenso) prima

della revoca stessa, e di questo l'interessato deve essere consapevole grazie a idonea informazione. L'interessato ha inoltre il diritto di ottenere dal titolare del trattamento la conferma che sia in corso un trattamento dei propri dati e, in caso positivo, il diritto di accedere (art. 15) ai dati personali e alle diverse informazioni, ovvero il diritto di sapere per quali fini sono stati adoperati i dati, quale categorie di dati sono state utilizzate, a chi sono stati comunicati, il periodo di tempo entro cui i dati saranno conservati (di sicuro o anche presumibile), la logica utilizzata nel processo decisionale automatizzato, e il diritto di proporre reclamo presso l'autorità di controllo. Di qui, la possibilità per l'interessato di esercitare i diritti di rettifica (art. 16), di cancellazione (c.d. 'diritto all'oblio' art. 17), di limitazione (art. 18), di portabilità dei dati (art. 20), come pure i diritti di opposizione al trattamento stesso (art. 21) o il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida significativamente sulla sua persona (art. 22). Com'è chiaro, perché siano riconosciuti questi diritti, in modo da controllare sempre le conseguenze del proprio consenso, occorre che il titolare del trattamento fornisca senza ingiustificato ritardo le informazioni richieste. Si configurano così veri e propri doveri (quali quelli di rettificare, di integrare, di limitare, di sospendere, di cancellare, di non trattare) corrispondenti sia ai diritti dell'interessato, sia ai divieti di trattare alcune specifiche categorie di dati personali (art. 9), sia ai più generali obblighi in capo al titolare e al responsabile del trattamento (artt. 24-31), in modo da garantire un adeguato livello di sicurezza dei dati (artt. 32-34) anche alla luce di valutazioni dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35).

III

1. Robot di vario tipo, di diversa struttura, di differente funzione

Intanto che i programmi di intelligenza artificiale vengono via via perfezionati, e cioè si trasformano in veri e propri sistemi au-

tonomi in grado di apprendere dall'esperienza e di superare in diverse occasioni lo stesso controllo umano, sempre più si studiano le forme che possono accogliere i programmi di IA. Si sviluppano macchine di vario tipo e di diversa struttura. In generale, queste macchine possono essere così classificate:

i) robot *estranei e opposti* all'uomo, nelle loro forme irte, metalliche, sferraglianti

"un grosso cilindro di metallo, che al posto delle gambe abbia quattro arti metallici simili alle zampe di un ragno, e al posto delle braccia quattro tentacoli pure metallici, simili a quelle delle piovre. L'essere era così: non era molto più alto di un uomo normale, e al posto della testa, sul corpo cilindrico c'era un cubo, una scatoletta squadrata che poteva girare in ogni direzione. Su ognuna delle quattro facce del cubo c'era un disco di morbida luce bianca" [35];

ii) robot *vicini e somiglianti all'uomo*, nelle loro forme morbide, sinuose, espressive (Sophia, androide in grado di rispondere alle domande e soprattutto di imitare le espressioni facciali degli umani, è presentata senza capelli, perché sia chiaro che si tratta di un automa!);

iii) *macchine del corpo-mente*, macchine mentali che vivono e si sviluppano nell'interazione con l'ambiente e rispondono in modo adattivo ed evolutivo alle sollecitazioni esterne tramite l'interfaccia omeostatica del corpo. Queste ultime – riprendendo le parole di Haraway – abitano

"un mutato regime spazio-temporale che chiamo tecnobiopotere. La temporalità dei cyborg è la condensazione, la fusione e l'implosione; essa interseca e talvolta spiazza l'evoluzione, il compimento e il contenimento tipico del realismo figurale […] Figure cyborg, quali il seme, il chip, il gene, il database, la bomba, il feto, la razza, il cervello e l'ecosistema di fine millennio, sono il frutto dell'implosione di soggetti e oggetti, e di naturale e artificiale" [36].

---

[35] A. CARONIA, *Il cyborg: saggio sull'uomo artificiale*, Roma-Napoli, Theoria, 1991, pp. 19-20.

[36] Secondo la significativa ricostruzione di D. HARAWAY, *Testimone_ Modesta@FemaleMan©_incontra_OncoTopo™. Femminismo e tecnoscienza*, trad. it., Milano, Feltrinelli, 2000, pp. 39-40.

2. *Segue*: dai cenni di robotica ad alcune recenti applicazioni

È sufficiente rinviare alle classificazioni principali della robotica, la scienza che si occupa della progettazione e dello sviluppo dei robot, per rendersi immediatamente conto della varietà e della complessità di questo tema. I robot si distinguono, infatti, secondo criteri funzionali (per manipolazione, per processi, per assemblaggio), secondo la struttura geometrica (cartesiani, cilindrici, sferici, ecc.), secondo mobilità (fissi, mobili, su rotaie, ecc.), secondo topologia parallela/seriale (paralleli, seriali, ibridi), secondo precisione (alta, media, bassa), secondo il grado evolutivo (robot playback, robot programmabili, robot con riconoscimento visivo, robot con IA e reti neuronali), secondo caratteristiche dinamiche (elevate o, al contrario, modeste), secondo la velocità (robot lenti, robot rapidi).

Per i nostri fini, e considerando che

> "l'umanità si trova ora sulla soglia di un'era nella quale robot, bot, androidi e altre manifestazioni dell'intelligenza artificiale sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali, rendendo imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza ostacolare l'innovazione" [37],

è sufficiente rinviare a quelle ormai tante copie, qualche volta quasi indistinguibili dagli esseri umani: si pensi ai robot umanoidi di Hiroshi Ishiguro, che lavorano in alcuni hotel, e non più solo giapponesi. Ma si pensi pure alle tante macchine autonome e intelligenti, in grado di prestare un'opera educativa (Einstein robot), terapeutica (Ask Nao, Zeno robot), sociale (Pepper robot, Romeo robot), ai tanti sofisticati programmi di intelligenza artificiale, per giocare (Thymio, Koov sony) o al contrario per combattere (robot sentinella, robot killer, droni militari), e alle numerose repliche di animali veri (robot fish) per le più varie applicazioni (dal campo ambientale al campo bellico).

Già questi pochi esempi mostrano come lo sviluppo della robotica e dell'intelligenza artificiale sia ormai in grado di trasfor-

---

[37] Così si legge nella *Risoluzione del Parlamento europeo* del 16 febbraio 2017 recante *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, Introduzione, lett. *B*.

mare le abitudini (di vita e di lavoro) degli esseri umani, di determinare un diverso equilibrio tra le generazioni, e al contempo di innalzare i livelli di efficienza, di risparmio e di sicurezza, nei più diversi settori (istruzione, agricoltura, trasporti, assistenza medica, ecc.), consentendo ad esempio di evitare di esporre esseri umani a condizioni pericolose (come nel caso della pulizia di siti contaminati da sostanze tossiche). D'altra parte, però, lo sviluppo della robotica e dell'intelligenza artificiale, intanto che migliorano le capacità di analisi dei dati, desta una serie di preoccupazioni circa gli effetti (diretti e indiretti) sulla società nel suo complesso, e in particolare rispetto al bisogno di garantire la trasparenza, la comprensibilità dei processi decisionali, la non discriminazione, il giusto processo. Di qui, l'esigenza che

"i soggetti coinvolti nello sviluppo e nella commercializzazione di applicazioni dell'intelligenza artificiale integrino gli aspetti relativi alla sicurezza e all'etica fin dal principio, riconoscendo pertanto che devono essere preparati ad accettare di essere legalmente responsabili della qualità della tecnologia prodotta" [38].

Del resto, le leggi di Asimov [39] si rivolgono ai progettisti, ai fabbricanti e agli utilizzatori di robot, e non ai robot anche se con capacità di autonomia e di autoapprendimento.

3. La risoluzione del Parlamento europeo sulla robotica

I cenni di robotica, qui in breve proposti, richiedono che sia rinvenuta, per un verso, una definizione largamente condivisa di robot e di intelligenza artificiale, e, per l'altro, che la stessa de-

[38] *Ivi*, Introduzione, lett. *M*.

[39] Come noto: *1*) Un robot non può recar danno a un essere umano né può permettere che, a causa del proprio mancato intervento, un essere umano riceva danno; *2*) Un robot deve obbedire agli ordini impartiti dagli esseri umani, purché tali ordini non contravvengano alla Prima Legge; *3*) Un robot deve proteggere la propria esistenza, purché questa autodifesa non contrasti con la Prima o con la Seconda Legge. A queste va aggiunta la legge 0, che con il suo carattere 'meta' è in grado di infrangere la prima legge: un robot, infatti, non può recar danno all'umanità e non può permettere che, a causa di un suo mancato intervento, l'umanità riceva danno.

finizione resti flessibile e non ostacoli l'innovazione. La questione diventa tanto più importante se si considera che autonomia, caratteristiche, natura (struttura e funzione) del robot, mettono in evidenza l'inadeguatezza delle norme tradizionali, insufficienti per attivare sia la responsabilità in caso di danni causati da un robot – non sempre consentirebbero di determinare il soggetto responsabile del risarcimento –, sia la responsabilità contrattuale nel caso di macchine progettate per scegliere le loro controparti, come pure per negoziare termini contrattuali e concludere contratti. Del resto, già quelle enormi capacità dei computer di memorizzare, confrontare e valutare *in tempo reale* rendono evidente che queste macchine non possono essere considerate meri strumenti e che le nuove regole devono necessariamente tenere conto di questo peculiare aspetto anche in vista di una eventuale responsabilità legale di alcuni soggetti (quali l'analista, il fabbricante, l'operatore, il proprietario, l'utente, ecc.) per le azioni o le omissioni *imputabili* agli strumenti stessi e per i danni che si sarebbero potuti evitare nel caso non si fossero seguite – decidendo qualche volta in pochi attimi – le valutazioni, le proposte, le allerte dei medesimi. Circostanza questa che ricorda l'ammarraggio fortunato dell'Airbus A320-214 nel fiume Hudson.

Conviene riprendere quanto detto: si definisce macchina mentale quel che vive e si sviluppa nell'interazione con l'ambiente e che risponde in modo adattivo ed evolutivo alle sollecitazioni esterne tramite – a seconda delle diverse ipotesi – software, hardware, interfaccia omeostatica del corpo. Più in particolare, secondo i principi generali riguardanti lo sviluppo della robotica e dell'intelligenza artificiale per uso civile della già citata Risoluzione, le caratteristiche di un robot intelligente sono le seguenti: *a*) la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente, e grazie allo studio e all'analisi di tali dati; *b*) la capacità di apprendimento attraverso l'esperienza e l'interazione; *c*) la forma del supporto fisico del robot; *d*) la capacità di adeguare il suo comportamento e le sue azioni all'ambiente; *e*) l'assenza di vita in termini biologici.

Del tutto evidente è l'importanza dell'ultima caratteristica (assenza di vita in termini biologici), se si pensa alle recenti applicazioni mediche dell'ingegneria biologica e della robotica, e con queste al progressivo cambiamento delle relazioni tra corpo e identità e alle nuove interazioni individuo-computer. Se ad esempio,

con Allucquère Rosane Stone, ci si domanda *dove si trovava*, *dove si fermava*, *chi era*, *come era* Stephen Hawking, si può tranquillamente osservare che una parte importante dello scienziato si estendeva alla scatola posta sulle sue ginocchia. E non solo: come un'immagine allo specchio, una parte importante di quel silicio e di quella plastica assemblata sulle sue ginocchia si estendeva analogamente *in* lui – per non parlare delle modalità invisibili, dislocate nello spazio e nel tempo, attraverso cui i discorsi di tecnologia medica e le loro estensioni corporee avevano e hanno già permeato sia lui sia noi. Altrimenti detto: *niente scatola, niente discorso!*

"Senza protesi l'intelletto di Hawking sarebbe (stato) come un albero che cade nella foresta, senza che nessuno lo possa sentire. D'altra parte, con la scatola la sua voce (era) al tempo stesso ascoltabile ed elettrica, in un modo radicalmente diverso da quella di una persona che *parla* al microfono. Dove *si* (fermava)? Quali (erano) i suoi confini? La sua persona e le sue protesi comunicazionali (ponevano) dei problemi attinenti al concetto di delimitazione, di terra di confine/*frontera*" [40].

Quanto da ultimo osservato è legato a questioni e temi proposti dalla Risoluzione. Qui (*Mezzi di trasporto autonomi* 24-40), oltre a considerare i veicoli autonomi e i droni (RPAS), come pure il trasferimento di compiti dannosi e pericolosi dall'essere umano al robot, si rinvia in particolare ai robot impiegati per l'assistenza (di anziani, di persone affette da demenza o disturbi cognitivi), che senza disumanizzare le pratiche di accudimento, possono svolgere compiti di ausilio automatizzati e agevolare così il lavoro di cura del personale sanitario. Si rinvia, inoltre, ai c.d. robot medici che continuano a migliorare le loro performance soprattutto nello svolgimento di mansioni di alta precisione e, da ultimo, si rinvia alle sempre più innovative protesi robotiche e ai più recenti software, i cui aggiornamenti sono essenziali per ovviare a malfunzionamenti e vulnerabilità, e d'altra parte la loro protezione è fondamentale per scongiurare il rischio di *hacking*, ovvero la possibile disattivazione o cancellazione della memoria dei CPS integrati nel corpo umano.

---

[40] A.R. STONE, *Desiderio e tecnologia. Il problema dell'identità nell'era di Internet*, trad. it., Milano, Feltrinelli, 1997, p. 17.

4. ...e i suoi principi etico-giuridici

Le questioni sono complesse e diverse. *Macchine della e per la mente*, *macchine del e per il corpo*, *macchine del e per il corpo-mente*, tutte richiamano comunque l'osservanza di principi e di regole. Non a caso *tecno*-etica e *robo*-etica [41] conquistano sempre più spazi, sia perché l'attuale sviluppo tecnologico entra in senso proprio nella vita delle persone – ora condizionandola e ora dominandola –, sia perché l'interrogativo iniziale e fondamentale è diventato: tra un'assimilazione verso l'alto delle macchine all'uomo e, al contrario, un'assimilazione verso il basso dell'uomo alle macchine, sino a che punto si può spingere la tecnologia? E d'altra parte, anche il *tecno*-diritto via via si afferma, quale insieme di norme e procedure che sono prodotte dalla tecnica e dal diritto che in modo sinergico si sviluppano ed evolvono.

Considerando che la robotica ha implicazioni sociali, mediche, bioetiche, la Risoluzione sotto il titolo *Principi etici* (punti 10 e 12) raccomanda di valutare l'uso della robotica dal punto di vista della sicurezza delle persone, della loro salute, della libertà, della vita privata, dell'integrità, della dignità, dell'autodeterminazione, della non discriminazione, nonché della protezione dei dati personali. Di qui il rilievo dato al principio di trasparenza, che in questo caso significa la possibilità di conoscere la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale e di ricondurre i calcoli di un sistema di IA a una forma comprensibile per l'uomo [42]. Di qui ancora l'auspicio

---

[41] Quale disciplina che ha come obiettivo quello di migliorare la comunicazione tra uomo e robot, aiutare studiosi, stakeholder e opinione pubblica ad apprezzare l'uso positivo della robotica, prevenirne gli abusi (v. in tal senso, G. VERUGGIO, F. OPERTO, *Roboethics: Social and Ethical Implications*, in B. SICILIANO, O. KHATIB (eds.), *Handbook of Robotics*, Berlin, Springer, 2008, p. 1499 ss.).

[42] Circa l'attenzione e il rilievo che l'Europa ha riconosciuto – e sta riconoscendo – all'Intelligenza Artificiale, merita d'esser qui ricordata la *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni* del 25 aprile 2018, recante *L'Intelligenza Artificiale per l'Europa.* Fra le finalità della Comunicazione quella di: 1) implementare gli investimenti nella ricerca e nell'innovazione; 2) preparare i cittadini europei ai mutamenti socioeconomici apportati dall'Intelligenza Artificiale; 3) predisporre e assicurare un quadro giuridico adeguato (Ulteriori indicazioni in materia sono reperibili anche

che i robot avanzati siano dotati di scatole nere, così da registrare i dati di ogni operazione effettuata dalla macchina, includendo i passaggi logici che hanno contribuito alle sue decisioni.

Un'attenzione speciale è inoltre riservata (punto 13) ai principi di beneficenza, non-malvagità, autonomia e giustizia, nonché ai principi e valori sanciti all'art. 2 del Trattato sull'Unione Europea e nella Carta dei diritti fondamentali dell'Unione (quali la dignità umana, l'uguaglianza, la giustizia, l'equità, la non discriminazione, il consenso informato, la vita privata e familiare, la protezione dei dati). Attenzione speciale perché nell'allegato Codice etico-deontologico degli ingegneri robotici i principi e valori accennati costituiscono l'orientamento di fondo per le azioni che in questo ambito si intraprendono.

Accanto a questi principi etico-giuridici, devono essere prese in seria considerazione le possibili soluzioni giuridiche relative alla questione della responsabilità. La caratteristica prima dei robot avanzati, pur nella loro varietà (di qui l'esigenza di un sistema di registrazione valido nell'Unione Europea), è quella di essere dotati di capacità autonoma di adattamento e apprendimento, capacità questa che determina una interazione con l'ambiente in base alle esperienze diversificate di ogni IA e un certo grado di imprevedibilità nella loro azione. Se così, l'attuale normativa, e nonostante l'ambito di applicazione della direttiva 85/374/CEE, non è sufficiente a coprire i danni causati dalla nuova generazione di robot (*Principi generali – Responsabilità* AI).

Si tratta intanto di capire quale approccio seguire, quello della responsabilità oggettiva, che richiede una semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo del robot e il danno subito dalla parte lesa, oppure quello della gestione dei rischi, che si concentra sulla persona che, in determinate circostanze, è in grado di minimizzare i rischi e affrontare l'impatto negativo? La soluzione non è affatto semplice e, del resto, anche l'idea di responsabilità in questo ambito non è agevole. Si pensi, ad esempio, a eventi provocati in generale da un mal funzionamento del sistema e per i quali va accertata la responsabilità. Potrebbe, infatti, trattarsi di un errore del sistema, verificatosi ora nella fase di programma-

---

nella nota strategica del Centro di Strategia Politica della Commissione, *The Age of Artificial Intelligence* del 2018).

zione e ora in quella di esecuzione. In ogni caso, bisognerebbe comprendere di che tipo di sistema si tratta e che grado di incognite di funzionamento ha, poiché se si dovesse trattare dei c.d. sistemi esperti, allora il cattivo funzionamento potrebbe essere determinato da cause insite nel motore inferenziale oppure nella base di conoscenza, la responsabilità, quindi, ricadrebbe su figure diverse e occorrerebbe, inoltre, rinviare a più persone per il lavoro di équipe che solitamente viene intrapreso. Quando, poi, il cattivo funzionamento del sistema riguardasse la fase di esecuzione, anche qui si tratterebbe di capire se sia l'operatore il vero responsabile, in quanto ha seguito procedure sbagliate o ha inserito dati errati, o se non lo sia piuttosto colui che ha fornito le istruzioni e i dati a fondamento dell'attività stessa.

Sotto questo profilo, una possibile soluzione alla complessità dell'attribuzione della responsabilità per il danno causato da robot avanzati potrebbe essere un regime di assicurazione obbligatorio (punto 57) per produttori e proprietari di robot, integrato da un fondo che consenta di risarcire i danni in caso di assenza di copertura assicurativa (punto 58) e che dia la possibilità alle diverse figure di questa catena (produttore, programmatore, proprietario, utente) di beneficiare di una responsabilità per dir così limitata qualora sottoscrivano un'assicurazione e/o costituiscano un fondo di risarcimento.

Qualsiasi soluzione giuridica si scelga di seguire (ad esempio la creazione di un fondo generale per tutti i robot oppure di un fondo individuale per ogni categoria di robot, e ancora il versamento di un contributo *una tantum* all'immissione sul mercato di un robot o versamenti regolari durante la vita stessa del robot), diventa ormai imprescindibile in particolare il c.d. numero d'immatricolazione individuale, così da associare il robot al suo fondo e consentire a chiunque interagisca con il robot di essere informato sulla natura del fondo, sui limiti della responsabilità in caso di danni alle cose, sui nomi e sulle funzioni dei contributori e su tutte le altre informazioni pertinenti. In generale, poi, diventa indispensabile non limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non-umano (punto 59 a-f).

IV

1. A proposito di *algoritmetica*

S/oggetto o s-oggetto, persona o personalità elettroniche, comunque si leggano queste espressioni, ormai riferite agli odierni robot, esse rendono tutte decisamente importanti la Carta sulla robotica e il Codice etico-deontologico degli ingegneri robotici.

I ricercatori della robotica, nell'osservare i principi citati della beneficenza (i robot devono agire nell'interesse degli esseri umani) e della non-malvagità (i robot non devono fare del male a un essere umano), dell'autonomia (la capacità di adottare una decisione informata e non imposta sulle condizioni di interazione con i robot) e della giustizia (l'equa ripartizione dei benefici associati alla robotica e l'accessibilità economica dei robot, in particolare per quelli addetti alla cura e all'assistenza sanitaria), devono rispettare i diritti fondamentali (primi tra tutti: dignità, benessere, autodeterminazione) e il diritto alla privacy (prima, durante e dopo l'interazione uomo-macchina, bisogna che siano garantiti: consenso, riservatezza, anonimato, equo trattamento, giusto processo). I ricercatori della robotica devono altresì rispettare: il principio di precauzione (prevedendo gli eventuali risvolti in termini di sicurezza del singolo, della società, dell'ambiente), il principio di inclusione (e cioè la partecipazione ai processi decisionali di tutti i soggetti coinvolti nelle attività di ricerca sulla robotica o di coloro i quali nutrono un interesse nella stessa), la rendicontabilità (ovvero rendere conto di possibili incidenze sociali, ambientali e sanitarie della robotica per le generazioni attuali e quelle future), la reversibilità (e cioè la possibilità di annullare l'ultima azione o una sequenza di azioni, così da ritornare alla fase ritenuta 'corretta'), la sicurezza (e quindi l'obbligo di segnalare quei fattori che potrebbero mettere a rischio i diritti umani, come pure la collettività o l'ambiente).

A tutto ciò va aggiunto l'obbligo per i ricercatori che si occupano di robotica di ridurre al minimo il danno e di massimizzare i vantaggi, e questo vale naturalmente in tutte le fasi (dalla progettazione alla realizzazione e all'uso). Detto in breve: ogni sistema robotico richiede un rigoroso processo di valutazione dei rischi, improntato ai principi di precauzione e di proporzionalità. In ogni caso, il rischio di danno non può mai essere superiore

rispetto a quello che si darebbe nella vita normale senza l'impiego dell'IA, del resto il ricorso all'intelligenza artificiale deve rappresentare sempre un'occasione e un'opportunità, anziché una minaccia e un pericolo [43].

L'intelligenza artificiale rappresenta un grande potenziale a beneficio dell'umanità, purché l'etica e il diritto sappiano affrontare quel livello 4.0 della realtà attuale, le cui direttrici di sviluppo sono dettate dall'interazione tra uomo e macchina (interfacce, realtà aumentata) e dall'uso e dall'analisi dei dati (big data, open data, Internet of Things, machine-to-machine, cloud computing, machine learning).

Ma per affrontare adeguatamente quel livello 4.0 proprio della realtà attuale bisogna che etica e diritto muovano dalla fondamentale distinzione tra scienza e pseudo-scienza, tra fatti e opinioni, e al contempo diano ampio spazio a quella ricerca di base che ha quale primo obiettivo l'avanzamento della conoscenza e la comprensione teorica delle diverse variabili in un determinato processo. Una ricerca, questa, che fornisce le fondamenta per ulteriori ricerche e che di solito non ha un particolare scopo pratico, sebbene i suoi risultati possano avere e abbiano delle ricadute applicative. Se così, bisogna che etica e diritto si adoperino – riprendendo Isabelle Stengers [44] – per un *manifeste pour un ralentissement des sciences*.

Per il nostro tema, diventa altresì rilevante che etica e diritto muovano dalla fondamentale distinzione tra ciò che può essere ricondotto all'attività computazionale, tale da poter essere programmato, e ciò che invece ne resta al di fuori, richiedendo delle scelte che coinvolgono complesse analisi e profonda riflessione. Diverso tempo fa Weizenbaum [45] scriveva che non è bene delegare alla macchina quelle funzioni che attengono al *giudizio*, al *rispetto*, alla *comprensione*, alla *cura*, all'*amore*. L'intelligenza artificiale incontra proprio qui il suo limite ed è a partire da qui che

---

[43] Come temono i firmatari di *Autonomous weapons: an open letter from AI & Robotics researchers*, presentata alla 24ª conferenza internazionale per l'Intelligenza Artificiale (IJCAI – 2015).

[44] *Une autre science est possible! Manifeste pour un ralentissement des sciences*, Parigi, La Découverte, 2013.

[45] *Il potere del computer e la ragione umana, i limiti dell'intelligenza artificiale*, cit.

l'*algoritmetica* può svilupparsi quale disciplina che abbia ad oggetto i criteri da seguire per le nostre scelte e per la loro protezione. Del resto, già il *mathwashing*, che presenterebbe come oggettivi e neutri gli algoritmi e le procedure solo perché strutturate in forma matematica, ha delle notevoli implicazioni economiche, giuridiche, politiche e sociali, che non lasciano inalterate le nostre capacità di scelta e la nostra stessa vita.

Proprio per le diverse implicazioni e le ricadute, diventa necessario che etica e diritto non perdano di vista quella che è una fondamentale linea di confine. Una linea questa che può essere conclusivamente rappresentata, grazie alla distanza tra il ritratto di *Edmond de Belamy*, prodotto di un software che sulla base di migliaia di dipinti ha appreso alcune regole, e *La ragazza col palloncino* (*L'amore è nel cestino*) creata da Banksy e che battuta all'asta si è in parte autodistrutta!

IV

ALCUNE NUOVE TECNICHE DI REGOLAZIONE

Sommario

I

1. Tecnologia e cambiamento

La tecnica, intesa in senso ampio, ha sempre avuto una funzione fondamentale, di impulso e di incentivo, nella costruzione e nella de-costruzione delle varie forme di regolazione sociale. Anche l'attuale sviluppo tecnico, a maggior ragione, svolge una funzione essenziale. L'ampia e travolgente rilettura di mezzi e di fini, proposta dalle contemporanee tecnologie, si apre al virtuale come mondo autonomo e facilita diverse forme di conoscenza, diversi e nuovi legami, con propri criteri di valutazione e con proprie regole.

Mille i piani, qualche volta si incrociano e talaltra si evitano, convergono o al contrario divergono, mille i piani di una fabbricazione incessante.

1.1. La tecnologia migliora la vita quotidiana. Si pensi alle applicazioni dei dispositivi mobili, hanno il compito importante di semplificare la vita delle persone, come pure di renderla interessante e divertente. C'è un'app per tutto e ogni giorno se ne creano di nuove: per fotografare, per dipingere, per consultare il quotidiano, per tradurre, per ottenere informazioni, per recuperare la mappa del luogo in cui ci si trova, o si intende andare, per leggere, per leggere un libro persino in 15 o 20 minuti come proposto da una delle app più usate in materia di libri per dir così condensati: *Blinkist*. Ci sono naturalmente programmi per giocare, per giocare ad esempio a catturare *Pokémon*, esplorando luoghi reali, fenomeno mondiale dell'estate 2016 con milioni e milioni di giocatori. E se si vuole, ci sono pure app che consentono di delegare le nostre risposte, tra queste *What would I say?* è l'app che a partire dai post che pubblichiamo su Facebook è in grado di generare in modo automatico nuovi *status* per esprimere cosa pensiamo, e pure un *Tumblr* che si chiama *What would I say poems?*

1.2. La tecnologia progredisce e supera se stessa. È ormai post-password. Ad esempio, *Nymi Band* è un dispositivo indossabile a forma di braccialetto, basato sul segnale bio-elettrico cardiaco, che fornisce un servizio di autenticazione continuo: *continuous authentication on the body*, e sicuro (si disattiva non appena è rimosso), per accedere a beni e servizi in maniera automatica.

L'odierna tecnologia consente così all'utente di servirsi soltanto dei c.d. *eDna* (*electronic Defined natural attributes*), vista l'unicità delle impronte digitali invisibili. Com'è intuitivo, la cattura delle caratteristiche biometriche e il processo prevalentemente computazionale di misura e di verifica della corrispondenza sono al contempo semplici (hanno il vantaggio di non richiedere sempre la collaborazione del soggetto), e complessi (implicano l'utilizzo di *Application Specific Processsor* per l'esecuzione real-time di algoritmi di autenticazione biometrica).

Tra le impronte digitali invisibili, oltre a quelle riguardanti le conformazioni fisiche interne (ad esempio, struttura del sistema circolatorio, del sistema cardiaco, del sistema fonatorio), sono particolarmente significative quelle relative al comportamento (modo di camminare, modo di scrivere, ecc.). Gli algoritmi sono in grado di individuare centinaia di comportamenti conside-

rati unici e identificativi di ciascuna persona (il ritmo con cui si digita sulla tastiera, la pressione esercitata sui tasti, l'angolo con cui si tiene il cellulare, ecc.). E nell'eseguire tutto ciò, diventano preferibili rispetto ai metodi tradizionali (chiavi e codici), perché garantiscono uno dei principali requisiti di sicurezza e cioè la non-duplicabilità.

Pare, però, che pure gli *eDna* comportamentali mutino in modo significativo a seconda dell'attività appena compiuta dal soggetto, nell'eventualità in cui egli sia sotto l'effetto di droghe, o per il fatto che sia un individuo a rischio di infarto nei mesi successivi. E anche questi ulteriori rischi e condizioni sarebbero individuabili. Tale tecnologia potrebbe, così, avere una portata ben più ampia, di segno diverso e persino opposto: potrebbe rivelarsi utile nella prevenzione di alcune malattie e in questo modo divenire un importante strumento per l'affermazione dei diritti, e al contempo potrebbe dotare aziende e istituzioni di nuove e più efficaci mezzi, compresi strumenti e sistemi utili per le varie attività di *intelligence* (economica, politica, militare), tali da facilitare una possibile negazione di diritti.

1.3. La tecnologia evolve e dà vita a nuove configurazioni di conoscenza. Non è necessaria particolare immaginazione per intuire la fatica nel compilare a mano diecimila schede, tutte dedicate all'inventario della particella *in* nell'opera di Tommaso. Si tratta dell'imponente opera di Roberto Busa [1], qui citato perché linguista informatico [2], precursore sia della interdisciplinare informatica umanistica (*Humanities Computing* o *Digital Humanities*), che è il campo di studi, di ricerca e di insegnamento nato dall'unione di discipline umanistiche e informatiche, sia dell'ipertesto [3], quell'insieme non lineare di documenti con informazioni di varia natura (testi, immagini, filmati, brani musicali),

---

[1] *Index Thomisticus Sancti Thomae Aquinatis Operum Omnium Indices et concordantiae*, Stuttgart-Bad Cannstatt, Frommann-Holzboog, 1974-1980, 56 volumi – *Sancti Thomae Aquinatis opera omnia cum hypertextibus in CD-ROM*, Milano, Editel, 1992.

[2] *Fondamenti di informatica linguistica*, Milano, Vita e Pensiero, 1987.

[3] Com'è noto, il termine si deve a T.H. NELSON (*The Hypertext*, in *Proceedings of the World Documentation Federation Conf.* 1965). Ma l'idea è anche di D. ENGELBART, a partire da *Augmenting human intellect: a conceptual Framework*, 1962 (http://www.dougengelbart.org/pubs/augment-3906.html).

unite tra loro per mezzo di connessioni logiche e rimandi (link), i cui collegamenti dinamici e la scelta della parola chiave consentono all'utente di predisporre e costruire un proprio percorso, un tracciato autonomo, di lettura e di scrittura.

Ben conscio della fatica di analizzare l'*opera omnia* di Tommaso, circa nove milioni di parole, per di più desideroso di connettere tra loro espressioni, frasi, citazioni e confrontarle con altre fonti disponibili, perché fondamentale dal punto di vista filosofico ed essenziale per una interpretazione della metafisica della presenza, Padre Busa ritenne necessario bussare alla porta (era il 1949) di Thomas Watson, fondatore dell'IBM. E con l'aiuto di quest'ultimo, in luogo dei numeri, fece usare alla macchina le parole.

1.4. La tecnologia evolve e dà vita a diversi e nuovi legami. Le attuali forme di comunicazione e le complesse dinamiche relazionali si svolgono oggi sempre più grazie a uno schermo. *Su, dentro, oltre*, lo schermo: il computer è uno strumento, col quale scriviamo, teniamo aggiornata la nostra contabilità, comunichiamo con gli altri, ma si tratta di uno strumento *sui generis*, la penetrazione dello schermo riflettente ha infatti conseguenze sulle nostre concezioni della mente, del corpo, di noi stessi, della macchina. Nel cyberspace si incontrano intimi sconosciuti, ci si imbatte in psicoterapeuti-computer, in insetti-robot, si sperimentano così nuove forme di comunicazione, si emerge in un mondo di sensazioni digitali, si riconsidera l'identità delle macchine e degli umani. E in gioco ci sono nuovi modi di pensare l'evoluzione, l'identità, le relazioni, la sessualità, i confini, la politica.

Lo schermo è la scena, il palcoscenico di azioni e relazioni qui e ora, l'ambiente in cui i soggetti vivono e (rap-)presentano le loro storie: *enhanced theatre* – la *scena aumentata*, caleidoscopica, di immagini frammentate e proiettate su più schermi, di comunicazioni ramificate e interattive, di attori sintetici che recitano insieme ai loro doppi in carne e ossa, di un pubblico che è sollecitato dalla compresenza di più punti di vista e sensorialmente coinvolto [4] –, è l'espressione di Dan Zellner che meglio d'ogni altra rende l'idea della vita sullo schermo. Non è a caso che il te-

[4] Ulteriori considerazioni nel mio *Corpi docili Corpi gloriosi*, Torino, Giappichelli, 2007, in part. p. 27 ss.

ma, ovvero il modello teatrale dell'interazione uomo-computer, è stato ed è oggetto di significative analisi. Basti pensare a *Computer as Theatre* di Brenda Laurel e a *Hamlet on the Holodeck* di Janet Murray. Non è a caso che i temi della contaminazione uomo-macchina, dell'interazione uomo-macchina per l'intimità, del rapporto tecnologia-libertà-genere, sono stati e continuano a essere oggetto di riflessione attenta e impegnata. Basti pensare a *Cyborg Manifesto* di Donna Haraway, a *Life on the Screen* di Sherry Turkle e a *The War of Desire and Technology at the Close of the Mechanical Age* di Allucquère Rosanne Stone.

Sin qui, gli esempi proposti ci parlano di nuove opportunità, come pure di nuove figure; di nuovi approcci, come pure di nuovi rischi; di nuovi paradigmi, come pure di più o meno nuove discipline, e di più o meno nuove forme di legami. In realtà, già attraverso questi pochi esempi, in vario modo e con diverso esito, la tecnologia si presenta non solo come strumento, ma anche come nuova struttura di pensiero critico, del singolo e della collettività. Una nuova struttura di pensiero critico, capace di rilanciare e favorire, ad esempio, il ruolo sociale delle scienze umaniste, messo in crisi da una visione epistemica e settoriale delle discipline: le nuove tecnologie, introducendo un linguaggio e una metodologia di ricerca comune, possono favorire il dialogo tra le *humanitas*, superando le barriere del sapere specifico e creando prodotti non solamente trans-mediali, ma anche trans-disciplinari.

Una nuova struttura di pensiero, al contrario, in grado di mettere tra parentesi proprio alcune prospettive critiche, di ostacolare alcuni diritti, di far perdere varie significative differenze. Ad esempio, nelle prigioni *high-tech* il detenuto è condannato a rinunciare a qualsiasi bisogno, scopo e significato. *Pelican Bay* non pretende corpi docili e stanchi, bensì immobili ed esausti. Qui infatti il detenuto ha messo fine al possibile, oltre ogni stanchezza, per continuare a finire. La postura dell'esausto, ricordata da Gilles Deleuze, è quanto mai emblematica:

"la sfinitezza non si lascia sdraiare e, a notte fatta, resta seduta al suo tavolo, testa svuotata su mani prigioniere" [5].

[5] *L'esausto*, trad. it., Napoli, Cronopio Edizioni, 2000, pp. 15-16.

2. Tecnologia e condizionamento

Entro questa cornice, e per meglio dire entro queste dinamiche, si sviluppa la c.d. tecno-regolazione. Con l'espressione si intende, in generale, il controllo e la registrazione (comprese la sistemazione, la riorganizzazione, la coordinazione) del comportamento umano attraverso l'uso di diverse tecniche e/o delle nuove tecnologie. Più in particolare è, con riferimento alle nuove tecnologie e ai complessi e rapidi calcoli matematici, la programmata capacità di influenzare il comportamento umano attraverso la messa a punto di valori, di norme e di regole, nei più diversi dispositivi tecnologici e con questi compatibili.

Com'è intuitivo, la tematica è decisamente ampia e pone diversi interrogativi. Non si tratta soltanto di ripensare e adeguare le leggi alle nuove tecnologie (ad esempio: al documento informatico, alla firma digitale, al sistema pubblico di connettività, al processo), né di rispondere a una sola domanda, del tipo: come dovremmo governare Internet e come possiamo regolare il comportamento online? Le nuove tecnologie, soprattutto nel loro combinarsi di tecnologia informazionale-comunicazionale (ICT), di bio-, nano-, neuro-tecnologia, e di robotica, influenzano e qualche volta determinano il comportamento degli individui, così che diventa necessario interrogarsi sugli aspetti e sui limiti etico-giuridici della tecno-regolazione, come pure sulle implicazioni dal punto di vista della legittimità e della tenuta dei valori democratici di una tecno-regolazione applicata su larga scala.

Tecno-regolazione, intesa in senso ampio, può essere ad esempio:

– *l'uso di dossi*. Tra le diverse opzioni: *i*) educare l'automobilista a rispettare la velocità prescritta, *ii*) mettere i segnali stradali, *iii*) inserire lungo la strada dei dossi, quest'ultima è quella che meglio delle altre determina il conducente a moderare la velocità e a rispettare il limite previsto dalle norme sulla circolazione.

– *l'uso di Clocky*. È la sveglia robotica che, se non ci si alza dal letto, rotola giù dal comodino, si allontana sulle sue ruote, trova ogni giorno un nuovo angolino in cui nascondersi e da lì suona di nuovo. Rientra nelle diverse strategie di autocontrollo, e al contempo trasforma il risveglio in qualcosa di divertente e più adatto a interpretare la relazione tra esseri umani e tecnologia.

– *l'interazione con Lovot*, una sorta di evoluzione del più noto e datato Tamagotchi, il cui nome è frutto della crasi fra le parole "Love" e "Robot". Ideato per consentire un'interazione simile a quella che si può avere con un cucciolo, Lovot avrebbe il pregio di poter 'rendere le persone più felici' offrendo loro dei benefici analoghi a quelli della pet terapy.

– *l'impegno preso con Stickk.com*, anche questo rientra in una strategia di autocontrollo. Si tratta della web company che offre due soluzioni per prendere impegni: chi opta per la soluzione finanziaria, scommette dei soldi e si impegna a raggiungere l'obiettivo entro una certa data. Se l'obiettivo è raggiunto, la persona ottiene indietro il suo denaro; in caso contrario, i soldi vanno in beneficenza. Chi opta per l'impegno non finanziario, può scegliere d'essere messo sotto pressione dai propri pari (e-mail ad amici o parenti per annunciare i propri successi o fallimenti) e monitorato attraverso un blog di gruppo.

– *l'arte della semplice presentazione*. Il nuovo imperativo categorico è diventato, per privati, per aziende, per gruppi e comunità di vario tipo e con diversi interessi, sii più coinvolgente e persuasivo, siate più coinvolgenti e persuasivi! I tutorial sono ormai ampiamente diffusi. Tanto la creazione quanto la loro fruizione sono fondate sulla c.d. scienza delle presentazioni più efficaci, che muovendo dal rilievo che il cervello umano è collegato a specifici contenuti (immagini, storie, interazioni), aiuta per l'appunto a creare presentazioni memorabili. Ad esempio, *Prezi* nel suo sito promette un potere di narrazione visiva senza precedenti, che unisce la libertà di una tela con la dimensione spaziale e il movimento, e che allo stesso tempo mantiene e guida il pubblico coinvolto attraverso il messaggio.

– *l'effetto della semplice misurazione*. Quando nei sondaggi si chiede agli intervistati se hanno intenzione di tenere un certo comportamento (andare a votare, comprare un prodotto, e così via), intanto che si misurano le diverse intenzioni degli individui, il loro comportamento viene influenzato. Altrimenti detto, gli individui intervistati si mostrano più propensi a conformarsi alla risposta data e, com'è evidente, la risposta dipende innanzitutto dalla domanda (modi, forme, contenuti). Il *mere-measurement effect* può quindi diventare una sorta di stimolo e incoraggiamento, o al contrario di freno e di scoraggiamento, a un certo comportamento, usato sia nel pubblico che nel privato.

– *il possibile filtro di civiltà*. I messaggi sono decisamente tanti e adempiono alle più varie funzioni. Ad esempio: annulla, riprova, tralascia? il messaggio di errore mostrato dai sistemi operativi MS-DOS e IBM PC DOS quando il sistema è incapace di leggere i dati necessari all'esecuzione di un programma, che è secondo i programmatori un messaggio vago e non concludente; è stato rilevato in questa pagina un potenziale rischio per la protezione. Continuare? il messaggio che avverte che falsi siti e applicazioni malevole (*malware* come *Trojan horse*, *backdoor*, *virus*, *worm*) potrebbero insinuarsi nella Rete locale, così da danneggiare o interrompere il sistema, da intercettare o impedire la comunicazione, da falsificare o alterare l'informazione [6]. Ma forse ne manca uno decisamente utile, un programma in grado di rilevare una e-mail poco educata, con la soluzione di default del tipo: Attenzione: il messaggio verrà spedito soltanto se tra 24 ore il mittente ne farà esplicita richiesta.

– *il messaggio subliminale e l'anticipatory computing*. La capacità della tecnologia di indirizzare, in vario modo: comprese le forme di persuasione occulta, i comportamenti e di anticipare il futuro. Basta poco: qualche segnale e qualche stimolo, percepiti a livello inconscio, alcuni tratti caratteristici del comportamento umano, qualche informazione pubblicata su Facebook, Twitter, Foursquare, e anche una lista di desideri su Amazon! L'algoritmo completa la procedura, suggerendo modelli previsionali ad aziende, a gruppi, a governi, che hanno in proposito un forte interesse economico e/o politico.

Sono i sistemi predittivi la vera sfida dell'intelligenza artificiale, già in parte rappresentati, ad esempio: da *Google Now*, ovvero dalle schede di informazioni *ad hoc* che assistono, grazie alle tante tracce lasciate, l'utente ancor prima che ne faccia richiesta; da *Osito*, che nel passare in rassegna informazioni e e-mail può anticipare alcune decisioni e iniziative; da *iMamma*, app in grado di aiutare sia la donna in gravidanza (sotto il profilo clinico, psicologico, nutrizionale, estetico, ludico), sia il medico, in quanto fonte di aggiornamento e supporto nella gestione del

[6] Ulteriori considerazioni in A.C. Amato Mangiameli, G. Saraceni, *I reati informatici. Elementi di teoria generale e principali fattispecie criminose*, Torino, Giappichelli, 2019.

paziente. Si tratta, come si può agevolmente notare, di ambiti diversi, diversi per la dimensione, per la natura e per la qualità dei dati, accomunati però dalla ricerca e dalla scelta dell'algoritmo più appropriato, che è tale in base al fine (quel che si intende fare con la risposta), secondo il modo (come i calcoli dell'algoritmo sono convertiti in istruzioni per il computer), in base al tempo (a disposizione).

Di importanza fondamentale, e con importanti ricadute anche rispetto a una pretesa autonomia decisionale, è il criterio temporale. In molti casi ormai sono sufficienti pochissimi secondi per definire in modo automatico l'uno o l'altro parametro, l'una o l'altra scelta. Basti pensare agli algoritmi che decidono le oscillazioni in borsa dei diversi titoli (*high-frequency Stock Trading software*), o al sistema di risoluzione dei conflitti di traffico aereo (*Airborne Collision Avoidance System II*).

3. *Segue*: la *nudge theory*

Non distante dalla tematica della tecno-regolazione è la *nudge theory*, un approccio questo che muove dall'efficacia che i suggerimenti e gli aiuti indiretti esercitano rispetto ai processi decisionali di individui e gruppi e che non sarebbe diversa dall'efficacia esercitata in modo diretto dai comandi e dalle norme. L'uso del termine *nudge*, ovvero *pungolo*, si deve a Richard Thaler e Cass Sunstein che nel loro *La spinta gentile* [7] ritengono importante migliorare il benessere delle persone, orientandone le decisioni per l'appunto con pungoli, piuttosto che con ordini. L'approccio è giustificato da una sorta di paternalismo libertario ed è basato sull'architettura della scelta.

L'architetto delle scelte è colui che ha la responsabilità di organizzare il contesto nel quale gli individui prendono decisioni. E per organizzare il contesto si serve innanzitutto degli strumenti per strutturare la presentazione delle opzioni. Il che significa: decisione sul numero di alternative da presentare, tenendo conto che troppe opzioni aumentano lo sforzo di ricerca del decisore; ausilio decisionale anche attraverso tecnologie che possano

[7] Trad. it., Milano, Feltrinelli, 2014.

combinare meglio e con il minimo sforzo le preferenze delle persone; scelta dei tempi, considerate le significative implicazioni per il decisore; uso di impostazioni predefinite, le c.d. opzioni di default che diventano effettive quando il decisore non intraprende alcuna azione per cambiarle, e la maggior parte delle volte sono accettate passivamente per inerzia o per *default bias*: le persone sembrano infatti avere una preferenza per l'opzione di default, anche quando non vi sono costi per cambiarla o quando essi sono minimi. Due le categorie di default: default di massa che non tengono conto delle caratteristiche individuali e default personalizzati che riflettono invece le differenze tra gli individui.

Secondo Thaler e Sunstein, questi strumenti insieme ad altri, fanno sì che l'architettura delle scelte nell'influenzare gli individui e i popoli migliori la stessa attività di governo, giacché in molti campi (incluse la tutela dell'ambiente, la tutela della salute, e così via), una migliore amministrazione è il risultato non tanto della coercizione e dell'imposizione di vincoli, quanto di una maggiore libertà di scelta. D'altra parte, se obblighi e divieti sono sostituiti da incentivi e pungoli, la pubblica amministrazione diventa (può diventare) più semplice e meno invadente.

Invero, il *nudging* – questa nuova strategia di comunicazione di massa – può avere dei risvolti positivi: ad esempio, convincere i cittadini a non ricorrere al pronto soccorso per ogni minimo malessere, convincerli a pagare le tasse, a non fumare, a mangiare in modo sano, ma nel frattempo minaccia la neutralità dello Stato e via via insinuandosi limita la libertà. Potrebbe accadere che in una situazione di grave crisi economica si usino strategie di *nudging* per persuadere i cittadini a ritenere necessario, e addirittura giusto, che anziani, portatori di handicap, malati terminali, muoiano subito, così da non gravare sul sistema sanitario nazionale. Potrebbe persino accadere, anche senza situazioni di crisi, che si usino strategie di *nudging* per indurre i cittadini a ritenere democratico l'obbligo volontario a morire [8].

[8] Riprendo l'espressione da C.H. WIJKMARK, *La morte moderna* (trad. it., Milano, Iperborea, 2008), che com'è noto, in modo provocatorio e precorrendo i tempi (data di pubblicazione del dramma è il 1978), prospetta il condizionamento psicologico degli anziani, così che siano loro stessi a voler farla finita. È in questo modo messa in scena una morte pianificata che giunge per tutti alla stessa età e proprio perché razionale, programmata, burocratizzata, rappresenterebbe la sola morte veramente ugualitaria e democratica.

L'uso del *nudge* tocca uno spettro incredibilmente ampio di questioni, che vanno dall'economia all'etica, al diritto, alla politica. C'è intanto da affrontare il grande tema dei limiti che l'economia può e deve incontrare, visto che nella società contemporanea

"è l'economia a consegnare all'umanità sul Sinai le tavole della Legge" [9].

Si tratta poi di prendere in esame se e sino a che punto società e Stato si possono spingere nell'orientare lo stile di vita, le abitudini e le tendenze, dei cittadini, si possono spingere nel decidere cosa è vero bene, si possono spingere nella scelta dei mezzi per conseguirlo ricomprendendo il *nudging*, tecnica sottile e silenziosa, in grado di compromettere la neutralità e la democrazia dello Stato di diritto [10]. Anche il diritto, e non potrebbe essere diversamente, è chiamato in causa: nell'età dei big data sempre più diffusamente si parla di diritti (all'oblio, all'informazione, all'accesso, ecc.) e intanto alcuni istituti si sgretolano e alcuni concetti giuridici necessitano di essere ripensati, tra questi l'idea di responsabilità [11]. Ci sono infine, ma non ultimi, i grandi problemi che investono l'etica e la 'natura informazionale dell'universo' [12], il diritto, la politica e il loro ruolo nel mondo glocale [13], come pure i quesiti che riguardano il modo in cui si formano il consenso e il dissenso, le questioni relative ai confini tra interno e esterno, privato e pubblico, nazionale e sovranazionale.

3.1. La *nudge theory*, proprio come recita il sottotitolo: *La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, affronta anche argomenti riguardanti il matrimonio,

---

[9] Così C. MAGRIS, *Democrazia della morte. Morte della democrazia* (Postfazione, *ivi*, p. 115).

[10] Si veda J. NIDA-RÜMELIN, *Democrazia e verità*, trad.it., Milano, Franco Angeli, 2015.

[11] V. in particolare F. BATTAGLIA, N. MUKERJI, J. NIDA-RÜMELIN (eds.), *Rethinking responsibility in science and technology*, Pisa, Pisa University Press, 2014.

[12] Secondo l'espressione di L. FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, Giappichelli, 2009.

[13] Cfr. A.C. AMATO MANGIAMELI (a cura di), *Persone e stati: le conseguenze della* glocalizzazione *e della innovazione tecnologica*, Milano, Giuffrè, 2006.

le unioni civili, le relazioni omosessuali. La proposta è – perché sia rispettata la libertà dei gruppi religiosi di decidere quali unioni riconoscere (in relazione all'età, al sesso, alla religione, ecc.) e protetta al tempo stesso la libertà individuale di farsi reciproche promesse di unioni durature (a prescindere dall'età, dal sesso, ecc.) – di privatizzare il matrimonio. Il che significa: la parola matrimonio non dovrebbe apparire in nessuna legge e la pubblicazione, l'autorizzazione, la celebrazione, non dovrebbero più dipendere, né essere riconosciute, da funzionari dello Stato. L'unico *status* giuridico che lo Stato conferirebbe alle coppie sarebbe un'unione civile, ovvero un contratto di associazione domestica.

La premessa e la spiegazione sono semplici:

"quando gli individui contraggono matrimonio, ricevono non soltanto una serie di benefici materiali ma anche una sorta di legittimità ufficiale, un sigillo d'approvazione, da parte dello stato".

La licenza di Stato è però anacronistica. La possibile e comprensibile ricostruzione dell'istituto matrimoniale quale strategia di impegno preventivo – non dissimile da quello adottato da Ulisse per affrontare le Sirene – confligge ormai con il suo scioglimento, in qualsiasi momento e per qualsiasi ragione. Il risultato di tutto questo è che le persone diventano vittime tanto dei capricci del caso quanto di un sistema giuridico caratterizzato da un grado di incertezza incredibilmente elevato. Tutto ciò comporta che, se si ricominciasse da zero,

"a nessuna persona raziocinante verrebbe in mente di elaborare un sistema come quello attuale, così pieno di confusione e di arbitrarietà che, in molti stati, persino gli avvocati esperti di divorzi non hanno idea di come una disputa andrà a finire. Come minimo, bisognerebbe modificare l'architettura delle scelte in modo che chi contrae matrimonio abbia una comprensione più chiara dei propri diritti e doveri" [14].

Anche in quest'ambito si tratterebbe di introdurre pungoli, spinte gentili, che indirizzino verso la scelta giusta (contratto di associazione domestica) le persone e le coppie, e di introdurre pungoli e regole di default che indirizzino i giudici verso la de-

[14] R.H. THALER, C.R. SUNSTEIN, *La spinta gentile*, cit., in part. p. 206 ss.

cisione giusta. Ad esempio, in mancanza di accordi pre-matrimoniali (visto l'ottimismo irragionevole: il 100 per cento delle persone è certa che non divorzierà mai, il 50 per cento ritiene probabile che altri possano divorziare!), pungoli e regole dovrebbero favorire gli esiti che proteggono le parti più deboli dalle perdite (economiche) più gravose.

L'idea di privatizzare il matrimonio, insieme all'idea di introdurre pungoli e regole di default, stimolerebbe secondo i teorici del *nudging*

"un gran numero di esperimenti, aumentando la libertà di individui e organizzazioni religiose e attenuando, al tempo stesso, l'accanimento inutile e talvolta sgradevole degli attuali dibattiti pubblici" [15].

Un approccio questo che tuttavia non può non risentire della complessità nella predisposizione di pungoli e regole di default, visto che: *a*) gli umani sono facilmente pungolabili, *b*) le influenze sociali in non pochi casi sono nient'affatto pianificate, *c*) le influenze sociali possono essere in molti casi pianificate a tavolino da architetti delle scelte che operano in favore di un determinato obiettivo e di una propria utilità, *d*) le regole di default sono stabilite in base a diversi orientamenti e interessi, e nella loro applicazione, pur in presenza di un numero esiguo di misure predefinite, c'è la possibilità di orientarsi verso l'una o verso l'altra regola in base a differenti interpretazioni.

4. *Soft law*…

È particolarmente interessante osservare il fenomeno nel suo articolarsi. Intanto che la tecno-regolazione, l'*anticipatory computing*, il *nudging*, richiedono impostazioni predefinite, regole di default giuridiche, anche la tecnica di produzione normativa registra una profonda evoluzione. Accanto all'attenzione per la regola e per il suo inserimento armonico nell'ordinamento giuridico, si sviluppa l'attenzione per il ciclo della regolazione. L'idea è che il legislatore debba seguire il provvedimento normativo anche nella fase di attuazione, implementazione e verifi-

[15] *Ivi*, p. 218.

ca dei risultati, in un contesto di maggiore coinvolgimento dei portatori di interessi (*stakeholder*) e dei cittadini. Simile idea è sostenuta dalla diffusione dell'utilizzo della Rete e dallo sviluppo delle diverse tecniche e metodologie, in grado di raccogliere in tempo reale i dati, monitorare gli sviluppi, valutare gli effetti.

Il ciclo della regolazione ha così inizio con le tecniche di consultazione di *stakeholder* e cittadini, indispensabili per comprendere le effettive esigenze degli stessi, e con gli strumenti di analisi dei possibili effetti che la nuova regolazione potrà produrre. Com'è intuitivo, queste tecniche e questi strumenti possono, oltre che l'impatto economico, misurare anche altre tipologie di effetti (ad esempio, quello ambientale). Una volta redatto il testo in base alle regole del drafting e con l'apporto della legimatica, la fase dell'attuazione è seguita da strumenti di monitoraggio e di verifica dei risultati che man mano si raggiungono, in grado di garantire opportuni *feedback* al legislatore in relazione ad eventuali criticità. Il ciclo della regolazione si conclude, una volta raggiunti gli obiettivi, con le tecniche di valutazione che, evidenziando gli effetti prodotti, pongono il decisore nella condizione di individuare e assumere misure di modifica o di abrogazione della regola adottata. Di qui, un nuovo e diverso intervento normativo. Il ciclo della regolazione può essere rappresentato come un circolo (virtuoso) della produzione normativa [16].

4.1. Forza e linguaggio del diritto via via conquistano nuovi significati e nuove espressioni. Il fenomeno è noto: il diritto si presenta sempre più come negoziato [17], oltre che combinato con mezzi e prospettive non propriamente suoi o persino in contraddizione. Peraltro, tra i teorici si è già da molto tempo diffusa l'idea di un diritto mite [18], di un diritto *soft*, quale insieme di norme leggere, regole di condotta che, in linea di principio, non so-

---

[16] Per ulteriori considerazioni Presidenza del Consiglio dei Ministri, Dipartimento per gli affari giuridici e legislativi, *Strumenti per il ciclo della regolazione*, aprile 2013, (http://presidenza.governo.it/DIE/attivita/pubblicazioni/manuale_dagl_09_07_web.pdf).

[17] F. OST, *Le rôle du droit: de la vérité révélée à la réalité négociée*, in G. TIMSIT, A. CLAISSE, N. BELLOUBET-FRIER (s.l.d.), *Les administrations qui changent. Innovations techniques ou nouvelles logiques?*, Paris, Puf, 1996, p. 73 ss.

[18] G. ZAGREBELSKY, *Il diritto mite. Legge diritti giustizia*, Torino, Einaudi, 1992.

no dotate per legge di forza vincolante ma che, nondimeno, possono produrre effetti. Un tale diritto, al quale si contrappone a prima lettura l'*hard law* e nel quale scricchiola la separazione rigorosa tra *ius* e *facta* [19], è inevitabilmente anche un diritto fluido, non tanto per il concorrere delle norme (proibitive, attributive, conformative) [20], o perché si moltiplicano i termini vaghi ed incerto diventa ogni confine, quanto per il fatto che il diritto espresso sotto-forma di principi, di valori o di standard, crea una zona di incertezza e di indeterminatezza. E in mancanza di predeterminazione, il significato degli enunciati giuridici dipende in massima parte dall'interpretazione, nell'operare del *soft law* teoria delle fonti e dell'interpretazione si intrecciano costitutivamente, di qui il ruolo di co-determinazione del giudice.

4.2. Entro questa dimensione, anche il linguaggio giuridico muta [21]. Lo scambio continuo tecnica-diritto determina insieme a nuovi contenuti una nuova terminologia. Per i contenuti è sufficiente qui rinviare alla normativa sul documento informatico, sulla firma digitale, sul sistema pubblico di connettività, come pure sulla proprietà intellettuale e sulla privacy [22]. Per la nuova terminologia è significativo rinviare all'uso del termine sperimentale in alcune norme di carattere organizzativo, che modificano determinati processi produttivi di beni e servizi della pubblica amministrazione e che sono sottoposte a verifica d'efficienza, d'efficacia e d'economicità. Un esempio di disposizione sperimentale [23] è l'art. 1, comma 205, della l. 28 dicembre 2015,

---

[19] Così P. GROSSI, *Globalizzazione e pluralismo giuridico*, http://www.gruppo sanmartino.it/GROSSI,%20Globaliz zazione.htm.

[20] Riprendendo, qui, la tripartizione fatta da N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, Laterza, 2003.

[21] Non solo nel senso della precipitazione e della sciatteria, secondo la critica di J. CARBONNIER, *Flessibile diritto*, trad. it., Milano, Giuffrè, 1997.

[22] Un quadro d'insieme nel mio *Informatica giuridica*, Torino, Giappichelli, 2015, in part. p. 255 ss.

[23] Riprendo l'esempio e rinvio agli interrogativi che le disposizioni sperimentali pongono, sia sotto il profilo della teoria generale del diritto sia dal punto di vista della filosofia del diritto, da F. COSTANTINI, *Società dell'Informazione e "diritto tecnologico". Il caso delle norme "sperimentali"*, in R. DE GIORGI (a cura di), *Limiti del diritto. Prospettive di riflessione e analisi*, Lecce, Pensa Multimedia Editore, 2018, p. 617 ss.

n. 208 – *Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato* (legge di stabilità 2016), che prevede:

"Il congedo obbligatorio per il padre lavoratore dipendente, da fruire entro i cinque mesi dalla nascita del figlio, nonché il congedo facoltativo da utilizzare nello stesso periodo, in alternativa alla madre che si trovi in astensione obbligatoria, previsti in via sperimentale per gli anni 2013, 2014 e 2015 dall'articolo 4, comma 24, lettera *a*), della legge 28 giugno 2012, n. 92, sono prorogati sperimentalmente per l'anno 2016 ed il congedo obbligatorio è aumentato a due giorni, che possono essere goduti anche in via non continuativa".

5. …e *high-tech law*

Tra l'ammirazione entusiastica o, al contrario, il distacco timoroso dal *computer law*, e quindi dalla tecno-regolazione, dal *nudging*, dai modelli previsionali automatici, di per sé non negativi, diventa necessario imparare a usarli correttamente, proprio a partire dalle differenze che certo si danno tra il *computer law* e la legge [24].

Qualche differenza. La tecno-regolazione tende a essere rigida, mentre le norme sono flessibili e aperte all'interpretazione, così flessibili e aperte all'interpretazione da creare qualche volta persino confusione e arbitrarietà. È quanto lamentato da sempre e da più parti, di recente come già detto anche dai sostenitori del *nudging*. Di qui, secondo alcuni, la necessità di regole di default, chiare, che influenzino le preferenze individuali e al contempo prospettino al giudice della controversia un ventaglio piuttosto ristretto di possibili accomodamenti.

Altra differenza, questa volta di segno diverso. La legge è relativamente statica, mentre in principio la tecnologia consente la flessibilità, grazie alle configurazioni aperte e alla plasticità del software. Questa flessibilità deve tuttavia essere letta alla luce delle tre fasi coinvolte nella tecno-regolazione, e cioè: individua-

[24] M. HILDEBRANDT, J. GAAKEER, *Human Law and Computer Law: Comparative Perspectives*, Heidelberg-New York-London, Springer, 2013 (qui in particolare v. U. PAGALLO, *What Robots Want: Autono mous Machines, Codes and New Frontiers of Legal Responsibility*, p. 47 ss.; B. VAN DEN BERG, R. LEENES, *Abort, retry, fail: Scoping techno-regulation and other techno-effects,* p. 67 ss.).

zione della norma giuridica, trasformazione della norma in regola tecnica, sua attuazione. È chiaro che la seconda fase, passaggio/trasformazione della norma in regola tecnica, è quella che nel contesto della tecno-regolazione svolge il ruolo principale e si articola in tre importanti livelli: *i*) sviluppo di strutture tecniche (ad esempio, i linguaggi di marcatura); *ii*) compilazione di schemi di casi concreti; *iii*) rispetto dei legami tra le azioni e le regole del *framework*.

Le implicazioni sono parecchio significative e le due differenze, qui brevemente proposte, mettono in evidenza come nella sempre possibile comparazione *computer law* e legge non si tratta in ogni caso di un *trade-off*, di una scelta tra due o più possibilità, in cui molto semplicemente la perdita di valore di una costituisce un aumento di valore di un'altra.

5.1. Che non si tratti di una scelta tra due o più possibilità, è agevole sottolinearlo visto che l'*high-tech law* offre delle opportunità, ma espone anche a delle sfide. E ciò vale sia quando è il risultato delle tecnologie informazionali-comunicazionali, sia quando è esito delle biotecnologie. Diversamente da Francis Fukuyama che teme le biotecnologie perché in grado di danneggiare la dignità dei cittadini, compromettendone la stessa umanità, e non invece le ICT [25], Roger Brownsword [26] ritiene che la

---

[25] Le ICT implicano due problemi: 1) il *digital divide* 2) la privacy. Il primo è un problema del terzo mondo, il secondo sembra ossessionare le nazioni civili ed economicamente sviluppate. Ad avviso di FUKUYAMA, nessuno di questi problemi sarebbe grave, non si tratterebbe di "*earth-shaking matters of justice and morality*". I veri problemi deriverebbero dagli interventi sull'*uomo oltre l'uomo*: "*no one can make a brief in favor (sic) of pain and suffering, but the fact of the matter is that what we consider to be the highest and most admirable human qualities [...] are often related to the way that we react to, confront, overcome, and frequently succumb to pain, suffering, and death. In the absence of these human evils there would be no sympathy, compassion, courage, heroism, solidarity, or strength of character. A person who has not confronted suffering or death has no depth. Our ability to experience these emotions is what connects us potentially to all other human beings, both living and dead*" (*Our Posthuman Future. Consequences of the Biotechnology Revolution*, New York, Farrar, Straus and Giroux, 2002, p. 172 ss.).

[26] *What the World Needs Now: Techno Regulation, Human Rights and Human Dignity*, in R. B. (*ed.*), *Global governance and the quest for justice*, volume IV, *Human rights*, Oxford and Portland Oregon, Hart, 2004, p. 203 ss.

dignità umana possa essere danneggiata tanto dalle ICT quanto dalle biotecnologie. Ove infatti si leghi la dignità all'idea di 'miglioramento', saremo maggiormente preoccupati dalle ICT piuttosto che dalle biotecnologie, se invece la si lega all'idea di 'conservazione', di difesa della natura umana, saremo invece più preoccupati dalla clonazione, dalla sperimentazione sugli embrioni, in breve dalle bio-, nano-, neuro-tecnologie.

Regulatory challenge e *regulatory opportunity* sembrano rincorrersi. Da un lato, la sfida che la tecnica lancia, o può di volta in volta lanciare, ai diritti e alla dignità dell'uomo. Dall'altro, le opportunità che le nuove tecnologie offrono anche per la tutela della dignità e lo sviluppo dei diritti. L'attuale fase richiede differenti forme di regolamentazione, compresa una disciplina giuridica che smentendo la successione *after high-tech war comes high-tech law* sia in grado di evitare il rischio che le nuove tecnologie finiscano col limitare la libertà e col diventare nuove forme, per di più ineluttabili e particolarmente efficaci, di disciplina e controllo.

5.2. Sempre tra sfida e opportunità: la tecnologia sfida l'ambiente e insieme i diritti delle generazioni future, così che non sempre si possono riporre molte speranze nel *techno-logos*, nella razionalità strumentale che esso implica e suppone, sarebbe qualche volta auspicabile la sua sostituzione con un *eco-logos*, ovvero con un logos che consideri l'ambiente come l'orizzonte di riferimento nel rispetto del quale siamo chiamati a vivere ed operare [27]. D'altra parte, però, la tecnologia è una opportunità: può e deve essere convenientemente utilizzata come una risorsa, una alleata preziosa, per combattere la possibile catastrofe ecologica e migliorare l'ambiente [28].

I temi si intrecciano. La crisi ecologica rinvia alla tecno-regolazione e questa a sua volta rimanda allo stato d'eccezione, quale zona di confine e di indecidibilità tra legge e fatto, in cui tutto

---

[27] L. CORRIAS, *Law in the Twilight of Enviromental Armageddon. A response to Han Somsen*, in *Netherlands Journal of Legal Philosophy – Boomjuridischtijdschriften*, *Aflevering* 1, 2011.

[28] In tal senso Oliver W. LEMBCKE, *Techno-regulation and law: rule, exception or state of exception? A comment to Han Somsen and Luigi Corrias*, in *Rechtsfilosofie & Rechtstheorie*, 40, 2/2011, 131 ss.

può accadere e ogni azione può essere a suo modo giustificata legalmente [29]. E nello stato d'eccezione la tecno-regolazione si presenta come pura forza [30], estremamente efficace nel ridurre gli spazi di libertà e impedire le diverse forme di disobbedienza civile. Uno scenario distopico:

"*Without civil disobedience there can be no civil obedience and thus no citizens but then ultimately no justice either*"! [31]

Uno scenario distopico anche con riferimento al diritto penale: al di là dei suoi scopi (retribuzione, rieducazione, intimidazione, ecc.) [32], il diritto penale è superato dalla tecno-regolazione, perché se applicata correttamente non lascia altra possibilità che adeguarsi al *pattern* individuato dall'architetto delle scelte [33].

6. Tecnica, società, diritto

La questione, in breve, diventa: far in modo che legge e *code* si vengano incontro e suppliscano l'uno alle carenze dell'altro. Le regole di diritto necessitano di uno spazio per respirare [34], esse

---

[29] Così come ricostruito da G. AGAMBEN, *Lo stato di eccezione*, Torino, Bollati Boringhieri, 2003.

[30] "*This is, of course, a horror scenario, but it illustrates the point that techno-regulations should only be the exception to the rule of law, because their legality tends to be reduced to pure force (Gesetzeskraft). For this reason they may supplement the legal system as a last resort regulation, similar to other legal provisions which exclude non-compliance by pure force*" (O.W. LEMBCKE, *Techno-regulation and law: rule, exception or state of exception?*, cit., in part. pp. 135-136).

[31] L. CORRIAS, *Law in the Twilight of Enviromental Armageddon. A response to Han Somsen*, cit.

[32] Ulteriori considerazioni nel mio *Filosofia del diritto penale. Quattro voci per una introduzione*, Torino, Giappichelli, 2014.

[33] "*Where techno-regulation is perfectly instantiated there is no need for either correction or enforcement*" (l'affermazione si trova, a commento dell'articolo di R. Brownsword, *Code, Control and Choice. Why East is East and West is West*, in B. MORGAN, K. YEUNG (eds.), *An Introduction to Law and Regulation*, Cambridge-New York, Cambridge University Press, 2007, p. 105).

[34] "*Rules need breathing space, and it still takes a human being to make a rule come to life*" (B.J. KOOPS, *The (In)Flexibility of Techno-Regulation and the Case of Purpose-Binding*, *Legisprudence*, 5, 2/2011, p. 171),

sono vive [35], create dall'uomo per l'uomo. Il che significa: contenuti in continua evoluzione che rispondono a nuove necessità, a nuove condizioni e a nuove questioni giuridiche. E rispondono proprio grazie al susseguirsi delle diverse interpretazioni, tutte ugualmente giustificate e molte sfuggite a ogni previsione: *cosa tesse non lo sa nessun tessitore* [36].

La tecno-regolazione, risultato di programmi che menti intelligenti hanno predisposto [37], necessita di sistemi e procedure, di sistemi esperti, di procedure inferenziali di ragionamento, di linguaggi di programmazione, resta comunque creata dall'uomo per l'uomo. È quindi necessario non sottovalutare i possibili rischi. Uno tra tutti, è quello che Weizenbaum, pioniere della scienza del computer, sottolineava in una conferenza oggi ancora più attuale sull'Intelligenza Artificiale:

"molti dei problemi tecnici che questa (sotto-)disciplina [...] si trova ad affrontare stimolano con particolare forza la fantasia e la creatività dei ricercatori a orientamento tecnico. Obiettivi come fare di un computer un essere pensante, dare al computer la capacità di capire il linguaggio parlato, mettere il computer in grado di vedere, obiettivi come questi offrono tentazioni quasi irresistibili a quelli fra noi che non hanno del tutto sublimato la tendenza a giocare con paletta e secchiello, o che intendono trovare sul palcoscenico del computer [...] soddisfazione alle loro illusioni di onnipotenza" [38].

---

[35] Nell'arringa in difesa di Danilo Dolci, alla domanda cosa sono le leggi? CALAMANDREI così rispondeva: "le leggi sono vive perché dentro le formule bisogna far circolare il pensiero del nostro tempo, lasciarvi entrare l'aria che respiriamo, mettervi dentro i nostri propositi, le nostre speranze e il nostro sangue. Altrimenti le leggi non restano che formule vuote, pregevoli giochi da legulei; affinché diventino sante, vanno riempite con la nostra volontà".

[36] Riprendo l'adagio da G. RADBRUCH, *Introduzione alla scienza del diritto*, trad. it., Torino, Giappichelli, 1958, p. 360 ss.

[37] Come amava ricordare R. BUSA S.I., qui all'inizio citato, il computer è figlio dell'intelligenza dell'uomo, è il risultato di menti che hanno saputo, e sanno, scrivere programmi. Il cosmo non è altro che un enorme e grandioso computer, creato da una mente superiore che scrive programmi così che altri ne scrivano (*Dal computer agli angeli*, Castel Bolognese, Itaca, 2000).

[38] *Non senza di noi*, in J.W., *Il potere del computer e la ragione umana. I limiti dell'intelligenza artificiale*, trad. it., Torino, Abele, 1986.

II

1. Tra *tecno*-etica, *tecno*-politica e *tecno*-scienza

Le parole hanno le loro stagioni. È stato di moda, e continua a esserlo, l'uso dell'espressione *bio-* per accompagnare termini più vari (si pensi a bio-etica, bio-diritto, bio-politica, come pure a bio-sicurezza, bio-solidale, bio-tecnologia). Da un po' di tempo è il turno dell'espressione *tecno-* per accompagnare, ancora una volta, parole quali etica, politica, scienza, ma anche diritto e pure uomo.

Com'è intuitivo, con il vocabolo tecno si rinvia in generale alla tecnica capace di influenzare contenuti, giudizi, prospettive, e di strutturare azioni e iniziative di individui e di gruppi, nei più diversi ambiti. E quanto sia essa capace di influire (su) e di ordinare informazione, conoscenza, lingua, lo mostra già la semplice ricerca di sinonimi e antonimi che, con l'uso del *thesaurus* del programma di videoscrittura, oltre che immediata e veloce, è diventata strumento indispensabile e ormai insostituibile. I database terminologici – sia quando si presentano come elenchi chiusi di lemmi e delle loro relazioni paradigmatiche [39] (ricordando così i classici dizionari dei sinonimi), sia quando si presentano attraverso un'architettura più complessa quale i thesauri che organizzano materiali presenti in Internet [40] (ricordando così i dizionari enciclopedici) – svolgono una funzione essenziale e in parte diversa rispetto ai tradizionali strumenti, in quanto sono in grado di indirizzare l'utilizzatore verso nuove abitudini, direzioni e regole.

Tecno-etica, *tecno*-politica, *tecno*-scienza, e anche *tecno*-diritto, *tecno*-regolazione. Si tratta di ambiti per certi versi autonomi, per altri versi dipendenti: qualche volta è possibile distinguere il loro oggetto, le loro interazioni e le loro funzioni, talaltra es-

[39] A.C. Amato Mangiameli, *Informatica giuridica*, cit., pp. 169-189.

[40] Si pensi ad esempio all'*Humanities and Social Science Electronic Thesaurus* (*HASSET*), realizzato e aggiornato dall'Università di Essex. Muovendo da una parola chiave, attraverso il suo motore di ricerca, è possibile ottenere informazioni gerarchicamente strutturate nel campo delle discipline umanistiche e delle scienze sociali (https://hasset.ukdataservice.ac.uk). Si pensi pure al *Basel Register of Thesauri, Ontologies & Classifications* (*BARTOC*), database di sistemi per l'organizzazione della conoscenza, sviluppato nel 2013 dalla biblioteca dell'Università di Basilea (https://bartoc.org/).

si sono a tal punto intrecciati e sovrapposti che sembrano perdersi i possibili confini e le probabili diversità. Conviene qui riprendere alcune considerazioni.

1.1. La *tecno*-etica, ovvero l'etica delle e per le tecnologie e le loro produzioni [41], è quell'insieme di norme, di valori, di criteri che regolano e consentono di giudicare l'uso della tecnologia e dell'artificio tecnico rispetto al bene e al male. Essa si occupa pertanto del ruolo che i valori e i criteri svolgono nella scelta, nell'uso e nella diffusione delle tecnologie. Né buona, né cattiva e neppure neutrale [42], la tecnologia offre diverse opportunità e libera l'uomo da una serie di limiti, può tuttavia costituire anche una minaccia e, in quanto forma di potere, può essere utilizzata allo scopo di manipolare, sorvegliare e opprimere. Tecnologia e artificio tecnico hanno così, per un verso, un intrinseco valore etico: sono prodotti ed espressione della libertà, sono strumenti per potere essere se stessi ed essere con gli altri, ovvero un modo di essere nel mondo attraverso la condizione e la dimensione artificiale che resta tuttavia pienamente umano; per un altro verso, tecnologia e artificio tecnico devono essere sottoposti all'analisi morale, visti i loro possibili e ambivalenti effetti (nello spazio e nel tempo) e considerati gli scopi della realtà individuale e collettiva.

Diversa dalla *tech*-noetica [43] e prossima alla *robo*-etica [44], la

---

[41] T. De Mauro, *La parola: tecnoetica*, in *Internazionale*, aprile 2007; *La parola: tecnoetica/2*, in *Internazionale*, maggio 2007.

[42] Rinvio qui alla prima delle leggi di Kranzberg: *Technology is neither good nor bad; nor is it neutral.* Le altre leggi sono: *Invention is the mother of necessity; Technology comes in packages, big and small; Although technology might be a prime element in many public issues, nontechnical factors take precedence in technology-policy decisions; All history is relevant, but the history of technology is the most relevant; Technology is a very human activity – and so is the history of technology* (*Technology and History: Kranzberg's Laws*, in *Technology and Culture*, 27, 3/1986, pp. 544-560).

[43] È il termine introdotto da Roy Ascott nell'ambito delle sue ricerche estetico-cibernetiche (*The Technoetic Dimension of Art*, in C. Sommerer, L. Mignonneau (a cura di), *Art@Science*, Wien-New York, Springer-Verlag, 1998, pp. 279-289; *Quando a onça se deita com a ovelha: a arte com mídias úmidas e a cultura pós-biológica*, in D. Domingues (a cura di), *Arte e vida no século XXI*, São Paulo, Editora UNESP, 2003, pp. 273-284).

[44] Quale disciplina che ha come obiettivo quello di migliorare la comunicazione tra uomo e robot, aiutare studiosi, stakeholder e opinione pub-

tecno-etica conquista sempre più spazi, sia perché l'attuale sviluppo tecnologico entra in senso proprio nella vita delle persone – ora condizionandola e ora dominandola –, sia perché l'interrogativo iniziale e fondamentale è diventato: sino a che punto si può spingere la tecnologia?

1.2. La *tecno*-politica è quell'insieme di attività (azioni, decisioni, provvedimenti) che, in combinato con le nuove tecnologie (soprattutto le c.d. ICT), governa la vita pubblica e i diversi contesti sociali in vista del raggiungimento di determinati fini. In particolare, l'espressione rinvia a quel complesso di trasformazioni prodotte dall'innovazione tecnologica, che influenza a tal punto la struttura del sistema politico e sociale da superare i canali tradizionali della politica e da creare modalità d'azione inedite e differenziate [45].

Le straordinarie possibilità di comunicazione, di aggregazione e di interazione, trasformano le modalità di partecipazione alla vita politica e potenziano gli strumenti di intervento diretto nei processi decisionali [46]. Altrimenti detto, l'uso ormai continuo di Internet accentua forme di associazionismo del tutto autonomo dall'*establishment* e ridimensiona le funzioni rappresentative e delegate (di partiti, di sindacati, ecc.). Così, il cittadino odierno può sperimentare nuove forme di intelligenza collettiva, più flessibili e democratiche, e divenire il protagonista assoluto di una politica del

"'presente per un avvenire', in opposizione a un presente fisso, dominato dal passato o da una trascendenza (eteronomia)" [47].

---

blica ad apprezzare l'uso positivo della robotica, prevenirne gli abusi (v. in tal senso G. VERUGGIO, *Chattiamo fra robot: tu non sai quello che io so già, chiedilo!*, in *MediaDueMila*, luglio-agosto 2005, pp. 58-63; G. VERUGGIO, F. OPERTO, G. BEKEY, *Roboetica*, in O. KHATIB, B. SICILIANO (eds.), *Handbook of Robotics*, cit., pp. 2135-2159).

[45] S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, Laterza, 1997.

[46] A.C. AMATO MANGIAMELI, *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Torino, Giappichelli, 2000, pp. 207-236.

[47] P. LÉVY, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milano, Feltrinelli, 1996, p. 90.

Non è detto però che l'agorà elettronica e la democrazia diretta istantanea siano da valutare sempre positivamente. D'altra parte, può anche essere una democrazia diretta, senza quindi intermediazione di rappresentanti, ma potrebbe presentarsi 'amputata' e 'impoverita', priva cioè del rapporto diretto che la sostanzia. La democrazia virtuale può infatti essere una democrazia *non dialogante*, solo espressione di una volontà senza ascolto e comprensione delle ragioni altrui, e l'interattività immediata si può trasformare in un pericoloso moltiplicatore di stupidità. È all'immagine del cittadino che solitario siede davanti alla sua postazione elettronica che rinviava Sartori [48] e così esclamava

"Dio ci salvi [...] dagli inesperti che ci propongono il governo diretto dall'inesperto trionfante, dal cittadino premi-bottone"!

Non è detto, inoltre, che l'odierna opulenza dell'informazione riesca sempre a identificare il cittadino *informato* con il cittadino *ideale*. Se è vero che l'informazione è strumento di arricchimento e quindi veicolo formidabile della cittadinanza democratica – in quanto colmerebbe il divario che separa le élite politiche dal *demos* – altrettanto vero è il rischio che essa possa diventare ridondante e possa condurre alla noia percettiva o persino al rigetto. Quando infatti i messaggi sono troppi e scarsamente differenziati

"non vengono più percepiti come figure contrapposte a un fondo. Tutto diventa fondo, rumore di fondo" [49].

1.3. La *tecno*-scienza si occupa del complesso delle conoscenze scientifiche in vista di una loro applicazione, in sintonia quindi con l'obiettivo della scienza moderna, che non si limita a conoscere (descrivere, comprendere e spiegare) il mondo, ma lo modifica e crea nuove realtà proprio grazie alla tecnologia che è la sua applicazione concreta.

In quest'ambito il settore di riferimento va sotto il nome di

---

[48] *Democrazia. Cosa è*, Milano, Rizzoli, 1993, p. 84 ss.

[49] T. MALDONADO, *Critica della ragione informatica*, Milano, Feltrinelli, 1997, p. 88 ss.

*Science and Technology Studie*s (STS) [50] e con l'espressione si intende in generale, per un verso, lo studio dei valori e dei principi (culturali, politici, sociali) capaci di influenzare la ricerca scientifica e l'intervento tecnologico e, per l'altro, l'analisi dell'influenza esercitata dal progresso scientifico e dall'innovazione tecnologica su cultura, politica e società. In particolare, poi, gli STS con la loro fondamentale interdisciplinarietà si propongono di rispondere a domande del tipo: *i*) qual è lo scopo della scienza e che cosa distingue la scienza dalla pseudo-scienza, che cosa è la tecnologia, come le tecnologie mediano la nostra percezione della realtà e come bisogna distribuire rischi e benefici della scienza e della tecnologia? *ii*) come si costruiscono le immagini pubbliche della scienza, quale responsabilità hanno gli scienziati per la conoscenza che producono, quale leggi di regolazione della scienza sono idonee per la protezione dei diritti e degli interessi individuali e collettivi? *iii*) qual è il rapporto tra scienza, tecnologia e democrazia, qual è il rapporto tra scienza, tecnologia e pari opportunità, come la scienza e la tecnologia influenzano l'economia, e, d'altra parte, come le multinazionali, i governi e le amministrazioni influenzano tendenze e sviluppi della scienza e della tecnologia?

Al di là della rilevanza degli Studi sociali della scienza e della tecnologia [51] e senza qui inoltrarsi in tematiche quali il sorgere della tecnologia – considerato conseguenza dell'adozione della macchina come modello interpretativo ed esplicativo di portata generale [52] –, va sottolineata la grande utilità della tecno-scienza là dove studia e testa i sistemi complessi attraverso la simulazione [53].

Assai spesso questi stessi studi si traducono anche in video-

---

[50] Cfr. innanzitutto D.J. HESS, *Science studies: an advanced introduction*, New York, New York University Press, 1997.

[51] Criticamente, cfr. U. FELT, *Sciences, science studies and their publics: speculating on future relations*, in J. BERAWARD, H. NOVOTNY (eds.), *Social Studies of Science and Technology: Looking Back, Ahead*, Dordrecht, Kluwer Academic Publishers, 2003, pp. 11-31.

[52] Sul punto, si veda E. AGAZZI, *Le rivoluzioni scientifiche e il mondo moderno*, Milano, Fondazione Achille e Giulia Boroli, 2008.

[53] Cfr. D. BENNATO, *Il computer come macroscopio.* Big data *e approccio computazionale per comprendere i cambiamenti sociali e culturali*, Milano, Franco Angeli, 2015.

giochi, nuovo fenomeno culturale di massa, che per le loro particolari caratteristiche (dinamicità, interattività, attrattività) sono unici rispetto a ogni altro mass media. Solo qualche esempio: in *Nukemap* [54] vengono simulati gli effetti di una esplosione nucleare e i parametri su cui si può intervenire sono diversi (mezzi, luoghi, effetti); in *Zombietown* [55] c'è la simulazione di un'epidemia zombie e i parametri su cui si può intervenire sono punto di inizio (paziente zero), tasso di mortalità, tempi di diffusione; in *Plague Inc.* [56] è simulata la diffusione di un virus e si scelgono le modalità di trasmissione, i possibili sintomi, le eventuali farmacoresistenze. E poi ancora: *Riot* (simulazione di proteste e guerriglie urbane), *We are data* (simulazione di una smart city hackerata), *Collapse* (simulazione di una catastrofe nucleare), *08:46* (attacco al World Trade Center), ecc.

1.4. Queste nuove combinazioni di termini (tecno-etica, tecno-politica, tecno-scienza) sono il prodotto dei tempi, tempi che richiedono nuovi contenuti, nuove funzioni, nuove velocità. E come sempre è accaduto, anche questa volta il diritto è chiamato in causa, ora come argine al dilagare di comportamenti dolosi e dannosi, ora come margine oltre il quale la tecnica non può spingersi, in ogni caso esso è chiamato a dare risposte (ad es.: per l'attività del programma, della macchina, del robot, chi può essere ritenuto responsabile, il progettista, il produttore, l'utente, il robot?) e ad offrire soluzioni ai conflitti che provengono dall'uso delle odierne tecnologie (ad es.: ha l'*host provider* un obbligo di impedire i reati commessi dagli utenti e quando può ipotizzarsi una sua responsabilità per illecito trattamento dei dati realizzata dagli *uploaders*? [57]).

---

[54] Il progetto è di A. WELLERSTEIN, storico delle esplosioni nucleari, e nel 2014 ha vinto la gara di visualizzazione al computer organizzato dalla National Science Foundation.

[55] Sviluppato da un gruppo di ricercatori della Cornell University, si avvale dei dati ufficiali dell'ufficio di statistica statunitense e applica l'algoritmo di Gillespie (modello di dinamica delle epidemie).

[56] Videogioco di strategia e simulazione del 2012 che nel corso degli anni ha avuto diverse versioni (dette mutazioni) con nuovi sviluppi.

[57] Per ulteriori considerazioni cfr. A.C. AMATO MANGIAMELI, *Informatica giuridica*, cit., pp. 24-26.

2. *Tecno*-diritto: diritto *con/della/per* la tecnologia

È possibile parlare di *tecno*-diritto[58]? Se sì, in che modo e in che senso la soluzione tecnica e la soluzione giuridica si associano e si integrano? C'è forse un ordine di priorità tra diritto e tecnica? Le domande qui proposte riassumono in breve la questione di fondo, e cioè la possibile autonomia di un settore rispetto ad altre aree, di un settore quale è quello del tecno-diritto che – proprio in nome dell'alleanza tra diritto e tecnica – può offrire soluzioni normativo-tecnologiche compatibili con la globalizzazione in atto e può essere persino più efficace rispetto alle tradizionali forme e garanzie, poiché la tutela è immediata e automatica (si pensi, e solo a mo' d'esempio, al *parental control* presente in dispositivi, quali computer, smartphone, tablet, console). Altrimenti detto, con l'espressione tecno-diritto, si intende qui rinviare a una sostanziale unità di visione del tecnico-giurista, che superi pertanto la divisione tra la pre-comprensione dei problemi e dei beni giuridici e la pre-comprensione dei limiti e delle potenzialità della tecnologia. Com'è intuitivo, ciò richiede che il giurista non si fermi sulla soglia delle applicazioni tecniche[59], ma bisogna che egli riceva una vera e propria educazione tecnologica, tanto più necessaria se si considerano le molteplici difficoltà e gli svariati dubbi creati dalla stessa evoluzione tecnologica.

---

[58] Sì certo, ne parla diffusamente IRTI che sostiene: "il volere, da cui nasce e si svolge il diritto, mira a raggiungere uno *scopo*. Volontà di scopo – potrebbe dirsi –, che sceglie mezzi e strumenti adatti. Già questo è un primo incontro con la tecnica, se per tecnica intendiamo l'*adeguazione dei mezzi al fine*, il non restare al di qua né andare al di là del risultato atteso. L'energia normativa non va sciupata e neppure risparmiata, ma messa a razionale servizio dello scopo" (*Il diritto nell'età della tecnica*, Napoli, Editoriale Scientifica, 2007, p. 13).

[59] Già BORRUSO, a proposito del rapporto giurista e informatico, sottolineava: se programmare un computer è "un'attività *altamente creativa*, *autoeducativa* e *tendenzialmente progressista*" e se l'analista ha il compito di individuare gli algoritmi delle attività umane, così da sostituire il computer all'uomo, allora l'analista non può essere il generico tecnico dell'informatica, bensì "*il tecnico del lavoro nel quale si vuole sostituire il computer all'uomo*: quindi, un ingegnere solo se tale lavoro attiene all'ingegneria, ma un chimico se esso attiene alla chimica, un medico se attiene alla medicina, [...] un giurista se attiene al diritto" (*La legge, il giudice, il computer. Un tema fondamentale dell'informatica giuridica, I, Il computer, II, Il computer per l'evoluzione del diritto*, *Miscellanea*, 4, 1993, p. 28 ss.).

Il tecno-diritto, ovvero il diritto con/della/per la tecnologia, è l'insieme di norme e procedure che sono prodotte: *i*) *dall'evoluzione tecnologica che è recepita dal diritto*; *ii*) *dalla tecnica e dal diritto che in modo sinergico si sviluppano ed evolvono; iii*) *dal diritto che con i suoi principi tratta e disciplina la tecnica*. Non si tratta di una mera formula di stile: il diritto con/della/per la tecnologia indica che l'interesse del giurista per la tecnologia non si può limitare alla sua regolamentazione perché non contrasti i fini dell'ordinamento [60], ma deve essere rivolto alla tecnologia per le sue enormi potenzialità con riguardo alla soluzione dei conflitti (si pensi all'identificatore di chiamata [61], in grado attraverso le sue funzioni di deterrenza e di protezione, di ostacolare in parte quanto previsto dall'art. 660 c.p. "chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito [...]").

2.1. Si è detto: il tecno-diritto è l'insieme di norme e procedure che sono prodotte *i) dall'evoluzione tecnologica che è recepita dal diritto*. In altri termini, la tecnologia svolge le funzioni di una norma già esistente che il diritto deve solo recepire.

È il caso dell'*e-commerce*, ovvero l'acquisto di beni e servizi attraverso piattaforme online. Ricorrendo a server sicuri (caratterizzati dall'indirizzo HTTPS, apposito protocollo per una comunicazione protetta dagli attacchi del *man in the middle*), si acquistano ormai biglietti aerei e ferroviari, capi d'abbigliamento, servizi finanziari, elettrodomestici, libri, ecc. Nel *Quadro di valutazione delle condizioni dei consumatori* della Commissione

---

[60] Ad esempio: "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito [...]" art. 640 *ter* c.p. In tema, per ulteriori considerazioni, si veda la ricostruzione di G. SARACENI, *I reati informatici: dalla diffusione di virus all'accesso abusivo*, in A.C. AMATO MANGIAMELI, G. S., *I reati informatici. Elementi di teoria generale e principali figure criminose*, cit., pp. 47-96.

[61] Le cui funzioni possono essere di segno opposto: utili le descrizioni dei diversi modi per ottenere informazioni e chiavi d'accesso ai sistemi informatici di K.D. MITNICK, W.L. SIMON, *L'arte dell'inganno*, trad. it., Milano, Feltrinelli, 2003; ID., *L'arte dell'intrusione*, trad. it., Milano, Feltrinelli, 2006.

UE si sottolinea come negli ultimi anni un numero sempre maggiore di consumatori dell'Unione Europea abbia effettuato acquisti online e che la fiducia nel commercio elettronico è aumentata, in particolare per quanto riguarda gli acquisti online da altri Paesi comunitari [62]. Restano ancora delle remore all'uso del mercato unico digitale. I commercianti al dettaglio, ad esempio, sono ancora restii a espandere le loro attività online e continuano a nutrire perplessità sulle vendite online a consumatori in altri Paesi membri, e ciò in quanto c'è un maggiore rischio di frode o di mancato pagamento nelle vendite transfrontaliere, ci sono, inoltre, diverse normative fiscali, come pure differenze nei diritti contrattuali nazionali e nelle norme a tutela dei consumatori.

Sempre in tema, non può non essere sottolineato qualche effetto significativo prodotto dalla tecnologia, prima ancora di qualsiasi intervento legislativo. Più in particolare, con riferimento al pagamento mediante carta di credito, la tecnologia pone il creditore in una posizione di massima tutela in quanto una volta ottenuto il numero della carta egli potrà, in base alle condizioni contrattuali, addebitare al debitore tutte le prestazioni che verranno effettuate nel corso del rapporto contrattuale, sostituendo così una tutela a un'altra; con riferimento invece all'informazione sui prezzi dei beni, la tecnologia consente con schermate immediate e puntuali la comparazione per un medesimo bene di tutti i prezzi rinvenibili in Rete. Motori di ricerca e software informano sui prezzi più vantaggiosi e intanto propongono acquisti online. La conseguenza diretta è, oltre alla possibile riduzione dei costi di transazione, un'informazione automatica e corretta, evitando così il possibile contenzioso tra consumatore e impresa per inadempienza al dettato normativo.

---

[62] Il Quadro di valutazione 2017 mostra che la fiducia dei consumatori nel commercio elettronico è sensibilmente aumentata: in dieci anni la percentuale di cittadini europei che acquistano online è quasi raddoppiata (passando dal 29,7% nel 2007 al 55% nel 2017). Rispetto all'edizione 2015 del Quadro di valutazione, i consumatori sono anche più consapevoli dei loro diritti (tutele, pagamenti, rimborsi). Vi sono però delle differenze, visto che le condizioni dei consumatori sono generalmente più favorevoli nei Paesi del nord e dell'ovest dell'UE rispetto a quelli dell'est e del sud. Ad esempio, il 94,5% dei finlandesi si lamenta quando incontra problemi, mentre in Bulgaria solo il 55,6% lo fa. Anche l'esposizione alle pratiche commerciali sleali varia considerevolmente, andando dal 40,9% in Croazia al 3,4% in Austria. Per affrontare tali questioni, la Commissione sta aggiornando le norme a tutela dei consumatori.

Altra ipotesi di tecnologia recepita dal diritto è l'*e-learning*, ovvero il processo di apprendimento e formazione a distanza grazie all'uso delle tecnologie multimediali e di Internet. Sono qui sfruttate le potenzialità della Rete, innanzitutto il fatto che si può accedere ai contenuti dei corsi in qualsiasi momento e in qualunque luogo esista una connessione, è perciò agevolato l'accesso a risorse e a servizi, come pure lo scambio in remoto. L'insegnamento in linea gode dell'interattività (continua e diffusa, avvalendosi del principio *learning by doing*), della dinamicità (sempre nuovi materiali e nuovi contributi, usando il detto *just in time*), della modularità (ovvero, adattabilità dei materiali e dei contenuti dei corsi secondo esigenze specifiche e particolari obiettivi formativi).

Sempre in argomento, si pensi ai vari software didattici [63], compresi quelli per il diritto [64], che integrano i vari modelli di insegnamento e apprendimento: dalla didattica assistita del calcolatore alla c.d. *extended classroom* e poi ancora al *classroom-free learning*. Sono qui predisposti pacchetti software altamente interattivi e flessibili che, grazie a sistemi tutoriali, esercitazioni e simulazioni, modificano in maniera sostanziale il modo di insegnare e di apprendere.

2.2. Si è detto inoltre: il tecno-diritto è l'insieme di norme e procedure che sono prodotte *ii*) *dalla tecnica e dal diritto che in modo sinergico si sviluppano ed evolvono*. In altri termini, la tecnologia presta al diritto le proprie applicazioni e i propri mezzi, il diritto disciplina la tecnologia con regole, leggi e piani d'azione, in un continuo andirivieni: dalla tecnologia al diritto, dal diritto alla tecnologia.

Crittografia, chiavi, documento informatico, firma digitale, posta elettronica certificata, marcatura temporale, e così via. Sono tutti termini le cui definizioni si trovano negli allegati tecnici che accompagnano le norme e che ne costituiscono parte integrante.

E intanto che il diritto disciplina i diversi settori e con essi l'impiego dei nuovi mezzi tecnologici, la sottoscrizione muta fi-

---

[63] Ad esempio, il progetto PhET, istituito nel 2002 dal Premio Nobel Carl Wieman, crea simulazioni interattive gratuite di matematica e scienze.

[64] Ad esempio: il *Center for Computer-Assisted Legal Instruction* (CALI) e la *British and Irish Legal Education Technology Association* (BILETA).

sionomia: non prova più la paternità del gesto (autografia cartacea), bensì l'uso di una chiave privata corrispondente a una chiave pubblica distribuita dal c.d. certificatore, quale soggetto pubblico o privato che gestisce i servizi di autenticazione delle firme. Cambiano inoltre i significati di categorie quali proprietà, possesso, vincolo. Si pensi agli strumenti finanziari (de-materializzati): per questi si configurano situazioni di titolarità e legittimazione, la registrazione sostituisce il possesso qualificato del documento al fine della legittimazione dell'esercizio, e sono ridefinite le eccezioni opponibili e mutano le modalità di imposizione dei vincoli.

Si trasforma pure il diritto alla riservatezza. Il trionfo di Internet e il flusso continuo, oltre che enorme, di dati personali fa sì che il concetto di privacy conquisti ulteriori significati. Non si tratta più semplicemente del diritto al riserbo della vita intima, o del diritto all'oblio, bensì del diritto di sapere e di controllare le informazioni che riguardano l'individuo e che costituiscono ormai la materia prima dell'economia contemporanea.

2.3. Si è detto da ultimo: il tecno-diritto è l'insieme di norme e procedure che sono prodotte *iii*) *dal diritto che con i suoi principi tratta e disciplina la tecnica*. In quest'ambito, hanno rilievo le questioni che attengono in generale alla sicurezza e insicurezza informatica, in particolare alle condotte e ai reati distinti a seconda che (*a*) siano concepibili solo ai danni di un computer o di una Rete telematica, oppure che (*b*) siano pensabili per il mondo reale, ancorché vengano realizzati attraverso la Rete.

Qui il tecno-diritto affronta le nuove fattispecie e le nuove tematiche riguardanti i crimini commessi attraverso Internet e, più in generale, attraverso la Rete informatica. Fenomeni quali la pirateria, la frode e la falsificazione informatiche, oppure le violazioni della proprietà intellettuale e dei diritti connessi, e ancora lo scambio e il commercio di materiale pedopornografico in Rete, non sono che alcune delle condotte che il legislatore – prevedendo, integrando e aggiornando la normativa – non lascia più impunite. Si tratta di casi legati alla nostra società dell'informazione e alla sua significativa informatizzazione.

Non diversamente dal crimine tradizionale, quello informatico copre una gamma molto ampia di condotte antigiuridiche; condotte che assumono varie forme a seconda delle tecniche usate e dei fini a cui tende l'autore del reato. In generale, sono detti

reati informatici sia quelle attività illecite nelle quali il computer è il mezzo per la commissione del reato, sia quelle attività nelle quali, invece, il sistema informatico è l'obiettivo della condotta illecita. Già così, è possibile distinguere la ricca serie di crimini informatici in due fondamentali categorie: quella che usa dispositivi e programmi come mezzi per altri fini (molestare, estorcere, ricattare, ecc.) e quella che considera proprio i dispositivi e i programmi i veri obiettivi (si pensi alla diffusione di virus e al danneggiamento informatico).

In particolare, poi, alla ricca serie di reati informatici appartengono tutte quelle attività quali le molestie, le molestie a minori, l'estorsione, il ricatto, la manipolazione dei mercati finanziari, lo spionaggio, il terrorismo, attività caratterizzate di solito da una serie continua di eventi che prevedono ripetute interazioni con l'obiettivo scelto. Com'è ovvio, le modalità possono essere le più disparate. Può accadere, ad esempio, che la vittima venga contattata in una chat da qualcuno che nel corso del tempo stabilisce, o tenta di stabilire, una qualche relazione, per poi commettere il reato. Può accadere, inoltre, che il forum pubblico sia usato per comunicare messaggi in codice, pianificando in tal modo le diverse attività criminose. Qui è agevole notare che tali attività generalmente non si servono di programmi che rientrano nella definizione di *crimeware*.

Alla ricca serie di reati informatici appartengono ancora quei reati quali il furto e la manipolazione di dati o servizi, il furto di identità e le frodi bancarie, la truffa nelle aste online; ovvero quei reati che sono accomunati dalle seguenti caratteristiche: l'attività è facilitata dall'impiego di programmi quali *keylogger*, *Trojan horse*, *virus*, ecc., i difetti e le vulnerabilità dei software offrono punti di appoggio all'aggressore per introdurre *crimeware*, la vittima inconsapevolmente scarica il programma o si collega a un sito che sembra noto, ma che, in realtà, è un sito ostile.

Sono certo cambiate le tecniche e le opportunità. Quanto alle tecniche è evidente: hardware e software sono strumenti formidabili che, grazie alle applicazioni principali dell'intelligenza artificiale, hanno reso possibile nel corso del tempo – per certi versi breve – tutta una serie di risposte anche nella gestione delle attività quotidiane prima impensabili. Quanto alle opportunità, è altrettanto evidente. Pure rispetto ai reati, le attività sono assai spesso di gran lunga più semplici da porre in essere e richiedono

poche risorse rispetto al potenziale profitto. E se i risvolti economici possono essere estremamente significativi, non sono certo di poco conto gli ostacoli al perseguimento giudiziario legati all'anonimato in cui si svolgono le comunicazioni e, soprattutto, alla separazione tra mondo fisico e mondo virtuale. In altri termini, non solo il reato informatico è, in via generale, più proficuo, così che la *cyber-criminalità* assume i contorni di una vera e propria economia sommersa, ma è anche un tipo di reato che – molto più facilmente rispetto ad altri – può restare impunito, visto che può essere commesso su un territorio senza bisogno che l'autore si trovi fisicamente lì. È un tipo di reato, inoltre, che può confliggere con i temi penalistici della giurisdizione e della competenza.

Anche il *cloud computing* – insieme di tecnologie che permettono di memorizzare, di archiviare e di elaborare dati, grazie all'uso di risorse hardware e software distribuite e virtualizzate in Rete in una architettura *client-server* – espone a particolari rischi e presenta diverse criticità [65]. Tra questi, è da segnalare la pirateria informatica. E infatti, l'utilizzo simultaneo delle risorse distribuite permette con più facilità ai criminali di monitorare attentamente l'entrata e l'uscita delle informazioni e di estrarre i dati sensibili. Sia nel caso di privati che di aziende e di industrie, la sicurezza costituisce un ostacolo all'adozione della nuvola informatica: l'utente può essere esposto a violazioni della privacy e può essere difficile il risarcimento del danno se il fornitore risiede in uno Stato diverso da quello dell'utente, l'azienda e l'industria d'altra parte corrono il serio rischio d'essere esposte a spionaggio industriale.

In realtà, il carico di dati spostati sulla nuvola genera ulteriori problematiche, non ultime quelle di tipo economico-politico, e chiama in causa il *digital divide* tra paesi ricchi e paesi poveri, che può essere corretto solo se alla localizzazione degli archivi della nuvola nei paesi ricchi corrisponde un libero accesso alle informazioni raccolte e memorizzate.

---

[65] M.N. Campagnoli, *Il cloud computing: vantaggi e problematicità*, in *Rivista di filosofia del diritto*, 1/2016, pp. 109-126.

3. Esempi di *tecno*-regolazione

La tecnologia evolve e dà vita a nuove forme di comunicazione, grazie a macchine che operano sostanziali trasformazioni (anche con il semplice: *Abort*, *Retry*, *Fail?* o con l'altrettanto semplice, quanto talvolta fastidioso, messaggio: *This page has an unspecified potential security risk. Would you like to continue?*).

La tecno-regolazione può essere ad esempio:

– *l'uso di limitatori di velocità a bordo del veicolo e di dispositivi di controllo basati sul distanziamento fra i veicoli*. Tra le diverse soluzioni, questi meccanismi rappresentano gli strumenti più efficaci per indurre il conducente a moderare la velocità e a rispettare i limiti previsti dal codice della strada.

– *l'uso di app*. Si pensi alle applicazioni per le diverse strategie di autocontrollo del tipo: *Carrot*, che regala i biscotti della fortuna se si completa un'attività e invece sorprese al limite del sadico se non la si conclude; *Finish*, qui le attività sono organizzate in breve, medio e lungo termine, ed è specificata la data di esecuzione, in modo da inviare una notifica quando l'attività deve essere completata; *Streaks*, che è creata essenzialmente per rispettare gli impegni presi con sé stessi (perdere peso, smettere di fumare, ecc.), ma che permette di ricordare le attività da svolgere nel corso della giornata, con la particolarità che per aggiungere nella lista una nuova attività bisogna che sia stata completata una vecchia; *Monkey on your back*, app di segno diverso dalle precedenti, permette di creare una lista di cose che si vuole siano fatte da qualcun altro, con la funzione di inviare e-mail di promemoria alla persona delegata e l'e-mail a chi ha delegato di attività scaduta o conclusa.

– *l'uso di Habitica*. Si tratta di un videogame che aiuta a migliorare le abitudini di vita, ad affrontare le diverse sfide e a non procrastinare, rendendo le attività (abitudini, azioni, impegni) dei mostri da combattere, che vengono sconfitti grazie alle *to do list* completate. C'è chi opta per un gioco di squadra e le *quest* sono imprese di gruppo che consistono nello sconfiggere un nemico oppure nel trovare degli oggetti, in entrambi i casi, più la squadra lavora duro, più la ricompensa è rapida.

– *l'uso dei sistemi di raccomandazione*. Il più importante aspetto, e anche il punto di forza, dei sistemi di intelligenza artificiale

è quello di imparare con l'esperienza. Possono imparare, ad esempio, i negozi che preferiamo, cosa ci piace guardare in TV, quale musica ci piace ascoltare, in quali ristoranti ci piace andare e che cosa di solito ordiniamo, e una volta ricostruiti i nostri gusti, gli algoritmi sono in grado di suggerire nuovi consumi e altri acquisti in linea con le nostre inclinazioni. Vi è così: Netflix che consiglia film, Spotify che segnala musica, Facebook che sceglie quali post farci vedere, Amazon che – vendendo di tutto (dall'elettronica agli alimentari) dispone di una enorme mole di dati e di schemi di consumo sempre aggiornati – elabora le nostre necessità e ce le propone in anteprima!

– *l'uso dei sistemi esperti*. Questi hanno tre componenti fondamentali: *i*) la base di conoscenza, ovvero il modulo che contiene le informazioni relative a uno specifico dominio e che sono necessarie per affrontare e risolvere i problemi che riguardano l'ambito; *ii*) il motore inferenziale, ossia la componente che combinando e ordinando secondo un processo logico le informazioni contenute nella base di conoscenza, costruisce la soluzione del problema; *iii*) l'interfaccia utente, e cioè il medium che consente all'utente di interagire con il motore inferenziale formulando delle domande e leggendo le relative risposte, e grazie al quale è possibile aggiornare la base di conoscenza con nuovi dati. Utilizzati in molteplici campi, e soprattutto in quello medico, dal punto di vista giuridico software di questo tipo svolgono un'attività di confronto fra la fattispecie in esame e le strutture rappresentative contenute nella base di conoscenza, e si dimostrano estremamente utili ogniqualvolta sia necessario individuare la disciplina da applicare [66].

Di importanza fondamentale, e con importanti ricadute nei nostri comportamenti e nelle nostre decisioni, sono in generale le applicazioni qui di seguito citate: gli *assistenti virtuali* (software che usano algoritmi di IA per riconoscere abitudini, linguaggio, preferenze), i *video-giochi* (applicazioni diffuse che usano algoritmi di IA e con i quali vengono creati personaggi, ambienti e storie, sempre nuovi e imprevedibili), i *servizi in linea* (app chiamate *chatbot* che si basano su sistemi di intelligenza artificiale

[66] Per ulteriori considerazioni cfr. A.C. Amato Mangiameli, *Informatica giuridica*, cit., pp. 80-88.

in grado di capire cosa chiede loro il cliente, qual è il suo problema e come risolverlo), l'*anticrimine* (software capaci di riconoscere, processando le migliaia di immagini al secondo delle telecamere di città, aeroporti, stazioni, le facce sospette e i comportamenti ambigui che possono destare allarme), la *prevenzione dalle frodi* (sistemi di IA che sorvegliano le transazioni bancarie ed evitano possibili truffe, quale l'uso improprio delle carte di credito), i *giornalisti digitali* (sistemi automatici per scrivere brevi notizie, di solito finanziarie o sportive, usati da siti di news online tra cui AP, Fox e Yahoo!), le *case intelligenti* (sistemi che gestiscono gli ambienti in termini di temperatura, illuminazione, sonorità, ottimizzano il funzionamento degli elettrodomestici, ecc., in base alle nostre abitudini, alle nostre preferenze, a nostre decisioni inviate tramite anche smartphone), le *macchine pensanti* (le *smart car* usano algoritmi di IA simili a quelli dei videogiochi, così che imparano e modificano i comportamenti secondo l'esperienza, e sono ad esempio in grado di tenere sotto controllo il traffico, di anticipare la frenata in seguito a rallentamenti, di seguire da sole le corsie della strada).

4. *Social engineering*, *neuro*-diritto e *neuro-tecno*-regolazione

Tra videogiochi, messaggi subliminali e *anticipatory computing*, la tecno-regolazione sfrutta i risultati che il processo di *data mining* offre. Con l'espressione si intende l'estrazione, con tecniche analitiche avanzate, di informazione sottintesa o nascosta da dati già strutturati, e l'analisi – eseguita in modo automatico o semi-automatico – su database di grandi dimensioni, al fine di scoprire e evidenziare *pattern* significativi. Così, fare una ricerca nel Web di una parola chiave e classificare i documenti trovati in base a un criterio semantico è un tipo di attività che rientra nel *data mining*. Oltre all'applicazione in molti ambiti della ricerca scientifica, le tecniche di *data mining* – fondate su specifici algoritmi e grazie ad applicazioni complesse – sono volte a risolvere problematiche diverse tra loro (ad es.: ottimizzazione di siti web, gestione delle relazioni, individuazione di comportamenti fraudolenti) e ad ampliare la conoscenza su cui basare i processi decisionali.

4.1. Sempre più diffuse sono anche le analisi di *social engineering*, ovvero le analisi dei comportamenti individuali, al fine di procurarsi (o anche di carpire) informazioni utili. Tale diffusione è legata a doppio filo con l'evoluzione stessa del software. E infatti, più i programmi presentano pochi errori (*bug*) e più diventa difficile, se non impossibile, aggredire un sistema informatico: non resta, allora, che attuare un attacco di ingegneria sociale. Il cosiddetto *social engineer*, le cui essenziali arti sono – per dirla con Kevin Mitnick [67] – quella dell'inganno e dell'intrusione, deve nella prima fase, che è detta *footprinting*, saper mentire, così da raccogliere tutte quelle informazioni che si considerano propedeutiche all'attacco vero e proprio, per poi passare alla fase di verifica delle stesse e, successivamente, sferrare l'attacco.

Spesso l'ingegnere sociale è utilizzato per ricavare informazioni su soggetti privati. Ecco una possibile tecnica: l'invio di una falsa e-mail, a nome di un amministratore di sistema, contenente la richiesta, alla vittima ignara, del nome utente e della password di un suo account, con la scusa di fare dei controlli sul database dell'azienda. Se la vittima cade nel tranello, l'ingegnere sociale avrà ottenuto il suo obiettivo, ossia quello di fare breccia nel suo sistema, così da iniziare una fase di sperimentazione volta a violare il sistema stesso.

Com'è chiaro, diversamente da altre tecniche, quella dell'ingegneria sociale offre al *cracker* delle metodologie assai semplici – ormai se ne parla diffusamente in diversi siti – e fondate su esempi della vita reale. Si pensi alla programmazione neuro-linguistica: di particolare importanza per scopi terapeutici – anche se non pare abbia validità scientifica – essa è diventata oggi parecchio interessante per quegli ingegneri sociali che intendono manipolare le proprie vittime e far compiere loro determinate azioni, quale quella, ad esempio, di disabilitare strumenti di sicurezza. In ogni caso, al di là della programmazione neuro-linguistica e dei suoi metodi, non c'è dubbio che nell'ipotesi di truffa – e questo vale anche per la frode informatica – si tiene innanzitutto conto di quegli schemi mentali e comportamentali solitamente usati, per poi raggirare la vittima. Si tiene, cioè, conto di tutti quei bisogni, timori ed emozioni, che sono alla base dei

[67] *Infra* nota 61.

rapporti interpersonali e che costituiscono la stessa comunicazione. Una comunicazione che può essere motivata, talvolta, dal rispetto dell'autorità (abbiamo fiducia nelle forze dell'ordine, nei medici, ecc.), talaltra, dalla pressione sociale e dall'attenzione per il giudizio altrui, e talaltra ancora da sentimenti e desideri. Ed è proprio entro queste diverse sfaccettature e pieghe, che si insinua chi intende approfittare della buona fede e/o dell'ignoranza altrui, inventando una storia credibile e richiedendo una reazione immediata. E per realizzare un attacco di ingegneria sociale basta poco: alcuni tratti caratteristici del comportamento umano, qualche informazione pubblicata su Facebook, Twitter, Foursquare, o più semplicemente una lista di desideri su Amazon!

4.2. Parecchio utili per la tecno-regolazione sono le ricerche di *neurolaw*. Si tratta di un ambito disciplinare di recente sviluppo [68], che affronta il legame neuroscienza e diritto, grazie al collegamento dei diversi saperi (filosofia, psicologia, neurologia, psichiatria, criminologia, sociologia) e agli sviluppi della tecnologia medica di ultima generazione (risonanza, tomografia, ecc.), la quale consente una mappatura dettagliata del cervello umano. Le domande pur diverse, in generale, ruotano attorno a un interrogativo di fondo: che ruolo svolge la neuroscienza nel diritto e nel processo e se essa possa e debba essere utilizzata nelle aule giudiziarie. In particolare, poi, le domande rinviano a vari contesti e sono del tipo: è possibile che alcune norme (riguardanti capacità, imputabilità, condanna, riabilitazione, recidiva, ecc.) possano essere ispirate dalla neuroscienza, in che misura una patologia e un danno al cervello può influenzare il comportamento o anche incidere sull'esecuzione penale, a chi può essere consentito la visione delle immagini del cervello di una persona, può essere il concetto di proprietà intellettuale meglio compreso grazie alla neuroscienza?

---

[68] Il termine è stato coniato per la prima volta da S.J. TAYLOR, J.A. HARP, T. ELLIOTT, *Neuropsychologists and Neurolawyers*, in *Neuropsychology*, 5, 4/1993, pp. 293-305. Più in particolare si veda S.J. TAYLOR, *Neurolaw: Brain and Spinal Cord Injury (Tort and personal injury/litigation library)*, New York, Atla Press, 1997. Negli ultimi anni la letteratura in tema ha avuto un grande impulso. Tra i diversi studi è da segnalare quello di L. CAPRARO, V. CUZZOCREA, E. PICOZZA, D. TERRACINA, *Neurodiritto. Una introduzione*, Torino, Giappichelli, 2011.

Il *neuro*-diritto studia – attraverso l'osservazione del sistema nervoso centrale, la comprensione delle funzioni cerebrali e l'analisi del nostro modo di pensare, compresa la capacità di adattarsi agli stimoli dell'ambiente esterno – il formarsi e l'uso di alcuni concetti giuridici (interesse, diritto, proprietà, dovere, divieto), l'affermarsi di termini e condizioni riguardanti la capacità, l'imputabilità, la responsabilità (ad es.: la maggiore età), il prodursi della conoscenza e dell'istruzione e l'uso di strumenti e metodi di manipolazione, non ultimo l'efficacia che suggerimenti e aiuti indiretti esercitano sui processi decisionali di individui e gruppi [69].

In particolare, grazie all'uso di tecnologie di neuro-immagine in combinato con lo studio dei comportamenti, è ormai possibile analizzare la relazione tra l'attività di determinate aree cerebrali e specifiche funzioni, come pure l'incidenza di lesioni cerebrali nella determinazione dello stato cognitivo. Ad esempio: per capire se è stata detta la verità, l'analisi di specifiche regioni del cervello può rivelarsi utile, visto che la corteccia prefrontale dorsolaterale ha dimostrato di attivarsi quando i soggetti fingono di conoscere informazioni che non sanno, anche se resta un importante ostacolo determinato dal richiamo involontario di falsi ricordi; per comprendere se la lesione o la malattia porta a uno stato vegetativo persistente, è utile sapere se vi siano segni di attenzione agli stimoli esterni e/o cicli di sonno e di riposo, e ciò è mostrato attraverso l'attività di alcune regioni del cervello rilevata dalla risonanza magnetica funzionale; per capire, visti gli effetti sul cervello dei neuro-farmaci, delle *smart drug*, dei dispositivi tecnologici [70], sino a che punto è lecito l'uso di sostanze o di macchine per il potenziamento cognitivo e per l'ascolto dell'attività elettrica del cervello [71].

---

[69] E che – secondo la *nudge theory* – non sarebbe diversa dall'efficacia esercitata in modo diretto dai comandi e dalle norme (R.H. THALER, C.R. SUNSTEIN, *La spinta gentile*, cit.).

[70] Si pensi al triangolo di plastica grande quanto il palmo di una mano, da applicare sulla tempia: serve per cambiare l'umore a comando, indurre uno stato di calma o di energia, secondo lo stato scelto nell'app del telefonino. Inventato dallo scienziato americano Jamie Tyler, è uno stimolatore che manda impulsi elettrici di bassa intensità ai nervi cranici e, in teoria, cervello e muscoli dovrebbero provare una sensazione di calma o di energia, ma non a tutti fa lo stesso effetto.

[71] Si pensi a *Brain Control*: è un drone, nato per aiutare le persone giunte

La lista dei temi che il neuro-diritto tocca e può toccare si amplia sempre di più: riguarda alcuni temi tipici del diritto civile, del diritto penale, del diritto costituzionale, del diritto internazionale, del diritto bellico. E intanto che si amplia, la *neuro-tecno*-regolazione si sviluppa: basti pensare all'uso di neuro-farmaci da parte dei militari per migliorare le loro attenzioni e le loro prestazioni, come pure per massimizzare le loro abilità cognitive, alterando il ritmo veglia/sonno e violando i loro stessi pensieri; basti pensare, in altro ambito e almeno per il momento con finalità ludica, all'uso del cerotto, usato da *nerd*, *hacker* e *game addicted*, che, messo sulla fronte, rilascia una scossa elettrica sfruttando quella che in medicina viene definita la stimolazione trans-cranica con correnti dirette [72].

5. Breve *excursus*

È particolarmente interessante osservare il fenomeno nel suo articolarsi storico. Tecno-diritto e neuro-diritto, tecno-regolazione e tecno-neuro-regolazione, sono il prodotto di importanti e differenti indagini [73], oltre che del progresso tecno-scientifico, che hanno avuto un significativo punto di arrivo durante il secolo scorso nell'opera di Wiener *Cybernetics: or the control and communication in the animal and the machine*.

Muovendo dall'idea che il mondo è un insieme di sistemi, che un sistema è un insieme di elementi in interazione e che l'interazione altro non è se non scambio di materia, energia, informa-

a stadi avanzati di sclerosi laterale amiotrofica e sclerosi multipla ad affrontare la sindrome di *locked-in*, l'imprigionamento nel corpo di una mente ancora attiva. Percepisce gli stimoli cerebrali, li comunica all'esterno, compie le azioni che il paziente pensa e vorrebbe fare. Detto in breve, *Brain Control* legge nella sua mente.

[72] All'apparenza simile agli elettro-stimolatori per i muscoli, Foc.us dovrebbe tonificare il cervello, portando un lieve miglioramento in persone con qualche difficoltà nei test logici e nel calcolo, anche se non si conoscono gli effetti a lungo termine.

[73] In campo filosofico, logico, matematico: è sufficiente qui rinviare al combinarsi di saperi e prospettive, prima che si potessero progettare e costruire le c.d. macchine pensanti (cfr. V. PRATT, *Macchine pensanti. L'evoluzione dell'intelligenza artificiale*, trad. it., Bologna, Il Mulino, 1990; ulteriori considerazioni in A.C. AMATO MANGIAMELI, *Informatica giuridica*, cit., pp. 140-165).

zione, Norbert Wiener ritenne il trasferimento di informazioni integralmente costitutivo di ogni fenomeno (naturale e artificiale). Di qui, la ricerca delle leggi generali della comunicazione, con riguardo alle macchine, agli animali, agli uomini, alla società; di qui ancora l'indagine sulle tecniche di regolazione, controllo e decisione, in campo politico, economico e sociale. Più in particolare, con la nota affermazione

"i problemi giuridici sono per loro natura problemi di comunicazione e di cibernetica, e cioè sono problemi relativi al regolato e ripetibile governo di certe situazioni critiche" [74],

il matematico americano pose l'accento sulla possibile comprensione di sistemi non-tecnici, quale ad esempio il sistema giuridico, grazie alla teoria delle reti, alla scienza della regolazione, alla teoria delle funzioni, alla statistica, al calcolo delle probabilità, in breve, grazie alla cibernetica che i risultati di quelle (e altre) scienze e teorie utilizza. Egli pose inoltre l'accento sul confronto uomo/macchina, cervello/computer: era innanzitutto l'uomo a essere osservato con il suo cervello, apparato di controllo e di calcolo, con le sue onde cerebrali la cui struttura può venire sottoposta a un preciso trattamento matematico, con la sua individualità biologica, la quale consiste di informazioni a livello cellulare che consentono i processi di rinnovamento permanente del corpo.

E che si tratti di vera e propria informazione è mostrato ampiamente dallo studio di alcune patologie: nell'atassia, ad esempio, si è incapaci di organizzare la propria azione, non già per i muscoli, bensì perché i messaggi in ingresso risultano affievoliti, se non del tutto annullati. Scriveva Wiener, a tal proposito, che per un'azione efficace sul mondo esterno, non solo è essenziale possedere buoni organi motori, ma è necessario che

"l'attività di tali organi sia adeguatamente segnalata a scopo di controllo al sistema nervoso centrale, e che i rilevamenti degli organi di controllo si combinino appropriatamente con le altre informazioni in arrivo dagli organi sensoriali per determinare un'uscita motoria regolata [...] Ogni organismo è tenuto assieme nell'azione dal possesso di strumenti per

---

[74] N. WIENER, *Introduzione alla cibernetica. L'uso umano degli esseri umani*, trad. it., Torino, Universale Scientifica Boringhieri, 1966, p. 135.

l'acquisizione, l'impiego, la conservazione e la trasmissione dell'informazione"[75].

5.1. Il lessico si arricchisce e i temi aumentano. Non solo cibernetica, ma anche giurimetria[76], gius-cibernetica[77], giuri-tecnica[78], termini questi che, pur nella loro diversità, rinviano all'integrazione diritto-macchina nei tre principali livelli: 1) informativo, 2) previsionale, 3) logico-decisionale, e per superare le cinque fallace logiche nelle quali spesso incorre il diritto: 1) non rispondenza alla logica, 2) applicabilità di uguali concetti a fattispecie diverse, 3) applicabilità di più norme a un singolo caso, 4) circolarità di definizioni e presupposti, 5) possibile ambiguità di alcuni termini giuridici.

Anche l'attuale attenzione per il ciclo della regolazione e l'idea che il legislatore debba seguire il provvedimento normativo pure nella fase di attuazione, implementazione e verifica dei risultati, in un contesto di maggiore coinvolgimento dei portatori di interessi (*stakeholder*) e dei cittadini, sono rese possibili dalle recenti e meno recenti acquisizioni teoriche, dallo sviluppo di tecniche e dispositivi di vario genere, dallo stesso uso della Rete. Una enorme quantità di informazione può essere processata (archiviata, aggiornata, estratta, evidenziata, gestita) in tempo reale, sono così favorite serie di operazioni particolarmente elaborate e gravose, prima impossibili visto il numero di variabili e di intrecci.

6. Considerazioni conclusive

Tecno-diritto e tecno-regolazione vanno compresi nei loro tratti caratteristici, proprio a partire dalle differenze che certo si

---

[75] N. WIENER, *La cibernetica. Controllo e comunicazione nell'animale e nella macchina*, trad. it., Milano, Il Saggiatore, 1968, p. 134 e p. 211.

[76] L. LOEVINGER, *Jurimetrics. The next stop forward*, in *Minnesota Law Review*, 33, 1949, p. 455 ss.; ID., *Jurimetrics: Science and prediction in the field of law*, in *Minnesota Law Review*, 46, 1961, p. 255 ss.; H.W. BAADE (ed.), *Jurimetrics*, New York-London, Basic Books, 1963.

[77] M.G. LOSANO, *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Torino, Piccola biblioteca Einaudi, 1969.

[78] V. FROSINI, *La giuritecnica: problemi e proposte*, in *Informatica e diritto*, 1/1975, pp. 26-35.

danno tra la regola tecnica e la norma, tra il c.d. *computer law* e la legge [79].

Richiamata dalla norma [80], la misura tecnica ha una fonte diversa rispetto alla creazione legislativa, sono infatti i tecnici del settore che introducono e definiscono i termini, gli strumenti e gli ambiti di applicazione. Ciò comporta che, per un verso, la tecno-regolazione tende a essere rigida [81], mentre le norme sono flessibili e aperte all'interpretazione, così flessibili e aperte all'interpretazione da creare qualche volta persino confusione e arbitrarietà – è quanto lamentato da sempre e da più parti –, e per l'altro, le norme tecniche sono dinamicamente mutevoli e necessitano di continuo adeguamento tecnologico, rispetto alla legge che invece è relativamente statica. È sufficiente qui ripensare all'evoluzione tecnica della firma digitale e al continuo aggiornamento delle architetture dei sistemi informatici, dei linguaggi e delle piattaforme di sviluppo, ovvero alla progressiva implementazione dei progetti di *e-Government*.

La regola tecnica è rigida – anche nel suo farsi e disfarsi secondo il progresso tecnologico e la plasticità del software – poiché ha uno statuto tecno-scientifico, si presenta attraverso algoritmi, usa un linguaggio che prova a rendere efficace, rigorosa, inequivoca la lettera della legge. La regola tecnica risolverebbe quindi i problemi pratico-ermeneutici e soddisferebbe al contem-

---

[79] Cfr. M. HILDEBRANDT, J. GAAKEER (eds.), *Human Law and Computer Law: Comparative Perspectives*, cit., qui, in particolare, si vedano U. PAGALLO (*What Robots Want: Autonomous Machines*, cit., p. 47 ss.); B. VAN DEN BERG, R.E. LEENES, *Abort, retry, fail*, cit., p. 67.

[80] Ad esempio, così recitano: l'art. 244 c.p.p., comma 2, "l'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione"; e l'art. 247 c.p.p., 1 *bis*, "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

[81] Si pensi, e solo a mo' d'esempio, alle definizioni di chiave privata (l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare), di chiave pubblica (l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico) e a tutte le altre definizioni con le quali ha inizio il Codice dell'Amministrazione digitale.

po l'antica illusione: il giudice bocca della legge e – riprendendo l'espressione weberiana – automa paragrafico, ovvero

"distributore automatico di diritto, vincolato alla pura interpretazione di paragrafi e di contratti, nel quale si introduce da una parte il fatto insieme alle spese, per estrarne dall'altra la sentenza con i motivi" [82].

Nel mondo contemporaneo tutto ciò si tradurrebbe in automatica applicazione della norma per mezzo di un robot che nel somigliare sempre più all'uomo, come nel dramma fantascientifico di Čapek, riesca a soddisfare proprio ciò che accomuna le macchine intelligenti e gli uomini che le hanno costruite: l'ideale della razionalità e di una comunicazione libera da ambiguità e oscurità.

Si consideri la legge: non sempre i suoi enunciati sono precisi, inequivoci, non contraddittori. Se essi lo fossero, potrebbero ben essere trasfusi in algoritmi e quindi in programma. Diversamente, gli enunciati normativi hanno una trama aperta e delle zone di penombra [83], così che l'interprete non può ridursi a logico puro applicatore e d'altra parte – come sottolineava Bobbio a proposito delle tre fasi di sviluppo della giurisprudenza [84] – il linguaggio del legislatore non è necessariamente rigoroso, né completo e neppure ordinato: il primo compito del giurista è allora quello di renderlo più rigoroso, il secondo è quello di completarlo quanto più è possibile, il terzo è di ridurlo a sistema.

---

[82] M. WEBER, *Economia e società, III, Sociologia del diritto*, trad. it., Milano, Edizioni di Comunità, 1997.

[83] Qui è ovvio il rinvio a H.L.A. HART: "La struttura aperta del diritto significa che vi sono, in realtà, delle sfere di condotta in cui deve essere lasciato molto spazio all'attività dei tribunali e dei funzionari che decidono, alla luce delle circostanze, tra interessi in conflitto che variano di importanza di caso in caso" (*Il concetto di diritto*, trad. it., Torino, Einaudi, 1965, pp. 158-159). Sull'idea di 'zona d'ombra' e 'zona di luce' cfr. le osservazioni di R. GUASTINI, *Trama aperta, scienza giuridica, interpretazione*, in U. SCARPELLI, P. DI LUCIA (a cura di), *Il linguaggio del diritto*, Milano, LED, 1994, p. 467 ss.

[84] "Quando per giurisprudenza si intenda appunto l'analisi linguistica che ha per oggetto le proposizioni normative di un determinato ordinamento [...] La prima fase è di *purificazione*, la seconda di *completamento*, la terza di *ordinamento* del linguaggio giuridico" (N. BOBBIO, *Scienza del diritto e analisi del linguaggio*, *ivi*, p. 97).

6.1. L'*high-tech law* offre delle opportunità, in piena sintonia con le tecnologie informazionali-comunicazionali. Si pensi a quelle due qualità riferite agli elaboratori elettronici: risparmiatori di tempo e amplificatori di intelligenza, qualità che se poste nella giusta luce possono considerarsi valido ed essenziale ausilio, sia diretto che indiretto, all'attività più tipica e propria del giudice, che è per l'appunto decidere della controversia e redigere la sentenza. E infatti, la ricerca veloce ed efficiente dei dati e dei documenti necessari per l'accertamento del fatto, come pure delle fonti normative utili per la valutazione giuridica del fatto medesimo, costituisce un primo e importante contributo di cui il giudice può servirsi ai fini della sua decisione. Ciò non è affatto da sottovalutare, poiché questo livello, usualmente definito documentale, in realtà nei sistemi esperti diventa un susseguirsi intelligente e ragionato di documenti. Così, il giudice nell'avvalersi di dati, di criteri e di interazioni, memorizzati in un programma, può rivedere le proprie ipotesi, e in un certo senso a suo modo si consiglia, oltre che con il proprio sentire, anche con la macchina e la sua capacità di acquisizione di nuove premesse maggiori e di nuove premesse minori.

Ma l'*high-tech law* espone pure a dei rischi. Ad esempio, grazie all'elaborazione elettronica dei dati, è possibile rintracciare quelle leggi non più applicate in sede giudiziaria da un certo numero di anni. Il rischio è che, nel salvare tutto, si perda il c.d. 'sollievo della dimenticanza' con la rilevante funzione giuridica svolta dalla norma obsoleta. Si tratta del quotidiano accomodamento del diritto, che consapevolmente o meno ratifica la prassi giudiziaria, spesso senza darne alcuna spiegazione. Può accadere così che alcuni presupposti della decisione, ritenuti prima fondamentali, vengano del tutto dimenticati, e che alcune premesse normative, ritenute prima rilevanti, siano invece considerate superate dalle circostanze reali e dallo sviluppo tecno-giuridico. In generale, può dirsi che, in tali processi di selezione e di accomodamento del diritto, diventa obsoleto quel che è meno utile per la prassi e quel che è anacronistico [85].

---

[85] R. ZIPPELIUS, *Juristische Methodenlehre*. *Eine Einführung*, München, C.H. Beck, 1985, pp. 107-108.

6.2. Bisogna che regola tecnica e norma, tecno-diritto e diritto, soddisfino comunque l'astrattezza e la generalità della legge (la legge non può e non vuole dire tutto per il caso concreto [86]), gli ampi contenuti esperienziali delle norme e lo spazio di gioco tra più significati (*Beduetungsspielraum* [87]), grazie al quale il giudice è in condizione d'optare per quella decisione che a suo avviso (e presumibilmente ad avviso del legislatore attuale) media tra le necessità del sistema giuridico e il riconoscimento di nuovi orizzonti d'aspettativa. In breve: per quella decisione giusta in senso corrente e che ha effetti sociali preferibili. In questo modo, l'applicazione del diritto è in qualche misura partecipazione alla produzione del diritto medesimo [88]. Tanto è vero che se di norma i giuristi affermano di dover applicare innanzitutto tutte le norme positive, al contempo non possono non convenire che

"nei casi non disciplinati dalla legge o in cui non sia data una norma *ad hoc*, essi s[ono] costretti a 'creare' [desumere] nuove regole dagli esistenti 'giudizi assiologici' del legislatore o dall"ordinamento giuridico' nel suo complesso".

---

[86] Scriveva a tal proposito A. MERKL (*Il duplice volto del diritto. Il sistema kelseniano e altri saggi*, trad. it., Milano, Giuffrè, 1987, pp. 286-287): la legge "non vuole dire tutto, perché vuole essere soltanto una forma nel processo di formazione del diritto, una forma ancora relativamente assai generale, vale a dire *non individualizzata*". Se così è, l'applicazione del diritto svolge una funzione essenziale. Essa compie ciò che la legge, in quanto forma giuridica generale che ancora "abbisogna di specificazione", non può compiere: il percorso "dall'astratto al concreto, condizione affinché all'ambiguità si sostituisca l'univocità".

[87] R. ZIPPELIUS, *Juristische Methodenlehre*, cit., p. 102 ss.

[88] Sempre utili le osservazioni di K. LARENZ (*Storia del metodo nella scienza giuridica*, trad. it., Milano, Giuffrè, 1966, pp. 192-193) al riguardo: "la tesi secondo la quale il diritto codificato può essere interpretato, messo in pratica e perfezionato esclusivamente in base a se stesso – sia in base alle vedute del legislatore sia in base al 'contenuto significativo immanente' in esso – non dovrebbe essere mantenuta dopo il libro di Esser, anche se crediamo, che Esser sottovaluta il significato autonomo di una disciplina legislativa ben equilibrata. Il giudice, anche in presenza di un diritto codificato, è molto spesso obbligato a ricorrere a fondamenti di valutazione extralegislativi e, precisamente, non soltanto nei casi in cui la legge rinvia esplicitamente a tali fondamenti. Il diritto vigente non è contenuto soltanto nella legge, ma è sempre il risultato di un processo evolutivo di concretizzazione, al quale la giurisprudenza partecipa in maniera decisiva".

E, come da più parti sottolineato ed accettato, questa creazione di nuove norme non è attività puramente logica (deduttiva). Si spiegano così le aspre critiche che vengono rivolte

"alla concezione del giudice come un 'automa della sussunzione' – la quale, peraltro, non è stata mai nulla di più e di diverso che un'immagine orrorifica" [89].

Il tecno-diritto e la tecno-regolazione, risultato di programmi che menti intelligenti hanno predisposto, necessitano di sistemi e di procedimenti, di sistemi esperti, di procedure inferenziali di ragionamento, di linguaggi di programmazione, restano comunque create dall'uomo per l'uomo. Bisogna così che alle menti intelligenti, nessuna esclusa e non importa quale sia l'orientamento (tecnico, scientifico, ecc.), siano familiari – come scriveva Krämer [90] – non solo criteri di valutazione difficilmente definibili in esatti termini scientifici (il senso vagamente definito dell'armonia, della misura e della tensione, la conoscenza non esattamente acquisibile dello stile e della sua evoluzione), ma anche la capacità di afferrare i suoni delle vibrazioni dell'anima nell'espressione artistica e la sensibilità per l'essenza che si cela dietro i fenomeni.

[89] H.M. PAWLOWSKI, *Introduzione alla metodologia giuridica*, trad. it., Milano, Giuffrè, 1993, p. 90.

[90] *Automat und Mensch*, in *Universitas*, 13, H. 5, 1958, pp. 511-522.

V

NUOVE CONDOTTE PENALMENTE RILEVANTI. *LA TECNOLOGIA ALIMENTA IL CRIMINE!*

Sommario

1. Tecnologia e codici malevoli

Più la tecnologia avanza, più gli individui e i gruppi se ne servono secondo le loro inclinazioni e decisioni. Rimedi e rischi si alternano senza sosta, sicurezza e insicurezza informatica si danno di continuo il cambio.

Solo due esempi. Il primo è quello di *Cain & Abel*. Si tratta di un programma di monitoraggio delle reti informatiche: uno strumento di recupero delle password per i sistemi operativi Microsoft, in grado di captare e intercettare i tanti dati e le molte credenziali che circolano in una Rete *Lan* (*local area network*) e che servono per effettuare il *login* a *social network*, a siti *home banking*, a *messenger VoIp* (*voice over Ip*) e così via. In breve, un programma in ogni caso ricco di funzionalità e parecchio versatile, il cui utilizzo può anche essere improprio e illegale.

Il secondo esempio riguarda lo *sniffing* e cioè quella particolare attività che prevede l'intercettazione dei dati che transitano

all'interno di una Rete e che di norma viene svolta per scopi legittimi, quali l'analisi dei problemi di comunicazione o l'individuazione di tentativi di intrusione, ma che può essere indirizzata anche verso scopi illeciti e in violazione di quella stessa sicurezza informatica che dovrebbe essere tesa a proteggere.

1.1. La tecnologia, con le sue tante applicazioni software (le c.d. app), è certo una formidabile opportunità. Non tutte le app meritano, però, di essere scaricate sul telefonino o sul *tablet*, ve ne sono, anzi, alcune che – contenendo cavalli di Troia (c.d. *Trojan*) – si rivelano particolarmente pericolose, poiché in grado di espugnare i cellulari a tutto vantaggio dei pirati informatici.

In Rete si assiste a una rapida evoluzione di programmi malvagi-codici malevoli (c.d. *malware*). Si tratta di hardware e di software che, qualche volta recuperano dati dell'utente del computer a scopo pubblicitario e per l'esercizio di attività commerciali, qualche altra volta, invece, ne danneggiano o ne alterano il funzionamento al fine di assumerne il controllo e per compiere ulteriori intrusioni ai danni di altre postazioni remote connesse alla Rete.

1.2. La lista non solo è particolarmente ampia, ma, come è intuitivo, è anche in continua crescita. Qui di seguito, solo qualche esempio.

Adware: programma che presenta inserzioni pubblicitarie, allo scopo di indurre l'utente a effettuare ulteriori acquisti o altri aggiornamenti del software, così da generare maggiori profitti alla società. Tale programma presenta però qualche rischio. Alcuni adware, infatti, aprendo di continuo pop-up pubblicitari, possono rallentare le prestazioni della macchina, altri, invece, possono modificare le pagine html direttamente nelle finestre del browser per includere link e messaggi pubblicitari propri, di modo che all'utente venga presentata una pagina diversa da quella voluta dall'autore. Molti adware, inoltre, comunicano le abitudini di navigazione degli utenti a server remoti, violando così assai spesso la loro privacy.

Backdoor: programma che consente un accesso non autorizzato al sistema, a prescindere dalla conoscenza e dall'uso dei co-

dici di utenza (username e password). Si tratta di un programma che può costituire una forma di accesso di emergenza e che viene installato dall'amministratore di sistema per permettere, ad esempio, il recupero di una password dimenticata, ma che può anche essere creato da qualche esperto informatico per accedere illegittimamente ai servizi di Rete. La backdoor, questa sorta di porta di servizio, è normalmente invisibile e versatile, ha cioè la capacità di eseguire comandi senza che l'utilizzatore se ne accorga e quella di adattarsi per superare i diversi sistemi di sicurezza che ogni pc può avere.

Dialer: programma che crea una connessione a Internet, o a un'altra Rete di calcolatori, oppure a un altro computer, tramite la comune linea telefonica. Un programma creato, assai spesso, per connettersi a numeri a tariffazione speciale, all'insaputa dell'utente. Il metodo seguito è di solito l'offerta gratuita, presente in alcuni siti web, ad esempio, di loghi o suonerie per il telefono, di canzoni e file mp3, di immagini pornografiche e così via, a condizione che venga installato – ancora una volta gratuitamente – un certo programma che, in realtà, è un dialer che si connette a numeri telefonici dal costo elevato.

Keylogger: hardware o software in grado di registrare tutto ciò che un utente digita sulla tastiera, di copiare e incollare password e altri dati, di monitorare i siti web visitati e i programmi avviati, di decifrare le conversazioni chat, in breve, di sorvegliare ogni azione che venga compiuta sul pc. Il keylogger hardware può essere installato tra la tastiera e il pc, oppure può essere nascosto all'interno della tastiera stessa, è completamente indipendente dal sistema operativo ed è capace di intercettare le password impiegate nella fase di avvio. Il keylogger software, invece, è un semplice programma installato sul computer da una persona che può insinuarsi nel pc o attraverso l'accesso remoto, oppure direttamente, rubando password e dati dell'utente. Il programma può essere anche trasportato nel computer da un Trojan o da un worm ricevuto tramite Internet.

Trojan horse: programma apparentemente utile che può contenere qualsiasi tipo di istruzione, di solito dannosa, e che – come nel mitico stratagemma adottato da Ulisse – induce la vitti-

ma ad eseguire il programma stesso. In genere, il Trojan è utilizzato per inviare messaggi spam e per appropriarsi di dati personali, è comunque un programma volto ad assumere il controllo del sistema informatico; non possiede funzioni di autoreplicazione – quindi per diffondersi richiede un intervento diretto dell'aggressore – ma può nascondersi nelle cartelle del sistema operativo.

Virus: programma specializzato nell'eseguire alcune semplici operazioni, ottimizzato per impiegare il minor numero di risorse e in grado di riprodursi e diffondersi generando copie di se stesso, così da infettare i file senza che l'utente se ne accorga. Il virus di solito danneggia direttamente solo il software della macchina che lo ospita, ma può indirettamente provocare danni anche all'hardware. Il veicolo preferenziale di infezione è oggi rappresentato dalle e-mail e dalle reti peer-to-peer.

Parasitic Virus: ossia i c.d. virus parassiti. In questo modo, vengono definiti quei *virus* che trovano ospitalità all'interno di un file eseguibile. Attivandosi subdolamente, questi programmi usufruiscono di tutte le autorizzazioni di cui gode il file che li ospita. Possono dunque replicarsi, installarsi automaticamente nella memoria e mettere in atto il proprio payload. Il più antico e celebre parasitic è stato *Jerusalem* che risale al 1987.

Companion Virus: questi virus prendono il nome di un file eseguibile già presente nel computer, ma utilizzano l'estensione '.com' invece della comune '.exe'. Quando il sistema Windows incontra due file con lo stesso nome, nell'incertezza, offre la precedenza al file '.com'. Il primo e più famoso companion virus mai scoperto fu il *Globe* (1992).

Link Virus: si tratta di virus che vengono scaricati e/o eseguiti cliccando su un link contenuto all'interno di un qualunque sito. Normalmente, il link sembra puntare verso una destinazione innocua o comunque non sospetta.

Worm: programma che modifica il sistema operativo della macchina ospite, in modo da essere eseguito automaticamente e da autoreplicarsi. Si tratta di un programma che, ad esempio,

ricerca indirizzi e-mail memorizzati nel computer ospite e invia una copia di se stesso come file allegato (attachment) a tutti, o a parte, degli indirizzi che è riuscito a raccogliere. I messaggi contenenti il worm il più delle volte utilizzano tecniche di ingegneria sociale per indurre il destinatario ad aprire l'allegato. Qualche worm sfrutta i difetti (bug) di alcuni programmi, per eseguirsi automaticamente al momento della visualizzazione del messaggio e-mail. Assai spesso il programma funge da strumento per l'installazione automatica – sul maggior numero di macchine possibile – di altri malware, quali i già citati backdoor e keylogger.

E ancora: *Hijacker*, programma che si appropria di applicazioni di navigazione e che determina l'apertura automatica di pagine web indesiderate; *Logic bomb*, ovvero codice inserito in un programma, all'apparenza innocuo, che – al verificarsi di determinate condizioni o stati del pc – per l'appunto esplode, ad esempio, modificando o cancellando file, bloccando il sistema, o cancellando l'intero contenuto di un disco; *Rabbit*, programma che esaurisce le risorse del computer creando copie di se stesso a grande velocità; *Scareware*, programma la cui installazione viene suggerita all'utente attraverso tecniche di *marketing*, o mediante i metodi di ingegneria sociale, e che simula il comportamento di un programma legittimo, notificando la presenza di problemi inesistenti e facendo installare malware che si fingono antivirus, come il noto *rogue antispyware*; *Spyware*, programma diretto a carpire informazioni (dalle abitudini di navigazione, sino alla password e alle chiavi crittografiche di un utente) e a trasmetterle ad un destinatario interessato; *Zip Bomb*, file che, una volta aperto, si espande fino a diventare un file di circa quattro petabyte, occupando quindi tutto lo spazio del disco rigido.

1.3. Può capitare che un malware possieda una natura ibrida, appartenendo a due o più categorie tra quelle elencate. Ad esempio, nel corso del 2017, si è registrata un'epidemia su larga scala dovuta alla diffusione di un malware denominato *WannaCry*, detto anche *WannaCryptor 2.0*. Questo *criptoworm*, appartenente alla famiglia dei *ransomware*, codificava i file del sistema ospite, minacciandone la definitiva cancellazione, impedendo il riavvio del sistema e chiedendo all'utente il pagamento di un riscatto in bitcoin. Il 12 maggio del 2017 *WannaCry* contagiò

i computer di molte importanti aziende in tutto il mondo (come, ad esempio, Portugal Telecom, Deutsche Bank, FedEx e Telefónica), colpendo anche istituzioni di rilievo internazionale (si pensi a quanto avvenuto al sistema operativo del Ministero degli Interni Russo).

Al fine di ingannare gli utenti, *WannaCry* sfruttava una falla presente nel *Server Message Block*: un protocollo normalmente utilizzato, soprattutto dai sistemi Windows, per condividere file, stampanti o porte seriali all'interno di una Rete. Più esattamente, esso si basava su di un exploit diffuso da un gruppo *hacker* denominato *The Shadow Brokers*, la cui prima apparizione risale al 2016. Dopo la diffusione di questo exploit, Microsoft corse immediatamente ai ripari, rilasciando una patch atta a proteggere gli utenti di Windows, ma in questo, come in molti altri casi, il mancato o non tempestivo aggiornamento dei sistemi giocò un ruolo di fondamentale importanza per la diffusione e il successo del malware.

WannaCry subì un duro colpo quando un ricercatore britannico scoprì che, prima di infettare un computer, il criptoworm provava a contattare un sito web non registrato. Si trattava di un *kill switch*: un codice inserito nel malware per reagire ai controlli degli antivirus. In tal modo è stato possibile sconfiggere uno dei più pericolosi *ransomware* mai elaborati e diffusi in Rete.

1.4. Com'è intuitivo, grazie alla diffusione di queste tecniche e di questi programmi, e di molti altri ancora, anche l'attività criminosa finisce con l'essere in qualche modo agevolata e incentivata. Del resto, esiste già un vero e proprio mercato nero legato ai programmi malvagi-codici malevoli: oltre alla compravendita di dati personali, è possibile infatti acquistare l'uso – per scopi personali e ad insaputa dei legittimi proprietari – di una certa quantità di computer controllati da remoto tramite backdoor.

In breve, per dirla con l'ex falsario statunitense, oggi consulente finanziario, Frank William Abagnale:

"fare oggi quello che ho fatto durante la mia giovinezza è molto più facile. La tecnologia alimenta il crimine!"

2. Intermezzo: il *manifesto hacker*

Si è detto all'inizio: più la tecnologia avanza, più gli individui e i gruppi se ne servono secondo le loro inclinazioni e decisioni. Rimedi e rischi si alternano senza sosta, sicurezza e insicurezza informatica si danno di continuo il cambio. Sempre più, comportamenti di segno diverso si sovrappongono e si contendono la scena.

Qualche volta è lo spirito creativo, la curiosità sovversiva, il gusto per il gioco senza alcun altro fine – in altri termini l'arte dell'*hacker* – che caratterizza la condotta. Qualche altra volta, la grande capacità tecnica non si accompagna e non è mossa dalla curiosità e dal divertimento fini a se stessi, ma, al contrario, abusa delle proprie capacità e il comportamento – tipico del *cracker* – è doloso e dannoso. Com'è intuitivo, non sempre il confine è netto. Anche di qui, la confusione tra hacker e cracker che il linguaggio comune, di solito, propone tramite la stessa analogia hacker-malvivente.

2.1. L'espressione *hacking* indica quell'insieme di tecniche e operazioni destinate a conoscere, accedere, modificare, un sistema hardware o software. Di solito, il termine rinvia a quell'attività interessata al funzionamento dei sistemi informatici e delle misure di sicurezza poste a loro protezione. Si tratta, quindi, di attività assolutamente lecita, svolta spesso a livello professionale da chi si occupa dell'amministrazione di sistemi informatici, o da chi ne cura lo studio e lo sviluppo.

Ad esempio, tale attività può riguardare un incremento di prestazioni hardware o una rimozione della limitazione del funzionamento che i produttori di componenti elettronici, o di applicazioni, hanno aggiunto ai loro prodotti per circoscrivere l'uso dei prodotti stessi in alcune circostanze (programmi non originali, componenti non certificate). Allo stesso modo, nelle attività di hacking rientra anche l'aggiunta di funzioni ad un programma.

In altri casi, poi, l'insieme delle tecniche e delle operazioni hacking può essere adottato come contromisura al fenomeno – quanto mai diffuso – degli attacchi a sistemi informatici e telematici pubblici e privati.

L'accezione positiva del termine deriva anche da quell'etica e cultura hacker che Steven Levy già negli anni '80 (nel suo

Hackers. Gli eroi della rivoluzione informatica) fonda su cinque principi fondamentali e, cioè: la condivisione, l'apertura, la decentralizzazione, il libero accesso alle tecnologie informatiche, il miglioramento del mondo. Non è a caso che gli hacker moderni – e tra questi innanzitutto Richard Stallman – siano stati strenui sostenitori del software libero e dell'*open source software* contro il software proprietario.

Del resto, così si legge in quel *Manifesto Hacker* scritto nel 1986 da Loyd Blankenship:

"Questo è il nostro mondo adesso [...] il mondo dell'elettrone e dello switch, la bellezza della banda.
Noi usiamo un servizio che esiste già […] gestito da avidi ingordi, e ci chiamate criminali. Noi esploriamo [...] e ci chiamate criminali. Noi cerchiamo la conoscenza [...] e ci chiamate criminali. Noi esistiamo senza colore della pelle, senza nazionalità, senza pregiudizi religiosi [...] e ci chiamate criminali. Voi costruite bombe atomiche, voi provocate guerre, voi uccidete, ingannate e mentite e cercate di farci credere che è per il nostro bene, eppure siamo noi i criminali.
Sì, sono un criminale. Il mio crimine è la curiosità. Il mio crimine è giudicare le persone per quello che dicono e pensano, non per il loro aspetto. Il mio crimine è stato surclassarvi, qualcosa per cui non mi perdonerete mai.
Io sono un hacker, e questo è il mio manifesto. Potrete anche fermare me, ma non potete fermarci tutti [...] dopotutto, siamo tutti uguali".

Alcune forme di protesta e di lotta – anche in nome dei diritti fondamentali – caratterizzano quel fenomeno che è proprio dell'ultimo decennio e, cioè, quella libera coalizione (meglio: 'la prima coscienza cosmica') degli abitanti di Internet detta *Anonymous*, i cui partecipanti provenienti da *imageboard* e *forum* si coordinano e agiscono, mobilitandosi in favore di diritti e rivendicazioni del mondo reale. Si pensi al primo attacco nei confronti del *social network Habbo Hotel*, attacco (conosciuto come il *Great Habbo Raid of '06* e seguito, l'anno successivo, dal *Great Habbo Raid of' '07*) legato alla notizia che un parco di divertimenti in Alabama aveva vietato a un minore affetto da Aids di immergersi in piscina. Si pensi, ancora, all'attuale presa di posizione degli attivisti di *Anonymous* contro *Isis* che ha innanzitutto preso di mira migliaia di account Twitter, Facebook, ecc., di e-mail di presunti appartenenti al c.d. Califfato, e che è riu-

scita a far chiudere un centinaio circa di siti di propaganda jihadista, riducendone così la portata.

2.2. Vi è poi tutta una serie di attività che – utilizzando metodi e tecniche dell'hacker – sono svolte, ad esempio, per aggirare l'acquisto delle licenze o per accedere a sistemi altrui, allo scopo di carpire dati riservati o di danneggiarne il funzionamento. Il fenomeno è detto *cracking* quando le attività alterano la struttura di un programma o aggiungono funzioni: nel software proprietario, i possibili interventi possono violare la licenza di utilizzo del software stesso rendendone illegale l'uso, anche se legalmente acquistato. Altre attività di cracking possono essere: l'accesso alla Rete di comunicazione pubblica e il suo uso senza esserne accreditati, come pure l'uso non autorizzato di una Rete di computer a diffusione locale, una particolare prassi, che è facilitata dalla diffusione delle reti wireless e che può violare le leggi che regolamentano le telecomunicazioni e la privacy.

La pratica del cracking che modifica un software per rimuovere la protezione che ne impedisce la duplicazione, oppure per ottenere accesso a un'area altrimenti riservata, usa il *reverse engineering*, ovvero una tecnica che permette di comprendere la logica che caratterizza il software analizzandone il funzionamento e le risposte che esso dà a determinati input, al fine di produrne uno nuovo. Com'è intuitivo, nel cosiddetto cracking, il processo di analisi dell'ingegneria inversa – di solito destinato alla comprensione e alla realizzazione di software – è usato allo scopo di realizzare e distribuire materiale, prevalentemente software, in violazione del copyright che lo ricopre.

E nel frattempo, tra violazioni e saccheggi, tra imbrogli e danni, i cracker si dividono in squadre (cracking crew) e si sfidano, spinti assai spesso dalla prospettiva del guadagno economico o, in qualche altra occasione, dall'esigenza di essere approvati all'interno di un gruppo di cracker.

3. Sicurezza e… *fake news*

La sicurezza degli utenti risulta oggi minacciata dalla sempre più preoccupante e pervasiva diffusione delle c.d. *fake news*. L'invenzione e la conseguente diffusione di notizie false non rappresenta certamente una diretta conseguenza della rivoluzione informatica, al contrario, si tratta di un fenomeno parecchio risalente nel tempo. Tuttavia, essa ha conosciuto un nuovo e significativo slancio con l'avvento di Internet e, più esattamente, con la nascita della versione 2.0 del Web, a sua volta strettamente connessa alla genesi e al successo dei *social network*.

La caratteristica fondamentale del World Wide Web è quella di costituire il primo mezzo di comunicazione *per* le masse. A differenza dei precedenti mezzi di comunicazione *di* massa, quali la televisione, la radio o i giornali, il Web non prevede la presenza di un mediatore culturale. Altrimenti detto, manca una specifica figura professionale preposta a stabilire cosa debba o cosa non debba essere pubblicato; in breve, manca qualcuno che svolga tutti quei compiti che nei tradizionali mezzi di comunicazione di massa sono comunemente affidati al Direttore Responsabile oppure all'Editore.

A ciò si aggiunga che, a differenza dei vecchi mezzi di comunicazione di massa che presentano tutti un'architettura di *broadcast* contraddistinta da un centro di diffusione del segnale tecnologicamente raffinato ed economicamente dispendioso (come, ad esempio, l'antenna dalla quale parte il segnale di una radio, quella che diffonde le immagini di uno studio televisivo, oppure la rotativa utilizzata per la stampa del giornale), la Rete è caratterizzata da miliardi di piccoli nodi che agiscono, contemporaneamente, da diffusori e da ricettori del segnale.

Ma se così, appare evidente che, grazie al World Wide Web, ciascun utente ha la possibilità di diffondere liberamente il proprio pensiero, senza che ci sia alcun controllo preventivo circa la veridicità, la correttezza o la scientificità dei messaggi che egli intende pubblicare. Per questo motivo, il Web è diventato nel giro di pochi anni l'habitat più favorevole per la diffusione delle *fake news*. In quest'ottica, non stupisce affatto che i social network si siano presto tramutati in strumenti in grado di consentire la realizzazione di veri e propri esperimenti di ingegneria sociale, basati sulla diffusione di notizie atte a influenzare le

masse, screditare gli avversari politici e pilotare i risultati elettorali.

Le ragioni per le quali le *fake news* rientrano a pieno titolo tra i principali e i più urgenti problemi di sicurezza informatica sono presto dette: 1) la diffusione di notizie inventate può minare sensibilmente l'ordine pubblico di uno Stato; 2) se queste notizie, come spesso accade, hanno ad oggetto cure miracolose o fantomatiche epidemie, esse possono risultare altrettanto pericolose per la salute pubblica; 3) nel caso in cui riguardino invece l'informatica, le fake news possono influenzare sensibilmente il contegno degli utenti, peggiorando la sicurezza dell'intera Rete. Pensiamo, ad esempio, alla ormai celebre catena sulla privacy. Questo post, che ha fatto più volte e letteralmente il giro del mondo, invita gli utenti dei social network a pubblicare sulla propria bacheca una sorta di disclaimer con il quale si intima al social di non utilizzare senza una preventiva autorizzazione le foto, idee o informazioni, che l'utente ha liberamente condiviso sul proprio profilo. Sebbene questo messaggio non possieda alcun valore giuridico e non determini alcuna conseguenza pratica, moltissimi utenti, ancora oggi, lo copiano e incollano, con la speranza di tutelare in questo modo la propria riservatezza.

A prescindere dal fatto che i concetti di social network e di privacy sono molto difficili da conciliare e al di là di tutte le tensioni irrisolte tipiche di una società che, da un lato, è affascinata dalla possibilità di condividere ogni esperienza in tempo reale e, dall'altro, è ossessionata dalla necessità di tutelare la privacy e l'utilizzo dei dati personali, giova qui sottolineare come l'esempio della catena sulla privacy presenti molte e gravissime ricadute sulla sicurezza dei cittadini che, dopo aver pubblicato quel determinato post, credono di essere veramente al riparo da qualsivoglia utilizzo non autorizzato delle proprie immagini o idee, dimenticando che dal punto di vista meramente fattuale ogni utente perde definitivamente il controllo su ciò che decide di condividere all'interno di un social network.

4. Crimini informatici e risposte legislative

La legislazione e la teoria generale del reato affrontano, ormai da tempo, nuove fattispecie e nuove tematiche riguardanti i

crimini commessi attraverso Internet e, più in generale, attraverso la Rete informatica.

4.1. Condotte e reati devono essere distinti a seconda che: *i*) *siano concepibili solo ai danni di un computer o di una Rete telematica*, oppure che *ii*) *siano pensabili per il mondo reale, ancorché vengano realizzati attraverso la Rete*.

E proprio a partire da questa prima grande divisione, ecco i reati informatici che il legislatore nazionale ha previsto: *a*) l'accesso abusivo ad un sistema informatico o telematico [1]; *b*) la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici [2]; *c*) la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico [3]; *d*) l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche [4]; *e*) l'installazione di apparecchiature atte ad intercettare, *f*) impedire o interrompere comunicazioni informatiche o telematiche [5]; *g*) la falsificazione, l'alterazione o la sop-

---

[1] L'art. 615 *ter* c.p. così recita: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. […]".

[2] L'art. 615 *quater* c.p. così recita: "Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. […]".

[3] L'art. 615 *quinquies* c.p. recita: "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

[4] L'art. 617 *quater* c.p. recita: "Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. […]".

[5] Art. 617 *quinquies* c.p. recita: "Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere

pressione di comunicazioni informatiche o telematiche [6]; *h*) il danneggiamento di informazioni, dati e programmi informatici [7]; *i*) la frode informatica e il furto dell'identità digitale [8]; *l*) la pirateria informatica [9]; *m*) l'ingiuria e la diffamazione attraverso Internet [10]; *n*) la prostituzione online [11]; *o*) la pornografia minorile, la detenzione di materiale pedopornografico, la pornografia virtuale [12].

---

comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. […]".

[6] L'art. 617 *sexies* c.p. recita: "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. […]".

[7] L'art. 635 *bis* c.p. recita: "Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. […]".

[8] L'art. 640 *ter* c.p. recita: "Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. […]".

[9] Legge sul diritto d'autore, art. 1 ("[…] Sono altresì protetti i programmi per elaboratore come opere letterarie […], nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore"), art. 2 ("In particolare sono compresi nella protezione […] i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. […]. Le banche di dati di cui al secondo comma dell'articolo 1 […]").

[10] L'art. 595 c.p. recita: "Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032. […]".

[11] Secondo la decisione della Corte di Cassazione (n. 37188/2010) il reato di sfruttamento e favoreggiamento dell'altrui affare di prostituzione si ha anche online. E infatti, anche nell'ipotesi di prestazioni sessuali eseguite a distanza e dietro corrispettivo di denaro, chi trae profitto da questa azione e/o la organizza, viola i dettami dell'art. 3, primo comma, numero 8, della Legge Merlin.

[12] Art. 600 *ter* c.p. ("[…] Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al pri-

4.2. Dietro queste espressioni che individuano i più comuni reati informatici, in realtà, si ritrovano, qualche volta, nuove tecniche e antichi obiettivi, qualche altra volta, invece, nuove tecniche e altrettanti nuovi obiettivi. La lista è particolarmente ampia e, ovviamente, in continua crescita. Qui di seguito, solo qualche esempio di condotta che mette a repentaglio diritti e sicurezza di individui, gruppi e nazioni, e che può costituire un reato informatico.

Cyberlaundering: è il fenomeno del riciclaggio che si manifesta secondo molteplici forme; la più classica è quella che prevede il trasferimento di denaro proveniente da attività illecita in conti resi disponibili e, da qui, la bonifica stessa delle somme. Una volta ottenuta la disponibilità delle somme, infatti, si possono predisporre, ad esempio, pagamenti a fronte di transazioni che sembrano lecite (si pensi alle vendite fittizie di immobili o alla costituzione di una società di copertura che commerci in oggetti d'antiquariato).

Ma le tecniche di riciclaggio nell'era digitale sono quanto mai varie. Sempre più spesso, per ripulire il denaro e per eludere le norme finanziarie in vigore nei diversi Paesi, alcune organizzazioni si avvalgono di sistemi bancari paralleli (*sotterranei*), sistemi clandestini che, nel caso cinese, hanno preso il nome di *fei chien* (denaro volante). Nell'ipotesi di trasferimento del denaro sporco dall'Italia alla Cina, la procedura è la seguente: deposito del denaro in un'agenzia italiana (che solitamente esercita attività di cambio-valuta, o che si presenta come agente di viaggio, call center, ecc.), consegna contestuale al richiedente di una password che funge da certificato di deposito, riconsegna del certificato di deposito al destinatario del denaro che opera in Cina e, infine, molto semplicemente, prelievo del denaro, al netto della provvigione. Altrimenti detto, il sistema bancario clandestino si fonda su un metodo di compensazione che opera tra soggetti che hanno bisogno di esportare denaro e altri che, invece, hanno necessità di importarlo, e si caratterizza per il fatto che il denaro

---

mo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645. […]").

non è mai trasferito materialmente e i conti sono regolati tramite scritture e registri.

A questo, si aggiunga che il più grande mercato nero digitale del mondo e cioè *Silk Road 3.0* – una piattaforma di e-commerce non indicizzata dai motori di ricerca e accessibile esclusivamente attraverso *Tor* (software gratuito che consente la navigazione del Web in assoluto anonimato) – rende possibile non soltanto l'acquisto di droghe, di armi, di kit fai-da-te per la costruzione di bombe, ecc., ma anche il riciclaggio dei proventi delle attività illecite. Qui, infatti, le transazioni non avvengono in valuta comune, bensì in bitcoin, ossia con una valuta elettronica che consente di garantire l'anonimato nell'operazione di compravendita online. Non è a caso che Ross Ulbricht – fondatore di *Silk Road* – sia attualmente sotto processo, dovendo rispondere di ben sette capi d'imputazione tra cui figura la pirateria informatica e il riciclaggio di denaro, e, se la difesa non riuscirà a provare che egli ha abbandonato l'amministrazione del portale subito dopo averlo fondato, dovrà scontare una pena che va da un minimo di 20 anni all'ergastolo.

La cornice legislativa nazionale antiriciclaggio è oggi rappresentata dal d.lgs. n. 231 del 21 novembre 2007 e dalle relative disposizioni di attuazione emanate dal Ministro dell'economia e delle finanze e, relativamente ai profili di contrasto del finanziamento del terrorismo e dell'attività di Paesi che minacciano la pace e la sicurezza internazionale, dal d.lgs. n. 109 del 22 giugno 2007, così come modificati dal più recente d.lgs. n. 90 del 25 maggio 2017 – recante Attuazione della direttiva (UE) 2015/849 (c.d. quarta direttiva antiriciclaggio) e del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi.

Cybersquatting: il termine indica l'occupazione di uno o più spazi virtuali – e cioè di uno o più domini web – presenti nell'immaginario comune, ma non utilizzati da quelli che potrebbero esserne i legittimi proprietari. Più in particolare, l'attività consiste nel registrare domini web riconducibili a marchi noti o a personaggi pubblici allo scopo di ricavarne un vantaggio economico.

Le tecniche del *cybersquatter* sono le seguenti: può registrare il dominio web – naturalmente laddove non sia stato registrato – per poi cercare di rivenderlo a chi ha, o ritiene di avere, un dirit-

to all'uso della denominazione corrispondente al dominio; può aspettare che la registrazione di un dominio web arrivi alla sua naturale scadenza – di solito la durata è di un anno dalla data di acquisto e deve essere rinnovata dietro pagamento di un canone –, per poi acquisirlo e provare a rivenderlo al precedente possessore che, di solito, ha tutto l'interesse a mantenere lo stesso indirizzo, così da essere raggiunto dai propri utenti su Internet. Per questo motivo, si sono sviluppati dei programmi in grado di indagare in Rete ed esaminare i registri web, alla ricerca di domini in scadenza.

Negli Stati Uniti, dove i casi di furto di dominio sono tutt'altro che rari, il cybersquatting è regolato da una legge (*Anticybersquatting Consumer Protection Act*) approvata dal Congresso già nel 1999 e che prevede pene pesanti per chi registra domini web riconducibili a marchi registrati con la sola intenzione di rivendere quel dominio al proprietario del marchio stesso.

In Italia, i nomi a dominio sono soggetti sia alla disciplina sul diritto al nome (come tutelato dagli artt. 6, 7, 8 e 9 del codice civile), sia alla disciplina dei marchi e dei segni distintivi del codice civile (artt. 2569 ss.) e del codice della proprietà industriale. Con riferimento al codice civile, ciò vuol dire che Tizio può citare in giudizio Caio se quest'ultimo apre un sito col nome a dominio tizio.it, danneggiando in questo modo il vero Tizio. Con riferimento alla disciplina dei marchi e dei segni distintivi (codice civile e codice della proprietà industriale), ciò significa che il nome a dominio ha una sua propria valenza distintiva dell'impresa che opera nel mercato e svolge anche una funzione pubblicistica. Di qui, l'equiparazione agli altri segni distintivi:

"1. È vietato adottare come ditta, denominazione o ragione sociale, insegna e nome a dominio di un sito usato nell'attività economica o di altro segno distintivo un segno uguale o simile all'altrui marchio se, a causa dell'identità o dell'affinità tra l'attività di impresa dei titolari di quei segni ed i prodotti o servizi per i quali il marchio è adottato, possa determinarsi un rischio di confusione per il pubblico che può consistere anche in un rischio di associazione fra i due segni. 2. Il divieto di cui al comma 1 si estende all'adozione come ditta, denominazione o ragione sociale, insegna e nome a dominio di un sito usato nell'attività economica o di altro segno distintivo di un segno uguale o simile ad un marchio registrato per prodotti o servizi anche non affini, che goda nello Stato di rinomanza se l'uso del segno senza giusto motivo con-

sente di trarre indebitamente vantaggio dal carattere distintivo o dalla rinomanza del marchio o reca pregiudizio agli stessi" [13].

Defacing: si tratta di quel fenomeno che in ambito informatico usa cambiare (de-facciare, ovvero sfigurare) illecitamente la home page di un sito web (la sua faccia, quindi), o modificarne, sostituendole, una, più o tutte le pagine interne. Com'è chiaro, tale pratica, vero e proprio atto vandalico, è attuata da persone non autorizzate – all'insaputa di chi gestisce il sito – per le motivazioni più disparate (dalla dimostrazione di abilità a ragioni ideologiche, sino alle motivazioni economiche) e, di solito, sfrutta i bug presenti nel software di gestione del sito oppure nei sistemi operativi sottostanti. Di rado, essa utilizza le tecniche di ingegneria sociale, ma, in ogni caso, è una pratica illegale.

Come detto, le motivazioni possono essere le più varie, e quindi il defacing può rappresentare: una sorta di ammonimento, così da sottolineare al webmaster la vulnerabilità del sito; una simpatica burla alla quale si prestano soprattutto i giovani; un controllo occulto, svolto dalla polizia per sapere quanti utenti accedono al sito, per identificarli e, qualche volta, per scoraggiarli, ad esempio facendo cadere la connessione dopo alcuni tentativi; una indiretta propaganda, svolta da chi cambia in parte o tutto il sito avversario, alfine di danneggiarlo e squalificarlo; un ricatto, e cioè, la minaccia di compiere reiterati defacing a scopo di estorsione o altro; una truffa perpetrata da un cracker che, trasformando la pagina in cui esiste un link per l'immissione di una carta di credito, reindirizza verso una pagina personale con l'intento di carpire le informazioni o anche prelevare denaro.

In Italia, il defacing si traduce in tre tipi di reato previsti dal codice penale, e cioè nei già citati accesso abusivo ad un sistema informatico (art. 615 *ter*), danneggiamento (art. 635 *bis*) e diffamazione (art. 595).

Pharming: il fenomeno rinvia alla tecnica usata per ottenere l'accesso a informazioni personali e riservate, muovendo dalla circostanza che l'indirizzo di una pagina web nella forma alfanumerica, digitato dall'utente nel proprio browser, è tradotto automaticamente dai calcolatori in un indirizzo Ip numerico, che

[13] Così, l'art. 22 del Codice della proprietà industriale.

serve al protocollo Ip per reperire nella Rete il percorso per raggiungere il server web corrispondente a quel dominio.

A seconda di quale sia l'obiettivo (il Server DNS dell'Internet Service provider oppure il pc della vittima) le tecniche d'attacco sono diverse. Nella prima ipotesi, il cracker opera, con sofisticate tecniche di intrusione, delle variazioni modificando gli abbinamenti tra il dominio e il relativo indirizzo Ip. Accade così che gli utenti connessi a quel provider, pur digitando il corretto indirizzo URL, siano reindirizzati a loro insaputa ad un server appositamente predisposto per carpire le informazioni. Va da sé che questo server-trappola è reperibile all'indirizzo Ip inserito dal cracker e che il sito si presenta esteticamente del tutto simile a quello vero. Nella seconda ipotesi, invece, il cracker opera, con l'ausilio di programmi (si pensi al Trojan horse) o tramite altro accesso diretto, una variazione nel pc della vittima. Questo è possibile, ad esempio, nei sistemi Windows, modificando il file hosts presente nella directory C:\windows\system32\drivers\etc. Qui possono essere inseriti, o modificati, gli abbinamenti tra il dominio interessato e l'indirizzo Ip corrispondente. Accade così che la vittima che ha il file hosts modificato, pur digitando il corretto indirizzo URL, venga reindirizzata a sua insaputa verso un server appositamente predisposto per carpire le informazioni. Può, inoltre, accadere che, una volta modificati nel registro di sistema i server DNS predefiniti, l'utente inconsapevolmente non utilizzi più i DNS del proprio Internet Service provider, bensì quelli del cracker, i cui abbinamenti (dominio-indirizzo Ip) sono stati manipolati.

Il pharming – quale pratica di clonazione delle pagine web – si traduce nel reato di frode informatica, di cui all'art. 640 *ter* c.p., che prevede che un soggetto, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procuri a sé o ad altri un ingiusto profitto con altrui danno. E qui, diversamente dalla truffa comune (*ex* art. 640 c.p.), non è necessario porre in essere artifici o raggiri, essendo sufficiente l'alterazione del sistema informatico con proprio profitto e altrui danno.

Phishing: il termine, ormai noto, indica l'uso di comunicazioni elettroniche finalizzato a ottenere l'accesso a informazioni per-

sonali. Ad esempio, tramite e-mail, in apparenza proveniente dall'istituto di credito, si invita il destinatario a digitare i propri dati personali (numero di conto, codice di identificazione, ecc.), con la scusa di una verifica di sicurezza. In realtà, con quei codici, l'agente è in condizione di operare sul conto e, quindi, di effettuare operazioni e disposizioni patrimoniali di vario genere e a favore proprio o di altri.

Si tratta di un'attività illegale che sfrutta le tecniche in precedenza dette di ingegneria sociale: oltre all'invio casuale di messaggi di posta elettronica, questa truffa può essere realizzata anche mediante contatti telefonici o con l'invio di *sms* (short message system).

Di solito, l'e-mail invita il destinatario a cliccare un link, presente nel messaggio, per evitare un addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.

Talvolta, l'e-mail contiene l'invito a cogliere una nuova opportunità di lavoro, quale, ad esempio, quella di operatore finanziario. Così, fornendo le proprie coordinate bancarie, si riceve – a fronte di una certa percentuale – l'accredito di somme che dovranno poi essere ritrasferite all'estero tramite sistemi di money trasfert. Com'è intuitivo, si tratta dell'attività di riciclaggio (prima detta cyberlaundering) di denaro rubato con il phishing, attività questa di particolare interesse per il phisher, visto che, in tal modo, e cioè disperdendo il denaro già sottratto in molti conti correnti e ritrasferendolo in diversi Paesi, diventa quanto mai difficile risalire all'autore, o agli autori, del reato, come pure ricostruire compiutamente il meccanismo illecito. A ciò si aggiunga che anche i tempi per la descrizione dei movimenti bancari possono allungarsi di molto, spesso infatti serve una rogatoria e l'apertura di un procedimento in ogni Paese interessato.

Di tale fenomeno, si è occupato per la prima volta in Italia il Tribunale di Milano: la sentenza del 10 dicembre 2007 (confermata in Cassazione nel 2011) ha condannato i membri di una associazione transnazionale dedita alla commissione di reati di phishing; la sentenza del 29 ottobre 2008 ha condannato per riciclaggio quei soggetti che – quali financial manager – si erano prestati alla attività di incasso e ri-trasferimento di denaro, frutto del phishing a danno dei correntisti italiani.

Sniffing: come già detto all'inizio, si tratta dell'attività di intercettazione dei dati che transitano in una Rete, che può avere sì degli scopi legittimi (ad esempio, l'analisi di problemi di comunicazione e/o l'individuazione di tentativi di intrusione), ma che qui rileva per i possibili scopi illeciti, quale l'intercettazione fraudolenta di password o di altre informazioni sensibili.

Al di là delle diverse modalità (a secondo della Rete, ad esempio se Rete *ethernet non-switched* o *ethernet switched*) e delle varie funzionalità (intercettazione, memorizzazione, ordinamento e filtraggio dati, ecc.), lo sniffing pone diversi problemi, in generale, rispetto alla privacy, in particolare, rispetto alle forme di accesso e ascolto delle informazioni. Si consideri lo sniffing volto alla difesa del diritto d'autore. In questa ipotesi, infatti, l'accesso avviene all'insaputa dell'utente a un computer di sua proprietà o ad una Rete che è proprietà di chi diffonde il software d'accesso, ed invece per l'accesso e la perquisizione di un'abitazione o altra proprietà privata è richiesto un mandato della magistratura. Per di più, nelle indagini per violazioni del diritto d'autore, i dati forniti dall'Internet Service provider non identificano la persona, bensì l'utenza telefonica. E la mancata identificazione di chi commette materialmente il fatto esclude un nesso di causalità tra la connessione alla Rete peer-to-peer e la violazione del copyright; in ogni caso non è una prova sufficiente per gli effetti penali previsti dalla legge poiché in ambito penale serve un accertamento univoco e inequivocabile della persona e delle sue responsabilità.

Tra le prime decisioni in materia, è da segnalare l'ordinanza del Tribunale di Roma del 17 marzo 2008, nel caso *Peppermint e Techland*. Come noto, la casa discografica tedesca e il produttore di videogiochi polacchi si erano rivolti a una società svizzera specializzata in intercettazioni nelle reti peer-to-peer. Rilevati gli indirizzi Ip di quegli utenti che hanno scambiato file musicali e giochi tramite le reti P2P, le società ottengono dai provider italiani i nominativi corrispondenti, al fine di ottenere un risarcimento del danno per la violazione del diritto d'autore. Il Tribunale di Roma rigetta le richieste di procedere, affermando che le società non hanno alcun diritto di accedere ai dati personali degli intercettati e che, quindi, i nominativi raccolti sono privi di valore probatorio, e non possono essere utilizzati in tribunale.

Anche il Garante per la privacy è intervenuto sul medesimo caso, con un provvedimento del 13 marzo 2008, affermando l'illiceità del trattamento dei dati personali, poiché

"la direttiva europea sulle comunicazioni elettroniche vieta ai privati di poter effettuare monitoraggi, ossia trattamenti di dati massivi, capillari e prolungati nei riguardi di un numero elevato di soggetti. È stato, poi, violato il principio di finalità: le reti P2P sono finalizzate allo scambio tra utenti di dati e file per scopi personali. L'utilizzo dei dati dell'utente può avvenire, dunque, soltanto per queste finalità e non per scopi ulteriori quali quelli perseguiti dalle società Peppermint e Techland (cioè il monitoraggio e la ricerca di dati per la richiesta di un risarcimento del danno). Infine non sono stati rispettati i principi di trasparenza e correttezza, perché i dati sono stati raccolti ad insaputa sia degli interessati sia di abbonati che non erano necessariamente coinvolti nello scambio di file".

Spoofing: un fenomeno questo che è solito sfruttare le comunicazioni elettroniche sotto la forma di richieste d'aiuto. I destinatari della richiesta sono generalmente amici e conoscenti della vittima del furto di identità, i cui indirizzi sono ripresi dalla sua mailing list.

Come già detto, il furto di identità digitale [14] è stato introdot-

[14] Che in mancanza di una fattispecie incriminatrice specifica è stato ricondotto dalla Cassazione nell'ambito del reato di cui all'art. 494 c.p.: "chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o un falso stato ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno". Secondo la Suprema Corte, la condotta di chi crea e utilizzi account o caselle di posta elettronica, servendosi dei dati anagrafici di un terzo soggetto, inconsapevole, è in grado di indurre in errore un'intera platea di utenti, i quali, convinti di interloquire con un soggetto, si troveranno ad interagire, invece, con una persona diversa da quella che a loro viene fatta credere, integrando così la fattispecie di reato prevista dalla norma. La tutela offerta dall'art. 494 c.p., infatti, interviene in presenza di inganni relativi "alla vera essenza di una persona o alla sua identità o ai suoi attributi reali", pertanto, laddove questi siano collocati in Rete, tale tutela può ben oltrepassare la ristretta cerchia di un destinatario specifico, estendendosi agli utenti dei rapporti telematici (Cass. Pen. n. 46674/2007). Tale orientamento, e cioè l'applicabilità dell'art. 494 c.p., è stato riconfermato più di recente sia nell'ipotesi di sostituzione di persona mediante *chat line* (Cass. Pen. n. 18826/2013) sia in quella in cui è creato un preciso profilo su un *social network* al quale è associata una immagine reale della persona offesa (Cass. Pen. n. 25774/2014).

to con la l. n. 119 del 2014, che ha modificato l'art. 640 *ter* c.p., con l'inserimento di un terzo comma che prevede la pena della reclusione da due e sei anni e la multa da 600,00 euro a 3.000,00 euro nel caso in cui il fatto sia commesso mediante furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Esistono diversi tipi di spoofing, quel che tuttavia li accomuna è il fatto di far credere alla vittima qualcosa di diverso: l'informazione falsa può riguardare un indirizzo Mac, un indirizzo Ip, e molto altro ancora, comprese le tecniche di spoofing destinate a colpire i protocolli di livello applicativo, o le applicazioni stesse, e il c.d. web spoofing.

Com'è intuitivo, quest'ultima definizione riguarda il Web e si tratta di far credere ad un utente di essere connesso a un determinato server, piuttosto che al server malevolo a cui è effettivamente connesso. La tecnica usata è di solito la seguente: costruzione di un server falso (detto anche server ombra), che può contenere una copia del server vero (le pagine sono copiate in locale sul server ombra), oppure può rigirare pagina per pagina le connessioni del client verso il server vero, così da falsificare l'associazione tra l'indirizzo web e l'indirizzo Ip.

Nell'ipotesi di *Transport Layer Security* – protocollo di crittografia utilizzato in ambito Web per proteggere le comunicazioni e lo scambio informativo tra due nodi della Rete (solitamente tra client e server), la cui protezione è affidata alla presenza di una o più autorità di certificazione (*Certificate Authority*) e di una infrastruttura a chiave pubblica per verificare la relazione tra il certificato e il suo possessore, così come per generare, firmare e amministrare la validità dei certificati –, il c.d. pirata genera un certificato server falso, totalmente uguale al certificato vero, seppur non firmato dall'autorità di certificazione. A questo punto, l'utente potrebbe cliccare per accettare e l'attaccante potrebbe, quindi, connettersi verso il server vero agendo da intermediario e intercettando le comunicazioni.

E ancora: *DNS cache poisoning*, attacco informatico che consente di reindirizzare un nome di dominio web verso un indirizzo Ip diverso da quello originale; *Eavesdropping*, attività di ascolto (e-mail, instant messaging, ecc.) senza esserne autorizzati; *Man in the middle attack*, condotta nella quale l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due

parti comunicanti tra di loro; *Spamming*, fenomeno molto noto e decisamente diffuso che consiste nell'invio indiscriminato di messaggi non richiesti; *SQL injection*, uso di *query* anomale che – se non opportunamente filtrate – consentono, ad esempio, al malintenzionato di ottenere i privilegi di amministratore, oppure di accedere al sito senza possedere le credenziali necessarie per il login; *Tampering*, attività di alterazione e manomissione di informazioni, di programmi e di sistemi.

4.3. Uno degli obiettivi ormai prevalente dell'economia sommersa è diventato il furto di capitale intellettuale aziendale, il cui valore è decisamente significativo visto che si tratta di copyright, di formule proprietarie, di codici sorgente, di piani di marketing, dei risultati della ricerca e dello sviluppo, di segreti commerciali. Il fenomeno del cyber-spionaggio industriale è reso possibile grazie alla presenza di esperti informatici interni all'organizzazione aziendale che – nell'eludere le diverse misure di controllo e di sicurezza – acquisiscono le informazioni riservate, per poi rivenderle al miglior offerente. Si pensi, ad esempio, all'operazione Aurora, un attacco progettato nel 2009 per rubare capitale intellettuale ai danni di numerose società, comprese Google, Adobe, Yahoo!, Symantec, Morgan Stanley, ecc. Secondo quanto rilevato da Google, l'attacco avrebbe avuto origine in Cina, sfruttando le falle nella sicurezza degli allegati di posta elettronica, così da introdursi nelle reti interne di grandi aziende e gruppi statunitensi. Sembra comunque che l'attacco avesse di mira molti altri obiettivi, non solo spionaggio aziendale, ma anche e soprattutto spionaggio politico, da parte di individui o gruppi [15].

4.4. Intanto che i nuovi mezzi e le attuali tecniche rendono estremamente facile numerose condotte, dall'innocua interazione con altre persone fino all'aggressivo furto di identità digitale, sempre più si pone l'accento sui difficili equilibri tra libertà di espressione degli utenti e tutela dei diritti fondamentali di terzi lesi dai contenuti diffusi in Rete. Si pone, altresì, l'accento sulla

[15] Oltre all'operazione Aurora, fra i più recenti attacchi, si ricordino quello del 22 giugno 2015 all'aeroporto Chopin di Varsavia, che ha causato un *blackout* del sistema informatico che definisce i piani di volo della compagnia aerea Lot, e quello del 9 luglio negli Stati Uniti, che ha coinvolto tutti i voli della United Airlines.

possibile responsabilità penale dell'host provider in ordine ai reati realizzati dagli utenti della Rete avvalendosi degli strumenti offerti dal provider stesso.

Si pensi alla nota vicenda *Google vs ViviDown*, e cioè al processo nato dalla pubblicazione di un filmato sul Web, che ritraeva un ragazzo disabile insultato e picchiato da alcuni compagni all'interno di un edificio scolastico, e in cui riecheggiavano anche frasi ingiuriose nei confronti dell'associazione *ViviDown*. Il processo vede coinvolti tre dirigenti di Google e i capi di imputazione sono: *a*) aver trattato illecitamente dati personali attinenti alla salute del ragazzo ripreso; *b*) non aver impedito il delitto di diffamazione nei confronti del minore e dell'associazione.

In breve: nel giudizio di primo grado, il Tribunale di Milano assolve gli imputati dal delitto di diffamazione, escludendo che vi sia in capo all'host provider un obbligo di impedire reati commessi dagli utenti, e invece li condanna per illecito trattamento di dati personali [16]. La Corte d'Appello, poi, conferma l'assenza di una posizione di garanzia in capo all'host provider e annulla anche la condanna in relazione all'illecito trattamento dei dati personali [17]. La Cassazione [18], infine, conferma innanzitutto l'assenza di una posizione di garanzia in capo agli Internet service provider, giacché nessuna disposizione prevede che vi sia in capo al provider (anche un hosting provider) un obbligo generale di sorveglianza dei dati immessi da terzi sul sito da lui gestito; allo stesso modo, nessuna norma incriminatrice punisce un ipotetico obbligo del provider di ricordare agli utenti di rispettare la legge. In particolare, nel caso di specie le limitazioni di responsabilità sono applicabili poiché il provider si è limitato a fornire ospitalità

[16] *Google* avrebbe dovuto avvisare gli *uploader* degli "obblighi agli stessi imposti dalla legge, del necessario rispetto degli stessi, dei rischi che si corrono non ottemperandoli", obbligo derivante dall'art. 13 del d.lgs. n. 196 del 2003, oltre che dal "buon senso" (Tribunale di Milano, 12 aprile 2010, n. 1972).

[17] Secondo il Giudice l'art. 167, letto in combinato disposto con l'art. 13, non prevede un obbligo di informare gli uploader sui doveri loro incombenti, derivanti dal Codice della privacy. Inoltre, i manager di Google non tratterebbero in alcun modo i dati contenuti nei video caricati dagli utenti: il soggetto responsabile del trattamento dei dati contenuti nelle riprese diffuse tramite Google resta quindi l'uploader (Corte d'Appello di Milano, 21 dicembre 2012, n. 8611).

[18] Cassazione penale, Sez. III, 17 dicembre 2013, n. 5107.

ai video inseriti dagli utenti, senza fornire alcun altro contributo rispetto alla determinazione del contenuto dei video stessi.

La decisione della Suprema Corte può essere così ricostruita: non è possibile attribuire all'host provider un obbligo di impedire i reati commessi dagli utenti; le attività compiute dall'host provider sui materiali caricati dagli utenti, che non importino un intervento sul contenuto degli stessi o la loro conoscenza, non fanno venir meno le limitazioni di responsabilità previste dagli artt. 16 e 17, d.lgs. n. 70 del 2003; solo dal momento della conoscenza dell'illiceità dei contenuti pubblicati dagli utenti può ipotizzarsi una responsabilità del provider per illecito trattamento dei dati realizzata dagli uploaders. Si badi però, la conoscenza dell'illiceità dei contenuti pubblicati dagli utenti assume rilevanza penalistica soltanto a seguito di una comunicazione dell'autorità, e non di qualsiasi cittadino. E infatti, l'host provider non è responsabile per le informazioni memorizzate, a patto che

"non sia effettivamente a conoscenza del fatto che il dato o l'informazione è illecita [...]; che non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni".

È scongiurato, in questo modo, il rischio di un'attribuzione al provider del ruolo di censore, magari comprensibile nel caso del video che umilia il minore disabile, meno comprensibile in altri casi, sia pure segnalati come diffamatori dai diversi utenti.

5. *Segue*: reati contro la persona

Mutano tecniche e opportunità, e nei mutamenti in atto – mutamenti in cui la libertà *della* Rete e la libertà *dalla* Rete sembrano rincorrersi, contraddirsi, sovrapporsi – altre condotte illecite si diffondono, mettendo a repentaglio i diritti e la sicurezza della persona. Qui di seguito, solo due esempi.

Cyber-bullying: si tratta di atti di molestia, di solito, tra minorenni e che si sviluppano online, come può essere l'invio di messaggi, di foto o di video, dai contenuti falsi, offensivi e/o minacciosi.

Allo stesso modo del bullismo, il cyber-bullismo può costituire una violazione del Codice civile, del Codice penale e del Codice della Privacy. Motivazione e finalità sono per lo più eguali: il bullo prende di mira chi ritiene essere diverso (per l'aspetto estetico, per l'orientamento sessuale, per la condotta, ecc.) e lo fa generalmente al fine di isolarlo ed escluderlo dal gruppo.

Diversamente dal primo, però, il cyber-bullismo si caratterizza per l'anonimato del molestatore e per la difficoltà che la vittima incontra nel rintracciarlo e nel porvi rimedio, anche in considerazione dell'ampio numero di persone che possono essere coinvolte già con il semplice inoltro. A ciò si aggiunga, una strutturale debolezza etica: la possibilità, quando si è in Rete, di essere un'altra persona, fa sì che si dicano o si facciano cose che non si direbbero o non si farebbero normalmente nella vita reale, inoltre, l'assenza di limiti spazio-temporali fa sì che le molestie investano la vittima ogni volta che si collega al mezzo elettronico usato dal cyber-bullo, il quale può inviare messaggi online violenti, volgari, ripetuti, al fine di suscitare battaglie verbali in un forum (flaming), oppure al fine di denigrare qualcuno ed emarginarlo dal gruppo online, o, ancora, allo scopo di incutere paura. Qualche altra volta accade che il cyber-bullo si faccia passare per un'altra persona, al solo fine di spedire messaggi e pubblicare testi decisamente scorretti e discutibili, qualche altra ottiene la fiducia di qualcuno con l'inganno per poi pubblicare e condividere con altri le informazioni confidate via mezzi digitali.

Al di là delle diverse modalità e dei possibili fini, il fenomeno del cyber-bullismo, secondo alcuni dati, coinvolge sempre più pre-adolescenti e adolescenti. In particolare, poi, in base ai risultati dell'indagine "Osservatorio adolescenti" – presentata da Telefono Azzurro e DoxaKids nel mese di novembre 2014, condotta su oltre 1500 studenti di scuole italiane di età compresa tra gli 11 e i 19 anni – il cyber-bullismo è un fenomeno ben noto ai ragazzi, visto che l'80,3% degli intervistati ne ha sentito parlare, 2 su 3 (39,2%) conoscono qualcuno che ne è stato vittima, 1 su 10 ne è stato vittima (10,8% degli intervistati; il 9,1% dei ragazzi ed il 12,6% delle ragazze). Dalla stessa indagine, è emerso anche che i ragazzi che sono stati vittime di molestie online manifestano più frequentemente di altri disagio e incapacità relazionali.

Cyber-stalking: è l'uso dei nuovi mezzi tecnologici, con l'intento di assediare, diffamare, inseguire, pedinare, minacciare, opprimere, molestare una persona o un gruppo di persone.

Allo stesso modo dello stalking, si tratta di una serie continua di azioni volte a invadere la sfera personale, sociale e professionale, della vittima designata. È il ripetersi costante, senza pausa e ossessivo, di forme d'aggressione – che possono essere anche le più varie – a caratterizzare tanto lo stalking quanto il cyber-stalking e a far sentire la vittima in condizioni di permanente assedio. Di qui, la valutazione degli atti di aggressione, non solo singolarmente considerati, ma anche e soprattutto nel loro insieme.

Come nello stalking, pure nel caso di cyber-stalking, il molestatore prova innanzitutto a diffamare la sua vittima. Così, ad esempio, pubblica informazioni false sul suo sito web, crea pagine web, blog, allo scopo di danneggiarne la reputazione, effettua affermazioni denigratorie su newsgroup, chat, forum, social network, etc., fa affermazioni false e denigratorie su pagine pubbliche (Wikipedia e altre simili). E intanto che diffama, penetra negli ambienti cyber frequentati dalla vittima, raccogliendo via via sempre più informazioni e assai spesso istigando terzi nell'attività di stalking.

Se entrambi, stalker o cyber-stalker, sono portati a sostenere – al di là di ogni evidenza – che è la vittima ad averli molestati, entrambi tentano in tutti i modi di ottenere un incontro e/o di stabilire un rapporto di complicità con essa, il cyber-stalker ha dalla sua tutti i nuovi strumenti e programmi: può inviare virus che danneggiano il computer, può interrompere la connessione mettendo a rischio il lavoro svolto, può eliminare o sospendere il profilo della sua vittima, può clonare le pagine creando un danno materiale e morale, può intercettare le comunicazioni. E ancora, il cyber-stalker può usare i dati della vittima per fare acquisti online a suo nome, può usare i dati della vittima per attivare servizi di spamming a suo carico.

Qualche volta, i cyber-stalker, alla ricerca ossessiva di dati, curiosità, notizie, soddisfano le loro esigenze anche semplicemente vedendo propagare nei canali di ricerca, nei forum online, nelle chat, ecc., le informazioni quasi sempre diffamanti riguardanti la vittima o le vittime. Di solito, però, nel pedinare la vittima o le vittime – seguendo, in altre parole, i siti Internet frequentati da

queste persone, i loro post lasciati in bacheca, ogni loro azione compiuta nel cyberspace – i cyber-stalker tentano di stabilire un rapporto, provano cioè a trasformare la relazione virtuale in relazione reale e, comunque, richiedono una risposta alle loro tante e continue provocazioni. Visti alcuni contenuti dei messaggi, considerate le modalità dell'azione e la stessa condizione nella quale versa la vittima, si può dire che il cyber-stalker sviluppa una condotta non diversa da quella che muove qualsiasi forma di relazione non consensuale, ivi compreso lo stupro. Intanto perché, come si è detto, non in pochi casi di cyber-stalking si compie una trasformazione dal virtuale al reale, il che, ad esempio, significa che il molestatore grazie alle informazioni può essere presente negli stessi luoghi in cui è presente la vittima, in momenti pubblici o privati e con le conseguenze facilmente intuibili. E poi perché, già da diverso tempo e in molti ordinamenti giuridici, il fenomeno stalking, sotto qualunque forma, è perseguito e punito in quanto forma di violenza, solitamente maschile sulle donne.

A tal proposito, va ricordato che l'art. 612 *bis* c.p., nell'ipotesi di minacce e molestie, reiterate e idonee a cagionare un perdurante e grave stato d'ansia e di paura, così da indurre a modificare le proprie abitudini di vita, prevede che la pena sia aumentata nel caso in cui il fatto sia commesso dal coniuge (ancorché separato o divorziato) o da persona che è, o è stata, legata da relazione affettiva alla persona offesa, ovvero se il fatto è commesso attraverso strumenti informatici o telematici.

Le ragioni dell'aumento di pena vanno certamente rintracciate nel fatto che, non solo il Web è a suo modo vita reale – ragione per cui nessuno può fare ciò che non può essere fatto nella vita reale – ma è anzi un (non-)luogo le cui dimensioni determinano in modo significativo un riprodursi e moltiplicarsi di atteggiamenti e comportamenti, di modo che la violenza, l'insulto, il dileggio, e/o la loro istigazione, diventano via via sempre più pervasivi e anche per questo ancora più violenti. A ciò si aggiunga che, se nella vita reale nell'ipotesi di atti persecutori si può ottenere una diffida, un ordine di allontanamento dai luoghi frequentati, nei (non-)luoghi virtuali – soprattutto per le loro due fondamentali caratteristiche: de-territorializzazione e de-centralizzazione – il tutto diventa più difficile e, non di rado, persino vano.

6. *Segue*: reati contro gruppi, organizzazioni e Stati

Nell'ambito quanto mai ampio e articolato del crimine informatico è opportuno ricordare quegli altri fenomeni che, sfruttando pur sempre la tecnologia informatica, si presentano più propriamente come:

Cyber-terrorism: si tratta dell'uso della Rete da parte delle organizzazioni terroristiche, per lo più a fini di propaganda e reclutamento. Assai spesso, infatti, attraverso la Rete, i gruppi terroristi intendono denigrare e delegittimare la politica di alcuni Stati, come pure diffondere la paura nelle diverse società. E intanto che ciò accade promettono ai futuri affiliati ricompense *eterne*.

Forse più interessati agli effetti sociali e politici delle loro intrusioni e minacce, piuttosto che a colpire infrastrutture rilevanti, quel che è certo è però che il cyber-terrorismo si sta sempre più diffondendo, come provano alcuni recenti episodi. Falsi affiliati al califfato di Abu Bakr al Baghdadi sono entrati nel profilo Twitter del quotidiano americano *Albuquerque Journal*, postando un messaggio minaccioso: "siamo già qui, nei vostri pc e nelle vostre case". Anche la homepage della *Malaysia Airways* è stata presa di mira, qui è apparsa la scritta: "errore 404 – aereo non trovato. Isis vincerà", per non parlare dell'attacco contro gli account Twitter e Facebook del Comando Centrale delle truppe Usa a Tampa, qui sono comparse frasi del tipo: "lo Stato Islamico vi insegue", "guardatevi le spalle".

Al di là delle intenzioni, in questi casi come in altri – si pensi all'intrusione del sedicente *Cyber Caliphate* nel profilo Twitter del Comando Centrale del Dipartimento della Difesa Usa, e secondo quanto osservato da James Lewis, esperto di cyber-sicurezza del *Center for Strategic and International Studies*: l'episodio avrebbe avuto un target simbolico, con pochi danni, che avrebbe evidenziato non tanto le abilità degli attaccanti, quanto invece l'assenza di capacità negli attaccati –, quel che effettivamente rileva è che in Rete si possono fare agevolmente proseliti, si possono creare e diffondere paure di vario genere, e si possono mettere fuori uso i gangli di trasmissione critica delle strutture, o dei processi, che attengono la sicurezza nazionale;

Cyber-spying o *cyber-espionage*: si tratta di quell'insieme di attività che sfruttano le potenzialità della Rete – come del resto nell'ipotesi di cyber-spionaggio da parte di individui o di gruppi (ad esempio, sottrazione di segreti industriali, a fini di concorrenza sleale, consumata nel mercato dei brevetti civili) – a favore di un governo o di più governi, per garantire loro una superiorità economica e/o strategica (ad esempio, sottrazione di disegni e apparecchiature militari, sottrazione di prodotti o tecnologie *dual-use*: civile e militare) rispetto ad un altro soggetto o ad altri soggetti esteri, ad altri attori statali o, ancora, rispetto ad altre organizzazioni.

Com'è intuibile, l'attività dei governi in questo versante è particolarmente intensa e sviluppata, vista anche la gran quantità di informazioni che può essere raccolta (su potenziali avversari, su controversie di politica interna ed estera, sulle reti finanziarie, come pure sulle reti terroristiche, sulle varie operazioni lecite o illecite, e così via) e che anzi viene raccolta. Negli Stati Uniti, la quantità di dati prelevati dalla Rete è aumentata e attualmente è pari a 2 *petabyte* all'ora, quasi 2,1 milioni di *gigabyte* (l'equivalente di centinaia di milioni di pagine di testo);

Cyber-warfare: è l'insieme di attività di preparazione e conduzione delle operazioni militari alla luce di una parola chiave che è informazione. Il che significa: potenziamento dell'informazione sul proprio fronte, e, invece, alterazione e distruzione dell'informazione e dei sistemi di comunicazione sul fronte nemico. Questo tipo di guerra è, infatti, combattuta attraverso il sistematico smantellamento delle barriere di protezione critica dell'avversario e, in particolare, tramite le azioni di disturbo o persino tramite la stessa disattivazione delle reti di comunicazione strategica. Va da sé che queste azioni, proprio per le loro caratteristiche – difficile tracciabilità, se non attraverso adeguati scudi di protezione, notevole distanza del server da cui muove l'offensiva e sua imprecisa identità – integrano nel migliore dei modi le attività propriamente belliche.

Solo un esempio tra i tanti: *Flame* (e più esattamente *Worm. Win32.Flame*) è un programma particolarmente evoluto, le cui funzionalità sono superiori rispetto a tutte le precedenti minacce informatiche, in grado di sottrarre i più diversi dati, sia i contenuti visualizzati sul display del computer sia le informazioni sui

sistemi, sia i file archiviati sia i contatti e le conversazioni audio. È un malware, così complesso e sofisticato, che è stato possibile tenerlo nascosto per oltre due anni, giacché nessun software di sicurezza in tutto quel periodo lo ha rilevato. Pare che la scoperta sia avvenuta in modo del tutto inatteso, intanto che gli esperti di sicurezza lavoravano all'identificazione di un altro programma nocivo, denominato *Wiper*. Sembra comunque che *Flame* – quest'arma informatica in grado di compiere attacchi mirati in diversi Paesi e che ha la capacità di riprodursi su una Rete locale utilizzando diversi metodi (la stessa vulnerabilità della stampante e il metodo di infezione tramite la porta Usb) – sia stato diffuso nel 2012 da Stati Uniti e da Israele e sia stato usato contro l'Iran.

7. Chi è il *cyber-criminale*? Dalla condotta all'elemento psicologico

Le tante modalità con le quali si sviluppano di solito i crimini informatici, mostrano subito le particolari doti di cui è fornito il soggetto criminale.

Alcuni studi hanno rilevato che il cyber-criminale ha un'istruzione medio-alta, ha grandi capacità di premeditazione, organizzazione, preordinazione, è un esperto di sistemi, in grado di accedere a reti informatiche protette, più in particolare di accedere al sistema e di adattarlo alle proprie esigenze. Le sue conoscenze, decisamente approfondite, che talvolta si accompagnano ad una ridotta percezione del significato illegale della sua condotta, causata dall'apparente separazione mondo reale/mondo virtuale, lo rendono un formidabile utilizzatore di software, capace di nascondere le tracce del proprio passaggio, o della propria presenza, e capace di sfruttare al meglio ogni tipo di vulnerabilità.

Se, per un verso, la Rete ha fatto sì che sia superata in un certo senso la contrapposizione tra professionista del crimine e non, visto che alcune forme di abuso e di illecito sono commesse da soggetti che prima della rivoluzione informatica non sarebbero stati dediti al crimine e, comunque, sarebbero rientrati nella categoria dei c.d. insospettabili, avviando così una sorta di democratizzazione sia del crimine sia delle motivazioni per le quali viene commesso, per l'altro verso, però, il cyber-criminale è a

suo modo un malvivente di serie A e perciò differente da ogni altro che, non avendo dimestichezza con metodi e tecniche informatiche, si colloca in una posizione inferiore. Il cyber-criminale, in genere, opera in solitudine, e mentre diffonde ad esempio un malware (si pensi a Evgeniy Bogachev, mago delle botnet) vede accrescere la propria autostima nella pratica di un gioco che deve considerare oltre che eccitante, anche estremamente redditizio.

È per questo che la repressione della criminalità informatica ha richiesto, e richiede, una specializzazione della polizia giudiziaria, la quale deve ormai tenere conto di relazioni e abitudini umane profondamente mutate, di una scena del crimine che può essere anche informatica, di una attenuazione della percezione del crimine causata dalla sostituzione del faccia-a-faccia con l'interfaccia, di una entrata nella categoria dei criminali di soggetti che, prima della rivoluzione informatica, erano estranei al mondo dell'illegalità.

7.1. Le considerazioni sin qui svolte hanno una loro rilevanza anche alla luce dei c.d. elementi psicologici (soggettivi) del reato, che il nostro ordinamento individua nel dolo, nella colpa e nella preterintenzione. Come noto, infatti, nessuno può essere punito per la propria azione od omissione, prevista dalla legge come reato, se non l'ha commessa con coscienza e volontà, e nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con dolo, salvi i casi di delitto preterintenzionale o colposo espressamente previsti dalla legge (art. 42 c.p.). Il legislatore distingue così il delitto in doloso ("o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione"), preterintenzionale ("o oltre l'intenzione, quando dall'azione od omissione deriva un evento dannoso o pericoloso più grave di quello voluto dall'agente"), e colposo ("o contro l'intenzione quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline") (art. 43 c.p.).

Anche per i reati informatici è richiesta la sussistenza del dolo, e cioè che il soggetto si sia rappresentato il fatto costituente reato e che egli abbia voluto che lo stesso si realizzasse, oppure

l'esistenza della colpa, come accade nell'uso incauto delle nuove tecnologie.

L'accertamento del dolo, tuttavia, è reso più complesso nei casi di reati informatici, anche per le circostanze che si può agire senza vedere i risultati della propria azione, si può agire celandosi dietro l'anonimato, si può agire senza poter controllare la diffusività della propria condotta, con effetti qualche volta non voluti e non prevedibili.

L'agire a distanza, ad esempio, fa sì che la vittima diventi invisibile, incorporea, come lo è, del resto, tutto ciò che la circonda nel cyberspace, e fa anche sì che il soggetto agente – non vedendo immediatamente gli effetti della propria condotta – sia agevolato nella sua stessa azione proprio in quanto la vittima che intende colpire è invisibile e astratta. Allo stesso modo, l'agire nella realtà virtuale – celando la propria identità e creandone una apocrifa – fa sì che condotte penalmente rilevanti si sviluppino in modo più deciso e ardito. In entrambi i casi è legittimo chiedersi se tutto ciò debba essere valutato in sede di accertamento della colpevolezza e comunque in che misura lo si debba valutare.

Va altresì considerato che il soggetto di solito commette un reato dopo aver utilizzato il computer a fini ludici e che, anzi, il reato spesso riproduce le finalità e le dinamiche del gioco medesimo. Anche di qui, la circostanza che in questo ambito è diffusa la criminalità giovanile. Del resto, uno dei canali di diffusione delle conoscenze informatiche è stato quello dei videogiochi, e come accade qualche volta nel gioco si può sviluppare una dipendenza da equiparare a psicopatologie comportamentali, si pensi all'*Internet Addition Disorder* e all'*Internet Related Psicopatology*. Simili tratti, ovvero criminalità informatica giovanile e dipendenza da cyberspace, possono incidere, ora in senso restrittivo ora in senso estensivo, sulla portata delle disposizioni relative ai soggetti che il nostro ordinamento considera totalmente o parzialmente non imputabili, per via dell'immaturità psichica (del minore: artt. 97 e 98 c.p.), del vizio di mente (artt. 88 e 89 c.p.), per gli effetti negativi che l'uso delle sostanze stupefacenti e alcoliche producono nella mente umana (artt. 91 ss. c.p.). E non è un caso proprio quest'ultimo riferimento, visto che in modo analogo all'uso di sostanze stupefacenti e alcoliche si parla ormai da tempo di abuso e di disintossicazione da Internet, e persino di Lsd elettronica e di app video-droga.

Al di là delle ipotesi riferite, che l'accertamento del dolo non sia affatto agevole, è provato già dalla previsione dell'art. 615 *quinquies* c.p., riguardante la diffusione di apparecchiature, dispositivi e programmi diretti a danneggiare o interrompere un sistema informatico. Se è punibile quel produttore di software, che perfettamente consapevole dell'esistenza di difetti e dei rischi di alterazione di funzionamento del sistema, distribuisce nonostante tutto il programma, non altrettanto potrebbe dirsi per coloro che forniscono programmi del tipo virus, soltanto per la creazione di anti-virus. Né sembra penalmente responsabile chi – effettuando gli ordinari interventi di manutenzione software e contraendo inconsapevolmente un virus della specie ancora sconosciuta alla diagnostica – contagi con lo stesso virus il sistema di elaborazione dati di altri durante un altro intervento di manutenzione. E non è penalmente responsabile, poiché il diritto penale non ricostruisce l'imputabilità sulla base del solo rapporto di causalità e secondo i criteri della responsabilità oggettiva.

Non meno difficoltà incontra l'accertamento della colpa nei reati informatici. Si pensi, a tal proposito, a eventi, anche tragici, nei quali è coinvolta la stessa vita umana, provocati in generale da un inadeguato funzionamento del sistema, in particolare da un errore del sistema, verificatosi ora nella fase di programmazione e ora in quella di esecuzione. In ogni caso, si tratta di capire che tipo di sistema è e che grado di incognite di funzionamento ha, poiché se si dovesse trattare dei c.d. sistemi esperti, allora il cattivo funzionamento potrebbe essere determinato da cause insite nel motore inferenziale oppure nella base di conoscenza, la responsabilità, quindi, ricadrebbe su figure diverse e occorrerebbe, inoltre, rinviare a più persone per il lavoro di *equipe* che solitamente viene intrapreso. Quando, poi, il cattivo funzionamento del sistema riguarda la fase di esecuzione, anche qui si tratta di capire se sia l'operatore il vero responsabile, in quanto ha seguito procedure sbagliate o ha inserito dati errati, o non lo sia piuttosto colui che ha fornito le istruzioni e i dati a fondamento dell'attività stessa.

Spesso il mal funzionamento del sistema, laddove penalmente rilevante, rinvia a carenze di gestione (ad esempio, cattiva manutenzione, mancato controllo, inidonee misure di sicurezza), che comunque violano gli obblighi di perizia e di diligenza e che, quindi, integrano responsabilità per colpa dei preposti alla gestione stessa.

7.2. Il dolo e la colpa, come pure la preterintenzione, devono misurarsi con i nuovi mezzi e con la dimensione del virtuale che è un reale in potenza. I parametri tradizionali, infatti, non sono per certi versi sufficienti, soprattutto se si considera che programmi sempre più sofisticati consentono di simulare il reale in modo perfetto, si ha così una confusione-sovrapposizione di piani, con la convinzione, in capo al soggetto agente, che quanto compiuto nel cyberspace non sia reale e non colpisca affatto diritti e interessi altrui. E i programmi altamente sofisticati assai spesso operano, per le loro connessioni e per la loro diffusività in modo imprevedibile, così che gli effetti potrebbero non essere quelli intenzionalmente voluti, e, per l'appunto, andare oltre l'intenzione del soggetto agente.

Ulteriore circostanza è che per alcuni reati informatici sembra mancare la consapevolezza dell'antigiuridicità, intanto perché alcuni soggetti (l'hacker tradizionale o l'hacker rivoluzionario) non percepiscono come illegali i loro atti, e in secondo luogo perché le norme penali sono giunte in ritardo a disciplinare un settore sviluppatosi senza regole e sviluppatosi così forse proprio grazie alla loro assenza.

La motivazione della condotta illecita è presa in esame ai fini della quantificazione della pena, allo stesso modo è dai motivi a delinquere che si desume la capacità a delinquere, parametro questo che, insieme alla gravità del reato, è valutato dal giudice ai fini della graduazione della pena da irrogare nel caso concreto.

Un compito particolarmente delicato attende quindi il giudice, specie se si considera che le motivazioni di per sé possono aprire la strada a diverse valutazioni, qualche volta persino opposte. Ad esempio, l'agire per fini ludici dell'hacker tradizionale potrebbe essere letto a favore del reo, di qui una diminuzione di pena, o al contrario, considerato come quell'agire per futili motivi previsto dalla norma (art. 61, punto 1, c.p.), di qui un aumento di pena. L'aver agito, poi, per fini quali la libertà, l'eguaglianza, l'identità, e così via, dell'hacker rivoluzionario, potrebbe essere letto a favore del reo, poiché la sua condotta può integrare quei motivi di particolare valore morale o sociale (art. 62, punto 1, c.p.), di qui l'attenuante, o invece può essere letto esattamente all'opposto, di qui l'aggravante.

8. Bene giuridico e competenza giurisdizionale

La nozione di bene giuridico è il risultato di una lunga elaborazione dottrinale e abbraccia tutti quei beni (e/o quegli interessi) che, essendo ritenuti socialmente rilevanti, vengono considerati meritevoli di tutela. Come è chiaro, si tratta di una categoria decisamente ampia, nella quale rientrano la vita, l'integrità fisica, l'onore, ma anche, il patrimonio, la fede pubblica, la proprietà intellettuale, ecc. Beni la cui tutela, nel nostro ordinamento, può essere affidata al diritto penale – nel caso in cui ci si trovi di fronte ad un'offesa, o a un pericolo, particolarmente rilevante da richiedere la punizione del colpevole – oppure al diritto civile, laddove invece la lesione può essere considerata tale da richiedere le sole funzioni reintegratorie e riparatorie.

Fra gli aspetti che maggiormente caratterizzano la nozione di bene giuridico c'è sicuramente una certa dinamicità, dettata dalla necessità dell'ordinamento di adeguarsi, e di rispondere, alle nuove, e sempre mutevoli, esigenze sociali [19]. E con l'avvento della c.d. società dell'informazione, tanto a livello internazionale ed europeo, quanto a livello nazionale, ci si è ben presto resi conto che la criminalità informatica – e, in modo particolare, i beni [20]

---

[19] Secondo ULRICH SIEBER, l'evoluzione che si è registrata nella concezione di bene giuridico e che ha richiesto interventi e adeguamenti soprattutto di natura penale, può essere schematicamente sintetizzata in sei grandi fasi, contraddistinte rispettivamente: 1) da una maggiore attenzione alla *tutela della privacy*, con l'emanazione di leggi volte alla protezione dei dati personali in Svezia (già nel 1973), negli Stati Uniti (nel 1974), nel Regno Unito (nel 1984), in Italia (nel 1996), in Germania (nel 1997); 2) dalla necessità di reprimere la *criminalità economica* correlata all'uso del computer, con particolare riferimento all'accesso abusivo a sistemi informatici e telematici; 3) dall'adozione di provvedimenti legislativi volti a tutelare la *proprietà intellettuale* e il *diritto d'autore*; 4) dalla repressione della *diffusione*, attraverso mezzi informatici, di *contenuti illegali e dannosi* (pornografia, istigazione razziale, diffamazione); 5) dalla previsione di una serie di fattispecie volte a punire il *sequestro e la sottrazione di apparecchiature informatiche*, nonché l'*intercettazione* di flussi di dati; 6) dall'introduzione di *misure di sicurezza tecniche* volte a tutelare la sicurezza e l'integrità dei dati (cfr. *Legal aspects of computer-related crimes in the Information Society*. *COMCRIME Study*, Bruxelles 1998).

[20] Si pensi, a titolo d'esempio, e nel più ampio quadro dei diritti della personalità, al diritto all'oblio, oggetto della nota sentenza della Corte di giustizia del 13 maggio 2014 (per un commento, si veda G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, 2014).

che essa, talvolta, mette solo in pericolo e, talaltra, compromette – meritano un'attenzione del tutto particolare.

Così, dopo una prima fase caratterizzata dal dibattito sulla necessità, o meno, di prevedere nuove norme che fossero volte a contrastare i reati informatici [21], già a partire dagli anni '80, numerosi Stati europei [22], e non solo [23], si sono dotati di una specifica legislazione penale volta a regolare quei comportamenti socialmente dannosi o pericolosi, legati alla diffusione e all'uso delle nuove tecnologie, come pure a risolvere il tema della giurisdizione e della competenza visto che la Rete può essere un (non-) *locus commissi delicti*.

8.1. Sul piano comunitario, con la Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest 23 novembre 2001), ratificata con l. n. 48 del 18 marzo 2008 – che nel Preambolo ha affermato la necessità di perseguire, come questione prioritaria, una politica comune in campo penale finalizzata alla protezione della società contro la criminalità informatica – all'art. 22 (Competenza) è così stabilito:

"1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione, quando i reati siano commessi: a. nel proprio territorio; b. a

---

[21] Secondo una prima corrente di pensiero, infatti, i nuovi illeciti realizzabili attraverso l'impiego delle tecnologie dell'informazione dovevano essere ritenuti come una variante – una sorta di evoluzione in chiave tecnologica – dei reati tradizionali, ragion per cui avrebbero dovuto trovare applicazione le disposizioni esistenti. Di contro, secondo quella che risultò, poi, l'opinione prevalente – in ossequio al principio di tassatività, proprio del diritto penale, e del divieto di analogia *in malam partem* – le nuove fattispecie delittuose realizzate attraverso le tecnologie informatiche e telematiche non potevano essere sanzionate in nome delle disposizioni previgenti, ma necessitavano di un'attenzione del tutto particolare e richiedevano un intervento *ad hoc* (per ulteriori approfondimenti si veda P. GALDIERI, *Reati informatici: normativa vigente, problemi e prospettive*, in AA.VV., *La criminalità informatica*, a cura di P. GALDIERI, *Rivista elettronica di diritto, economia e management*, n. 3, 2013, 19-43, in part. p. 20).

[22] Si ricordino, ad esempio, la Danimarca (con la l. n. 229 del 1985), la Norvegia (con la l. n. 54 del 1987), l'Austria (con la l. n. 605 del 1987), l'Italia (con la l. n. 547 del 1993).

[23] Come gli Stati Uniti, con il *Counterfeit Access Device and Computer Fraud and Abuse* del 1984, poi sostituito dal *Computer Fraud and Abuse Act* del 1986.

bordo di una nave battente bandiera della Parte; c. a bordo di un aeromobile immatricolato presso quella Parte; d. da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato.
2. Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza definite ai paragrafi 1.b – 1.d del presente articolo o in una parte qualunque di essi.
3. Ogni Parte deve adottare le misure che dovessero essere necessarie per stabilire la propria competenza in ordine alle infrazioni di cui all'articolo 24, paragrafo 1 della presente Convenzione, nel caso in cui l'autore presunto dell'infrazione si trovi nel proprio territorio e non è estradabile verso un'altra Parte solo in virtù della sua nazionalità, dopo una richiesta di estradizione.
4. La presente Convenzione non esclude alcuna competenza penale esercitata da una Parte in base al proprio diritto interno.
5. Quando più di una Parte rivendica la propria competenza per una presunta infrazione prevista dalla presente Convenzione, le Parti coinvolte si consultano, laddove sia opportuno, al fine di stabilire la competenza più appropriata per esercitare l'azione penale".

8.2. Nella Risoluzione legislativa del Parlamento europeo del 4 luglio 2013 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, che abroga la decisione quadro 2005/222/GAI del Consiglio, l'art. 12 (Competenza giurisdizionale) così recita:

"1. Gli Stati membri stabiliscono la propria competenza giurisdizionale relativamente ai reati di cui agli articoli da 3 a 8 quando il reato sia stato commesso: a) in tutto o in parte sul loro territorio; o b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso.
2. Nello stabilire la propria competenza giurisdizionale conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora: a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.
3. Uno Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora: a) l'autore del

reato risieda abitualmente nel suo territorio; o b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio".

8.3. Nella Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI del Consiglio, l'art. 17 (Giurisdizione e coordinamento dell'azione penale) stabilisce:

"1. Gli Stati membri adottano le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 7 nei seguenti casi: a) il reato è stato commesso in tutto o in parte sul loro territorio; oppure b) l'autore del reato è un loro cittadino.
2. Lo Stato membro informa la Commissione in merito alla decisione di stabilire la propria giurisdizione anche per i reati di cui agli articoli da 3 a 7 commessi al di fuori del suo territorio, tra l'altro nei casi seguenti: a) il reato è stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio; b) il reato è stato commesso a vantaggio di una persona giuridica che ha sede nel suo territorio; oppure c) l'autore del reato risiede abitualmente nel suo territorio.
3. Gli Stati membri provvedono affinché rientrino nella loro giurisdizione i casi in cui un reato contemplato dagli articoli 5 e 6 e, nella misura in cui sia pertinente, dagli articoli 3 e 7, sia stato commesso a mezzo di tecnologie dell'informazione e della comunicazione a cui l'autore ha avuto accesso dal loro territorio, a prescindere dal fatto che la tecnologia in questione sia basata o meno su tale territorio.
4. Per le azioni penali relative ai reati di cui all'articolo 3, paragrafi 4, 5 e 6, all'articolo 4, paragrafi 2, 3, 5, 6 e 7 e all'articolo 5, paragrafo 6, commessi al di fuori del territorio dello Stato membro interessato, per quanto riguarda il paragrafo 1, lettera b), del presente articolo, ciascuno Stato membro adotta le misure necessarie affinché la sua giurisdizione non sia subordinata alla condizione che i fatti costituiscano reato nel luogo in cui sono stati commessi.
5. Per le azioni penali relative ai reati di cui agli articoli da 3 a 7 commessi al di fuori del territorio dello Stato membro interessato, per quanto riguarda il paragrafo 1, lettera b), del presente articolo, ciascuno Stato membro adotta le misure necessarie affinché la sua giurisdizione non sia subordinata alla condizione che il reato sia perseguibile solo su querela della vittima nel luogo in cui è stato commesso o su segnalazione dello Stato in cui è stato commesso".

8.4. Dalle disposizioni qui riportate, la questione della competenza è stata quindi risolta dal legislatore comunitario innanzi-

tutto in base al criterio della territorialità e, in secondo luogo, in base al criterio del soggetto attivo ("da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato", così la Convenzione citata).

Con la Risoluzione legislativa del Parlamento europeo del 4 luglio 2013, ai criteri della territorialità e del soggetto attivo si aggiunge il criterio del c.d. destinatario del profitto ("il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio").

Con la Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 2011 – direttiva il cui ambito d'azione è anche quello di rafforzare le tutele nei confronti delle vittime di reati quali l'abuso e lo sfruttamento sessuale dei minori [24] – ai criteri della territorialità e del soggetto attivo si aggiunge il criterio del soggetto passivo [25].

Com'è evidente, i criteri devono in ogni caso essere utilizzati con il fine di evitare una molteplicità di procedimenti penali, cosa questa che trova riconoscimento sia nella Convenzione [26], sia nella Risoluzione, qui attraverso l'individuazione delle diverse ipotesi [27], e sia nella Direttiva [28].

---

[24] "Ciascuno Stato membro adotta le misure necessarie affinché la sua giurisdizione non sia subordinata alla condizione che i fatti costituiscano reato nel luogo in cui sono stati commessi […] [e] non sia subordinata alla condizione che il reato sia perseguibile solo su querela della vittima nel luogo in cui è stato commesso o su segnalazione dello Stato in cui è stato commesso".

[25] "Il reato è stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio".

[26] Così, l'art. 22, punto 5: "quando più di una Parte rivendica la propria competenza per una presunta infrazione prevista dalla presente Convenzione, le Parti coinvolte si consultano, laddove sia opportuno, al fine di stabilire la competenza più appropriata per esercitare l'azione penale".

[27] Art. 12: "quando il reato sia stato commesso: a) in tutto o in parte sul loro territorio; o b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso […] Qualora: a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato [...] Anche qualora: a) l'autore del reato risieda abitualmente nel suo territorio; o b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio".

[28] Art. 17: "a) il reato è stato commesso in tutto o in parte sul loro terri-

D'altra parte, però, il riconoscimento dei diversi criteri e l'affermarsi pur sempre della prevalenza del criterio della territorialità, devono comunque, con riguardo al nostro tema, tener conto della natura del cyberspace, e non è a caso che nella Risoluzione legislativa del Parlamento europeo del 4 luglio 2013 si rinvii al luogo della condotta [29] e nella Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 2011 si faccia riferimento al luogo di accesso alla Rete [30].

8.5. La natura non-territoriale e comunicativa della Rete, fa sì che qui i messaggi e le condotte raggiungono una tale diffusività da doverla considerare anche alla luce delle questioni relative alla competenza.

Così, la Suprema Corte ha avuto modo di affermare – a proposito di diffamazione attraverso Internet – che il reato si consuma al momento della ricezione del messaggio diffamatorio da parte di terzi rispetto all'agente e alla persona offesa, trattandosi di un reato di evento non fisico, ma psicologico, consistente nella percezione da parte del terzo dell'espressione offensiva (Cass. pen., sez. V, 17 novembre 2000, n. 4741). La Suprema Corte ha, inoltre, ritenuto che il reato di diffamazione – ovvero l'immissione nella Rete di frasi offensive e/o di immagini denigratorie – deve ritenersi commesso nel luogo in cui le offese e le denigrazioni sono percepite da più fruitori della Rete, anche nel caso in cui il

---

torio; oppure b) l'autore del reato è un loro cittadino". Nell'ipotesi dei reati di cui agli artt. 3-7 commessi al di fuori del territorio dello Stato, ha competenza se "a) il reato è stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio; b) il reato è stato commesso a vantaggio di una persona giuridica che ha sede nel suo territorio; oppure c) l'autore del reato risiede abitualmente nel suo territorio". Rientra inoltre nella giurisdizione degli Stati membri quanto "sia stato commesso a mezzo di tecnologie dell'informazione e della comunicazione a cui l'autore ha avuto accesso dal loro territorio, a prescindere dal fatto che la tecnologia in questione sia basata o meno su tale territorio".

[29] Art. 12, punto 2: "a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio".

[30] Art. 17, punto 3: "sia stato commesso a mezzo di tecnologie dell'informazione e della comunicazione a cui l'autore ha avuto accesso dal loro territorio, a prescindere dal fatto che la tecnologia in questione sia basata o meno su tale territorio".

sito web sia registrato all'estero. Di qui, la competenza del giudice italiano a conoscere il reato di diffamazione, laddove l'offesa sia stata percepita in maggioranza da fruitori residenti in Italia (Sez. 2, 21 febbraio 2008, n. 36721).

Vale la pena qui ricordare, sia pure in estrema sintesi, i diversi sviluppi della giurisprudenza penale e della giurisprudenza civile. In base alla prima, rispetto alle offese realizzate via Internet – considerato che è difficile l'individuazione di criteri oggettivi (ad esempio: prima pubblicazione, primo accesso) e che non è utilizzabile il luogo in cui è situato il server – si applica l'art. 9 c.p.p. che, al secondo comma, prevede la competenza del giudice della residenza o del domicilio dell'imputato (Cass., 15 marzo 2011, n. 16307). Secondo la giurisprudenza civile, invece, essendo rilevante l'accesso effettivo alla Rete nelle domande di risarcimento dei danni derivanti da pregiudizi dei diritti della personalità recati da mezzi di comunicazione di massa, il luogo nel quale si verifica il pregiudizio effettivo è quello in cui il danneggiato

"aveva il domicilio al momento della diffusione della notizia o del giudizio lesivi, perché la lesione della reputazione e degli altri beni della persona è correlata all'ambiente economico e sociale nel quale la persona vive e opera e costruisce la sua immagine, e quindi 'svolge la sua personalità' (art. 2 Cost.)" [31].

9. Strategie europee

Per il nostro tema, infine, una certa importanza rivestono le conclusioni adottate dal Consiglio europeo dei Capi di Stato e di governo riunitosi a Ypres il 26-27 giugno 2014, che delineano i nuovi orientamenti strategici per lo spazio europeo di libertà, sicurezza e giustizia. Tali orientamenti, subentrati al c.d. Programma di Stoccolma, e sottoposti a revisione intermedia il 1 dicembre 2017, sono destinati a guidare l'azione dell'Unione Europea in quest'ambito durante il quinquennio 2015-2020 [32]. Il Consi-

[31] Cass., Sez. Un., 29 settembre 2009, n. 21661.

[32] A tali interventi ha poi fatto seguito l'agenda strategica 2019-2024, adottata dal Consiglio europeo nel giugno 2019.

glio europeo ha, così, ottemperato al compito di fissare la programmazione legislativa e operativa, compito affidatogli dall'art. 68 Tr. FUE che puntualizza e rafforza, per il titolo V del Trattato, la funzione tipica del Consiglio europeo, consistente nel dare all'Unione gli impulsi necessari al suo sviluppo e definirne gli orientamenti e le politiche generali (art. 15 TUE). I destinatari di tale programmazione sono gli Stati membri e le altre istituzioni politiche dell'Unione, innanzitutto la Commissione, in quanto titolare del potere di iniziativa legislativa.

9.1. Come si può notare i nuovi orientamenti strategici per lo spazio europeo di libertà, sicurezza e giustizia, non sono definiti 'programma' e l'articolazione interna ha tredici punti non titolati, a fronte dei sette capitoli, con numerosi paragrafi e sottoparagrafi, del programma di Stoccolma. A questa diversità strutturale si accompagna una ben diversa capacità di orientamento in ambito penale.

Le nuove linee guida risultano principalmente dedicate al tema di una politica comune per la gestione delle migrazioni e al controllo delle frontiere europee. E in quest'ambito particolare risalto è dato alla dimensione esterna dello Spazio di libertà, sicurezza e giustizia, spazio in cui è attribuito un ruolo chiave alla collaborazione coi Paesi terzi, al fine di evitare ulteriori perdite di vite umane, e alla lotta contro il traffico e la tratta di esseri umani.

Oltre al fenomeno migratorio, nelle linee guida si presta particolare attenzione alla politica di contrasto al terrorismo e a tal fine è prospettato lo sviluppo di un sistema di codice di prenotazione (*passenger name record*) europeo, che consiste nella creazione di una banca-dati tra tutti gli Stati membri, dove dovrebbero essere raccolte, conservate e analizzate, quelle informazioni personali dei passeggeri che si trovano nella disponibilità delle compagnie aeree. A tal proposito, è degno di nota che tale misura – se adottata – si potrebbe tradurre in una incisiva compressione del diritto alla riservatezza e alla protezione dei dati personali per i cittadini europei, anche in considerazione del fatto che le linee guida non recepiscono quei criteri di necessità e proporzionalità che invece dovrebbero sorreggere il bilanciamento tra i suddetti diritti e le esigenze di sicurezza collettiva, in conformità a quanto statuito dalla sentenza della Corte di Giustizia (8 aprile

2014) che ha invalidato la direttiva 2006/24/Ce (c.d. direttiva Frattini) relativa alla raccolta e trattamento a fini di indagine dei dati personali legati al traffico telefonico e telematico.

9.2. L'obiettivo fondamentale dell'azione dell'Unione è quello di "garantire un autentico spazio di sicurezza ai cittadini europei attraverso la cooperazione operativa di polizia e la prevenzione e la lotta contro la criminalità organizzata e le forme gravi di criminalità, tra cui la tratta e il traffico di esseri umani e la corruzione". Di qui, l'implementazione di un maggiore ruolo di supporto dell'UE alle autorità nazionali per il tramite del coordinamento *Europol* e *Eurojust*, prevedendo tra l'altro il "miglioramento dello scambio transfrontaliero di informazioni, compreso quello sui casellari giudiziari". Di qui, ancora, la necessità di un approccio globale alle questioni riguardanti cyber-sicurezza e cyber-crimine, anche in considerazione della recente strategia dell'Unione Europea per la cyber-sicurezza elaborata dalla Commissione e della proposta di direttiva volta a stabilire regole comuni di sicurezza delle Reti d'informazione.

Educare alle nuove tecnologie

Mappe di sintesi

Un nuovo spazio. Il cyberspace

Concetti e passaggi-chiave

- Reale/Virtuale
- Assenza di confine: de-territorializzazione e de-centralizzazione
- Nastro di Moebius
- Panottico *vs*. Sinòttico
- Viglianza e data-veglianza
- Identità reale/identità virtuale
- Identità plurime e/o apocrife
- La rete come spazio per la socializzazione?

Un nuovo bene: l'*informazione*

Concetti e passaggi-chiave

- Dalla conoscenza… all'informazione (spazi di archiviazione, banche dati, motori di ricerca)
- L'informazione (e i dati). Il nuovo potere, il nuovo motore dell'economia, il nuovo petrolio
- Informazioni *per tutti* o informazioni *di tutti*?
- Opulenza delle informazioni come indigenza: *chiacchiere e fake news*

Tutorial

Giornali online

TG online

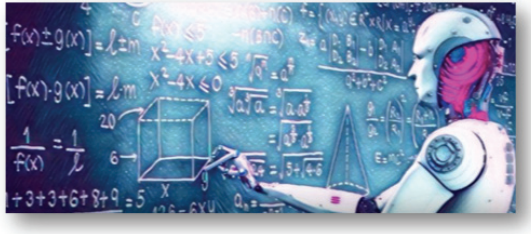
Qualche nuovo

s/oggetto

Tra algoritmi, intelligenza artificiale e big-data

Concetti e passaggi-chiave

- Dalle machine ai robot: supporto dell'uomo o sua sostituzione?
- Intelligenza e/o coscienza digitale (scelta, imputazione, responsabilità, autonomia…)
- Dai dati ai big-data. Vantaggi (conoscitivi e predittivi) e rischi (per la privacy e la sicurezza)
- Robotica e diritto: un dialogo necessario su questioni aperte (GDPR, Risoluzione del Parlamento Europeo sulla Robotica)



Alcune nuove tecniche di regolazione

Concetti e passaggi-chiave

- Tecnologia: cambiamento e… condizionamento
- *Nudge theory* e le c.d. spinte gentili
- Tecno-regolazione tra induzioni e dissuasioni (sistemi esperti, sistemi di raccomandazione, sistemi di controllo)
- *Social engineering*
- Neuro-diritto e neuro-tecno-regolazione
- Oltre il sollievo della dimenticanza?

Nuove condotte
penalmente rilevanti

Concetti e passaggi-chiave

- *Web/DarkWeb; Hacker/Cracker*
- Alternanza di vantaggi e rischi, opportunità e pericoli
- *Malware* (adware, backdoor, dialer, keylogger, trojan horse, virus, worm) e *Cyber crimes*
- Reati contro la persona, i gruppi, le organizzazioni, gli Stati (cyber-bullying, cyber-stalking, cyber-terrorism, cyber-spying)
- Dalla Convenzione di Butapest agli scenari attuali. Strategie e risposte dell'Unione Europea

Materiali normativi

Dichiarazione dei diritti in Internet [1]

Preambolo

Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet deve essere considerata come una risorsa globale e che risponde al criterio della universalità.

L'Unione europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall'articolo 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale.

Questa Dichiarazione dei diritti in Internet è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale.

Internet si configura come uno spazio sempre più importante per l'autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale.

I principi riguardanti Internet tengono conto anche del suo confi-

[1] Questo documento costituisce il nuovo testo della Dichiarazione elaborato dalla Commissione per i diritti e i doveri relativi ad Internet della Camera dei Deputati, a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015.

gurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico.
Una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale.

Art. 1
Riconoscimento e garanzia dei diritti

1. Sono garantiti in Internet i diritti fondamentali di ogni persona riconosciuti dalla Dichiarazione universale dei diritti umani delle Nazioni Unite, dalla Carta dei diritti fondamentali dell'Unione Europea, dalle costituzioni nazionali e dalle dichiarazioni internazionali in materia.
2. Tali diritti devono essere interpretati in modo da assicurarne l'effettività nella dimensione della Rete.
3. Il riconoscimento dei diritti in Internet deve essere fondato sul pieno rispetto della dignità, della libertà, dell'eguaglianza e della diversità di ogni persona, che costituiscono i principi in base ai quali si effettua il bilanciamento con altri diritti.

Art. 2
Diritto di accesso

1. L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Art. 3
Diritto alla conoscenza e all'educazione in rete

1. Le istituzioni pubbliche assicurano la creazione, l'uso e la diffusione della conoscenza in rete intesa come bene accessibile e fruibile da parte di ogni soggetto.

2. Debbono essere presi in considerazione i diritti derivanti dal riconoscimento degli interessi morali e materiali legati alla produzione di conoscenze.
3. Ogni persona ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali.
4. Le Istituzioni pubbliche promuovono, in particolare attraverso il sistema dell'istruzione e della formazione, l'educazione all'uso consapevole di Internet e intervengono per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di Internet da parte delle persone.
5. L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla Rete tra attori economici, Istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.

Art. 4
Neutralità della rete

1. Ogni persona ha il diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone.
2. Il diritto ad un accesso neutrale ad Internet nella sua interezza è condizione necessaria per l'effettività dei diritti fondamentali della persona.

Art. 5
Tutela dei dati personali

1. Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza.
2. Tali dati sono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili.
3. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano, di ottenerne la rettifica e la cancellazione per motivi legittimi.
4. I dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa.

5. I dati possono essere raccolti e trattati con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge. Il consenso è in via di principio revocabile. Per il trattamento di dati sensibili la legge può prevedere che il consenso della persona interessata debba essere accompagnato da specifiche autorizzazioni.
6. Il consenso non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento.
7. Sono vietati l'accesso e il trattamento dei dati con finalità anche indirettamente discriminatorie.

Art. 6
Diritto all'autodeterminazione informativa

1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano.
2. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata.

Art. 7
Diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici

1. I sistemi e i dispositivi informatici di ogni persona e la libertà e la segretezza delle sue informazioni e comunicazioni elettroniche sono inviolabili. Deroghe sono possibili nei soli casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria.

Art. 8
Trattamenti automatizzati

1. Nessun atto, provvedimento giudiziario o amministrativo, decisione comunque destinata ad incidere in maniera significativa nella sfera delle persone possono essere fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

Art. 9
Diritto all'identità

1. Ogni persona ha diritto alla rappresentazione integrale e aggiornata delle proprie identità in Rete.
2. La definizione dell'identità riguarda la libera costruzione della personalità e non può essere sottratta all'intervento e alla conoscenza dell'interessato.
3. L'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano.
4. Ogni persona ha diritto di fornire solo i dati strettamente necessari per l'adempimento di obblighi previsti dalla legge, per la fornitura di beni e servizi, per l'accesso alle piattaforme che operano in Internet.
5. L'attribuzione e la gestione dell'Identità digitale da parte delle Istituzioni Pubbliche devono essere accompagnate da adeguate garanzie, in particolare in termini di sicurezza.

Art. 10
Protezione dell'anonimato

1. Ogni persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure.
2. Limitazioni possono essere previste solo quando siano giustificate dall'esigenza di tutelare rilevanti interessi pubblici e risultino necessarie, proporzionate, fondate sulla legge e nel rispetto dei caratteri propri di una società democratica.
3. Nei casi di violazione della dignità e dei diritti fondamentali, nonché negli altri casi previsti dalla legge, l'autorità giudiziaria, con provvedimento motivato, può disporre l'identificazione dell'autore della comunicazione.

Art. 11
Diritto all'oblio

1. Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica.
2. Il diritto all'oblio non può limitare la libertà di ricerca e il diritto

dell'opinione pubblica a essere informata, che costituiscono condizioni necessarie per il funzionamento di una società democratica. Tale diritto può essere esercitato dalle persone note o alle quali sono affidate funzioni pubbliche solo se i dati che le riguardano non hanno alcun rilievo in relazione all'attività svolta o alle funzioni pubbliche esercitate.
3. Se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all'autorità giudiziaria per garantire l'interesse pubblico all'informazione.

Art. 12
Diritti e garanzie delle persone sulle piattaforme

1. I responsabili delle piattaforme digitali sono tenuti a comportarsi con lealtà e correttezza nei confronti di utenti, fornitori e concorrenti.
2. Ogni persona ha il diritto di ricevere informazioni chiare e semplificate sul funzionamento della piattaforma, a non veder modificate in modo arbitrario le condizioni contrattuali, a non subire comportamenti che possono determinare difficoltà o discriminazioni nell'accesso. Ogni persona deve in ogni caso essere informata del mutamento delle condizioni contrattuali. In questo caso ha diritto di interrompere il rapporto, di avere copia dei dati che la riguardano in forma interoperabile, di ottenere la cancellazione dalla piattaforma dei dati che la riguardano.
3. Le piattaforme che operano in Internet, qualora si presentino come servizi essenziali per la vita e l'attività delle persone, assicurano, anche nel rispetto del principio di concorrenza, condizioni per una adeguata interoperabilità, in presenza di parità di condizioni contrattuali, delle loro principali tecnologie, funzioni e dati verso altre piattaforme.

Art. 13
Sicurezza in rete

1. La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone.
2. Non sono ammesse limitazioni della libertà di manifestazione del pensiero. Deve essere garantita la tutela della dignità delle persone da abusi connessi a comportamenti quali l'incitamento all'odio, alla discriminazione e alla violenza.

Art. 14
Governo della rete

1. Ogni persona ha diritto di vedere riconosciuti i propri diritti in Rete sia a livello nazionale che internazionale.
2. Internet richiede regole conformi alla sua dimensione universale e sovranazionale, volte alla piena attuazione dei principi e diritti prima indicati, per garantire il suo carattere aperto e democratico, impedire ogni forma di discriminazione e evitare che la sua disciplina dipenda dal potere esercitato da soggetti dotati di maggiore forza economica.
3. Le regole riguardanti la Rete devono tenere conto dei diversi livelli territoriali (sovranazionale, nazionale, regionale), delle opportunità offerte da forme di autoregolamentazione conformi ai principi indicati, della necessità di salvaguardare la capacità di innovazione anche attraverso la concorrenza, della molteplicità di soggetti che operano in Rete, promuovendone il coinvolgimento in forme che garantiscano la partecipazione diffusa di tutti gli interessati. Le istituzioni pubbliche adottano strumenti adeguati per garantire questa forma di partecipazione.
4. In ogni caso, l'innovazione normativa in materia di Internet è sottoposta a valutazione di impatto sull'ecosistema digitale.
5. La gestione della Rete deve assicurare il rispetto del principio di trasparenza, la responsabilità delle decisioni, l'accessibilità alle informazioni pubbliche, la rappresentanza dei soggetti interessati.
6. L'accesso e il riutilizzo dei dati generati e detenuti dal settore pubblico debbono essere garantiti.
7. La costituzione di autorità nazionali e sovranazionali è indispensabile per garantire effettivamente il rispetto dei criteri indicati, anche attraverso una valutazione di conformità delle nuove norme ai principi di questa Dichiarazione.

Risoluzione del Parlamento europeo recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)) [2]

Il Parlamento europeo,
visto l'articolo 225 del trattato sul funzionamento dell'Unione europea,
vista la direttiva 85/374/CEE del Consiglio,
visto lo studio sugli aspetti etici dei sistemi cyberfisici svolto per conto del comitato di valutazione delle opzioni scientifiche e tecnologiche (STOA) del Parlamento e gestito dall'unità Prospettiva scientifica dello STOA (DG Servizi di ricerca parlamentare),
visti gli articoli 46 e 52 del suo regolamento,
visti la relazione della commissione giuridica e i pareri della commissione per i trasporti e il turismo, della commissione per le libertà civili, la giustizia e gli affari interni, della commissione per l'occupazione e gli affari sociali, della commissione per l'ambiente, la sanità pubblica e la sicurezza alimentare, della commissione per l'industria, la ricerca e l'energia e della commissione per il mercato interno e la protezione dei consumatori (A8-0005/2017),

Introduzione

A. considerando che, dal mostro di Frankenstein ideato da Mary Shelley al mito classico di Pigmalione, passando per la storia del Golem di Praga e il robot di Karel Čapek, che ha coniato la parola, gli esseri umani hanno fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane;

B. considerando che l'umanità si trova ora sulla soglia di un'era nella quale robot, bot, androidi e altre manifestazioni dell'intelligenza artificiale sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali, rendendo imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza ostacolare l'innovazione;

C. considerando che è necessario creare una definizione generalmente accettata di robot e di intelligenza artificiale che sia flessibile e non ostacoli l'innovazione;

---

[2] Approvata il 16.02.2017.

D. considerando che tra il 2010 e il 2014 la crescita media delle vendite di robot era stabile al 17% annuo e che nel 2014 è aumentata al 29%, il più considerevole aumento annuo mai registrato, e che i fornitori di parti motrici e l'industria elettrica/elettronica sono i principali propulsori della crescita; che le richieste di brevetto per le tecnologie robotiche sono triplicate nel corso dell'ultimo decennio;

E. considerando che negli ultimi duecento anni il tasso di occupazione è aumentato costantemente grazie agli sviluppi tecnologici; che lo sviluppo della robotica e dell'intelligenza artificiale è potenzialmente in grado di trasformare le abitudini di vita e lavorative, innalzare i livelli di efficienza, di risparmio e di sicurezza e migliorare il livello dei servizi, nel breve e medio termine, e considerando che la robotica e l'intelligenza artificiale promettono di portare benefici in termini di efficienza e di risparmio economico non solo in ambito manifatturiero e commerciale, ma anche in settori quali i trasporti, l'assistenza medica, l'istruzione e l'agricoltura, consentendo di evitare di esporre esseri umani a condizioni pericolose, come nel caso della pulizia di siti contaminati da sostanze tossiche;

F. considerando che l'invecchiamento è il risultato dell'allungamento della speranza di vita dovuto ai progressi nell'ambito delle condizioni di vita e della medicina moderna e che rappresenta una delle maggiori sfide politiche, sociali ed economiche del XXI secolo per le società europee; che entro il 2025 oltre il 20 % dei cittadini europei avrà 65 anni o più e che si assisterà a un aumento particolarmente rapido di chi ne avrà 80 o più, il che comporterà un equilibrio sostanzialmente diverso tra generazioni all'interno delle nostre società, e che è interesse della società che le persone anziane rimangano in salute e attive quanto più a lungo possibile;

G. considerando che l'andamento attuale, che tende a sviluppare macchine autonome e intelligenti, in grado di apprendere e prendere decisioni in modo indipendente, genera nel lungo periodo non solo vantaggi economici ma anche una serie di preoccupazioni circa gli effetti diretti e indiretti sulla società nel suo complesso;

H. considerando che l'apprendimento automatico offre enormi vantaggi economici e innovativi per la società migliorando notevolmente le capacità di analisi dei dati, sebbene ponga nel contempo alcune sfide legate alla necessità di garantire la non discriminazione, il giusto processo, la trasparenza e la comprensibilità dei processi decisionali;

I. considerando che i cambiamenti economici e le conseguenze per l'occupazione derivanti dalla robotica e dall'apprendimento automatico devono essere parimenti valutati; che, nonostante i vantaggi innegabili apportati dalla robotica, essa può comportare una trasformazione del mercato del lavoro e rendere necessaria, di conseguenza, una riflessione sul futuro dell'istruzione, dell'occupazione e delle politiche sociali;

J. considerando che l'uso diffuso di robot potrebbe non portare automaticamente alla sostituzione di posti di lavoro, ma le mansioni meno qualificate nei settori ad alta intensità di manodopera potrebbero essere maggiormente esposte all'automazione; che questa tendenza potrebbe riportare i processi di produzione nell'UE; che la ricerca ha dimostrato che l'occupazione aumenta in modo particolarmente veloce nei settori caratterizzati da un maggiore impiego dei computer; che l'automazione dei posti di lavoro è potenzialmente in grado di liberare le persone dalla monotonia del lavoro manuale, consentendo loro di avvicinarsi a mansioni più creative e significative; che l'automazione richiede che i governi investano nell'istruzione e in altre riforme al fine di migliorare la ridistribuzione delle tipologie di competenze di cui avranno bisogno i lavoratori di domani;

K. considerando che, a fronte delle crescenti divisioni della società e della riduzione delle dimensioni della classe media, è importante tenere presente che gli sviluppi della robotica possono condurre a una forte concentrazione di ricchezza e potere nelle mani di una minoranza;

L. considerando che lo sviluppo della robotica e dell'intelligenza artificiale eserciterà sicuramente un'influenza sul mondo del lavoro, il che potrebbe dare luogo a nuove preoccupazioni in materia di responsabilità ed eliminarne altre; che occorre chiarire la responsabilità giuridica per quanto concerne sia il modello di impresa sia le caratteristiche dei lavoratori, in caso di emergenza o qualora sorgessero problemi;

M. considerando che la tendenza all'automazione esige che i soggetti coinvolti nello sviluppo e nella commercializzazione di applicazioni dell'intelligenza artificiale integrino gli aspetti relativi alla sicurezza e all'etica fin dal principio, riconoscendo pertanto che devono essere preparati ad accettare di essere legalmente responsabili della qualità della tecnologia prodotta;

N. considerando che il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (regolamento generale sulla protezione dei dati) stabilisce un quadro giuridico volto a proteggere i dati personali; che altri aspetti riguardanti l'accesso ai dati e la protezione dei dati personali e della privacy potrebbero ancora dover essere affrontati, dal momento che potrebbero ancora sorgere preoccupazioni in materia di privacy per quanto riguarda le applicazioni e gli apparecchi che comunicano tra di loro e con le banche dati senza l'intervento umano;

O. considerando che gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo tale da preservare la dignità, l'autonomia e l'autodeterminazione degli individui, soprattutto nei campi dell'assistenza e della compagnia da parte di esseri umani e nel contesto delle apparecchiature mediche atte alla "riparazione" o al "miglioramento" degli esseri umani;

P. considerando che è possibile che a lungo termine l'intelligenza artificiale superi la capacità intellettuale umana;

Q. considerando che l'ulteriore sviluppo e il maggiore ricorso a processi decisionali automatizzati e algoritmici hanno senza dubbio un impatto sulle scelte compiute da un privato (ad esempio un'impresa o un internauta) e da un'autorità amministrativa, giudiziaria o da un qualsiasi altro ente pubblico al fine di rappresentare la decisione finale di un consumatore, un'impresa o un'autorità; che i dispositivi di sicurezza e la possibilità di verifica e controllo umani devono essere integrati nei processi decisionali automatizzati e algoritmici;

R. considerando che alcuni Stati esteri quali Stati Uniti, Giappone, Cina e Corea del Sud stanno prendendo in considerazione, e in una certa misura hanno già adottato, atti normativi in materia di robotica e intelligenza artificiale, e che alcuni Stati membri hanno iniziato a riflettere sulla possibile elaborazione di norme giuridiche o sull'introduzione di cambiamenti legislativi per tenere conto delle applicazioni emergenti di tali tecnologie;

S. considerando che l'industria europea potrebbe trarre beneficio da un approccio efficiente, coerente e trasparente alla regolamentazione a livello dell'UE, che fornisca condizioni prevedibili e sufficientemente chiare in base alle quali le imprese possano sviluppare

applicazioni e pianificare i propri modelli commerciali su scala europea, garantendo nel contempo che l'Unione e i suoi Stati membri mantengano il controllo sulle norme regolamentari da impostare e non siano costretti ad adottare e subire norme stabilite da altri, vale a dire quei paesi terzi che sono anche in prima linea nello sviluppo della robotica e dell'intelligenza artificiale;

Principi generali

T. considerando che le leggi di Asimov devono essere considerate come rivolte ai progettisti, ai fabbricanti e agli utilizzatori di robot, compresi i robot con capacità di autonomia e di autoapprendimento integrate, dal momento che tali leggi non possono essere convertite in codice macchina;

U. considerando che è necessaria una serie di norme che disciplinino in particolare la responsabilità, la trasparenza e l'assunzione di responsabilità e che riflettano i valori intrinsecamente europei, universali e umanistici che caratterizzano il contributo dell'Europa alla società; che tali regole non devono influenzare il processo di ricerca, innovazione e sviluppo nel settore della robotica;

V. considerando che l'Unione potrebbe svolgere un ruolo essenziale nella definizione dei principi etici fondamentali da rispettare per lo sviluppo, la programmazione e l'utilizzo di robot e dell'intelligenza artificiale e per l'inclusione di tali principi nelle normative e nei codici di condotta dell'Unione al fine di configurare la rivoluzione tecnologica in modo che essa serva l'umanità e affinché i benefici della robotica avanzata e dell'intelligenza artificiale siano ampiamente condivisi, evitando per quanto possibile potenziali insidie;

W. considerando la carta sulla robotica allegata alla relazione, elaborata con l'assistenza dell'unità Prospettiva scientifica dello STOA (DG Servizi di ricerca parlamentare), che propone un codice etico per gli ingegneri robotici, un codice per i comitati di etica della ricerca, una "licenza" per progettisti e una "licenza" per utenti;

X. considerando che per l'Unione dovrebbe essere adottato un approccio graduale, pragmatico e cauto del tipo auspicato da Jean Monnet per quanto riguarda qualsiasi iniziativa futura sulla robotica e sull'intelligenza artificiale al fine di garantire che l'innovazione non sia soffocata;

Y. considerando che è opportuno, dato lo stadio raggiunto nello sviluppo della robotica e dell'intelligenza artificiale, iniziare con le questioni di responsabilità civile;

Responsabilità

Z. considerando che, grazie agli strabilianti progressi tecnologici dell'ultimo decennio, non solo oggi i robot sono in grado di svolgere attività che tradizionalmente erano tipicamente ed esclusivamente umane, ma lo sviluppo di determinate caratteristiche autonome e cognitive – ad esempio la capacità di apprendere dall'esperienza e di prendere decisioni quasi indipendenti – li ha resi sempre più simili ad agenti che interagiscono con l'ambiente circostante e sono in grado di alterarlo in modo significativo; che, in tale contesto, la questione della responsabilità giuridica derivante dall'azione nociva di un robot diventa essenziale;

AA. considerando che l'autonomia di un robot può essere definita come la capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna; che tale autonomia è di natura puramente tecnologica e il suo livello dipende dal grado di complessità con cui è stata progettata l'interazione di un robot con l'ambiente;

AB. considerando che più i robot sono autonomi, meno possono essere considerati come meri strumenti nelle mani di altri attori (quali il fabbricante, l'operatore, il proprietario, l'utilizzatore, ecc.); che ciò, a sua volta, pone il quesito se le regole ordinarie in materia di responsabilità siano sufficienti o se ciò renda necessari nuovi principi e regole volte a chiarire la responsabilità legale dei vari attori per azioni e omissioni imputabili ai robot, qualora le cause non possano essere ricondotte a un soggetto umano specifico, e se le azioni o le omissioni legate ai robot che hanno causato danni avrebbero potuto essere evitate;

AC. considerando che, in ultima analisi, l'autonomia dei robot solleva la questione della loro natura alla luce delle categorie giuridiche esistenti e dell'eventuale necessità di creare una nuova categoria con caratteristiche specifiche e implicazioni proprie;

AD. considerando che, nell'attuale quadro giuridico, i robot non possono essere considerati responsabili in proprio per atti o omis-

sioni che causano danni a terzi; che le norme esistenti in materia di responsabilità coprono i casi in cui la causa di un'azione o di un'omissione del robot può essere fatta risalire ad uno specifico agente umano, ad esempio il fabbricante, l'operatore, il proprietario o l'utilizzatore, e laddove tale agente avrebbe potuto prevedere ed evitare il comportamento nocivo del robot; che, inoltre, i fabbricanti, gli operatori, i proprietari o gli utilizzatori potrebbero essere considerati oggettivamente responsabili per gli atti o le omissioni di un robot;

AE. considerando che, in base all'attuale quadro giuridico, la responsabilità da prodotto (secondo la quale il produttore di un prodotto è responsabile dei malfunzionamenti) e le norme che disciplinano la responsabilità per azioni dannose (in virtù delle quali l'utente di un prodotto è responsabile di un comportamento che conduce al danno) sono applicabili ai danni causati dai robot e dall'intelligenza artificiale;

AF. considerando che, nell'ipotesi in cui un robot possa prendere decisioni autonome, le norme tradizionali non sono sufficienti per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati;

AG. considerando che sono palesi le carenze dell'attuale quadro normativo anche in materia di responsabilità contrattuale, dal momento che le macchine progettate per scegliere le loro controparti, negoziare termini contrattuali, concludere contratti e decidere se e come attuarli rendono inapplicabili le norme tradizionali; considerando che ciò pone in evidenza la necessità di norme nuove, efficaci e al passo con i tempi che corrispondano alle innovazioni e agli sviluppi tecnologici che sono stati di recente introdotti e che sono attualmente utilizzati sul mercato;

AH. considerando che, per quanto riguarda la responsabilità extracontrattuale, la direttiva 85/374/CEE riguarda solamente i danni causati dai difetti di fabbricazione di un robot e a condizione che la persona danneggiata sia in grado di dimostrare il danno effettivo, il difetto nel prodotto e il nesso di causalità tra difetto e danno e che pertanto la responsabilità oggettiva o la responsabilità senza colpa potrebbero non essere sufficienti;

AI. considerando che, nonostante l'ambito di applicazione della direttiva 85/374/CEE, l'attuale quadro giuridico non sarebbe sufficiente a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile;

Principi generali riguardanti lo sviluppo della robotica e dell'intelligenza artificiale per uso civile

1. invita la Commissione a proporre definizioni europee comuni di sistemi cyberfisici, di sistemi autonomi, di robot autonomi intelligenti e delle loro sottocategorie, prendendo in considerazione le seguenti caratteristiche di un robot intelligente:
– l'ottenimento di autonomia grazie a sensori e/o mediante lo scambio di dati con il suo ambiente (interconnettività) e lo scambio e l'analisi di tali dati;
– l'autoapprendimento dall'esperienza e attraverso l'interazione (criterio facoltativo);
– almeno un supporto fisico minore;
– l'adattamento del proprio comportamento e delle proprie azioni all'ambiente;
– l'assenza di vita in termini biologici;

2. ritiene che debba essere introdotto un sistema globale dell'Unione per la registrazione dei robot avanzati nel mercato interno dell'Unione, laddove necessario e pertinente per categorie specifiche di robot, e invita la Commissione a stabilire criteri per la classificazione dei robot da registrare; invita, in tale contesto, la Commissione a valutare se sia opportuno affidare la gestione del sistema di registrazione e del registro a un'agenzia designata dell'UE per la robotica e l'intelligenza artificiale;

3. sottolinea che lo sviluppo della tecnologia robotica dovrebbe mirare a integrare le capacità umane e non a sostituirle; ritiene che sia fondamentale, nello sviluppo della robotica e dell'intelligenza artificiale, garantire che gli uomini mantengano in qualsiasi momento il controllo sulle macchine intelligenti; ritiene che dovrebbe essere prestata un'attenzione particolare alla possibilità che nasca un attaccamento emotivo tra gli uomini e i robot, in particolare per i gruppi vulnerabili (bambini, anziani e disabili), e sottolinea gli interrogativi

connessi al grave impatto emotivo e fisico che un tale attaccamento potrebbe avere sugli uomini;

4. sottolinea che un approccio a livello dell'Unione può agevolare il progresso evitando la frammentazione nel mercato interno e, al contempo, evidenzia l'importanza del principio di riconoscimento reciproco nell'utilizzo transfrontaliero dei robot e dei sistemi robotici; rammenta che il collaudo, la certificazione e l'autorizzazione all'immissione nel mercato dovrebbero essere richiesti soltanto in uno Stato membro; sottolinea che tale approccio dovrebbe essere accompagnato da un'efficace vigilanza del mercato;

5. sottolinea l'importanza di misure a sostegno delle piccole e medie imprese e delle start-up nel settore della robotica che creano nuovi segmenti di mercato nel settore o che si avvalgono di robot;

Ricerca e innovazione

6. sottolinea che molte applicazioni robotiche sono ancora in fase sperimentale; accoglie con favore il fatto che sempre più progetti di ricerca sono finanziati dagli Stati membri e dall'Unione; ritiene essenziale che l'Unione e gli Stati membri, per mezzo dei finanziamenti pubblici, restino leader nella ricerca in ambito della robotica e dell'intelligenza artificiale; invita la Commissione e gli Stati membri a rafforzare gli strumenti finanziari per i progetti di ricerca nella robotica e nelle TIC, compresi i partenariati pubblico-privati, e ad attuare nelle rispettive politiche di ricerca i principi della scienza aperta e dell'innovazione etica responsabile; sottolinea che è necessario destinare risorse sufficienti alla ricerca di soluzioni alle sfide sociali, etiche, giuridiche ed economiche poste dallo sviluppo tecnologico e dalle sue applicazioni;

7. invita la Commissione e gli Stati membri a promuovere i programmi di ricerca, a incentivare la ricerca sui possibili rischi e sulle possibili opportunità a lungo termine dell'intelligenza artificiale e delle tecnologie robotiche e a promuovere quanto prima l'avvio di un dialogo pubblico strutturato sulle conseguenze dello sviluppo di tali tecnologie; invita la Commissione, nell'ambito del riesame intermedio del quadro finanziario pluriennale (QFP), ad aumentare il suo sostegno a favore del programma SPARC finanziato a titolo di Orizzonte 2020; invita la Commissione e gli Stati membri a unire i loro sforzi per monitorare da vicino tali tecnologie e garantire una loro transizione più agevole dalla ricerca alla commercia-

lizzazione e all'utilizzo sul mercato, dopo le opportune valutazioni della sicurezza e nel rispetto del principio di precauzione;

8. sottolinea che l'innovazione nella robotica e nell'intelligenza artificiale e la loro integrazione nell'economia e nella società richiedono un'infrastruttura digitale che garantisca una connettività universale; invita la Commissione a definire un quadro che soddisfi i requisiti di connettività per il futuro digitale dell'Unione e a garantire che l'accesso alla banda larga e alla rete 5G sia pienamente conforme al principio di neutralità della rete;

9. è fermamente convinto che un'interoperabilità tra i sistemi, i dispositivi e i servizi di cloud, basata sulla sicurezza e sulla tutela della vita privata fin dalla progettazione, sia fondamentale per ottenere flussi di dati in tempo reale che consentano ai robot e all'intelligenza artificiale una maggiore flessibilità e autonomia; invita la Commissione a promuovere un ambiente aperto, che spazi da norme aperte a modelli innovativi per la concessione delle licenze e dalle piattaforme aperte alla trasparenza, al fine di evitare la dipendenza da sistemi proprietari che limitano l'interoperabilità;

Principi etici

10. osserva che le possibilità di realizzazione personale che derivano dall'uso della robotica sono relativizzate da un insieme di tensioni o rischi e dovrebbero essere valutate in modo serio dal punto di vista della sicurezza delle persone e della loro salute, della libertà, la vita privata, l'integrità, la dignità, dell'autodeterminazione e la non discriminazione nonché della protezione dei dati personali;

11. considera che l'attuale quadro giuridico dell'Unione debba essere aggiornato e integrato, se del caso, da principi etici di orientamento che riflettano la complessità della robotica e delle sue numerose implicazioni sociali, mediche, bioetiche; è del parere che un quadro etico di orientamento chiaro, rigoroso ed efficiente per lo sviluppo, la progettazione, la produzione, l'uso e la modifica dei robot sia necessario per integrare le raccomandazioni legali della relazione e l'acquis nazionale e dell'Unione esistente; propone, in allegato alla presente risoluzione, un quadro sotto forma di una carta contenente un codice di condotta per gli ingegneri robotici, un codice per i comitati etici di ricerca relativo al loro lavoro di revisione dei protocolli di robotica e modelli di licenze per progettisti e utenti;

12. pone l'accento sul principio della trasparenza, nello specifico sul fatto che dovrebbe sempre essere possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale che possa avere un impatto rilevante sulla vita di una o più persone; ritiene che debba sempre essere possibile ricondurre i calcoli di un sistema di intelligenza artificiale a una forma comprensibile per l'uomo; ritiene che i robot avanzati dovrebbero essere dotati di una "scatola nera" che registri i dati su ogni operazione effettuata dalla macchina, compresi i passaggi logici che hanno contribuito alle sue decisioni;

13. sottolinea che il quadro etico di orientamento dovrebbe essere basato sui principi di beneficenza, non maleficenza, autonomia e giustizia, nonché sui principi sanciti all'articolo 2 del trattato sull'Unione europea e nella Carta dei diritti fondamentali dell'Unione europea – quali la dignità umana, l'uguaglianza, la giustizia e l'equità, la non discriminazione, il consenso informato, la vita privata e familiare e la protezione dei dati, così come sugli altri principi e valori alla base del diritto dell'Unione come la non stigmatizzazione, la trasparenza, l'autonomia, la responsabilità individuale e sociale – e sulle pratiche e i codici etici esistenti;

14. ritiene che un'attenzione speciale dovrebbe essere prestata ai robot che rappresentano una minaccia significativa alla riservatezza in virtù del loro posizionamento in spazi tradizionalmente protetti e privati e della loro capacità di estrarre e trasmettere dati personali e sensibili;

Un'agenzia europea

15. ritiene che sia necessaria una cooperazione rafforzata tra gli Stati membri e la Commissione per garantire nell'Unione norme transfrontaliere coerenti che promuovano la collaborazione tra le industrie europee e consentano la diffusione nell'intera Unione di robot che soddisfino i livelli richiesti di sicurezza nonché i principi etici sanciti dal diritto dell'Unione;

16. chiede alla Commissione di esaminare la possibilità di istituire un'agenzia europea per la robotica e l'intelligenza artificiale incaricata di fornire le competenze tecniche, etiche e normative necessarie a sostenere l'impegno degli attori pubblici pertinenti, a livello sia di Unione che di Stati membri, per garantire una risposta tempestiva, etica e ben informata alle nuove opportunità e sfide, in par-

ticolare quelle di carattere transfrontaliero, derivanti dallo sviluppo tecnologico della robotica, come ad esempio nel settore dei trasporti;

17. ritiene che, alla luce delle potenzialità della robotica, dei problemi connessi al suo utilizzo e delle attuali dinamiche d'investimento, risulti giustificato dotare l'agenzia europea di un bilancio proprio e di personale, come regolatori ed esperti tecnici ed etici esterni incaricati di monitorare, a livello intersettoriale e multidisciplinare, le applicazioni basate sulla robotica, individuare norme relative alle migliori prassi e, ove opportuno, raccomandare misure regolamentari, definire nuovi principi e affrontare eventuali questioni di tutela dei consumatori e difficoltà sistemiche; chiede alla Commissione (e all'agenzia europea, qualora fosse istituita) di riferire annualmente al Parlamento europeo circa gli ultimi sviluppi della robotica e le eventuali azioni che devono essere intraprese;

Diritti di proprietà intellettuale e flusso di dati

18. rileva che non esistono disposizioni giuridiche che si applichino specificamente alla robotica, ma che ad essa possono essere facilmente applicati i regimi e le dottrine giuridici esistenti, sebbene alcuni aspetti richiedano una considerazione specifica; invita la Commissione a sostenere un approccio orizzontale e neutrale dal punto di vista tecnologico alla proprietà intellettuale applicabile ai vari settori in cui la robotica potrebbe essere impiegata;

19. invita la Commissione e gli Stati membri a garantire che le norme di diritto civile nel settore della robotica siano coerenti al regolamento generale sulla protezione dei dati e in linea con i principi della necessità e della proporzionalità; invita la Commissione e gli Stati membri a tenere conto della rapida evoluzione tecnologica del settore della robotica, compreso lo sviluppo dei sistemi cyberfisici, e ad assicurare che il diritto dell'Unione non resti indietro rispetto all'andamento dello sviluppo e dell'adozione delle tecnologie;

20. sottolinea che il diritto al rispetto della vita privata e alla protezione dei dati personali, quale stabilito dagli articoli 7 e 8 della Carta e dall'articolo 16 del trattato sul funzionamento dell'Unione europea (TFUE), si applica a tutti gli ambiti della robotica e che il quadro giuridico dell'Unione per la protezione dei dati deve essere pienamente rispettato; chiede a tale proposito che, nel quadro dell'attua-

zione del regolamento generale sulla protezione dei dati, si chiariscano le norme e i criteri relativi all'uso di fotocamere e sensori nei robot; invita la Commissione a garantire che siano rispettati i principi della protezione dei dati, come la tutela della vita privata fin dalla progettazione e per impostazione predefinita, la minimizzazione dei dati e la limitazione delle finalità, così come meccanismi di controllo trasparenti per i titolari dei dati e misure correttive adeguate conformi alla legislazione dell'Unione in materia di protezione dei dati e che siano promosse adeguate raccomandazioni e norme da integrare nelle politiche dell'Unione;

21. sottolinea che la libera circolazione dei dati è indispensabile per l'economia digitale e lo sviluppo nel settore della robotica e dell'intelligenza artificiale; evidenzia che un elevato livello di sicurezza dei sistemi della robotica, compresi i loro sistemi di dati interni e i flussi di dati, è fondamentale per un utilizzo adeguato dei robot e dell'intelligenza artificiale; sottolinea che deve essere garantita la protezione delle reti di robot e intelligenza artificiale interconnessi onde prevenire eventuali violazioni della sicurezza; sottolinea che un elevato livello di sicurezza e di protezione dei dati personali, congiuntamente al rispetto della vita privata, è fondamentale nella comunicazione tra gli uomini e i robot e le forme di intelligenza artificiale; sottolinea la responsabilità dei progettisti di robot e di intelligenza artificiale di sviluppare prodotti sicuri e adatti agli scopi previsti; invita la Commissione e gli Stati membri a sostenere e incentivare lo sviluppo della tecnologia necessaria, inclusa la sicurezza fin dalla progettazione;

Normazione, sicurezza e protezione

22. evidenzia che la questione della definizione delle norme e della concessione dell'interoperabilità è fondamentale per la concorrenza futura nell'ambito delle tecnologie di robotica e di intelligenza artificiale; invita la Commissione a continuare a lavorare sull'armonizzazione internazionale delle norme tecniche, in particolare assieme agli organismi europei di normazione e all'Organizzazione internazionale di normazione, per favorire l'innovazione, evitare la frammentazione del mercato interno e garantire un livello elevato di sicurezza dei prodotti e di protezione dei consumatori che includa, ove opportuno, norme minime di sicurezza nell'ambiente di lavoro; sottolinea l'importanza dell'ingegneria inversa legale e degli standard aperti al fine di massimizzare il valore dell'innovazione e garantire che i robot possano comunicare tra loro; accoglie favore-

volmente, a tal proposito, l'istituzione di speciali comitati tecnici, quali l'ISO/TC 299 Robotics, che si dedicano esclusivamente all'elaborazione di norme in materia di robotica;

23. sottolinea che testare i robot in condizioni reali è essenziale per individuare e valutare i rischi che potrebbero comportare, nonché il loro sviluppo tecnologico successivo alla fase puramente sperimentale di laboratorio; sottolinea, a tale proposito, che testare i robot in situazioni reali, in particolare nelle città e sulle strade, solleva un gran numero di problemi, tra cui ostacoli che rallentano lo sviluppo di queste fasi di collaudo, e richiede una strategia e un meccanismo di monitoraggio efficaci; invita la Commissione a elaborare criteri uniformi in tutta l'Unione, che i singoli Stati membri dovrebbero utilizzare per identificare le aree in cui autorizzare gli esperimenti con robot, nel rispetto del principio di precauzione;

Mezzi di trasporto autonomi

a) Veicoli autonomi

24. sottolinea che la nozione di trasporto autonomo include tutte le forme a pilotaggio remoto, automatizzate, connesse e autonome di trasporto stradale, ferroviario, aereo e per vie d'acqua, compresi i veicoli, i treni, le imbarcazioni, i traghetti, i velivoli, i droni e tutte le forme future di innovazione e sviluppo in questo settore;

25. ritiene che il settore automobilistico sia quello in cui è avvertita con maggiore urgenza la necessità di norme efficaci a livello unionale e mondiale che garantiscano lo sviluppo transfrontaliero di veicoli automatizzati e autonomi, in modo da sfruttarne appieno il potenziale economico e beneficiare degli effetti positivi delle tendenze tecnologiche; sottolinea che approcci normativi frammentari ostacolerebbero l'attuazione dei sistemi di trasporto autonomi e metterebbero a repentaglio la competitività europea;

26. sottolinea che il tempo di reazione del conducente svolge un ruolo fondamentale qualora egli debba inaspettatamente assumere il controllo del veicolo e invita pertanto le parti interessate a fornire dati realistici per la definizione delle questioni relative alla sicurezza e alla responsabilità;

27. è del parere che il passaggio ai veicoli autonomi avrà un impat-

to sui seguenti aspetti: la responsabilità civile (responsabilità e assicurazione), la sicurezza stradale, tutte le tematiche relative all'ambiente (ad esempio, efficienza energetica, utilizzo di tecnologie e fonti di energia rinnovabili) e le problematiche relative ai dati (ad esempio, accesso ai dati, protezione dei dati personali e privacy, condivisione di informazioni), le questioni relative all'infrastruttura TIC (ad esempio, un livello elevato di comunicazione efficiente e affidabile) e all'occupazione (ad esempio, la creazione e la perdita di posti di lavoro, la formazione dei conducenti di veicoli commerciali pesanti per la guida dei veicoli automatizzati); evidenzia che saranno necessari notevoli investimenti nelle infrastrutture stradali, energetiche e delle TIC; invita la Commissione a considerare i suddetti aspetti nel suo lavoro sui veicoli autonomi;

28. sottolinea l'importanza critica dell'affidabilità delle informazioni sul posizionamento nello spazio e nel tempo fornite dai programmi europei di navigazione satellitare Galileo e EGNOS ai fini dell'introduzione dei veicoli autonomi e sollecita, a tale proposito, la messa a punto e il lancio dei satelliti necessari per completare il sistema di posizionamento europeo Galileo;

29. richiama l'attenzione sull'elevato valore aggiunto dei veicoli autonomi per le persone con mobilità ridotta, in quanto permettono loro di partecipare più efficacemente alla circolazione stradale, facilitando in tal modo la loro vita quotidiana;

b) Droni (RPAS)

30. prende atto dei progressi positivi compiuti dalla tecnologia dei droni, in particolare nel settore della ricerca e del soccorso; sottolinea l'importanza di un quadro unionale relativo ai droni al fine di tutelare la sicurezza e la vita privata dei cittadini dell'Unione e invita la Commissione a dare seguito alle raccomandazioni contenute nella risoluzione del Parlamento europeo del 29 ottobre 2015 sull'uso sicuro dei sistemi aerei a pilotaggio remoto (RPAS), noti come veicoli aerei senza equipaggio (UAV), nel settore dell'aviazione civile(5); esorta la Commissione a fornire valutazioni sui problemi di sicurezza connessi all'uso su larga scala dei droni; invita la Commissione a valutare la necessità di introdurre un sistema di tracciabilità e identificazione obbligatorio per gli RPAS che consenta di individuare in tempo reale la posizione dei velivoli durante il loro utilizzo; ricorda che l'uniformità e la sicurezza dei velivoli senza pilota

dovrebbero essere garantite dalle misure stabilite nel regolamento (CE) n. 216/2008 del Parlamento europeo e del Consiglio(6);

Robot impiegati per l'assistenza

31. sottolinea che la ricerca e lo sviluppo di robot per l'assistenza agli anziani sono diventati, nel tempo, più diffusi ed economici, permettendo così di produrre dispositivi dotati di maggiori funzionalità e più facilmente accettati dai consumatori; evidenzia l'ampia gamma di applicazioni di tali tecnologie utilizzate per la prevenzione, l'assistenza, il monitoraggio, lo stimolo e l'accompagnamento degli anziani, come pure delle persone affette da demenza, disturbi cognitivi o perdita della memoria;

32. sottolinea che il contatto umano è uno degli aspetti fondamentali delle cure umane; ritiene che la sostituzione del fattore umano con i robot potrebbe, da una parte, disumanizzare le pratiche di accudimento, ma riconosce, d'altra parte, che i robot potrebbero svolgere compiti di assistenza automatizzati e agevolare il lavoro degli assistenti sanitari, migliorando, nel contempo, le cure fornite dal personale sanitario e rendendo il percorso di riabilitazione più mirato, consentendo così al personale medico e agli assistenti di dedicare più tempo alla diagnosi e a una migliore pianificazione delle opzioni terapeutiche; sottolinea che, sebbene la robotica abbia le potenzialità per migliorare la mobilità e l'integrazione delle persone con disabilità e delle persone anziane, gli assistenti in carne e ossa continueranno a essere necessari e a svolgere un ruolo importante e non completamente sostituibile nella loro interazione sociale;

Robot medici

33. sottolinea l'importanza di un'adeguata istruzione, formazione e preparazione per il personale sanitario, quali i medici e gli assistenti sanitari, al fine di garantire il grado più elevato possibile di competenza professionale nonché per salvaguardare e proteggere la salute dei pazienti; evidenzia la necessità di definire i requisiti professionali minimi che un chirurgo deve possedere per poter far funzionare ed essere autorizzato a usare i robot chirurgici; considera fondamentale rispettare il principio dell'autonomia supervisionata dei robot, in base al quale la programmazione iniziale di cura e la scelta finale sull'esecuzione spetteranno sempre a un chirurgo umano; sottolinea la particolare importanza della formazione onde consentire agli utenti di familiarizzarsi con i requisiti tecnologici del

settore; richiama l'attenzione sulla tendenza crescente all'autodiagnosi mediante l'uso di un robot mobile e, di conseguenza, sulla necessità che i medici siano formati per gestire i casi di autodiagnosi; ritiene che l'utilizzo delle tecnologie in questione non debba sminuire o ledere il rapporto medico-paziente, bensì fornire al medico un'assistenza nella diagnosi e/o nella cura del paziente allo scopo di ridurre il rischio di errore umano e di aumentare la qualità della vita e la speranza di vita;

34. è convinto che, in campo medico, i robot continuino a compiere progressi nello svolgimento di operazioni chirurgiche ad alta precisione e nell'esecuzione di procedure ripetitive e reputa che tali robot dispongano del potenziale per migliorare i risultati della riabilitazione e fornire un sostegno logistico altamente efficace negli ospedali; osserva che i robot medici possono anche ridurre i costi sanitari, consentendo al personale medico di spostare la propria attenzione dal trattamento alla prevenzione e rendendo disponibili maggiori risorse finanziarie per un migliore adeguamento alla diversità delle esigenze dei pazienti, la formazione continua del personale sanitario e la ricerca;

35. invita la Commissione a garantire che le procedure di sperimentazione per testare i nuovi dispositivi medici robotici siano sicure, in particolare nel caso di dispositivi che vengono impiantati nel corpo umano, prima della data di applicazione del regolamento (UE) 2017/745 sui dispositivi medici;

Interventi riparativi e migliorativi del corpo umano

36. osserva gli enormi progressi compiuti dalla robotica e l'ulteriore potenziale di quest'ultima nel campo della riparazione e della sostituzione degli organi danneggiati e delle funzioni umane, ma anche le complesse questioni sollevate in particolare dalle possibilità di interventi migliorativi del corpo umano, dal momento che i robot medici e specialmente i sistemi cyberfisici (CPS) possono modificare il nostro concetto di corpo umano in salute, dato che possono essere portati direttamente sul corpo umano o essere impiantati nel corpo umano; sottolinea l'importanza di istituire con urgenza, negli ospedali e in altri istituti sanitari, comitati di roboetica con personale adeguato che abbiano il compito di esaminare e aiutare a risolvere problemi etici complessi e insoliti riguardanti la cura e il trattamento di pazienti; invita la Commissione e gli Stati membri a elaborare orientamenti per l'istituzione e il funzionamento di tali comitati;

37. sottolinea che nel campo delle applicazioni mediche essenziali, quali le protesi robotiche, deve essere garantito l'accesso continuo e sostenibile alle manutenzioni, alle migliorie e, in particolare, agli aggiornamenti dei software che ovviano a malfunzionamenti e vulnerabilità;

38. raccomanda la creazione di enti di fiducia indipendenti che dispongano dei mezzi necessari per fornire servizi alle persone che utilizzano avanzati dispositivi medici salvavita, ad esempio in termini di manutenzione, riparazioni e migliorie, inclusi gli aggiornamenti software, soprattutto in caso di interruzione di tali servizi di manutenzione da parte del fornitore originale; suggerisce l'introduzione dell'obbligo per i produttori di fornire a tali enti di fiducia indipendenti istruzioni di progettazione esaustive, incluso il codice sorgente, come accade per il deposito legale di una pubblicazione presso la biblioteca nazionale;

39. sottolinea i rischi correlati alla possibilità di hacking, disattivazione o cancellazione della memoria dei CPS integrati nel corpo umano, dato che possono mettere in pericolo la salute o, in casi estremi, anche la vita umana, per cui evidenzia il carattere prioritario da attribuire alla protezione di tali sistemi;

40. pone in evidenza l'importanza di garantire l'accesso equo di tutti i cittadini a tali innovazioni, strumenti e interventi tecnologici; chiede alla Commissione e agli Stati membri di promuovere lo sviluppo di tecnologie assistive in modo da favorire lo sviluppo e l'adozione di queste tecnologie da parte dei soggetti che ne hanno bisogno, in conformità con l'articolo 4 della Convenzione dell'ONU sui diritti delle persone con disabilità, che l'Unione ha sottoscritto;

Educazione e lavoro

41. richiama l'attenzione sulla previsione della Commissione secondo cui entro il 2020 l'Europa potrebbe trovarsi ad affrontare una carenza di professionisti delle TIC fino a 825 000 persone e il 90 % dei posti di lavoro richiederà per lo meno competenze digitali di base; accoglie con favore l'iniziativa della Commissione di proporre una tabella di marcia per l'eventuale uso e revisione del quadro delle competenze digitali e dei descrittori delle competenze digitali per tutti i livelli di discenti, e invita la Commissione a fornire un sostegno concreto per lo sviluppo delle competenze digitali in

tutte le fasce di età e a prescindere dalla posizione lavorativa, come primo passo in direzione di una maggiore corrispondenza tra la domanda e le carenze sul mercato del lavoro; sottolinea che lo sviluppo della robotica impone agli Stati membri di sviluppare sistemi di istruzione e formazione più flessibili, in modo da garantire la corrispondenza tra le strategie delle conoscenze e le esigenze dell'economia della robotica;

42. ritiene che avviare un numero maggiore di giovani donne a una carriera nel digitale e inserire un maggior numero di donne nel mercato del lavoro digitale recherebbe beneficio all'industria digitale, alle donne stesse e all'economia europea; invita la Commissione e gli Stati membri a lanciare iniziative per sostenere le donne nel settore TIC e rafforzarne le competenze digitali;

43. invita la Commissione a iniziare ad analizzare e a monitorare più da vicino le tendenze occupazionali di medio e lungo periodo, prestando un'attenzione particolare alla creazione, alla dislocazione e alla perdita di posti di lavoro nei diversi campi/settori di qualifica, in modo da individuare i campi in cui vengono creati posti di lavoro e quelli in cui vengono persi a seguito dell'aumento dell'uso dei robot;

44. sottolinea l'importanza di prevedere i cambiamenti della società, tenendo conto dei possibili effetti dello sviluppo e della diffusione della robotica e dell'intelligenza artificiale; chiede alla Commissione di analizzare diversi scenari possibili e le relative conseguenze sulla sostenibilità dei sistemi di sicurezza sociale degli Stati membri;

45. evidenzia l'importanza della flessibilità delle competenze e delle capacità sociali, creative e digitali nell'ambito dell'istruzione; è certo che, oltre alle conoscenze accademiche impartite a scuola, l'apprendimento permanente debba essere realizzato attraverso un'azione permanente;

46. osserva le grandi potenzialità offerte dalla robotica per migliorare la sicurezza sul posto di lavoro mediante il trasferimento di alcuni compiti pericolosi e dannosi dagli esseri umani ai robot, ma rileva nel contempo che può creare anche una serie di nuovi rischi, dovuti al numero crescente di interazioni fra esseri umani e robot sul luogo di lavoro; sottolinea, al riguardo, l'importanza di applicare norme rigorose e lungimiranti alle interazioni fra esseri umani e robot al fine di garantire la salute, la sicurezza e il rispetto dei diritti fondamentali sul luogo di lavoro;

Impatto ambientale

47. osserva che lo sviluppo della robotica e dell'intelligenza artificiale dovrebbe essere condotto in modo tale da limitare l'impatto ambientale mediante un consumo energetico efficiente, l'efficienza energetica mediante la promozione dell'uso delle energie rinnovabili e dei materiali di difficile reperibilità, nonché la riduzione al minimo dei rifiuti – ad esempio quelli elettrici ed elettronici – come pure la riparabilità; incoraggia quindi la Commissione a integrare i principi dell'economia circolare in tutte le politiche dell'Unione sulla robotica; osserva altresì che l'uso della robotica avrà un impatto positivo sull'ambiente, in particolare nel campo dell'agricoltura, dell'approvvigionamento alimentare e dei trasporti, nello specifico attraverso le dimensioni ridotte dei macchinari e l'uso ridotto di fertilizzanti, energia e acqua, nonché tramite l'agricoltura di precisione e l'ottimizzazione dei percorsi;

48. sottolinea che i CPS porteranno alla creazione di sistemi energetici ed infrastrutturali in grado di controllare il flusso di elettricità dal produttore al consumatore e condurranno altresì alla creazione di "prosumer" – ovvero produttori e consumatori allo stesso tempo – di energia, con conseguenti vantaggi ambientali importanti;

Responsabilità

49. ritiene che la responsabilità civile per i danni causati dai robot sia una questione fondamentale che deve essere altresì analizzata e affrontata a livello di Unione al fine di garantire il medesimo livello di efficienza, trasparenza e coerenza nell'attuazione della certezza giuridica in tutta l'Unione europea nell'interesse tanto dei cittadini e dei consumatori quanto delle imprese;

50. prende atto del fatto che lo sviluppo della tecnologia robotica richiederà una maggiore comprensione per trovare il terreno comune necessario ai fini dell'attività congiunta umano-robotica, che dovrebbe basarsi su due relazioni interdipendenti essenziali, quali la prevedibilità e la direzionalità; evidenzia che queste due relazioni interdipendenti sono cruciali per determinare quali informazioni è opportuno che gli umani e i robot condividano e come individuare una base comune tra umani e robot che consenta un'efficace azione congiunta umano-robotica;

51. chiede alla Commissione di presentare, sulla base dell'articolo 114 TFUE, una proposta di atto legislativo sulle questioni giuridiche relative allo sviluppo e all'utilizzo della robotica e dell'intelligenza artificiale prevedibili nei prossimi 10-15 anni, in associazione a strumenti non legislativi quali linee guida e codici di condotta come indicato nelle raccomandazioni figuranti nell'allegato;

52. ritiene che il futuro strumento legislativo, a prescindere dalla soluzione giuridica che applicherà alla responsabilità civile per i danni causati dai robot in casi diversi da quelli di danni alle cose, non dovrebbe in alcun modo limitare il tipo o l'entità dei danni che possono essere risarciti, né dovrebbe limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non umano;

53. ritiene che il futuro strumento legislativo debba essere fondato su una valutazione approfondita della Commissione che stabilisca se applicare l'approccio della responsabilità oggettiva o della gestione dei rischi;

54. osserva al contempo che la responsabilità oggettiva richiede una semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo del robot e il danno subito dalla parte lesa;

55. constata che l'approccio di gestione dei rischi non si concentra sulla persona "che ha agito con negligenza" in quanto responsabile a livello individuale bensì sulla persona che, in determinate circostanze, è in grado di minimizzare i rischi e affrontare l'impatto negativo;

56. ritiene che, in linea di principio, una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere proporzionale all'effettivo livello di istruzioni impartite al robot e al grado di autonomia di quest'ultimo, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore; osserva in particolare che, nella determinazione della responsabilità reale per il danno causato, le competenze derivanti dalla "formazione" di un robot non dovrebbero essere confuse con le competenze che dipendono strettamente dalle sue abilità di autoapprendimento; osserva che, almeno nella fase attuale, la responsabilità deve essere imputata a un essere umano e non a un robot;

57. sottolinea che una possibile soluzione al problema della complessità dell'attribuzione della responsabilità per il danno causato da robot sempre più autonomi potrebbe essere un regime di assicurazione obbligatorio, come già avviene, per esempio, con le automobili; osserva tuttavia che, a differenza del regime assicurativo per i veicoli a motore, che copre azioni o errori umani, l'assicurazione dei robot dovrebbe tenere conto di tutte le potenziali responsabilità lungo la catena;

58. ritiene che, come avviene nel caso dell'assicurazione dei veicoli a motore, tale regime assicurativo potrebbe essere integrato da un fondo per garantire la possibilità di risarcire i danni in caso di assenza di copertura assicurativa; invita il settore assicurativo a elaborare nuovi prodotti e tipologie di offerte in linea con i progressi della robotica;

59. invita la Commissione a esplorare, esaminare e valutare, nell'ambito della valutazione d'impatto del suo futuro strumento legislativo, le implicazioni di tutte le soluzioni giuridiche possibili, tra cui:
a) l'istituzione di un regime assicurativo obbligatorio, laddove pertinente e necessario per categorie specifiche di robot, in virtù del quale, come avviene già per le automobili, venga imposto ai produttori e i proprietari dei robot di sottoscrivere una copertura assicurativa per i danni potenzialmente causati dai loro robot;
b) la costituzione di un fondo di risarcimento non solo per garantire il risarcimento quando il danno causato dal robot non è assicurato;
c) la possibilità per il produttore, il programmatore, il proprietario o l'utente di beneficiare di una responsabilità limitata qualora costituiscano un fondo di risarcimento nonché qualora sottoscrivano congiuntamente un'assicurazione che garantisca un risarcimento in caso di danni arrecati da un robot;
d) la scelta tra la creazione di un fondo generale per tutti i robot autonomi intelligenti o di un fondo individuale per ogni categoria di robot e tra il versamento di un contributo una tantum all'immissione sul mercato di un robot o versamenti regolari durante la vita del robot;
e) l'istituzione di un numero d'immatricolazione individuale, iscritto in un registro specifico dell'Unione, al fine di associare in modo evidente il robot al suo fondo, onde consentire a chiunque interagisce con il robot di essere informato sulla natura del fondo, sui limiti della responsabilità in caso di danni alle cose, sui nomi e sulle funzioni dei contributori e su tutte le altre informazioni pertinenti;

f) l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi;

Aspetti internazionali

60. osserva che le attuali norme generali di diritto internazionale privato sugli incidenti stradali applicabili all'interno dell'Unione non hanno bisogno urgente di essere modificate in modo sostanziale per adattarsi allo sviluppo di veicoli autonomi, tuttavia la semplificazione dell'attuale duplice sistema per definire la legge applicabile (basato sul regolamento (CE) n. 864/2007 del Parlamento europeo e del Consiglio e sulla convenzione dell'Aia del 4 maggio 1971 sulla legge applicabile in materia di incidenti della circolazione stradale) migliorerebbe la certezza del diritto e limiterebbe le possibilità di scelta opportunistica del foro;

61. prende atto della necessità di valutare la possibilità di modificare gli accordi internazionali quali la Convenzione di Vienna sul traffico stradale dell'8 novembre 1968 e la Convenzione dell'Aia sulla legge applicabile in materia di incidenti della circolazione stradale;

62. si aspetta che la Commissione assicuri che gli Stati membri attuino in modo coerente il diritto internazionale, ad esempio la convenzione di Vienna sulla circolazione stradale, che deve essere modificata, al fine di consentire la guida senza conducente e invita la Commissione, gli Stati membri e il settore industriale ad attuare il più rapidamente possibile gli obiettivi della dichiarazione di Amsterdam;

63. incoraggia vivamente la cooperazione internazionale nella valutazione delle sfide di carattere sociale, etico e giuridico e, successivamente, per la definizione delle norme regolamentari, sotto l'egida delle Nazioni Unite;

64. sottolinea che le restrizioni e le condizioni di cui al regolamento (CE) n. 428/2009 del Consiglio sul commercio dei prodotti a duplice uso (beni, software e tecnologie che possono avere applicazioni sia civili che militari e/o possono contribuire alla proliferazione del-

le armi di distruzione di massa) dovrebbero applicarsi anche alle applicazioni di robotica;

Aspetti finali

65. chiede alla Commissione, a norma dell'articolo 225 TFUE, di presentare, sulla base dell'articolo 114 TFUE, una proposta di direttiva relativa a norme di diritto civile sulla robotica, seguendo le raccomandazioni figuranti nell'allegato alla presente relazione;

66. conferma che tali raccomandazioni rispettano i diritti fondamentali e il principio di sussidiarietà;

67. ritiene che la proposta richiesta avrebbe incidenze finanziarie qualora si istituisse una nuova agenzia europea;

68. incarica il suo Presidente di trasmettere la presente risoluzione e le raccomandazioni figuranti in allegato alla Commissione e al Consiglio.

ALLEGATO ALLA RISOLUZIONE: RACCOMANDAZIONI CONCERNENTI IL CONTENUTO DELLA PROPOSTA RICHIESTA

Definizione e classificazione dei "robot intelligenti"

È opportuno stabilire una definizione comune europea di robot autonomo intelligente, comprese eventualmente le definizioni delle sue sottocategorie, tenendo conto delle seguenti caratteristiche:
– la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati;
– la capacità di apprendimento attraverso l'esperienza e l'interazione;
– la forma del supporto fisico del robot;
– la capacità di adeguare il suo comportamento e le sue azioni all'ambiente.

Registrazione dei robot intelligenti

Ai fini della tracciabilità e onde agevolare l'applicazione di ulteriori raccomandazioni, è opportuno prevedere un sistema di registrazione dei robot avanzati, sulla base dei criteri fissati per la classificazione dei robot. Il sistema di registrazione e il registro dovrebbero essere istituiti a livello di Unione, coprendo il mercato interno, e potrebbero essere gestiti da un'agenzia designata dell'UE per la robotica e l'intelligenza artificiale, qualora tale agenzia sia istituita.

Responsabilità civile

Qualsiasi soluzione giuridica si scelga da applicare alla responsabilità per i robot e l'intelligenza artificiale in casi diversi da quelli di danni alle cose non dovrebbe in alcun modo limitare il tipo o l'entità dei danni che possono essere risarciti, né dovrebbe limitare le forme di risarcimento che possono essere offerte alla parte lesa per il semplice fatto che il danno è provocato da un soggetto non umano.
Il futuro strumento legislativo dovrebbe essere fondato su una valutazione approfondita della Commissione che stabilisca se applicare l'approccio della responsabilità oggettiva o della gestione dei rischi.
Dovrebbe inoltre essere istituito un regime assicurativo obbligatorio, che potrebbe basarsi sull'obbligo del produttore di stipulare una copertura assicurativa per i robot autonomi che produce.
Il regime assicurativo dovrebbe essere integrato da un fondo per ga-

rantire il risarcimento dei danni in caso di assenza della copertura assicurativa.
Qualunque decisione politica relativa alle norme sulla responsabilità civile applicabili ai robot e all'intelligenza artificiale dovrebbe essere presa di concerto con un progetto di ricerca e sviluppo di portata europea dedicato alla robotica e alla neuroscienza, con scienziati ed esperti in grado di valutarne tutti i rischi correlati e le possibili conseguenze.

Interoperabilità, accesso al codice e diritti di proprietà intellettuale

È opportuno garantire l'interoperabilità dei robot autonomi collegati in rete che interagiscono tra di loro. Dovrebbe essere possibile accedere al codice sorgente, ai dati di input e ai dettagli costruttivi in caso di necessità, per poter indagare su eventuali incidenti e danni causati dai robot intelligenti e per garantirne il funzionamento ininterrotto, la disponibilità, l'affidabilità e la sicurezza.

CARTA SULLA ROBOTICA

La Commissione, nel proporre atti legislativi in materia di robotica, dovrebbe tener conto dei principi sanciti nella seguente Carta sulla robotica.

La proposta di codice etico-deontologico nel settore della robotica getterà le basi per l'identificazione, il controllo e il rispetto di principi etici fondamentali dalla fase di progettazione e di sviluppo.

Il quadro, elaborato di concerto con un progetto di ricerca e sviluppo di portata europea dedicato alla robotica e alla neuroscienza, deve essere concepito in maniera riflessiva, che permetta di effettuare adeguamenti individuali di volta in volta, allo scopo di determinare se un determinato comportamento sia o meno corretto in una data situazione e adottare decisioni in base a una gerarchia prestabilita di valori.

Il codice non dovrebbe sostituirsi alla necessità di affrontare tutte le principali questioni giuridiche in materia, bensì avere una funzione complementare. Piuttosto, faciliterà la classificazione etica della robotica, potenzierà gli sforzi di innovazione responsabile in tale ambito e verrà incontro alle preoccupazioni del pubblico.

Dovrebbe essere riservata particolare attenzione alle fasi di ricerca e sviluppo della pertinente traiettoria tecnologica (processo di progettazione, esame etico, controlli di verifica, ecc.). La sua finalità dovrebbe essere quella di rispondere alla necessità che ricercatori, professionisti, utenti e progettisti rispettino le norme etiche, ma anche di introdurre una procedura per risolvere i dilemmi etici e consentire a tali sistemi di funzionare in maniera eticamente responsabile.

CODICE ETICO-DEONTOLOGICO DEGLI INGEGNERI ROBOTICI

Preambolo

Il codice deontologico invita tutti i ricercatori e i progettisti ad agire in modo responsabile, tenendo pienamente conto della necessità di rispettare la dignità, la privacy e la sicurezza delle persone.
Il codice deontologico chiede una stretta cooperazione tra tutte le discipline al fine di garantire che la ricerca sulla robotica sia condotta nell'Unione europea in modo sicuro, etico ed efficace.
Il codice deontologico copre tutte le attività di ricerca e sviluppo nel settore della robotica.
Il codice deontologico è volontario e offre una serie di principi generali e orientamenti per le azioni che tutte le parti interessate devono intraprendere.
Gli organismi di finanziamento della ricerca sulla robotica, gli organismi di ricerca, i ricercatori e le commissioni etiche sono incoraggiati a prendere in esame, in una fase quanto più precoce, le future implicazioni delle tecnologie o degli oggetti cui la ricerca è dedicata e a sviluppare una cultura della responsabilità in vista delle sfide e delle opportunità che possono presentarsi in futuro.
Gli organismi pubblici e privati di finanziamento della ricerca sulla robotica dovrebbero esigere che ogni proposta di finanziamento di attività di ricerca in materia sia corredata di una valutazione dei rischi. Tale codice dovrebbe considerare che la responsabilità incombe alle persone e non ai robot.
I ricercatori del settore della robotica dovrebbero impegnarsi a tenere un comportamento etico e deontologico quanto più rigoroso possibile e a rispettare i seguenti principi:
– **beneficenza**: i robot devono agire nell'interesse degli esseri umani;
– **non-malvagità**: la dottrina del "primum, non nocere", in virtù della quale i robot non devono fare del male a un essere umano;
– **autonomia**: la capacità di adottare una decisione informata e non imposta sulle condizioni di interazione con i robot;
– **giustizia**: un'equa ripartizione dei benefici associati alla robotica e l'accessibilità economica dei robot addetti all'assistenza a domicilio e, in particolare, a quelli addetti alle cure sanitarie.

Diritti fondamentali

Le attività di ricerca nel campo della robotica dovrebbero rispetta-

re i diritti fondamentali e, nella loro concezione, attuazione, divulgazione nonché nel loro impiego, dovrebbero essere condotte nell'interesse del benessere e dell'autodeterminazione del singolo e della società nel suo complesso. La dignità umana e l'autonomia – sia fisica che psicologica – vanno sempre rispettate.

Precauzione

Le attività di ricerca nel campo della robotica dovrebbero essere condotte nel rispetto del principio di precauzione, prevedendo le eventuali incidenze dei risultati in termini di sicurezza e adottando le debite precauzioni, proporzionalmente al livello di protezione, incoraggiando allo stesso tempo il progresso a vantaggio della società e dell'ambiente.

Inclusione

Gli ingegneri robotici garantiscono la trasparenza e il rispetto del legittimo diritto di accesso all'informazione di tutti i soggetti interessati. Tale inclusività consente la partecipazione ai processi decisionali di tutti i soggetti coinvolti nelle attività di ricerca sulla robotica o di quelli che nutrono un interesse nella stessa.

Rendicontabilità

Gli ingegneri robotici dovrebbero rendere conto delle eventuali incidenze sociali, ambientali e sanitarie della robotica per le generazioni attuali e quelle future.

Sicurezza

I progettisti dei robot dovrebbero tenere in considerazione e rispettare il benessere fisico, la sicurezza, la salute e i diritti delle persone. Un ingegnere robotico deve preservare il benessere umano, rispettando nel contempo i diritti umani, e segnalare senza indugio i fattori che potrebbero mettere a rischio la collettività o l'ambiente.

Reversibilità

La reversibilità, che costituisce una condizione necessaria per la controllabilità, è un concetto fondamentale nel programmare i robot a comportarsi in maniera sicura e affidabile. Un modello di reversibilità indica al robot quali azioni sono reversibili e le modalità di tale reversibilità. La possibilità di annullare l'ultima azione o una sequenza di azioni permette agli utenti di annullare le azioni indesiderate e ritornare alla fase "corretta" del loro lavoro.

Vita privata

Il diritto alla privacy deve essere sempre rispettato. Un ingegnere robotico dovrebbe garantire che le informazioni private siano conservate in maniera sicura e utilizzate soltanto in modo appropriato. Inoltre, un ingegnere robotico dovrebbe garantire che le persone non siano identificabili personalmente, salvo in circostanze eccezionali e comunque soltanto con un chiaro e inequivocabile consenso informato. Il consenso informato della persona deve essere richiesto e ottenuto prima di qualsiasi interazione uomo-macchina. Di conseguenza, gli ingegneri robotici sono chiamati a definire e applicare le procedure per garantire il consenso valido, la riservatezza, l'anonimato, il trattamento equo e il giusto processo. I progettisti rispetteranno le eventuali richieste di soppressione dei dati e della loro rimozione da qualsiasi insieme di dati.

Massimizzare i vantaggi e ridurre al minimo il danno

I ricercatori dovrebbero puntare a massimizzare i vantaggi del loro lavoro in tutte le fasi, dal momento della concezione fino alla diffusione. Deve essere evitato qualsiasi danno a chi partecipa alla ricerca/ai soggetti umani/ai partecipanti o soggetti di esperimenti, prove o studi. Ove emergano rischi quali elementi inevitabili e integranti della ricerca, è opportuno porre in essere e rispettare validi protocolli di valutazione e gestione dei rischi. Di norma, il rischio di danno non dovrebbe essere superiore a quello incontrato nella vita normale, il che significa che le persone non dovrebbero essere esposte a un rischio maggiore o aggiuntivo rispetto a quelli cui sono esposte con il loro normale stile di vita. Il funzionamento di un sistema robotico dovrebbe sempre basarsi su un rigoroso processo di valutazione dei rischi, che dovrebbe essere improntato ai principi di proporzionalità e di precauzione.

CODICE PER I COMITATI ETICI DI RICERCA (CER)

Principi

Indipendenza

Il processo di esame etico dovrebbe essere indipendente dalla ricerca stessa. Tale principio mette in rilievo la necessità di evitare conflitti d'interesse tra ricercatori e addetti all'esame del protocollo etico e tra questi ultimi e le strutture organizzative della governance.

Competenza

Il processo di esame etico dovrebbe essere condotto da persone dotate di competenze adeguate, tenendo conto della necessità di esaminare attentamente la diversità della composizione e la formazione specifica dei CER in materia di etica.

Trasparenza e rendicontabilità

Il processo di esame dovrebbe essere responsabile e verificabile. I CER devono prendere coscienza delle proprie responsabilità ed essere opportunamente collocati all'interno di strutture organizzative che garantiscano la trasparenza del funzionamento dei CER e delle procedure di gestione e riesame delle norme.

Il ruolo di un comitato etico di ricerca

Un CER è di norma incaricato di esaminare tutte le attività di ricerca che coinvolgano soggetti (umani) condotte dal personale impiegato all'interno dell'organismo interessato o da quest'ultimo; di assicurare l'indipendenza, la professionalità e la tempestività dell'esame etico; di tutelare la dignità, i diritti e il benessere dei soggetti che partecipano alla ricerca; di tenere in considerazione la sicurezza del ricercatore o dei ricercatori; di tenere in considerazione gli interessi legittimi di altri soggetti in causa; di formulare pareri informati sul merito scientifico delle proposte; di formulare raccomandazioni informate per il ricercatore se la proposta risulta in qualche modo inadeguata.

La costituzione di un comitato etico di ricerca

Un CER dovrebbe di norma essere multidisciplinare, includere uomini e donne, essere composto da membri con una vasta esperienza e competenza nel settore della ricerca sulla robotica. Il meccanismo di designazione dovrebbe assicurare che i membri del comi-

tato offrano un adeguato equilibrio tra competenze scientifiche, formazione filosofica, giuridica o etica e opinioni dei non addetti ai lavori, e che includano quanto meno un membro con conoscenze specialistiche in etica, fruitori di servizi speciali di sanità, istruzione o servizi sociali ove questi siano al centro delle attività di ricerca, nonché soggetti con competenze metodologiche specifiche pertinenti alla ricerca che passano in rassegna; la composizione del comitato deve inoltre essere tale da evitare conflitti d'interesse.

Monitoraggio

Tutti gli organismi di ricerca dovrebbero definire opportune procedure per monitorare le attività di ricerca che hanno ottenuto l'approvazione etica fino alla loro conclusione e per garantire una costante verifica se il progetto di ricerca prevede eventuali variazioni nel tempo che potrebbero dover essere trattate. Il monitoraggio dovrebbe essere proporzionato alla natura e al grado di rischio associato alla ricerca. Se un CER ritiene che una relazione di monitoraggio sollevi sostanziali timori circa la conduzione etica dello studio, dovrebbe chiedere un resoconto completo e dettagliato delle ricerche ai fini di una valutazione etica esaustiva. Ove si ritenga che uno determinato studio sia svolto in maniera non etica, è opportuno prendere in considerazione la possibilità di revocarne l'approvazione ed esigere la sospensione o l'interruzione delle attività di ricerca.

LICENZA PER PROGETTISTI

– Il progettista dovrebbe tener conto dei valori europei di dignità, autonomia e autodeterminazione, libertà e giustizia prima, durante e dopo i processi di progettazione, sviluppo e diffusione di tali tecnologie, tra cui l'esigenza di non ledere, ferire, ingannare o sfruttare gli utenti (vulnerabili).
– Il progettista dovrebbe introdurre principi affidabili di progettazione dei sistemi in tutti gli aspetti del funzionamento di un robot, tanto per la progettazione dell'hardware che del software e per qualsiasi trattamento dati "on platform" o "off platform" ai fini della sicurezza.
– Il progettista dovrebbe introdurre funzionalità di "privacy by design" (tutela della vita privata fin dalla progettazione), in modo da garantire la sicurezza delle informazioni private e assicurare che queste ultime siano utilizzate soltanto in modo appropriato.
– Il progettista dovrebbe integrare evidenti meccanismi di opt-out (pulsanti di arresto d'urgenza), che devono essere coerenti con gli obiettivi di progettazione ragionevole.
– Il progettista dovrebbe garantire che un robot funzioni in modo conforme ai principi etici e giuridici locali, nazionali e internazionali.
– Il progettista dovrebbe garantire che le fasi decisionali del robot possano essere ricostruibili e tracciabili.
– Il progettista dovrebbe garantire l'obbligo della massima trasparenza nella programmazione di sistemi robotici, come pure la prevedibilità del comportamento dei robot.
– Il progettista dovrebbe analizzare la prevedibilità di un sistema umano-robotico, esaminando l'incertezza di interpretazione e azione ed eventuali errori robotici o umani.
– Il progettista dovrebbe sviluppare strumenti di localizzazione fin dalla fase di progettazione del robot. Questi strumenti aiuteranno a rendere conto e a spiegare il comportamento dei robot, seppur in maniera limitata, ai vari livelli previsti per esperti, operatori e utenti.
– Il progettista dovrebbe elaborare protocolli di progettazione e di valutazione e collaborare con potenziali utenti e soggetti interessati in sede di valutazione dei vantaggi e dei rischi della robotica, tra cui quelli di natura cognitiva, psicologica e ambientale.
– Il progettista dovrebbe garantire che i robot siano identificabili come tali all'atto di interagire con esseri umani.

– Il progettista dovrebbe preservare la sicurezza e la salute dei soggetti che interagiscono e vengono a contatto con robot, dato che questi ultimi, in quanto prodotti, devono essere progettati mediante processi che ne garantiscano la sicurezza attiva e passiva. Un ingegnere robotico deve preservare il benessere umano, rispettando nel contempo i diritti umani, e non può azionare un robot senza garantire la sicurezza, l'efficacia e la reversibilità del funzionamento del sistema.
– Il progettista dovrebbe ottenere il parere favorevole di un comitato etico di ricerca prima di collaudare un robot in condizioni reali o coinvolgere esseri umani nelle sue procedure di progettazione e sviluppo.

LICENZA PER GLI UTENTI

– L'utente è autorizzato ad avvalersi di un robot senza rischi né il timore di un danno fisico o psicologico.
– L'utente dovrebbe avere il diritto di attendersi che un robot svolga qualsiasi compito per cui è stato espressamente concepito.
– L'utente dovrebbe essere consapevole del fatto che i robot possono avere limitazioni percettive, cognitive e di azionamento.
– L'utente dovrebbe avere rispetto per la fragilità umana, sia fisica che psicologica, e per i bisogni emotivi degli esseri umani.
– L'utente dovrebbe tenere conto del diritto alla privacy dei cittadini, inclusa la disattivazione degli schermi video durante procedure intime.
– L'utente non è autorizzato a raccogliere, utilizzare o comunicare informazioni personali senza l'esplicito consenso della persona interessata.
– L'utente non è autorizzato a utilizzare un robot in alcun modo che sia contrario ai principi e alle norme etiche o giuridiche.
– L'utente non è autorizzato a modificare un robot per servirsene come arma.

Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica (D.L. n. 2688 del 2017) [3]

Art. 1

Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche

1. Dopo l'articolo 656 del codice penale è inserito il seguente:
"Art. 656-bis. – (Pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche). – Chiunque pubblica o diffonde, attraverso piattaforme informatiche destinate alla pubblicazione o diffusione di informazione presso il pubblico, con mezzi prevalentemente elettronici o comunque telematici, notizie false, esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi, è punito, se il fatto non costituisce un più grave reato, con l'ammenda fino a euro 5.000".
2. Nel caso in cui le fattispecie previste dall'articolo 656-bis del codice penale, introdotto dal comma 1 del presente articolo, comportino anche il reato di diffamazione, la persona offesa può chiedere, oltre il risarcimento dei danni ai sensi dell'articolo 185 del codice penale, una somma a titolo di riparazione. La somma è determinata in relazione alla gravità dell'offesa e alla diffusione della notizia, ai sensi dell'articolo 12 della legge 8 febbraio 1948, n. 47. Si applica altresì il terzo comma dell'articolo 595 del codice penale.
3. L'articolo 656-bis del codice penale, introdotto dal comma 1 del presente articolo, non si applica ai soggetti e ai prodotti di cui alla legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-bis, della legge 7 marzo 2001, n. 62.

Art. 2

Diffusione di notizie false che possono destare pubblico allarme, fuorviare settori dell'opinione pubblica o aventi ad oggetto campagne d'odio e campagne volte a minare il processo democratico

1. Dopo l'articolo 265 del codice penale sono inseriti i seguenti:
"Art. 265-bis. – (Diffusione di notizie false che possono destare pub-

[3] Testo del 07.02.2017.

blico allarme o fuorviare settori dell'opinione pubblica). — Chiunque diffonde o comunica voci o notizie false, esagerate o tendenziose, che possono destare pubblico allarme, o svolge comunque un'attività tale da recare nocumento agli interessi pubblici o da fuorviare settori dell'opinione pubblica, anche attraverso campagne con l'utilizzo di piattaforme informatiche destinate alla diffusione online, è punito con la reclusione non inferiore a dodici mesi e con l'ammenda fino a euro 5.000.

Art. 265-ter. – (Diffusione di campagne d'odio o volte a minare il processo democratico). – Ai fini della tutela del singolo e della collettività, chiunque si rende responsabile, anche con l'utilizzo di piattaforme informatiche destinate alla diffusione online, di campagne d'odio contro individui o di campagne volte a minare il processo democratico, anche a fini politici, è punito con la reclusione non inferiore a due anni e con l'ammenda fino a euro 10.000".

Art. 3

Comunicazione al tribunale e obblighi dell'amministratore del sito

1. Al fine di accrescere la trasparenza e di contrastare l'anonimato, all'atto dell'apertura di una piattaforma informatica destinata alla pubblicazione o diffusione di informazione presso il pubblico, non soggetta agli obblighi di cui all'articolo 5 della legge 8 febbraio 1948, n. 47, e di cui all'articolo 1, comma 3-bis, lettera a), della legge 7 marzo 2001, n. 62, l'amministratore della piattaforma medesima deve, entro quindici giorni dalla diffusione online, darne apposita comunicazione, tramite posta elettronica certificata, al tribunale territorialmente competente, trasmettendo il nome e l'URL (Uniform resource locator) della piattaforma elettronica e le seguenti informazioni personali:

a) cognome e nome;

b) domicilio;

c) codice fiscale;

d) l'indirizzo di posta elettronica certificata.

2. L'amministratore della piattaforma informatica di cui al comma 1 deve indicare in modo visibile e pienamente accessibile all'utente della stessa l'indirizzo di posta elettronica certificata per qualsivoglia comunicazione.

Art. 4

Rettifica

1. L'amministratore di cui all'articolo 3 è tenuto a pubblicare le dichiarazioni o le rettifiche dei soggetti di cui siano state pubblicate

immagini o ai quali siano stati attribuiti atti o pensieri o affermazioni da essi ritenuti lesivi della loro dignità o contrari a verità, purché le dichiarazioni o le rettifiche non abbiano contenuto suscettibile di incriminazione penale.
2. Le dichiarazioni o le rettifiche di cui al comma 1 sono pubblicate, non oltre due giorni da quello in cui è avvenuta la richiesta, sulla pagina principale della piattaforma e con la medesima evidenza riservata al contenuto contestato.
3. Le rettifiche o dichiarazioni devono fare riferimento allo scritto che le ha determinate e devono essere pubblicate nella loro interezza.
4. La mancata o incompleta ottemperanza all'obbligo di cui al presente articolo è punita con la sanzione amministrativa da 500 a 2.000 euro.

Art. 5
Misure a tutela del soggetto diffamato o del soggetto leso nell'onore o nella reputazione

1. Fermo restando il diritto di ottenere la rettifica o l'aggiornamento delle informazioni contenute nell'articolo ritenuto lesivo dei propri diritti ai sensi dell'articolo 4, l'interessato può chiedere l'eliminazione, dai siti internet e dai motori di ricerca, dei contenuti diffamatori o dei dati personali trattati in violazione di disposizioni di legge e delle notizie sulla propria persona che non rivestano una rilevanza attuale o motivo di pubblico interesse.
2. L'interessato, in caso di rifiuto o di omessa cancellazione dei dati, ai sensi dell'articolo 14 del decreto legislativo 9 aprile 2003, n. 70, può chiedere al giudice di ordinare la rimozione, dai siti internet e dai motori di ricerca, delle immagini e dei dati ovvero di inibirne l'ulteriore diffusione.
3. In caso di morte dell'interessato, le facoltà e i diritti di cui al comma 2 possono essere esercitati dagli eredi o dal convivente.

Art. 6
Modifiche alla legge 13 luglio 2015, n. 107

1. All'articolo 1 della legge 13 luglio 2015, n. 107, sono apportate le seguenti modificazioni:
a) al comma 7, dopo la lettera f) sono inserite le seguenti:
"f-bis) potenziamento delle attività di formazione continua e professionale con particolare riferimento alle norme e ai meccanismi necessari a prevenire il rischio di distorsione delle informazioni o di manipolazione dell'opinione pubblica;

f-ter) alfabetizzazione mediatica e sostegno ai progetti di sensibilizzazione e ai programmi di formazione mirata volti a promuovere l'uso critico dei media online";
b) dopo il comma 10 è inserito il seguente:
"10-bis. Nelle scuole secondarie di primo e di secondo grado sono realizzate, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica, iniziative di formazione rivolte agli studenti, per sostenere la formazione alla professione di giornalista";
c) al fine di sensibilizzare gli studenti all'importanza di veicolare una corretta informazione, anche attraverso i media online, al comma 34, dopo le parole: "o con gli ordini professionali," sono inserite le seguenti: "o presso i media online".

Art. 7
Disposizioni concernenti la responsabilità dei gestori delle piattaforme informatiche in caso di pubblicazione o diffusione di notizie non attendibili o non veritiere

1. I gestori delle piattaforme informatiche sono tenuti ad effettuare un costante monitoraggio dei contenuti diffusi attraverso le stesse, con particolare riguardo ai contenuti verso i quali gli utenti manifestano un'attenzione diffusa e improvvisa, per valutarne l'attendibilità e la veridicità.
2. Quando i gestori rintracciano un contenuto di cui al comma 1 e ne stabiliscono la non attendibilità sono tenuti alla rimozione dello stesso dalla piattaforma.
3. Nel caso in cui i gestori non rimuovano tali contenuti sono soggetti alla sanzione di cui all'articolo 656-bis del codice penale, introdotto dall'articolo 1 della presente legge.
4. I soggetti di cui al comma 1, nella loro azione di monitoraggio, devono avvalersi anche delle segnalazioni degli utenti effettuate attraverso appositi strumenti accessibili dalla piattaforma medesima.

Art. 8
Modifiche alla legge 14 aprile 1975, n. 103

1. All'articolo 4, primo comma, della legge 14 aprile 1975, n. 103, dopo il primo capoverso è inserito il seguente:
"monitora gli standard editoriali delle piattaforme informatiche destinate alla pubblicazione e diffusione di informazione con mezzi

telematici delle emittenti radiotelevisive pubbliche, verificando la corrispondenza tra i livelli qualitativi offline e quelli online ed incentivando una particolare attenzione ai contenuti generati dagli utenti e pubblicati su tali piattaforme telematiche e adotta le deliberazioni necessarie all'osservanza di tale indirizzo".

PARTE II

EDUCARE *CON* LE NUOVE TECNOLOGIE

Maria Novella Campagnoli

I

NUOVI PARADIGMI: IL CLOUD

Sommario

1. Brevi cenni introduttivi

Sempre più diffuso e utilizzato [1] il cloud computing (la c.d. nuvola informatica) è, già da alcuni anni, oggetto di dibattito e di attenzione da parte di giuristi e informatici. La ragione è presto detta: nell'ambito di quella che è stata definita come la quarta rivoluzione tecnologica [2], nella quale i dati [3] rappresentano la ri-

[1] Non a caso, stando agli studi dell'"Osservatorio Cloud Transformation" della School of Management del Politecnico di Milano, il mercato del cloud in Italia, nel 2018, ha raggiunto i 2,34 miliardi di euro, con una crescita del 19% rispetto al 2017.

[2] D'obbligo il rimando a L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina, 2017.

[3] "[…] Ogni giorno viene generato un numero sufficiente di dati da riempire tutte le biblioteche americane più di otto volte. […] sono numeri che continueranno a crescere rapidamente e ininterrottamente nel prossimo futuro". Siamo, dunque, alle prese con un vero e proprio "[…] tsunami di dati che sta sommergendo il nostro ambiente" (*ivi*, p. 13). In tal senso, anche BEYUNG-CHUL HAN: "ogni click che faccio viene registrato; ogni passo che compio diventa ricostruibile. Ovunque dietro di noi lasciamo tracce digitali" (*Nello sciame. Visioni del digitale*, trad, it., Roma, Nottetempo, 2015). In merito al controllo dei dati si veda anche G. ZICCARDI, *Internet, controllo e*

sorsa più importante (non solo a livello cognitivo ma anche e soprattutto economico [4]), il cloud – per sua natura direttamente chiamato in causa nei processi di archiviazione, gestione e trattamento delle informazioni – non può non acquisire un ruolo di primo piano.

Incarnazione e metafora di quella de-territorializzazione e di quella de-centralizzazione che, da sempre, individuano e connotano il Cyberspace [5], il cloud computing, come un novello Giano bifronte, mostra una certa ambiguità. Per un verso, rappresenta uno straordinario supporto ed un'irrinunciabile fonte di risorse, a cui – più o meno volontariamente e più o meno consapevolmente – ricorriamo di continuo, sia durante lo svolgimento delle attività lavorative che nel corso di quelle relazionali, ludiche o persino sportive (dall'invio delle e-mail ai servizi di messaggistica e alle chat; dalla condivisione di foto e filmati audio-video al sal-

---

libertà. Trasparenza, sorveglianza e segreto nell'era della tecnologia, Milano, Raffaello Cortina, 2015, in part. p. 143 ss.

[4] A proposito della crescente importanza economica dei dati, meritano d'esser qui ricordate le osservazioni di MAYER-SCHÖNBERGER e CUKIER: "dalle scienze all'assistenza sanitaria, dal settore bancario a Internet, i vari settori nel loro insieme raccontano una storia più o meno identica: la quantità di dati disponibili nel mondo sta crescendo rapidamente, e supera non solo la capacità delle nostre macchine ma anche la nostra immaginazione". "Ognuno di noi è investito da un 'diluvio digitale'", un flusso di dati che "possono diventare una fonte di potere economico". Si tratta di vere e proprie "nuove forme di valore" che modificano "i mercati, le organizzazioni, le relazioni fra cittadini e governi, e altro ancora" (*Big data. Una rivoluzione che sta trasformando il nostro modo di vivere e già minaccia la nostra libertà*, trad. it., Milano, Garzanti, 2013, pp. 18, 20, 22 e p. 16). Sul punto anche D. TALIA, *La società globale e i big data. Algoritmi e persone nel mondo digitale*, Soveria Mannelli, Rubettino, 2018. L'odierna "corsa ai dati" è ben testimoniata da *Weople*: l'app che promette agli iscritti una remunerazione in cambio della cessione dei loro dati personali.

[5] Il Cyberspace, infatti, è contraddistinto dalla de-territorializzazione, in luogo della territorializzazione, e dalla de-centralizzazione, in luogo della centralizzazione. Ciò è da attribuirsi al fatto che "[…] la realtà virtuale che il cyberspace propone riduce drasticamente l'importanza dell'elemento geografico". Per questo motivo, ogni differenza si rarefà, diventa sfumata, fluida e, via via, i luoghi "reali" vengono soppiantati dai c.d. non-luoghi virtuali. Ovviamente, il Cyberspace è anche de-centralizzato. La Rete, difatti, non conosce centro, periferia e nemmeno gerarchie, in essa tutto è al contempo centro e periferia, tutto è qui e ora (cfr., infra, A.C. AMATO MANGIAMELI, *Parte Prima* e, per una più ampia e diffusa trattazione, ID., *Informatica giuridica. Appunti e materiali ad uso di lezioni*, Torino, Giappichelli, 2015, pp. 72 e 74).

vataggio di file; dall'accesso alle piattaforme social all'uso di particolari e sempre nuove app [6]). Per un altro verso, però, il cloud è ammantato da un'alea di indeterminatezza e di incertezza. Non a caso, anche a causa di una scarsa o erronea conoscenza [7], la nuvola è tuttora oggetto di diffidenza e qualche volta anche di timori. Timori che, nella maggioranza dei casi, sono legati alle possibili ricadute sulla privacy e, in particolar modo, al rischio di perdere il controllo dei dati [8]. Dati, informazioni e profili, che – come si è già accennato all'inizio – rappresentano un valore e una ricchezza e che, proprio per questa ragione, vengono definiti come il petrolio del neocapitalismo digitale [9].

---

[6] L'elenco delle applicazioni di cui ci avvaliamo quotidianamente è in costante evoluzione e, per questa ragione, potenzialmente infinito. Tra le più note app, tuttavia, possono qui ricordarsi: *Google Eart* (che consente la visualizzazione della maggior parte dei luoghi a partire dalla digitazione di un indirizzo); *Waze* (app di condivisione delle informazioni sul traffico in tempo reale); *IOS Salute* (che consente il controllo degli indicatori del nostro stato di salute); *Runtastic* (che permette di scaricare piani e programmi di allenamento); *Period Calendar* (pensato per monitorare ciclo e periodi di fertilità); *Anti-Theft-Alarm* (che funziona da antifurto/allarme); *Emergency Light, Panic Button Red, BeSafe* e *Google Contatti fidati* (che hanno funzioni di allarme e difesa).

[7] È interessante ricordare che, già nel 2011, l'"Osservatorio Internet" condotto da Nextplora per conto di Microsoft aveva sottolineato che l'88% di chi navigava nel Web utilizzava più o meno consapevolmente il cloud.

[8] Consentendo l'accesso alle risorse distribuite e virtualizzate, il cloud "espone [l'utente-cliente] a particolari rischi e a diverse criticità. Tra questi, è da segnalare la pirateria informatica". Invero, "l'utilizzo simultaneo delle risorse […] permette con più facilità ai criminali di monitorare attentamente l'entrata e l'uscita delle informazioni e di estrarre dati sensibili". Ragion per cui, sia nel caso di privati, che di imprese, che di pubbliche amministrazioni, "la sicurezza costituisce un ostacolo all'adozione della nuvola informatica" (A.C. AMATO MANGIAMELI, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica*, in A.C. AMATO MANGIAMELI, G. SARACENI, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, Giappichelli, 2019, p. 27). Per un'analisi dei rischi e delle perplessità legate all'adozione della nuvola, cfr. anche M.N. CAMPAGNOLI, *Il cloud computing: vantaggi e problematicità*, in *Rivista di Filosofia del Diritto*, V, 1/2016, pp. 109-126.

[9] Così D. TALIA, *La società globale e i big data*, cit., pag. 48.

2. Definizioni, caratteristiche, forme

Fornire una definizione univoca della nuvola non è cosa agevole. Svariate le caratteristiche, tante le implicazioni, moltissimi i risvolti che di volta in volta la contraddistinguono. In prima battuta, è importante sottolineare che il cloud non rappresenta, in senso proprio, una nuova tecnologia ma, più che altro, individua un nuovo paradigma tecnologico [10]. Invero, si tratta di una risorsa sussidiaria e propedeutica ad agevolare e a semplificare l'accesso e la fruizione di alcune ICT già esistenti. In modo particolare, anche grazie alla sua notevole versatilità di impiego – che lo rende utilizzabile da privati, imprese e pubbliche amministrazioni – il cloud contribuisce a rendere più agile, economico, scalabile e flessibile [11], l'utilizzo delle diverse risorse hardware e software disponibili online.

Di qui, come è ovvio, l'evidente ed indissolubile nesso che lega la nuvola alla Rete [12]. Basta infatti accedere ad Internet – da qualunque luogo e con un qualsiasi device – per poter godere della straordinaria capacità di storage, di analisi, di elaborazione e di condivisione che contraddistingue il cloud [13]. Ma non è tutto,

[10] In modo particolare, il cloud rappresenta un "'nuovo' sviluppo di una tecnologia già disponibile […]". Vale a dire, "un modo nuovo di organizzare e rendere fruibili le tecnologie esistenti, integrandone le componenti e presentando all'utente solo le loro funzioni di uso" (E. ACQUATI, S. MACELLARI, A. OSNAGHI (a cura di), *Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, Firenze, Passigli, 2012, pp. 32-33).

[11] La flessibilità – intesa quale possibilità di usufruire, di volta in volta, della tipologia e dell'esatto quantitativo di risorse tecnologiche di cui si ha necessità – costituisce senza dubbio uno dei maggiori "punti di forza" della nuvola (vd. ASTRID, *L'impatto del cloud computing sull'economia italiana*, con prefazione di F. Bassanini e E. Belloni, Roma, Astrid, 2011, p. 11).

[12] In merito al rapporto fra il cloud e la Rete, bisogna, però, sottolineare che – nonostante la relazione che lega – il cloud è qualcosa di ulteriore e di diverso rispetto ad Internet. La nuvola non coincide col Web, non rappresenta né un "generico spazio di navigazione", né soltanto un luogo di condivisione di contenuti. Essa è, piuttosto, uno "spazio virtuale" che consente, a chi se ne serve, di utilizzare le risorse tecnologiche – solo ed esclusivamente – per il tempo necessario a soddisfare esigenze e bisogni, senza sostenere investimenti onerosi e senza sopportare costi fissi (G. REESE, *Cloud computing. Architettura, infrastrutture, applicazioni*, trad. it., Milano, Tecniche Nuove, 2010, p. 2).

[13] Ad esempio, grazie al cloud, il titolare ha sempre accesso ai suoi dati e alle sue informazioni, a prescindere da dove si trovi in quel momento;

perché la connessione alla Rete, oltre a rappresentare la chiave di accesso alle tante potenzialità offerte dalla nuvola, ne costituisce anche la *conditio sine qua non*. Altrimenti detto ed in breve, senza il Web il cloud non solo non sarebbe possibile, ma non sarebbe neppure pensabile.

Chiarito il *fil rouge* che lega il cloud ad Internet, è necessario passare a considerare quali sono le principali caratteristiche e le differenti tipologie di nuvola che, di volta in volta, possono aversi. Anzitutto, va detto che non esiste un solo cloud ma che se ne possono dare vari a seconda della struttura e/o dei servizi erogati [14].

Con riguardo alla collocazione spaziale e alla differente gestione, si possono distinguere:

– il *cloud privato*, che risponde alle esigenze di una specifica impresa ed è collocato all'interno della stessa, secondo la più tradizionale e consueta forma del *local hosting*. Va da sé che, proprio perché si tratta di una nuvola ad uso esclusivo [15], essa non suscita problemi in ordine alla sicurezza o alla gestione delle informazioni;

– il *cloud pubblico*, per mezzo del quale un fornitore-provider mette a disposizione di una pluralità di utenti (privati, aziende o pubbliche amministrazioni) i propri sistemi di elaborazione e di archiviazione dei dati, condividendo con loro hardware e software. Rapportata alla nuvola privata, quella pubblica presenta una maggiore economicità e superiori livelli di performance, ma, al contempo, induce nell'utente anche una più elevata percezione dei rischi, aspetto che, molto spesso, ne frena la diffusione;

– i c.d. *cloud ibridi*, che presentano elementi tipici sia della nuvola privata che di quella pubblica e che si connotano per la

---

inoltre, egli può visualizzare un documento o scaricare un file senza essere obbligato a ricorrere ad un pc o ad un altro dispositivo fisico.

[14] Riprendo, qui, la tradizionale e nota distinzione proposta anche dal GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Cloud computing. Proteggere i dati per non cadere dalle nuvole*, 2012, pp. 9-10.

[15] Il principale vantaggio del cloud privato è costituito proprio dal fatto che i servizi erogati sono forniti da elaboratori collocati in un ambiente di proprietà dell'utente, che, per questo motivo, conserva il pieno controllo delle macchine deputate alla conservazione e all'elaborazione dei dati (cfr. AGENZIA PER L'ITALIA DIGITALE, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica amministrazione*, 2012, pp. 8 e 9).

loro infrastruttura mista, e le *community cloud*, nuvole comunitarie che vengono condivise da un gruppo di organizzazioni [16].

Abbandonando gli aspetti prettamente strutturali-organizzativi e considerando la tipologia dei servizi offerti, emergono ulteriori distinzioni [17]:

– il *cloud infrastructure as a service* (*IaaS*), che, dietro pagamento di un canone commisurato all'utilizzo, fornisce hardware virtuali che possono essere impiegati a supporto o in sostituzione delle infrastrutture di proprietà dell'utente-cliente [18]. Emblematici i CPU, le RAM, gli spazi di storage, le schede di rete e i *server* virtuali;
– il *cloud software as a service* (*SaaS*), per mezzo del quale vengono erogate applicazioni di uso comune e servizi che non richiedono particolari prerequisiti tecnici. È il caso, ad esempio, delle webmail oppure dei social network;
– il *cloud platform as a service* (*PaaS*), che fornisce piattaforme software e soluzioni di sviluppo pensate appositamente per rispondere alle necessità di un determinato utente-cliente [19]. Ba-

---

[16] Sulle community cloud cfr., fra gli altri, F. BASSANINI, E. BELLONI, *L'impatto del cloud computing sull'economia italiana*, cit., p. 12.

[17] Ripropongo qui la classificazione del "National Institute for Standards and Technology" (NIST).

[18] "Il modello di servizio *Infrastructure as a Service* prevede che il servizio offerto consista in una infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale l'utente possa installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni. Nel caso di servizio computazionale, l'utente può richiedere al fornitore di servizi un insieme di macchine virtuali, sulle quali può installare (o richiedere che venga installato direttamente dal fornitore stesso) i sistemi operativi ed i software necessari a risolvere il suo problema. L'utente può richiedere che le macchine virtuali siano connesse tra di loro da una rete virtuale. Le macchine virtuali sono raggiungibili per la loro gestione ed utilizzo tramite l'interfaccia offerta dal fornitore del servizio. Una volta che le macchine virtuali sono state assegnate all'utente, egli può richiederne delle nuove o rilasciarne alcune, in base alle sue esigenze. Nel caso di servizio di memorizzazione, invece, l'utente può richiedere uno spazio di memorizzazione per caricarvi i suoi dati e, successivamente, può aumentarlo o ridurlo a seconda delle sue esigenze" (AGENZIA PER L'ITALIA DIGITALE, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica amministrazione*, cit., p. 7).

[19] "Il modello di servizio *Platform as a Service* prevede che il fornitore del servizio metta a disposizione dell'utente una interfaccia di programmazio-

sti pensare agli applicativi utilizzati in ambito finanziario, a quelli adoperati per la gestione della contabilità, oppure a quelli che trovano impiego nel settore della logistica.

– il *cloud desktop as a service* (*DaaS*), grazie al quale è possibile accedere a dati e/o applicazioni con la modalità *pay-per-use* e *on-demand*;

– il *cloud disaster recovery as a service* (*DraaS*), una particolare tipologia di nuvola in grado di fornire soluzioni di disaster recovery efficaci e all'avanguardia che, proprio in virtù del costo particolarmente contenuto, possono essere adottate anche da imprese di piccole e medie dimensioni;

– il *cloud backup as a service* (*BaaS*), con il quale vengono messi a disposizione dell'utente sistemi di salvataggio dei dati notevolmente più aggiornati e sicuri di quelli normalmente disponibili in *local hosting*;

– il *cloud storage as a service* (*StaaS*), grazie al quale è possibile il salvataggio, la condivisione e la sincronizzazione dei dati su più device. Si pensi a *ICloud*, a *Dropbox*, a *Google Drive* e a *One Drive*;

– il *cloud security as a service* (*SECaaS*), che mette a disposizione degli utenti firewall virtuali contro i possibili attacchi informatici;

– il *cloud network as a service* (*NaaS*), in grado di migliorare e ottimizzare la connettività.

Al di là delle evidenti differenze e delle moltissime specificità, ciò che accomuna tutti i cloud è l'economicità, ovvero la capacità di ridurre sensibilmente le spese di utilizzo e di gestione delle infrastrutture tecnologiche, grazie all'approvvigionamento in outsoursing. E proprio l'economicità – unita alla scalabilità e alla flessibilità – concorre a far sì che la nuvola rappresenti una

---

ne (API) con la quale l'utente può scrivere applicazioni che interagiscono con il servizio. Le specifiche funzionalità offerte dalla API dipendono dal servizio offerto, e la loro esecuzione viene assicurata dal fornitore del servizio. Il fornitore può mettere a disposizione dell'utente anche un ambiente di sviluppo (e di *testing*) per le applicazioni che sfruttano le sue API. Un esempio di servizio cloud di tipo PaaS è costituito da Windows Azure Compute, che permette di utilizzare il framework .NET per sviluppare applicazioni. Poiché utilizza IIS7, è anche possibile gestire applicazioni sviluppate utilizzando ASP.NET, Windows Communication Foundation (WCF) o altre tecnologie Web. Inoltre, supporta anche linguaggi quali PHP e Java" (*ivi*, pp. 7 e 8).

soluzione tecnologica, non solo estremamente efficiente [20], ma anche particolarmente duttile ed appetibile [21]. Una soluzione che, favorendo la diffusione di nuovi servizi e di nuove applicazioni, ha già modificato buona parte del nostro stesso modo di vivere [22].

3. Profili negoziali

Passando all'analisi degli aspetti negoziali, ci si rende immediatamente conto che con il cloud computing siamo di fronte ad un contratto del tutto particolare [23]. In primo luogo, perché esso presenta elementi propri dell'appalto, della licenza e dell'out-

[20] È sufficiente pensare al passaggio dalla *capacity on demand* alla *capability on demand*, alla scalabilità delle soluzioni, come pure alla possibilità di favorire l'attività delle amministrazioni pubbliche. (A proposito del passaggio dal diritto di proprietà al c.d. diritto d'accesso cfr. J. RIFKIN, *L'era dell'accesso. L'evoluzione della new economy*, trad. it., Milano 2000, p. 5 ss. Invece, circa i possibili vantaggi del cloud per la pubblica amministrazione, soprattutto con riferimento all'interoperabilità e alla cooperazione applicativa, si vedano E. ACQUATI, S. MACELLARI, A. OSNAGHI (a cura di), *Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, cit., p. 135 ss.).

[21] Non a caso, già nel 2012, la Commissione Europea aveva indirizzato al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo, e al Comitato delle Regioni, la Comunicazione *Sfruttare il potenziale del cloud computing in Europa* (COM(2012)529), con la quale esortava gli Stati Membri ad aderire alla tecnologia *cloud*, così da superare i divari e favorire lo sviluppo di un mercato unico digitale (cfr. AGENZIA PER L'ITALIA DIGITALE, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, cit., p.7).

[22] Sulle ricadute delle ICT sulla nostra esistenza e, in modo particolare, sulla dimensione giuridica, cfr. A.C. AMATO MANGIAMELI, *infra*, *Prima Parte*.

[23] In verità, circa la qualificazione del contratto di cloud computing, la dottrina appare divisa: per alcuni, si tratterebbe di un contratto *atipico* o *innominato*, per altri, invece, sarebbe un contratto di tipo *misto*. (Con specifico riferimento ai contratti atipici o innominati, fra i tanti, cfr.: G. DE NOVA, *Il tipo contrattuale*, Padova, Cedam,1974; M. COSTANZA, *Il contratto atipico*, Milano, Giuffrè, 1981; F. MESSINEO, *Contratto innominato*, in *Enc. dir.*, X, p. 95; C. BIANCA, *Il contratto*, Milano, Giuffrè, 1997, pp. 449-450 e pp. 450-452. Sui contratti misti, invece: G. DE GENNARO, *I contratti misti*, Padova, Cedam, 1934; A. CATAUDELLA, *La donazione mista*, Milano, Giuffrè, 1970; G. SICCHIERO, *Il contratto a causa mista*, Padova, Cedam, 1995).

sourcing [24]; in secondo luogo, perché – a causa dell'intrinseca *a-geograficità* [25] e *geo-ambiguità* [26] che connota la nuvola – il contratto di cloud solleva tutta una serie di perplessità e di criticità. Si pensi alla difficoltà nell'individuare la normativa applicabile e il foro competente, come pure, al bisogno di garantire adeguati livelli di sicurezza a quello sciame di dati [27] che, per mezzo della nuvola, viene immesso in data center delocalizzati. Criticità che, soprattutto a seguito della nota pronuncia della Corte Europea del 6 ottobre del 2015 [28], hanno iniziato ad essere oggetto di attenzione e di revisione [29] da parte del legislatore europeo.

---

[24] Sul confronto fra il contratto di cloud e l'outsourcing, si vedano: A.R. POPOLI, *Il contratto di cloud computing: natura giuridica e clausole limitative di responsabilità*, in *Giustizia Civile*, 11/2015, p. 4 ss.; G. FIORIGLIO, *Contratto di cloud computing*, in *#Diritto dell'informatica.it*, settembre 2014; A. MANTELERO, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali*, in *Il diritto dell'informazione e dell'informatica*, 26, 4-5/2010, p. 673; ID., *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contratto e impresa*, 4-5/2012, p. 1216 ss.; F. TOSI, *Il contratto di outsourcing di sistema informatico*, Milano, Giuffrè, 2001; M. PITTALIS, *Outsourcing*, in *Contratto e impresa*, 16, 2/2000, p. 1010 ss.

[25] Cfr. M.M. WINKLER, J. MOSCA, *Cloud computing e protezione dei dati personali*, in M. FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Napoli, Editoriale Scientifica, 2015, p. 130 ss.

[26] Vd. F.F. WANG, *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction*, in *Eur. Bus. Law Rev.*, 2013, in part. p. 595. Sulle difficoltà legate alla de-localizzazione tipica della nuvola anche W.K. HON, *Data Localization Laws and Policy*, Northampton, Edward Elgar, 2017.

[27] Faccio mia la suggestiva ed efficace espressione B.-C. HAN, *Nello sciame*, cit.

[28] Ossia della pronuncia relativa alla causa *C-362/14 Schrems/Data Protection Commissioner*, che ha visto contrapposti il cittadino austriaco Maximillian Schrems e l'Autorità irlandese per la protezione dei dati immessi su Facebook. Si tratta di una pronuncia che potremmo definire "storica" anche perché ad essa è seguito l'annullamento dell'accordo *Safe Harbor*.

[29] Fra i più importanti interventi dell'Unione Europea in tema di tutela dei dati, meritano d'esser qui ricordati: la *Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* del 28 gennaio 1981 e il relativo *Protocollo addizionale*; la *Raccomandazione del Comitato dei Ministri del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto della attività di profilazione*, del 23 novembre 2010; il Parere del Garante europeo della protezione dei dati dal titolo *Meeting the challenges of big data; a call for transparency, user control, data protection by design and accountability*, del 19 novembre 2015; il Parere del Garante eu-

Quanto ai soggetti coinvolti, va detto subito che, di solito, il contratto di cloud computing prevede almeno due figure: quella del *cloud provider* [30] – cioè del fornitore che gestisce le infrastrutture e che assicura l'esecuzione dei programmi e delle applicazioni – e quella del *cloud consumer* – ovvero del cliente-utente finale (che, come s'è accennato, può essere un privato, un'impresa, un ente o una pubblica amministrazione).

A questi possono affiancarsi altri soggetti, come, ad esempio:

– il *cloud carrier*, il c.d. cliente amministratore, ovvero colui che funge da intermediario fra il fornitore del servizio e l'utente finale;

– il *cloud auditor*, a cui è affidato il controllo del rispetto degli standard di servizio e di sicurezza;

– il *cloud broker* [31], una figura di congiunzione fra quella del provider e dei consumer, che si occupa dell'integrazione dei servizi.

Una peculiarità non trascurabile è data dal fatto che, di norma, il documento contenente il testo dell'accordo (*Term of Ser-*

---

ropeo dal titolo *Opinion on coherent enforcement of fundamental rights in the age of big data*, del 23 settembre 2016; la *Dichiarazione del Gruppo di Lavoro "Articolo 29" sull'impatto dello sviluppo dei big data sulla protezione delle persone rispetto al trattamento automatizzato dei loro dati personali nell'Unione Europea*, del 16 settembre 2014; la *Relazione del Parlamento Europeo, Commissione per le libertà civili, la giustizia e gli affari interni sulle implicazioni dei big data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI)); le linee guida internazionali sui big data e sulla tutela dei dati personali *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, *Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data*, del 23 gennaio 2017; il *General Data Protection Regulation* (GDPR) 2016/679; la *Risoluzione del Parlamento europeo sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy*, del 5 luglio 2018.

[30] È importante sottolineare che si danno diversi livelli di cloud provider. Al c.d. primary cloud provider che eroga i servizi direttamente all'utente finale, si aggiunge anche il c.d. intermediary cloud provider che eroga servizi provenienti da altri provider.

[31] Si noti che, diversamente dal cloud intermediary, il cloud broker offre un'unica interfaccia che raccoglie i servizi offerti da più cloud providers. Inoltre, mentre il cloud intermediary ingloba nel suo servizio finale tutti i servizi provenienti dal primary cloud provider, il cloud broker rende nota la provenienza di tali servizi da altri cloud providers.

vice)[32] è accompagnato da allegati tecnici che stabiliscono i livelli di qualità dei servizi (i c.d. *Service Level Agreement*)[33] e la privacy policy (l'*Acceptable Use Policy*)[34].

Un altro aspetto di grande rilievo è rappresentato dal fatto che si tratta di un contratto standard. Vale a dire, di un negozio nel quale l'utente si limita ad aderire, senza che vi siano margini di trattazione, modifica o deroga rispetto alle condizioni e alle clausole generali previste. Come è intuitivo, tale aspetto – associato al diverso grado di conoscenza e di competenza tecnologica che differenzia il fornitore rispetto all'utente – concorre a determinare un'asimmetria contrattuale ed una sorta di sbilanciamento a favore del provider[35], che di solito stabilisce *ex ante*, ed in maniera del tutto unilaterale, termini e modalità del servizio[36]. Si aggiunga, poi, che alle questioni di carattere generale, riguardanti la durata del contratto, il corrispettivo previsto, la legge applicabile e la giurisdizione competente, si accompagnano pure quelle di natura informativa. Vale a dire, quelle che attengono espressamente alla gestione e alla sicurezza dei dati e che, solitamente, ricadono nei c.d. *Non Disclosure Agreement* (NDA)[37].

Di qui – e non potrebbe essere altrimenti – la necessità di interrogarsi sulla reale possibilità da parte dei buyer (siano essi privati, imprese e/o pubbliche amministrazioni) di imporre al for-

---

[32] Vd. S. Branshaw, C. Millard, I. Walden, *Standard contracts for cloud services*, in C. Millard (eds.), *Cloud Computing Law*, Oxford, Oxford University Press, 2014, pp. 44-46.

[33] Cfr. G. Rizzo, *La responsabilità contrattuale nella gestione dei dati nel cloud computing*, in *Diritto Mercato Tecnologia* (DMT), 8 aprile 2013.

[34] S. Branshaw, C. Millard, I. Walden, *Standard contracts for cloud services*, cit., p. 44.

[35] Cfr., fra gli altri, E. Bellisario, *Cloud computing*, Assago, Altalex, 2011, p. 13 ss. Sul ruolo dei contratti nella regolazione dei rapporti fra i vari livelli della *governance* della Rete, si vedano L. Bygrave, *Contract versus statute in Internet governance*, in I. Brown (ed.), *Research Handbook on Governance of the Internet*, Oxford, University of Oxford, 2012, pp. 168-197 e U. Pagallo, *The Realignment of the Sources of the Law and their Meaning in an Information Society*, in *Philosophy & Technology*, I, 28, 2015, pp. 57-73.

[36] Vd. A.R. Popoli, *Il contratto di cloud computing: natura giuridica e clausole limitative di responsabilità*, in *Giustizia civile*, 11/2015, p. 10.

[37] Autentici accordi di riservatezza con i quali le parti individuano le informazioni che intendono mantenere confidenziali e che – come tali – si impegnano a non svelare (né rendere accessibili) a terzi.

nitore regole di ingaggio che garantiscano un'adeguata tutela dei dati personali e che prevedano delle responsabilità del provider in caso di violazioni.

Va da sé che i nodi più problematici della nuvola siano quelli connessi alle nozioni di *privacy* [38], di *sicurezza* e di *responsabilità* e sono legati alla paura che il trasferimento e la concentrazione dei dati possa determinare una perdita di controllo sugli stessi [39]. Timori che – come si vedrà – possono però essere facilmente superati se si considera che, pur ricadendo nella disponibilità del fornitore-provider, i dati e le informazioni inserite nella nuvola restano pur sempre di proprietà esclusiva dell'utente che, infatti, in qualsiasi momento, può disporne il trasferimento e la migrazione [40].

Da un lato, la privacy, la sicurezza e la responsabilità sono le tre parole chiave attorno alle quali orbitano tutti i dibattiti sul cloud e sulle quali si incentrano, sia coloro che guardano alla nuvola con preoccupazione [41], sia coloro che la considerano un im-

---

[38] Per un interessante approfondimento sul diritto alla privacy e nell'era digitale vd.: A.C. AMATO MANGIAMELI, *Sul diritto alla privacy. Variazioni sul tema e spunti normativi*, in ID., *Informatica giuridica*, cit., p. 319 ss.; G. ZICCARDI, *La fine della privacy e la svendita dei dati*, in ID., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era della tecnologia*, cit., p. 143 ss.; T. FROSINI, *Liberté Egalité Internet*, Napoli, Editoriale Scientifica, 2015, p. 90 ss., D. BIANCHI, *Difendersi da Internet. Dalla privacy al diritto all'oblio: i nuovi scenari della responsabilità in rete*, Milano, Il Sole 24 Ore, 2014, come pure, E. BERTOLINI, V. LUBELLO, O. POLLICINO, *Internet: regole e tutela dei diritti fondamentali*, Roma, Aracne, 2013, p. 27 ss.

[39] Nel panorama italiano, particolarmente significative, le osservazioni G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Torino, Giappichelli, 2012, p. 64; A. MANTELERO, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali*, in *Il Diritto dell'Informazione e dell'Informatica*, 26, 4-5/2010, pp. 691-692. A livello europeo e internazionale, invece, si vedano SUN MICROSYSTEMS, *Introduction to Cloud Computing Architecture. White Paper*, 2009, p. 29 s. e l'AGENZIA EUROPEA PER LA SICUREZZA DELLE RETI E DELL'INFORMAZIONE (ENISA), *Cloud computing. Benefits, risks and recommendations for information security*, 2012.

[40] Rischi che sono oggetto di dibattito e, sui quali, l'Agenzia per l'Italia Digitale (AgID) – già alcuni anni fa – è intervenuta (cfr. *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione* e alle *Linee guida dell'Agenzia per l'Italia Digitale. Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione*, entrambe del 2012; *Strategia per la crescita digitale 2014-2020* e *Strategia italiana per la banda ultralarga*).

[41] Tanti gli autori che, occupandosi del *cloud*, ne mettono in evidenza i possibili rischi. Fra questi: M. LIMONE, *Cloud computing. Aspetti contrattuali, ri-*

prescindibile ed irrinunciabile volano di cambiamento [42]. Da un altro lato, e quasi specularmente, proprio la privacy, la sicurezza e la responsabilità costituiscono le questioni alle quali il General Data Protection Regulation (GDPR) ha dedicato maggiore attenzione. Ciò anche, e soprattutto, nel rispetto di quanto sancito dall'art. 8 della Carta dei Diritti Fondamentali [43] e dall'art. 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE) [44], che annoverano il diritto alla protezione dei dati di carattere personale fra i diritti fondamentali dei cittadini europei.

4. Il Regolamento (UE) 2016/679. Quali le novità per la nuvola?

Adottato il 27 aprile del 2016 ed entrato in vigore il 25 maggio del medesimo anno, il General Data Protection Regulation

svolti normativi e tutela della privacy, Lecce, Youcanprint, 2018; A. CALDARELLI, L. FERRI, M. MAFFEI, *I rischi derivanti dall'implementazione del cloud computing: un'indagine empirica nelle PMI Italiane*, Milano, Franco Angeli, 2016; M.C. DE VIVO, *Cloud computing. Il contesto giuridico e le aziende di fronte ad un fenomeno controverso*, in *JLIS.it*, vol. 6, n. 2, 2015; G. NOTO LA DIEGA, *Cloud Computing e protezione dei dati nel Web 3.0*, in *http://www.giustiziacivile.it*, 2014; M. LIMONE, *Il contratto di cloud*, in *www.comparazionedirittocivile.it*, 2013.

[42] Molti anche coloro che mettono in luce le potenzialità della nuvola. Si ricordino, ad esempio: F. PIROZZI, *Il cloud computing*, Milano, Giuffrè, 2016; E. PRANDELLI, *Il vantaggio competitivo in rete. Dal Web 2.0 al cloud computing*, Milano, Giuffrè, 2011; A. FERRARI, E. ZANLEONE, *Cloud computing. Aspettative, problemi, progetti e risultati di aziende passate al modello "as a service"*, Milano, Franco Angeli, 2011.

[43] Così, l'art. 8: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

[44] Nel quale può leggersi: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

(GDPR) è pienamente operativo in Italia e in tutti gli altri Stati dell'Unione Europea a decorrere dal 25 maggio del 2018; con significative ricadute in tema di privacy e tutela dei dati personali. Basti notare che nel nostro Paese, a seguito della l. 25 ottobre 2017, n. 163 con la quale il Governo è stato delegato a riordinare e ad adeguare il quadro normativo nazionale a quello europeo, sono state emanate le *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679* (d.lgs. 10 agosto 2018, n. 101). Disposizioni che hanno apportato variazioni di rilievo sia al *Codice in materia di protezione dei dati personali* (d.lgs. 30 giugno 2006, n. 196), sia alle *Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione* (d.lgs. 1° settembre 2011, n. 150) [45].

Va detto subito che, con il GDPR, l'Unione Europea ha voluto porre fine alla previgente situazione di incertezza e di frammentarietà normativa in tema di trattamento, circolazione e condivisione dei dati personali [46], e ha tentato di ovviare alle svariate criticità emerse nel corso di questi anni. Criticità che, come è noto, sono poi culminate nell'annullamento dell'accordo *Safe Harbor* [47] e nell'adozione del *Privacy Shield* [48].

---

[45] A commento della normativa, si veda L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del D. Lgs. 101/2018*, Milano, Giuffrè, 2018.

[46] Basti pensare alla vertenza fra Cambridge Analytica e Facebook (in tema, cfr. D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 20/2018.

[47] Come è noto, l'accordo *Safe Harbor* (letteralmente "approdo sicuro"), in virtù del quale le aziende americane potevano "spostare" i dati personali dei cittadini europei nei server di provider collocati negli Stati Uniti, è stato annullato a seguito dalla menzionata sentenza della Corte di Giustizia Europea del 6 ottobre del 2015. In quella sede, infatti, la Corte ha rilevato l'inadeguatezza di tale accordo a garantire il diritto alla tutela dei dati dei cittadini europei. In commento, si veda: A. Mantelero, *Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo*, in *Diritto dell'Informazione e dell'Informatica*, 4-5/2015, p. 887 ss.; D. Borrelli, *Safe Harbour: gli USA non sono poi così sicuri*, in Inside Marketing, ottobre 2015; O. Pollicino, M. Bassini, *Schrems. La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Roma Tre-Express* (disponibile e on-line al sito *http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/5/5*).

[48] A proposito dell'adozione del Privacy Shield, cfr.: G. Resta, V. Zeno-

Autentico esempio di convergenza normativa sovranazionale, il regolamento europeo per la protezione dei dati concorre in modo davvero significativo alla realizzazione di uno spazio comune di libertà, sicurezza e giustizia [49] all'interno dell'Unione Europea. In particolare, la tutela dei dati personali dei cittadini europei viene rafforzata e parificata, indipendentemente dalla nazionalità e dalla residenza dei soggetti interessati.

Com'è naturale, tale regolamento ha già avuto – e sta via via avendo – delle ricadute determinanti anche sulla nuvola, ridefinendone i parametri di sicurezza e riducendo sensibilmente i rischi connessi alla perdita di controllo delle informazioni e alla c.d. data gravity, ossia alla coagulazione incontrollata dei dati presso i data lake [50].

Il nesso fra il cloud e il GDPR è dunque stretto oltre che decisamente intenso. Si tratta di un legame che nasce dall'attenzio-

---

ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbor principles" al "Privacy Shield"*, Roma, Roma Tre Press, 2016.

[49] Imprescindibile il richiamo agli artt. 3 e 67 del TFUE. Disposizioni in cui, nell'ordine, può leggersi: "L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, che garantisce la libera circolazione delle persone, insieme a misure appropriate in materia di controllo delle frontiere esterne, d'asilo, d'immigrazione, oltre alla prevenzione della criminalità e la lotta contro questo fenomeno" (art. 3, paragrafo 2). "1. L'Unione realizza uno spazio di libertà, sicurezza e giustizia nel rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri. 2. Essa garantisce che non vi siano controlli sulle persone alle frontiere interne e sviluppa una politica comune in materia di asilo, immigrazione e controllo delle frontiere esterne, fondata sulla solidarietà tra Stati membri ed equa nei confronti dei cittadini dei paesi terzi. […] 3. L'Unione si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali. 4. L'Unione facilita l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia civile" (art. 67).

[50] Particolari ambienti di archiviazione dei dati nel loro formato nativo o in copia, quasi perfetta, del loro formato nativo. Tali ambienti semplificano e, al contempo, amplificano le capacità e le possibilità di stoccaggio, gestione e analisi delle informazioni e in particolare dei big data. Non a caso, lo scopo dei data lake è quello di condividere e correlare fra loro ingenti masse di dati.

ne per la tutela dei dati personali – quali diritti fondamentali – e che si estende ai big data. Vale a dire, a quell'incessante proliferare di enormi masse di dati, originate dall'accumulo e dalla ricombinazione, continua e casuale, di tutte quelle tracce digitali e di quelle informazioni granulari che, ogni giorno, inconsapevolmente generiamo [51].

A riprova dell'importanza che il Regolamento 2016/679 riconosce ai dati personali e al loro trattamento, è sufficiente richiamare i considerando iniziali [52]. In essi, infatti, si sottolinea anche che l'evoluzione tecnologica, unita alla sempre condivisione e alla circolazione dei dati, richiede un quadro normativo *adeguato*, *solido*, *coerente* ed *uniforme*, capace di garantire un *effettivo*, ed *eguale*, godimento dei diritti fondamentali in tutti gli Stati membri, in modo che non si possano più dare differenze in ordine alle modalità di trattamento e agli standard di sicurezza [53].

---

[51] Cfr., A.C. Amato Mangiameli, *infra*, *Prima Parte*.

[52] In modo particolare dei punti 2 e 4: "I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche". "Il trattamento dei dati dovrebbe essere al servizio dell'uomo […]".

[53] Così, nell'ordine, i punti 6, 7, 10 e 14: "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. […] Sempre più spesso le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. […]". "Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche". "Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezio-

Oggetto, finalità e ambito di applicazione del nuovo regolamento sono individuati dall'art. 1 [54] e dall'art. 2 [55], mentre i principi che ne compongono l'architrave e che vanno ad incidere in senso proprio sul trattamento e sulla tutela dei dati si ritrovano soprattutto negli artt. 5 e 7.

Nel dettaglio, l'art. 5 stabilisce che il trattamento dei dati deve sempre essere *lecito*, *corretto* e *trasparente*:

"1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato […];
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità […];
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati […];
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati […];
e) conservati in una forma che consenta l'identificazione degli interes-

---

ne dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. […]". "È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. […]".

[54] "1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

[55] "1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. 2. Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse".

sati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato […];
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali […]".

L'art. 7, invece, richiede che il consenso dell'interessato sia sempre *libero*, *specifico*, *informato*, *inequivocabile*, *revocabile* e *non-condizionato* [56]:

"1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. […].
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

Ulteriori, e non trascurabili, conquiste in termini di tutela

[56] Sulla libertà del consenso, cfr. S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e Diritto Privato*, 2/2016, pp. 513-557; ID., *I requisiti al consenso del trattamento dei dati personali*, Santarcangelo di Romagna. Maggioli, 2016.

sono introdotte dagli artt. 17 e 21. L'art. 17 [57], infatti, prevede il c.d. diritto all'oblio, ovvero, il diritto dell'interessato ad ottenere dal titolare del trattamento la cancellazione dei propri dati. Mentre, l'art. 21 sancisce il diritto di opposizione al trattamento dei propri dati, compresa la profilazione.

A queste importanti novità [58], se ne aggiungono delle altre, che comportano ricadute significative soprattutto sulla gestione e sull'erogazione dei servizi cloud, dal momento che impongono specifici oneri in capo ai titolari del trattamento.

In tal senso, senza dubbio significativa è l'introduzione – di cui all'art. 37 [59] – dell'obbligo dei titolari e dei responsabili del

---

[57] Nel quale, si legge: "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: *a*) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; *b*) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; *c*) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; *d*) i dati personali sono stati trattati illecitamente; *e*) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; *f*) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato […] a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

[58] In merito al consenso e ai diritti riconosciuti all'interessato dal Regolamento (UE) 2016/679, cfr., A.C. AMATO MANGIAMELI, *infra*, *Prima Parte*.

[59] Dove, nel paragrafo 1, si legge: "Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: *a*) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; *b*) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure *c*) le attività principali del titolare del trattamento o del responsabile

trattamento di designare un responsabile della protezione dei dati: il *Data Protection Officer* (DPO) a cui è affidato il compito di assicurarne la corretta gestione [60].

Ma non è tutto. Il GDPR ha, infatti, anche stabilito in capo al titolare del trattamento l'onere di adottare tutta una serie di misure tecniche (art. 24) e di accortezze atte a garantire un'efficace e concreta tutela dei dati personali. Fra queste, spiccano la *pseudonimizzazione* (consistente nel ricorso a tecniche di pseudonimia e di cifratura che, in assenza di informazioni aggiuntive, rendono i dati personali non direttamente attribuibili all'interessato) e la *minimizzazione* (volta a limitare le operazioni di trattamento dei dati personali dell'interessato a quelle che sono strettamente necessarie al perseguimento delle finalità del titolare) (art. 25).

Sempre al fine di scongiurare eventuali trasgressioni e di rafforzare la tutela effettiva dei dati personali, il GDPR prescrive la tenuta di appositi registri delle attività di trattamento (art. 30); richiede il rispetto di determinati livelli di sicurezza (art. 32); prevede, da parte del titolare del trattamento, l'obbligo di notifica delle eventuali violazioni all'autorità di controllo (art. 33); stabilisce che il titolare – senza ingiustificato ritardo – debba avvisare l'interessato dell'avvenuta violazione dei dati nel caso in cui si diano dei rischi per i diritti e per le libertà delle persone fisiche (art. 34); incoraggia l'istituzione di meccanismi di certificazione e promuove l'adozione di sigilli e di marchi che garantiscano la conformità dei trattamenti effettuati (art. 42); individua le condizioni e i limiti al trasferimento dei dati personali dei cittadini europei verso i paesi terzi e/o le organizzazioni internazionali [61]. Con-

---

del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. […]".

[60] Sulla figura del DPO, cfr., fra i tanti, G. SATTA, *La nuova figura del Data Protection Officer*, in *Amministrazione e finanza*, 3/2018, pp. 49-54; AIEA, *La figura del Data Protection Officer nel nuovo Regolamento Europeo*, maggio 2017.

[61] In tal senso, l'art. 44 afferma: "Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto

dizioni e limiti, in cui rientra anche la valutazione di adeguatezza (e in certi casi persino l'autorizzazione) della Commissione al trasferimento dei dati [62].

Parecchie, dunque, le novità introdotte dal Regolamento 2016/679. Novità che, come è *ictu oculi* evidente, sono destinate ad avere un riverbero immediato e, almeno ad avviso di chi scrive, alquanto positivo sulla nuvola. Non foss'altro perché, più o meno direttamente, ne elevano i livelli di sicurezza.

5. Un primo bilancio e qualche buona notizia

Tra buone e/o cattive ragioni, censure e difese, rischi e vantaggi, tirare le fila del percorso svolto e abbozzare un primo bilancio degli effetti che il General Data Protection Regulation sta avendo sul cloud non è per nulla semplice. Non soltanto perché il quadro normativo (così come quello dottrinale e giurisprudenziale) è in continuo divenire, ma anche perché – al di là di quelle che sono le attese – il recente regolamento europeo deve ancora sostenere la prova dei fatti. Invero, per quanto i principi sanciti siano senza dubbio promettenti, non è detto che l'adozione del GDPR si dimostri sufficiente ad ovviare a tutte le criticità che, soprattutto negli ultimi anni, si sono registrate in tema di tutela dei dati e di utilizzo della nuvola.

Detto ciò, non si può fare a meno di notare che ci sono dei segnali che lasciano ben sperare in quanto, muovendosi nella direzione tracciata dal regolamento, denotano la concreta volontà di tradurne in pratica i principi. Uno di questi è senza

---

se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

[62] All'art. 45, paragrafo 1, infatti, si legge "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".

dubbio rappresentato dalla nascita del *Cloud Infrastructure Services Providers in Europe* (CISPE): una coalizione alla quale – conformemente all'art. 40 del GDPR [63] – hanno aderito i provider di sedici Stati membri [64]. Coalizione alla quale, si deve l'adozione del primo codice di condotta dei fornitori dei servizi cloud.

Vari i meriti del codice CISPE: non solo offre risposte concrete alle esigenze e alle istanze degli utenti, ma chiarisce anche le ripartizioni di responsabilità tra cliente e provider, assicura un determinato livello di trasparenza, soddisfa i requisiti di adeguatezza richiesti, individua un marchio di conformità agli standard di sicurezza, consente il controllo della collocazione dei dati – scongiurando, fra le altre cose, il pericolo che il gestore li riutilizzi o li rivenda a terzi – e, ancora, utilizza una connessione sicura *end-to-end* e si avvale della crittografia Advanced Encryption Standard (AES).

Al CISPE, di recente, si è aggiunto anche un altro importante segnale positivo, che testimonia la volontà di dare seguito al GDPR e di permettere un uso più consapevole e soprattutto più sicuro del cloud. Si tratta della costituzione del nuovo Comitato per la Protezione dei Dati (EDPB) [65], che ha sostituito il Working Party art. 29. L'EDPB ha fondamentale, e delicatissimo, compito di vigilare sulla corretta applicazione del Regolamento europeo da parte delle Autorità nazionali.

Ed è proprio all'EDPB che si debbono, ad esempio, le *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b)*

---

[63] Che, così, recita: "Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese".

[64] Fra i provider CISPE: *Arsys, Art of Automation, Aruba, BIT, Daticum, Dominion, Fasthosts, FjordIT, Gigas, Hetzner Online, Home, Host Europe Group, IDS, Ikoula, LeaseWeb, Lomaco, Outscale, OVH, Seeweb, Solidhost, UpCloud, VTX, XXL Webhosting, 1&1 Internet*.

[65] Organo europeo indipendente, l'EDPB contribuisce all'applicazione coerente delle norme sulla protezione dei dati all'interno dell'Unione e promuove la cooperazione tra le autorità competenti in materia di protezione dei dati. L'EDPB è composto dai rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (cfr. https://edpb.europa.eu/about-edpb/about-edpb_it).

GDPR in the context of the provision of online services to data subjects [66], come pure le successive *Guidelines 3/2019 on processing of personal data through video devices*, volte proprio a adeguare il trattamento dei dati alle disposizioni del GDPR.

[66] Cfr. F. PIZZETTI, *GDPR, tutela della concorrenza e dei consumatori: le linee guida EDPB sui servizi online*, in *Agenda Digitale*, 03 maggio 2019 (articolo disponibile online: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-tutela-della-concorrenza-e-dei-consumatori-le-linee-guida-edpb-sui-servizi-online/).

II

NUOVI MEDIA: I SOCIAL NETWORK

Sommario

1. Brevi cenni introduttivi

Muovo da alcune singolari *breadcrumbs* [1] fotografiche. Immagini che, con eloquenza ed efficacia, danno l'idea dell'impatto che la diffusione dei social network ha avuto – e sta avendo – sulle nostre vite: modificando le abitudini [2], trasformando gli atteggiamenti [3], alterando i linguaggi e ridisegnan-

[1] Mi avvalgo di questa singolare espressione (ultimamente sempre più usata nel campo dell'informatica), che indica sia le "tracce" lasciate dagli utenti, sia i link inseriti all'interno dei menu dei siti e/o delle pagine web per favorire la navigazione.

[2] Sugli effetti dei social network, particolarmente significative le osservazioni di G. LOVINK che, con l'acume che lo contraddistingue e senza sfociare nel pessimismo, invita ad un approccio critico (*Ossessioni collettive. Critica dei social media*, trad. it., Milano, Università Bocconi, 2012; ID., *Nichilismo digitale. L'altra faccia delle piattaforme*, trad. it., Milano, Università Bocconi, 2019). Ben diversa è la posizione di J. LANIER che, invece, prospetta una critica assai più aspra e perentoria (*Dieci ragioni per cancellare subito i tuoi account social*, trad. it., Milano, Il Saggiatore, 2018).

[3] In merito alle ripercussioni che i social hanno sui nostri comportamenti, inducendoci a gesti e approcci inconsueti, interessanti gli studi di P. WALLACE, *La psicologia in internet*, trad. it., Milano, Raffaello Cortina, 2017.

do le interazioni e le relazioni [4].

i) Una prima indicazione proviene da *Removed Social* [5], l'originale progetto realizzato, nel 2012, dall'americano Eric Pickersgill, che illustra con lucida ironia la solitudine e l'isolamento di chi è iperconnesso. Removed Social propone una nutrita photo-gallery nella quale sono ritratte scene di vita quotidiana: persone attorno ad un tavolo, sul divano, in salotto, in barca, in poltrona, a letto, dal barbiere, alla guida e perfino al cimitero. Tutti frangenti che, solitamente, vengono vissuti con lo smartphone (o con un qualunque altro device) a portata di mano [6]. Pur nella varietà delle scene e nella diversità dei contesti e dei soggetti, in ogni foto si rinviene un denominatore comune: il dispositivo elettronico del caso non compare, è stato infatti rimosso. Scelta che simboleggia l'invettiva di Pickersgill contro l'uso smodato dei tools digitali e della mania di essere connessi alla Rete in ogni momento della nostra giornata. Fra le raffigurazioni più significative: quella che immortala due novelli sposi appoggiati al cofano di un'autovettura bardata per l'occasione: lo sposo da un lato, la sposa dall'altro. Entrambi mimano l'atteggiamento di chi è intento a controllare il proprio smartphone. Il paradosso è evidente: i due sono *appena sposati* (come è scritto sul cartello affisso alla vettura) eppure si comportano come se fossero *già separati* [7].

---

[4] E proprio a proposito della perdita della capacità di conversare "faccia a faccia" e dei diversi risvolti patologici dei social, come la dissociazione psichica o la riduzione delle capacità emotive e affettive, particolarmente interessante la ricostruzione di S. TURKLE (*La conversazione necessaria. La forza del dialogo nell'era digitale*, trad. it., Torino, Einaudi, 2016).

[5] Cfr. *https://www.ericpickersgill.com/removed*.

[6] Tendenza, questa, che è stata confermata anche da D. MEREDITH e R. JAMES. In particolare, secondo i ricercatori della Baylor University, stiamo assistendo ad una preoccupante inversione di prospettiva. Anziché pensare ai social come ad un elemento di distrazione dalla vita reale, accusiamo la vita reale di distoglierci dalla frequentazione dei social network (*My life has become a major distraction from my cell phone: Partner phubbing and relationship satisfaction among romantic partners*, in *Computers in Human Behavior*, 54, 2016, pp. 134-141).

[7] Guardando l'immagine, potremmo dire – con TURKLE – che i due sposi sono insieme ma soli. Cosa che, è ovvio, non ci si aspetta, soprattutto da due novelli sposi (*Insieme ma soli. Perché ci aspettiamo sempre più dalla tecnologia e sempre meno dagli altri*, trad. it., Torino, Einaudi, 2019).

ii) Un secondo spunto è fornito dallo stravagante ritratto, a firma di Oliviero Toscani, che è apparso su *Elle Man France* nell'aprile del 2014 [8]. La fotografia – che come vuole lo stile dell'artista è spregiudicata, irriverente e provocatoria – ritrae un ragazzo e una ragazza distesi su un letto e completamente nudi. Sensualità e imbarazzo sono, però, scongiurati dalla presenza dei dispositivi tecnologici, che dominano il campo visivo e polarizzano l'attenzione dello spettatore. La ragazza regge in grembo un pc e indossa delle vistose cuffie, mentre il ragazzo tiene in mano uno smartphone collegato a degli auricolari. Il contrasto è particolarmente forte. Al contesto e alla mancanza di indumenti (che di per se stessi presupporrebbero una certa confidenza ed intimità tra i due) fa da contraltare l'assenza di ogni forma di prossimità, di contatto e/o di comunicazione.

iii) Una terza occasione di riflessione, infine, è suggerita da *Sur-Fake* [9]. La serie di scatti realizzati dal fotografo francese Antoine Geiger nel 2015, dove a venir meno sono addirittura i volti, attratti e letteralmente risucchiati dallo smartphone. Professionisti che vanno al lavoro, giovani che si fanno un selfie, persone che camminano, che sono in bicicletta o che si trovano nel bel mezzo di una mostra, da un'immagine all'altra, cambiano le situazioni ma la scena in sé è la medesima. I soggetti ritratti hanno sempre la stessa postura: tengono la testa china e hanno in mano un dispositivo che catalizza il loro interesse e che attrae e inghiotte il loro volto.

Fotografie *della* e *dalla* realtà, quelle realizzate da Pickersgill, da Toscani e da Geiger. Suggestioni distinte eppure concordi che – oltre ad essere particolarmente intense, disincantate e, a tratti, persino crude – hanno il pregio di cogliere e di mettere bene in evidenza alcuni dei nodi critici attorno ai quali orbita l'attenzione degli scienziati della Rete e di chi, a vario

---

[8] Nel dettaglio, la fotografia alla quale rinvio corredava il dossier di J. LEUIL, *Ce que le porno nous apprend*.

[9] Tutte le immagini sono pubblicate online sul sito del fotografo all'indirizzo *https://antoinegeiger.com/SUR-FAKE*. È interessante ricordare che il progetto *Sur-fake* – in cui, per l'appunto, i volti vengono risucchiati dal cellulare è stato anticipato da un lavoro di senso "opposto": *Sur-face*, che, invece di risucchiarli, nascondeva i volti delle persone sotto una specie di cono.

titolo, si interessa allo studio dei social e dei loro tanti riverberi (informatici, sociologi, filosofi, psicologi, matematici, ingegneri sociali, giuristi ed economisti). Ripercorrendo l'ordine delle immagini, possiamo, così, sintetizzare gli aspetti salienti messi a fuoco.

i) *I social network sono parte integrante della nostra quotidianità*. È un dato di fatto. Abbiamo sviluppato un'abitudine compulsiva, una vera e propria ossessione, quella di avere lo smartphone sempre con noi e di controllarlo di continuo. Per la precisione – stando al documentario *It's people like us* [10] – lo controlliamo in media circa centocinquanta volte al giorno, in pratica, ogni sette minuti [11]. Inseparabile protesi, sempre connessa alla Rete e ai social, lo smartphone è come una finestra alla quale ci affacciamo ogniqualvolta ne sentiamo l'esigenza (per pubblicare un contenuto, per aggiornare e/o modificare il nostro stato, oppure, semplicemente, per distrarci curiosando fra i profili e le pagine altrui). Il rovescio della medaglia – come nota Manfred Spitzer – è che quando i nostri device non sono con noi, o quando non abbiamo la possibilità di connetterci alla Rete, "ci sentiamo come un insetto girato sulla schiena, che dimena impotente le zampe, del tutto inutilmente" [12].

ii) *I social network comportano una riconfigurazione profonda*

---

[10] Realizzato dalla regista australiana premio Oscar Eva Orner, e presentato a Melburne il 21 settembre 2017, Il documentario segue la giornata di cinque australiani, filmandone gli atteggiamenti. Presi dalla smania di controllare il cellulare in qualsiasi momento, anche quando sono alla guida, i protagonisti non si avvedono nemmeno dei rischi ai quali espongono la loro incolumità e quella degli altri. Il filmato integrale è disponibile in streaming al seguente indirizzo: *http://www.itspeoplelikeus.com.au*.

[11] Sull'uso (e sull'abuso) dello smartphone, merita d'esser menzionata la campagna di informazione dal titolo *Il tuo cellulare è intelligente usalo con intelligenza* avviata – dal Ministero della Salute, Ministero dell'Ambiente, Ministero della Tutela del Territorio e del Mare, Ministero dell'Istruzione, Ministero dell'Università e della Ricerca – il 19 luglio 2019. Iniziativa, adottata in ottemperanza alla sentenza n. 500/2019 del TAR del Lazio, che mira ad incentivare l'adozione di corrette modalità di utilizzo dei dispositivi telefonici e a sensibilizzare la popolazione (e in special modo i più giovani) sulle ripercussioni che un utilizzo improprio del cellulare può avere sulla salute e sull'ambiente (cfr. *www.salute.cellulari.gov.it*).

[12] *Solitudine digitale. Disadattati, isolati, capaci solo di una vita virtuale?*, trad. it., Milano, Corbaccio, 2017, p. 15.

della comunicazione e delle relazioni [13]. La perdita dell'interazione vis-à-vis – nella quale sia io che l'altro siamo il nostro corpo – ed il passaggio ad una comunicazione in cui l'oggettività del corpo è assente e il soggetto-comunicante è ridotto al contenuto del suo messaggio, infatti, porta con sé tutta una serie di ripercussioni sulla sfera emotiva [14]. Ciò che ne consegue, è il possibile sviluppo di dipendenze [15] e anche di vere e proprie patologie [16]. Fra le più recenti e allarmanti, senza dubbio, la c.d. *sindrome da ritiro sociale*, meglio nota come sindrome da *hikikomori*. Una situazione patologica che coinvolge soprattutto i più giovani (ne sono colpiti prevalentemente gli adolescenti) e che prevede l'azzeramento delle relazioni sociali e il ritrarsi del soggetto fra le mura domestiche, dove resta letteralmente incollato ad uno schermo anche per diciotto ore filate [17]. Isolato dalla società, l'hikikomori è un *Neet* (ossia uno di quei giovani "*neither in employment nor in education or training*"), immerso nel *mondo manga* [18] o prigio-

---

[13] G. RIVA, *I social network*, Bologna, Il Mulino, 2016, in part. p. 27.

[14] Basti pensare che – come sottolineato da GOLEMAN – l'intelligenza emotiva si sviluppa grazie alla capacità di intravedere e di cogliere le emozioni e i sentimenti degli altri. Una capacità, questa, che – come è evidente – i social network affievoliscono e riducono molto (cfr. D. GOLEMAN, *Intelligenza emotiva*, trad. it., Milano, BUR, 1995).

[15] Sul punto, K.S. YOUNG, *Internet Addiction: Symptoms, Evaluation, And Treatment*, in L. VANDE CREEK, T. JACKSON (eds.), *Innovations in Clinical Practice*, 17, Hawthorne, Professional Resource Exchange, 1999, pp. 19-31. Inoltre, per un agile approfondimento cfr. S. BERNARDI, S. PALLANTI, *Internet addiction. A descriptive clinical study focusing on comorbidities and dissociative symptoms*, in *Comprehensive Psychiatry*, 50, 2009, pp. 510-516; T. CANTELMI, *IAD. La nuova dipendenza patologia da Internet*, in Fatto&Diritto, aprile 2014; come pure, A. MONTANO, A. VALZANIA, *Dipendenza da Internet*, Roma, Istituto A.T. Beck, 2018.

[16] Fra le patologie: 1) la *nomofobia* (che sta per "*no mobile fobia*") e indica la paura di rimanere senza smartphone e senza connessione mobile; 2) la *fomo* (ossia "*fear of mission out*") e, dunque, la paura di perdersi qualcosa, qualche notizia, qualche post e – in breve – di essere "tagliato fuori" da ciò che accade in Rete e nei social.

[17] Cfr., fra gli altri, C. RICCI, *Hikikomori: adolescenti in volontaria reclusione*, Milano, Franco Angeli, 2017; M.R. PARSI, M. CAMPANELLA, *Generazione H. Comprendere e riconnettersi con gli adolescenti sperduti nel web tra Blue whale, Hikikomori e sexting*, Milano, Piemme, 2017.

[18] In merito alla stretta relazione fra giovani affetti dalla sindrome di hikikomori e fumetti manga (A.M. CARESTA, *Generazione hikikomori. Isolarsi dal mondo, fra web e manga*, Roma, Castelvecchi, 2018).

niero delle *virtual communities* [19].

iii) *I social network ci permettono di scegliere come vogliamo apparire agli occhi degli altri, consentendoci di avere il profilo e le parvenze che più ci piacciono*. Disincarnati e svincolati dalla dimensione fisica, siamo – come afferma Sherry Turkle – ciò che appare sullo schermo [20] o, meglio, "ciò che le nostre dita fanno trapelare di noi attraverso lo schermo" [21]. Sempre in divenire, fluida e pronta ad essere ridisegnata quando vogliamo la nostra identità online, è un'identità che però, non sempre rispecchia fedelmente la realtà e che – come ci avverte a suo modo Antoine Geiger – può anche venirci sottratta assieme alle informazioni che ci riguardano [22].

Tre snodi importanti, questi, sui quali si avrà modo di ritornare nel corso della trattazione.

2. Origini

La storia dei social network assomiglia ad una parabola dall'ascesa rapida ed intensa. Per quanto veloce e significativa, però,

---

[19] In generale, a proposito delle comunità virtuali, meritano d'esser qui ricordate le parole di RHEINGOLD: "[…] c'è sempre qualcun altro là. È come essere in un bar, circondato dai soliti vecchi amici e da nuove presenze, molto simpatiche; al posto di mettermi, però, in giacca, spegnere il computer e camminare verso l'angolo, mi basta accendere il mio modem e essi sono là" (H. RHEINGOLD, *Comunità virtuali: parlare, incontrarsi, vivere nel ciberspazio*, trad. it., Milano, Sperling & Kupfer, 1994, p. 24).

[20] Cfr. S. TURKLE, *Crisi d'identità*, in ID., *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, trad. it., Milano, Feltrinelli, 1997, pp. 307-325.

[21] Così, G. PRAVETTONI, *Web Psycology*, Milano, Guerini e associati, 2002, in part. p. 46.

[22] In merito all'utilizzo che i social fanno delle informazioni che ci riguardano, TALIA osserva: "tutti o quasi usiamo quei servizi senza chiederci come mai siano gratuiti, come mai questi colossi informatici regalino tutto questo. […] le monete con cui paghiamo […] [sono] le informazioni". Informazioni che, ad esempio, una volta tratte dai network, possono poi essere utilizzate per formulare proposte commerciali *ad hoc*. Emblematico l'*anticipatory shipping* proposto da Amazon (D. TALIA, *La società globale e i big data. Algoritmi e persone nel mondo digitale*, Soveria Mannelli, Rubettino, 2018, in part. pp. 47-49 e pp. 25 e 26).

si tratta di una storia relativamente recente, che trae avvio dalla convergenza sinergica di due fattori, reciprocamente collegati. Vale a dire: *a*) la diffusione del computer e la sua trasformazione da strumento per eseguire calcoli a strumento di scrittura (prima) e di comunicazione (poi); *b*) l'avvento, nel 1991, del World Wide Web [23], che – a detta del suo ideatore Tim Benrers-Lee – più che un'innovazione tecnologica, avrebbe dovuto rappresentare un'innovazione sociale, destinata ad aiutare le persone a comunicare e a migliorare la loro esistenza reticolare nel mondo [24].

Diversamente da quanto si potrebbe pensare, quindi, la primissima tappa dello sviluppo e dell'evoluzione dei nuovi network non si colloca nel 1997 – anno in cui si assiste alla comparsa della piattaforma *SixDegrees.com* [25] – ma risale a qualche anno prima. È, infatti, concomitante all'invenzione del Web o – mutuando le parole di Manuel Castells – di quel nuovo ambiente di interazione e di condivisione delle informazioni che è la *Galassia Internet* [26]. Il perché è presto detto. Internet ha ampliato e

---

[23] È interessante ricordare che – sebbene sia nato ufficialmente il 6 aprile del 1991 presso il *CERN* di Ginevra – il Web è stato anticipato da una (più rudimentale) versione precedente: *ARPANET*. Realizzata a partire dal 1969 dalla *DARPA* (*Defence Advanced Research Projetcs Agency*) ARPANET aveva lo scopo di collegare centri di calcolo e terminali di Università, Laboratori di ricerca ed Enti militari.

[24] T. BERNERS LEE, *L'architettura del nuovo web. Dall'inventore della rete il progetto di una comunicazione democratica, interattiva e intercreativa*, trad. it., Milano, Feltrinelli, 2001, in part. p. 113.

[25] Creato nel 1997 da Andrew Weinreich e attivo sino al 2001, anno in cui è stato chiuso per carenza di fondi, *SixDegrees.com* è considerato da molti come l'antenato di *Facebook*. Nel dettaglio, si trattava di un sito di incontri che – a partire dalla nota teoria dei *sei gradi di separazione* formulata, per la prima volta, nel 1929 dallo scrittore ungherese Frigyes Karinthy – consentiva ai suoi utenti di stringere amicizia solo con coloro i quali erano distanti al massimo tre gradi di separazione e, dunque, solo con *gli amici degli amici degli amici*. Singolare restrizione che era volta a permettere di: a) verificare la veridicità delle notizie pubblicate sui profili; b) di ottenere informazioni indirette; c) favorire i contatti fra persone provenienti da analoghi contesti socio-culturali. (Cfr., fra gli altri, A. MARION, O. OMOTAYO, *Development of a Social Networking Site with a Networked Library and Conference Chat*, in *Journal of Emerging Trends in Computing and Information Sciences*, 2, 8/2011, pp. 396-401). Circa la teoria dei sei gradi di separazione e – in particolar modo – dei "mondi piccoli", cfr. A.L. BARÁBASI, *Link. La scienza delle reti*, trad. it., Torino, Einaudi, 2004.

[26] "Internet è la trama delle nostre vite. Se la tecnologia dell'informazio-

stravolto l'uso e le funzioni del computer, convertendolo in un mezzo di comunicazione di massa o, più correttamente, in un nuovo *medium* [27]. Ovverosia, in uno strumento che – superando i limiti spazio-temporali e interponendosi fra gli interlocutori – trasforma l'interazione da *esperienza diretta* dell'Altro ad *esperienza indiretta* (poiché, per l'appunto, mediata) [28].

Affinché i social network potessero fare la loro comparsa è stato, però, necessario un ulteriore e fondamentale passaggio. Dal Web (Web 1.0) – e dunque da un'interfaccia che consentiva di trasmettere lo stesso messaggio ad un consistente numero di riceventi, ma nella quale l'accesso alla produzione comunicativa era riservato a pochi e, in generale, a quegli stessi colossi che già controllavano l'editoria, la radio o la televisione [29] – si è dovuti passare al Web 2.0 [30]. Vale a dire, ad un ambiente digitale ancor

---

ne è l'equivalente odierno dell'elettricità nell'era industriale, Internet potrebbe essere paragonata sia alla rete elettronica sia al motore elettrico, grazie alla sua capacità di distribuire la potenza dell'informazione in tutti i campi dell'attività umana. […] Internet è la base tecnologica della forma organizzativa nell'età dell'informazione: è il network" (M. CASTELLS, *Galassia internet*, trad. it., Milano, Feltrinelli, 2010, p. 13). Sull'affermazione dei nuovi network come forma dominante di organizzazione sociale, cfr. anche B. WELLMAN, *Phisical place and cyberplace: the rise of networked individualism*, in "*International Journal of Urban and Regional Research*", 1/2001, p. 1.

[27] A proposito della *comunicazione mediata dal computer* (CMC), cfr. R. STELLA, C. RIVA, C.M. SCARCELLI, M. DRUSIAN, *Sociologia dei New Media*, Novara, De Agostini Scuola, 2014, in part. pp. 31-33.

[28] In merito ai riverberi dei media sulla comunicazione, cfr. G. RIVA, C. GALIMBERTI, G. MANTOVANI, *La comunicazione virtuale: un'analisi del legame tra psicologia sociale e nuovi ambienti di comunicazione*, in A. QUADRIO, L. VENINI (a cura di), *La comunicazione nei processi sociali e organizzativi*, Milano, Franco Angeli, 1997; G. RIVA, *Web usability revisited. A situated approach*, in *PsychNology Journal*, 1/2003, pp. 18-27; L. PACCAGNELLA, *La comunicazione al computer. Sociologia delle reti telematiche*, Bologna, Il Mulino, 2000; ID., Sociologia della comunicazione, Bologna, Il Mulino, 2010; A. MICONI, *Teorie e pratiche del Web*, Bologna, Il Mulino, 2014.

[29] Nel Web "[…] la massa dei soggetti riceventi non ha la possibilità di influenzare le caratteristiche e i contenuti dei messaggi trasmessi, che sono invece definiti da un élite di professionisti, spesso sotto il controllo diretto o indiretto del potere politico ed economico" (così, G. RIVA, *I social network*, cit., p 56).

[30] Val la pena ricordare che il termine Web 2.0 si deve alla casa editrice americana O'Reilly Media (fondata da Tim O'Reilly) che, nel 2004, scelse l'espressione "Web 2.0" come titolo per una serie di conferenze dedicate alla "nuova generazione" dei servizi Internet.

più aperto, nel quale ogni utente, oltre alla possibilità di accedere alle informazioni e ai contenuti, avesse anche quella di crearne e diffonderne di nuovi.

Con il Web 2.0 (web *partecipativo*), difatti, chiunque abbia accesso alla Rete e alle piattaforme social può – *ipso facto* – realizzare e pubblicare testi, immagini, audio e video, rendendoli visibili agli altri utenti che, oltre a guardarli e a commentarli, possono anche condividerli e divulgarli a loro volta. Altrimenti detto, se con il Web 1.0 ci trovavamo ancora di fronte ad un mezzo di comunicazione di massa (ossia rivolto alla massa), che presentava parecchie limitazioni nell'accesso alla creazione e alla divulgazione dei contenuti, con il Web 2.0 queste limitazioni vengono meno.

È, così, che si assiste al profilarsi dei social network: piattaforme che possono assolvere a diverse funzioni e che fungono anche da mezzi di comunicazione *di* e *per* la massa [31]. E cioè, media che si *rivolgono alla* massa e che *sono a disposizione della* massa: con i quali quest'ultima comunica e – a seconda dei casi e delle situazioni – diffonde informazioni e notizie. Nuovi vettori che sono alla portata di chiunque abbia accesso ad Internet e ai tantissimi social che, in questi anni, sono nati. Un elenco in continua crescita [32] di cui YouTube, Facebook, Instagram, Pinterest, Linkdln, Twitter, Skype, Messenger, Viber, Telegram, Signal, Snapchat e WhatsApp sono soltanto alcuni dei più noti e diffusi.

Figli di Internet e dell'evoluzione della sua interfaccia resa possibile grazie al Web 2.0 e alle app, i social network non ci permettono soltanto di condividere esperienze, sentimenti, pun-

---

[31] Sulla differenza fra mezzi di massa e mezzi per le masse con particolare riferimento alla responsabilità del provider, cfr. G. SARACENI, *I reati informatici. Dalla diffusione di virus all'accesso abusivo*, in A.C. AMATO MANGIAMELI, G. SARACENI, *I reati informatici. Elementi di teoria generale e principali fattispecie criminose*, Torino 2019, in part., p. 105.

[32] Stando alle più recenti indagini pare che, ad oggi, in Rete siano disponibili all'incirca duecentocinquanta piattaforme social differenti. Con specifico riferimento all'Italia, poi, è interessante ricordare che – stando ai risultati dell'indagine *We are social* del gennaio del 2019 – il numero degli utenti attivi sui social si attesta attorno ai 35mln, pari al 59% della popolazione totale. La classifica dei social network più usati dagli italiani, inoltre, vede in testa YouTube, seguito da WhatsApp, Facebook, Instagram e Messenger, mentre Skype si attesta soltanto all'ottava posizione (l'indagine di cui si riportano qui sommariamente gli esiti è disponibile online all'indirizzo: *https://wearesocial.com/it/digital-2019-italia*).

ti di vista e stati d'animo – come in una sorta di diario aperto alla lettura degli altri utenti [33] – ma ci consentono anche di raggiungere un triplice risultato:

– quello di avere un ruolo attivo-creativo nella definizione della nostra identità sociale (cioè della nostra posizione nell'ambito del network e/o del gruppo di cui facciamo parte) [34];

– quello di poter visionare, monitorare e controllare i profili altrui [35];

– e, infine, quello di estendere la nostra rete sociale, ad esempio, ampliando il numero dei nostri amici (nel caso di Facebook), dei nostri followers (in quello di Twitter) degli iscritti (nel caso di YouTube), oppure delle persone collegate e in contatto (nel caso di Linkdln).

Tutto ciò, nell'ambito del cyberspazio [36] (quel particolare ambiente virtuale e interattivo che Geert Lovink definisce *spazio tecnosociale* [37]) e sullo sfondo di continue e vorticose trasformazioni che, passando per il Web 3.0 (web *semantico* [38]), sembrano averci già proiettato verso altri ed ulteriori scenari.

---

[33] È il caso di Facebook. Nota con singolare efficacia ed ironia SCRIMA: "La frase con cui Facebook ci accoglie ogni volta che ci connettiamo è 'A cosa stai pensando?'. E noi, lusingati da cotanta attenzione, gli confidiamo tutto, anche i segreti più intimi – che smettono così di esserlo" (S. SCRIMA, *Socrate su Facebook. Istruzioni filosofiche per non rimanere intrappolati nella rete*, Roma, Castelvecchi, 2018, p. 10)

[34] È interessante sottolineare che – da questo punto di vista – i social network si rifanno alla c.d. *Teoria dell'identità sociale* (*Social Identity Theory*) elaborata, a partire dagli anni Settanta, da Tajfel e Turner (cfr. H. TAJFEL, J.C. TURNER, *An integrative theory of intergroup conflict. The social psychology of intergroup relations?*, in W.G. AUSTIN, S. WORCHEL (ed.), *The Social Psychology of Intergroup Relations*, Monterey, Brooks/Cole Pub, 1979, pp. 33-47).

[35] Cfr. quanto osservato da G. RIVA, *I social network*, cit., p. 13.

[36] Sul *cyberspazio*, sulle caratteristiche che lo individuano (de-territorializzazione e de-centralizzazione) e sulle nuove relazioni che si generano al suo interno (tribù virtuali e agorà digitali), d'obbligo il rinvio alle osservazioni di A.C. AMATO MANGIAMELI, *infra*, *Prima Parte*.

[37] Vd. G. LOVINK, *Nichilismo digitale*, cit., p. X.

[38] Fase che implica la trasformazione del World Wide Web in una sorta di database dove i documenti pubblicati vengono associati ad informazioni e dati (metadati) che ne specificano il contesto semantico. Cfr., fra gli altri, V. ELETTI, *Complessità, cambiamento, comunicazioni. Dai social network al web 3.0*, Rimini, Guaraldi, 2012.

È il caso dell'attuale Web 4.0 (web della *realtà aumentata* e dei *big data* [39]) e dell'imminente Web 5.0 [40] (il cosiddetto web *emotivo*). Uno spazio basato sull'interazione uomo-macchina/uomo-IA, del quale *R.E.A.D. System* (presentato al "CES" di Las Vegas nel gennaio del 2019 [41]), gli esoscheletri, i droni e i robot-chirurghi (recentemente mostrati al "World Robot Conference" [42] di Pechino) ci offrono già qualche affascinante anticipazione [43]

3. Definizione, struttura, *appeal*

Reti informazionali alimentate da Internet e basate sui nuovi media, i social network sono piattaforme che consentono all'utente di scegliere e di gestire la propria identità e la propria rete sociale [44]. Piattaforme che, grazie alla loro intrinseca flessibilità

---

[39] Cfr. L. MONTAGNA, *Realtà virtuale e realtà aumentata. Nuovi media per nuovi scenari di business*, Milano, Hoepli, 2018; F. ALMEIDA, *Concept and Dimensions of Web 4.0*, in *International journal of Computers and Technology*, novembre 2017, pp. 7040-7046; N. CHOUDHURY, *World Wide Web and Its Journey from Web 1.0 to Web 4.0*, in *International Journal of Computer Science and Information Technologies*, 2014, pp. 8096-8100.

[40] Cfr. K. PATEL, *Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0*, in *International Journal of Advanced Research in Computer Science and Software Engineering*, ottobre 2013, pp. 410-417).

[41] Proposto da KIA, il *R.E.A.D. System* è un prototipo di "guida emotiva" e "adattiva", grazie alla quale il veicolo è in grado di "leggere" le emozioni del pilota e dei passeggeri, adattando così le condizioni di guida e l'habitat interno all'abitacolo.

[42] Per una più dettagliata descrizione delle novità presentate nel corso dell'evento – svoltosi dal 20 al 25 agosto 2019 – rinvio al sito ufficiale *http://en.worldrobotconference.com*.

[43] Nonostante tali "anteprime" testimonino gli enormi passi in avanti fatti nel campo della robotica e della domotica – secondo l'autorevole parere di FAGGIN (fisico al quale si deve l'invenzione del microprocessore e del touchscreen) – l'IA sembra essere ancora molto lontana dall'eguagliare il ragionamento umano (F. FAGGIN, *Silicio. Dall'invenzione del microprocessore alla nuova scienza della consapevolezza*, Milano, Tecniche Nuove, 2019).

[44] "*We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*" (D.M. BOYD, N.B. ELLISON, *Social network sites. Definition, history, and scholarship*, in "*Journal of Computer-Mediated Communications*", 13, 1/2007, pp. 210-230, in part. 211).

e adattabilità, comportano parecchi vantaggi sotto il profilo organizzativo [45], ma che, al contempo, modificando radicalmente il nostro modo di comunicare, determinano anche una trasformazione (e, per certi versi, una vera e propria rivoluzione) sul piano antropologico [46].

Indissolubilmente legati all'avvento della digitalizzazione (e, cioè, al passaggio dalla rappresentazione analogica-continua [47] a quella digitale-discontinua [48] e alla successiva codifica delle informazioni [49]), i social network si contraddistinguono per la presenza di alcune particolari caratteristiche strutturali, quali:

a) la *modularità*, ossia la possibilità di scomporre tutti i contenuti in moduli dotati di un'identità distinta e separata rispetto all'oggetto di cui fanno parte. È il caso dei pixel di un'immagine, dell'audio di un filmato o degli script di una pagina web. In pratica, ciascun modulo può essere cambiato, sostituito, unito ad altri oppure estrapolato e riutilizzato. Si pensi alla possibilità di scaricare un'immagine da un sito per poi inserirla nell'ambito di un altro contesto o di un altro sito [50];

---

[45] Ed "è per questa ragione che stanno proliferando in tutti i campi dell'economia e della società, superando nella competizione e nelle prestazioni le imprese organizzate verticalmente e le burocrazie centralizzate" (M. CASTELLS, *Galassia Internet*, cit., p. 13).

[46] "La comunicazione consapevole (il linguaggio umano) è ciò che determina la specificità biologica della specie. Dato che la nostra attività è basata sulla comunicazione e Internet trasforma il nostro modo di comunicare, le nostre vite sono segnate profondamente da questa nuova tecnologia di comunicazione […]" (*ivi*, p. 16).

[47] Un tipico esempio di rappresentazione analogica è costituito dall'orologio automatico, all'interno del quale lo scorrere del tempo viene descritto dal movimento continuo della lancetta dei secondi sul quadrante.

[48] Paradigmatico della rappresentazione digitale è, invece, l'orologio a cristalli liquidi, dove il passare del tempo viene descritto in maniera discontinua (o discreta) dalla successione di scatti che determina l'avanzamento dei numeri.

[49] La codifica delle informazioni – e, dunque, la loro traduzione in forma codice binario (0/1, spento/acceso) e, successivamente, in algoritmi – costituisce un passaggio imprescindibile per consentirne l'elaborazione da parte dei microprocessori, che, per l'appunto, sono in grado di elaborare solo informazioni digitalizzate e rese discrete. Per un ulteriore e più approfondita analisi rinvio a A.C. AMATO MANGIAMELI, *Tra leggi del pensiero e linguaggio giuridico*, in ID., *Informatica giuridica*, cit., pp. 89-165, in part. pp. 127-134.

[50] Vantaggio, ma anche pericolo, in quanto talvolta la modularità può anche aprire il varco a violazioni del diritto d'autore. Aspetto particolarmen-

b) la *variabilità*, ovvero, la facoltà di modificare a piacimento tutti i contenuti multimediali. Emblematiche le variazioni che si possono apportare alle fotografie: da un'unica immagine iniziale, infatti, se ne possono ricavare parecchie semplicemente applicando dei filtri, ritagliandone delle parti, oppure ricorrendo a programmi come photoshop;

c) l'*interattività*, caratteristica connessa all'ipertestualità, grazie alla quale il lettore può interagire con l'autore, in un continuo scambio di ruoli [51]. Basti pensare al funzionamento di Wikipedia, basata proprio su di un costante "passaggio di testimone" tra chi scrive e chi legge;

d) l'*automazione*, grazie alla quale alcune operazioni possono essere svolte in maniera automatica. Paradigmatiche alcune applicazioni ludiche di Facebook, come Farmville e Bubble Island, che seguitano a funzionare anche quando l'utente non è connesso.

Alla modularità, alla variabilità, all'interattività e all'automazione, si aggiungono altresì:

e) lo *spazio virtuale* all'interno del quale gli utenti possono costruire e mostrare il proprio profilo, visibile agli altri;

---

te delicato sul quale si segnala la *Risoluzione del Parlamento europeo del 26 marzo 2019 sulla proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale (COM(2016)0593 – C8-0383/2016 – 2016/0280(COD))*.

[51] Sull'ipertesto e sui suoi effetti, meritano d'esser qui ricordate le parole di Lévy: "l'ipertesto […] [è] un testo costituito da nodi (gli elementi di informazione, paragrafi, immagini, sequenze musicali, ecc.) e da collegamenti tra questi nodi (riferimenti, note, link, 'pulsanti' che indirizzano il passaggio da un nodo all'altro. […] [È] un testo mobile, caleidoscopico, che mostra tutte le sue facce, gira, si piega e si spiega a volontà di fronte al lettore". Ed è questo motivo che – come spiega il filosofo francese – "l'ipertestualizzazione […] può essere definita come una tendenza all'indistinzione, alla parziale sovrapposizione delle funzioni di lettura e scrittura". "[…] Un movimento ininterrotto tra interiorità e esteriorità, […] [fra] l'intimità dell'autore e l'estraneità del lettore rispetto al testo. […] [un] costante passaggio dal dentro al fuori come in un anello di Moebius" (P. Lèvy, *La virtualizzazione del testo*, in Id., *Il virtuale*, trad. it., Milano, Raffaello Cortina, 1997, pp. 25-41, in part. pp. 34-35). Sull'ipertesto, cfr. anche: J. Nyce, P. Kahn (eds.), *Da Memex a Hypertext: Vannevar Bush e la macchina per la mente*, trad. it., Padova, Muzio, 1992; G.P. Landow, *Ipertesto. Il futuro della scrittura*, trad. it., Bologna, Baskerville, 1993, p. 132; J.D. Bolter, *Lo spazio dello scrivere. Computer, ipertesto e la ri-mediazione della stampa*, trad. it., Milano, Vita e Pensiero, 2002.

f) la *lista (rete) di utenti (contatti)* con i quali è possibile comunicare, scambiare informazioni e condividere contenuti multimediali;

g) la *facoltà di monitorare e di analizzare* l'andamento del proprio profilo e della propria rete (i messaggi, il numero di contatti, le condivisioni, i like, ecc.);

h) la *notevole facilità di utilizzo*, dovuta al fatto che tutte le piattaforme social, grossomodo, presentano la medesima impostazione grafica e lo stesso approccio, cosa che le rende immediatamente accessibili e utilizzabili senza bisogno di particolari spiegazioni e/o istruzioni;

i) la *dimensione espressiva*, che consente agli utenti di generare nuovi contenuti multimediali;

l) la *dimensione comunicativa*, grazie alla quale tutto ciò che viene pubblicato nel social è visibile (salvo limitazioni) a tutti gli altri utenti della piattaforma;

m) la *dimensione comunitaria*, che fa sì che la versione finale delle informazioni sia frutto dell'interazione con la comunità, che visualizza i contenuti, li valuta, concorre alla loro circolazione e contribuisce al loro eventuale successo [52].

Sempre guardando alle caratteristiche strutturali, ma con specifico riferimento alle interazioni e ai legami che si possono instaurare fra gli utenti, va detto che – a seconda delle situazioni e dei network – si possono avere:

– *legami bidirezionali*, individuati dalle c.d. *amicizie*, particolari rapporti che permettono di accedere in maniera completa al profilo dell'amico e che rendono possibile contattarlo direttamente, vederne le attività realizzate sulla piattaforma, nonché commentarne, condividerne e/o modificarne i contenuti pubblicati. Una forma d'interazione, questa, che è diffusa soprattutto su Facebook;

– *relazioni di gruppo*, basate su reti create *ad hoc* e volte a consentire ad un novero ristretto e chiuso di utenti di scambiarsi foto, video, collegamenti e messaggi, elementi la cui visione resta del

[52] Cfr.: E. Arielli, P. Bottazzini, *Idee virali. Perché i pensieri si diffondono*, Bologna, Il Mulino, 2018; C. Palazzini, L. Galli, *YouTubers. Chi sono e perché hanno successo*, Roma, San Paolo, 2017.

tutto preclusa agli "esterni". Modalità molto in voga, ad esempio, su WhatsApp;

– *interazioni a stella*, legami c.d. *uno-a-molti*, in quanto, potenzialmente aperti a tutti gli utenti del network. Interazioni in cui, un unico emittente può scegliere se rivolgersi ad un destinatario solo (tramite l'invio di un messaggio individuale-privato), oppure a molti, come avviene con il Tweet.

Al di là degli aspetti strutturali e dei numerosi vantaggi che ne conseguono, è interessante sottolineare che l'*appeal* dei social network – la chiave del loro successo e la ragione della loro diffusione trasversale [53] e intergenerazionale [54] – risiede nella loro singolare capacità di rispondere alle diverse attese degli utenti: quelle di chi li utilizza come mezzo espressivo, per condividere pensieri e frangenti di vita; quelle di chi se ne avvale come strumento professionale per farsi conoscere e/o per soddisfare esigenze di marketing; e, non da ultimo, anche quelle di chi, attraverso i social, instaura, realizza e sviluppa la propria sfera relazionale.

Più in particolare – ricordando la *teoria degli usi e delle gratificazioni* [55] e riproponendo l'ordine dei *bisogni sociali* individuato dalla

---

[53] L'approccio ai social network può essere, infatti, determinato da una serie di ragioni assolutamente distinte: personali, ludiche e di svago, professionali, politiche, religiose, di marketing, ecc.

[54] Un altro elemento non trascurabile è dato dal fatto che ai social accedono fasce eterogenee d'età e che, spesso, all'interno del social, tutte quelle differenze che nella vita appaiono evidenti e fungono in un certo qual modo da freno e da filtro alla comunicazione e al contatto, sembrano dissolversi.

[55] Teoria, in base alla quale, più un individuo percepisce che un *medium* è in grado di soddisfare i suoi bisogni e più sarà indotto a farne uso, soprattutto per ovviare a quelle necessità che, in altra maniera, non riesce ad appagare (cfr. E. KATZ, J.G. BLUMLER, M. GUREVITCH, *Utilization of Mass Communication by the Individual*, in J.G. BLUMLER, E. KATZ (eds.), *The Uses of Mass Communications: Current Perspectives on Gratifications Research*, Beverly Hills, Sage Publications, 1974, pp. 19-31; E. KATZ, J.G. BLUMLER, H. HASS, *On the use of mass media for important things*, in *American Sociological Review*, 38, 1973, pp.164-181; E. KATZ, *Communication research since Lazarsfeld*, in *Public Opinion Quarterly*, 51, 1987, pp.525-545; E. KATZ, *Mass communication research and the study of culture*, in *Studies in Public Communications*, 2, 1959, pp.1-6; D. MCQUAIL, *With the benefit of hindsight. Reflections on uses and gratifications research*, in *Critical Studies in Mass Communication*, 1, 1984, pp.177-193).

piramide di Abraham Maslow[56] – si può affermare che i social appagano:

– il *bisogno di sicurezza*, ossia il desiderio di protezione e tranquillità. Non a caso, all'interno delle piattaforme social e nell'ambito della rete di contatti che ogni utente si costruisce, non ci sono persone estranee o ostili, ma soltanto amici che – nel caso in cui non si dimostrino tali oppure divengano indesiderati e molesti – possono essere cancellati e/o persino bloccati;

– il *bisogno associativo*, vale a dire l'esigenza di sentirsi parte di un gruppo, di essere apprezzati, amati e di interagire e collaborare con gli altri. È sufficiente pensare ai frequenti scambi di opinioni e risorse multimediali che i social permettono, indipendentemente dagli orari, dalle distanze, dal luogo in cui ci troviamo e da cosa stiamo facendo;

– il *bisogno di autostima* e, dunque, la necessità di sentirsi apprezzati, rispettati e tenuti in considerazione. Necessità alla quale i social rispondono offrendo la possibilità di scegliere di continuo a chi si desidera chiedere l'amicizia e di chi si intendono accettare le rispettive richieste. Va da sé che se le persone che ci chiedono (o che ci hanno chiesto) l'amicizia sono parecchie, vuol dire che valiamo e che godiamo dell'interesse e dell'apprezzamento degli altri utenti;

– il *bisogno di autorealizzazione*, ovvero l'esigenza di sviluppare e di esternare la propria personalità, realizzare le proprie aspettative e raggiungere una posizione gratificante e pregevole all'interno del gruppo sociale. Aspirazioni che i social soddisfano dotandoci di un profilo sempre in divenire e di una cerchia più o meno ampia di "amici" (nel caso di *Facebook*) o di "seguaci" (nel caso di *Twitter*).

---

[56] Secondo il noto psicologo americano i bisogni che ognuno di noi avverte non sono isolati e "a sé stanti", ma tendono a seguire in una gerarchia e un ordine di priorità. Per questo motivo, Maslow dispone le principali necessità dell'individuo all'interno di una piramide dove, alla base, ci sono i bisogni fisiologici di tipo primario (ossia tutte le necessità direttamente connesse alla sopravvivenza), mentre, al vertice, quelli che hanno a che vedere con l'autorealizzazione personale. Ciò che è importante sottolineare è che, all'interno della piramide, il passaggio da un bisogno ad un altro avviene "per soddisfazione". In pratica, per accedere – e avvertire – il bisogno successivo (più complesso ed elevato), è necessario aver già appagato quello precedente (di livello inferiore) (A.H. MASLOW, *Motivation and Personality*, New York, Edition by Harper & Row, 1954).

Le cose, però, non sono così semplici. Il desiderio di sicurezza, la voglia di essere accettati e di far parte di un gruppo, la necessità di dimostrare il proprio valore, l'esigenza di affermarsi sono, sì, bisogni eterogenei che i social network soddisfano, ma – paradossalmente – sono anche necessità che vengono accresciute in maniera esponenziale proprio dagli stessi social.

Vetrine virtuali che ospitano *esplosioni autobiografiche* [57], i nuovi network, infatti, prestano il fianco alle inclinazioni narcisistiche [58] ed alimentano quella particolare smania di consenso e di approvazione che – con un'insolita ma efficace formula – viene definita *mipiacismo* [59]. Non a caso, una delle prime e delle maggiori preoccupazioni di chi pubblica un post, o un qualsiasi altro contenuto sui social, è quasi sempre quella di riuscire ad "accaparrarsi" quanti più *like* possibile [60], anche se per far ciò è necessario "dire tutto di sé" [61].

Ed è proprio questo il motivo per cui – Bauman sostiene – che la società odierna è una *società confessionale*, dove tutti e, in modo particolare i ragazzi, non avvertono più alcuna gioia nell'avere dei segreti:

"[…] I teenager muniti di confessionali elettronici portatili non sono che

---

[57] Vd. F. COLOMBO, "*Il 'dire di sé' sul Web 2.0*", in ID., *Il potere socievole. Storia e critica dei social media*, Milano, Mondadori, 2013, p. 138 ss.

[58] Cfr. G. RIVA, *Selfie. Narcisismo e identità*, Bologna, Il Mulino, 2016.

[59] Neologismo, sempre più diffuso ed in voga, che riprendo da S. SCRIMA, *Socrate su Facebook*, cit., in part., p. 8. Cfr. anche G. LOVINK, *Ossessioni collettive. Critica dei social media*, cit., *passim*.

[60] Like che, oramai, non hanno più solo la funzione di gratificare l'autostima di chi pubblica, ma che hanno acquisito anche un vero e proprio valore economico. Come avviene, ad esempio, su YouTube, dove i profitti dei video caricati sono direttamente proporzionali al numero degli utenti iscritti al canale e ai consensi che – di volta in volta – riscuotono i diversi filmati (vlog, tutorial, ecc.). (A proposito del "fenomeno like", cfr., fra gli altri: G. LOVINK, *Zero comments. Teoria critica di internet*, Milano, Mondadori, 2008; ID., *L'abisso dei social media. Nuove reti oltre l'economia dei like*, trad. it., Milano, Università Bocconi, 2016).

[61] A questo proposito, merita d'esser ricordato quanto affermato, alcuni anni fa, da LEWIS: "[…] Al cuore del social networking c'è uno scambio di informazioni personali. Gli utenti sono ben contenti di rivelare dettagli intimi della propria vita personale, di postare informazioni accurate, di condividere fotografie" (P. LEWIS, *Teenager networking websites face anti-paedophilie investigation*, *Guardian*, 03 luglio 2006).

apprendisti che si formano e vengono formati all'arte di vivere in una società-confessionale, una società contraddistinta dal fatto di aver cancellato il confine che separava un tempo pubblico e quello privato, di aver trasformato l'esibizione pubblica del privato in una pubblica virtù e in un pubblico dovere e di aver spazzato via dalla comunicazione pubblica tutto ciò che non si lascia ridurre a confidenza privata e tutti coloro che rifiutano di confidarsi". "[…] [Così si] mettono in mostra avidamente ed entusiasticamente le proprie qualità sperando di attirare l'attenzione e possibilmente di ottenere il riconoscimento e l'approvazione necessari per non essere esclusi dal gioco della socializzazione […]" [62].

4. Nuovi scenari

Diversi anni fa, in un noto lavoro pubblicato su *New Media & Society*, Roger Silverstone – fra i primi ad occuparsi di questi temi – si chiedeva quali fossero gli aspetti inediti dei nuovi media [63]. Pur nell'ambito di studi e di approcci fra loro molto diversi [64], questo stesso interrogativo si è poi riproposto con una certa ciclicità e – ancora oggi – può rivelarsi un utile spunto per ragionare sulle prerogative e sugli aspetti inconsueti dei social network [65].

Dei nuovi network all'inizio del nostro percorso s'è detto che: *i*) *fanno parte della nostra quotidianità; ii*) *determinano una riconfigurazione della comunicazione e dei rapporti; iii*) *ci permet-*

---

[62] Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, trad. it., Roma-Bari, Laterza, 2015, pp. 15-17.

[63] *What's New about New Media?*, in *New Media & Society*, Vol. 1, 1, 1999, pp. 10-12.

[64] Moltissimi gli studiosi che si sono occupati della questione, fra questi: J.D. BOLTER, R. GRUSIN, *Remediation. Competizione e integrazione tra media vecchi e nuovi*, trad. it., Milano, Guerini e associati, 2003; L. GITELMAN, G.B. PINGREE (a cura di), *New Media. 1740-1915*, Massachusetts, MIT Press, 2003; D. GAUNTLETT, R. HORSLEY (eds.), *Web.Studies*, London, Arnold, 2004; L. GORMAN, D. MCLEAN, *Media e società nel mondo contemporaneo*, trad. it., Bologna, Il Mulino, 2011; JT. FLEW, *New Media: an introduction*, Melburne, Oxford University Press, 2008; M. LISTER, J. DOVEY, I.H. GRANT, K. KELLY (a cura di), *New Media. A critical introduction*, London, Routledge, 2008; N. COULDRY, *Sociologia dei nuovi media. Teoria sociale e pratiche mediali digitali*, trad. it., Milano, Pearson, 2015.

[65] Sulla distinzione fra vecchi e nuovi media cfr. anche G. GRANIERI, *La società digitale*, Roma-Bari, Laterza, 2006.

tono di scegliere il nostro profilo e la nostra identità. Osservazioni senza dubbio significative, ma che – da sole – non sono sufficienti a rispondere e a soddisfare pienamente il quesito posto da Silverstone. Proviamo, seppur in maniera molto sintetica e per punti, a ricostruire.

i) È vero: *i social permeano la nostra vita*. E pressoché ogni giorno siamo subissati da messaggi che ci ricordano quanto siano utili, e che ci suggeriscono quali siano i network e le soluzioni tecnologiche più adatte a soddisfare le nostre esigenze. Messaggi, che suonano più o meno così:

"Ti senti solo? – Perché non sei su Facebook?
Single? – Perché non provi con gli incontri online?
Problemi a scuola? – Ti manca solo la giusta App per studiare!
Vuoi recuperare la linea? – Non hai ancora la App per la dieta?
Non hai tempo? – Metti la tua agenda su cloud!
Malato? – Watson ti aiuta nella diagnosi e nella terapia! / Fame? – Dai fast food alle ricette gurmet: tutto online!
Niente soldi? – Il credito online è più veloce di qualsiasi altra banca!
Sei svogliato? – Prova la giusta App motivazionale!
Dedichi troppo tempo al tuo smartphone? – Basta un'App per lo spegnimento automatico!" [66].

Malgrado ciò, però, non si può non ammettere che tutti i media, che via via si sono succeduti nel corso della storia [67], hanno sempre comportato profondi mutamenti non solo nello svolgimento e nella gestione delle attività quotidiane, ma anche nel nostro stesso modo di pensare e di rapportarci al mondo. Emblematici – come avverte Lévy – i tanti cambiamenti legati all'invenzione della scrittura e, più di quattromila anni dopo, a quella della stampa.

"All'interno delle culture prettamente orali, che hanno caratterizzato il 95% del tempo che la nostra specie ha trascorso su questo pianeta, la memoria umana era circoscritta alla capacità di ricordare dei gruppi di anziani. Gli strumenti, i gioielli, le statue, i monumenti di pietra e le immagini dipinte erano i soli supporti capaci di trasmettere concetti astrat-

---

[66] M. SPITZER, *Solitudine digitale*, cit., p. 18.

[67] Cfr., fra gli altri, R. SILVERSTONE, *Televisione e vita quotidiana*, trad. it., Bologna, Il Mulino, 2000; R. STELLA, C. RIVA, C.M, SCARCELLI, M. DRUSIAN, *Sociologia dei New Media*, cit., in part. pp. 6-7.

ti. Con la scrittura […] le conoscenze hanno cominciato ad essere registrate in maniera più efficace. […] La nuova abbondanza di testimonianze […] permise di mettere in prospettiva le conoscenze legate al presente, così come i progetti legati al futuro […] [abituando] lo spirito umano ad utilizzare uno sguardo analitico, logico, critico e comparativo nei confronti della realtà" [68].

Una vera e propria rivoluzione culturale, alla quale, anche Victor Hugo non manca di dedicare un significativo rimando. Celebre l'espressione dell'arcidiacono di Notre-Dame, Claude Frollo: "*ceci tuera cela*". Formula con la quale Hugo accenna proprio ai riverberi connessi all'invenzione di Gutenberg [69].

ii) È altresì vero: *i social trasformano la comunicazione e le relazioni*. Non solo, Internet e i nuovi network trasformano anche lo spazio e il tempo [70]. Assistiamo, così, all'emergere di quella particolare dimensione che Paul Virilio definisce *dromosfera* [71]. Una dimensione che è contraddistinta dall'accelerazione continua e, all'interno della quale, il tempo risulta per così dire contratto (grazie alla riduzione delle durate necessarie al compimento delle diverse attività), mentre la geografia (intesa come spazio fisico fatto di confini, frontiere e distanze) sembra condannata a perdere qualunque significato.

"Più che alla 'fine della storia' assistiamo dunque a quella della geografia. […] il GLOBALE è l'*interno* […] e il LOCALE è l'*esterno*. […] i semi non sono più all'interno delle mele, né gli spicchi al centro dell'arancia: *la scorza è rovesciata*" [72].

Tuttavia, non si può fare a meno di osservare che il principale scopo dei media (*di tutti i media! vecchi e/o nuovi che siano!*) è quello di "mediare la comunicazione". Vale a dire, proprio quello di superare i vincoli spazio-temporali e di rendere possibile il

---

[68] P. LÉVY, *Il nuovo spazio pubblico*, in ID., *Cyberdemocrazia*, trad. it., Milano, Raffaello Cortina, 2008, p. 37.

[69] Cfr. V. HUGO, *Notre-Dame de Paris*, trad. it., Torino, Einaudi, 2007.

[70] D'obbligo il rinvio a M. SERRES, *Non è un mondo per vecchi*, trad. it., Torino, Bollati Boringhieri, 2013, *passim*.

[71] Cfr. *L'orizzonte negativo. Saggio di dromoscopia*, trad. it., Genova, Costa & Nolan, 2005.

[72] *La bomba informatica*, trad. it., Milano, Raffaello Cortina, 2000, in part. p. 9.

passaggio dall'interazione sincronica e contingente, a quella diacronica e differita. Altrimenti detto, anche in questo caso, così come per il precedente, non si può dunque dire di aver individuato una vera e propria novità.

iii) Ed è pure vero: *i social ci permettono di scegliere come mostrarci* [73]. Eccellenti strumenti di *impression management* e di *self-empowerment*, i social network ci consentono di scegliere come presentarci, cosa mostrare di noi e, soprattutto, ci permettono di creare dei *nuovi sé sociali*. Non a caso, Floridi osserva che

"il sé sociale […] [costituisce] il principale canale attraverso cui le ICT e, in particolar modo i social media interattivi, esercitano il loro profondo impatto sulle nostre identità personali. […] [Basta infatti che] cambiamo le condizioni sociali in cui viviamo, mutiamo le reti di relazioni e il flusso di informazioni di cui godiamo e ridisegniamo natura e novero dei limiti e delle possibilità che regolano come ci presentiamo al mondo e indirettamente a noi stessi, […] [perché] il nostro sé sociale […] [possa] essere radicalmente aggiornato […]" [74].

Un fenomeno, questo della costruzione e della *micronarrazione* del sé, al quale James [75] e Proust [76] hanno dedicato parti-

---

[73] Per un ulteriore approfondimento, si vedano, fra gli altri, K.Y.A. McKenna, J.A. Bargh, *Causes and conseguences of social interaction on the Internet. A conveptual framework*, in *Media Psychology*, 1, 3/1999, 249-269; K.Y.A. McKenna, *Through the Internet looking glass. Expressing and validating the true self*, in A. Joinson, K.Y.A. McKenna, T. Postmes, U.D. Reips (eds.), *The Oxford handbook of Internet psychology*, Oxford, Oxford University Press, 2007, pp. 205-221; A.L. Gonzales, J.T. Hancock, *Mirror, mirror on my Facebook wall: Effects of exposure to Facebook on self-exteem*, in *Cyberpsychology, Behavior, and Social Networking*, 14, 1-2/2011, pp. 79-83.

[74] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, cit., in part. p. 69. A proposto del rapporto fra new media e costruzione del sé, cfr. anche G. Riva, *I social network*, cit., p. 119; F. Colombo, *Il potere socievole*, cit., p. 139.

[75] *Principi di psicologia. Il flusso di coscienza*, cap. IX-X, trad. it., Milano, 1998.

[76] "Perfino nei più insignificanti dettagli della nostra vita, non siamo un tutto costruito materialmente, identico per tutto il mondo e di cui ciascuno potrebbe avere coscienza come di un quaderno delle spese o di un testamento; la nostra personalità sociale è una creazione del pensiero altrui. […] Riempiamo l'apparenza fisica dell'essere che ci sta davanti di tutte le nozioni che abbiamo su di lui, e, nell'insieme che ci rappresentiamo, queste nozioni costituiscono la parte più importante. Finiscono per

colare attenzione, e che – seppur con tecniche e modalità molto meno penetranti rispetto a quelle dei social media – ha sempre accompagnato la storia dell'uomo. A riprova di ciò, e semplicemente a titolo d'esempio, si può ricordare quanto osservato da Rifkin a proposito di quella straordinaria "finzione" che, fra il Settecento e l'Ottocento, è stata il romanzo. Una finzione che – come nota il celebre economista e sociologo statunitense – ha infatti permesso a "milioni di persone […] di definire i propri sentimenti più intimi e di manifestarli" [77].

Ma, se così, è evidente che si deve compiere un passo ulteriore, tornando a domandarsi – con Silverstone – *what's new about new media?* Per rispondere, è necessario soffermarsi sull'*aspetto sociale* che contraddistingue i nuovi network. Una scelta che, parlando di media – e cioè di strumenti di mediazione volti a favorire i rapporti sociali – potrebbe anche apparire auto-evidente [78], o persino banale, e che, invece, ci permette di mettere a fuoco alcuni elementi di nodale importanza.

Nati per abilitare le collaborazioni partecipative e per incentivare le comunicazioni orizzontali "dal basso" [79] (secondo la logica *peer-to-peer*), i social network hanno portato a maturazione quella trasformazione che aveva già avuto inizio con l'avvento di Internet [80], favorendo la comparsa di nuove forme di aggregazione, basate solo ed esclusivamente sull'interazione online: le *communities*. Più in particolare, i social media hanno contri-

---

riempire così perfettamente le guance, per seguire con tale esatta aderenza la linea del naso, si industriano così bene di sfumare la sonorità della voce come se questa non fosse che un involucro trasparente, che ogni volta che vediamo quel viso, che sentiamo quella voce, ritroviamo e diamo retta soltanto a quelle nozioni" (M. PROUST, *Alla ricerca del tempo perduto. Dalla parte di Swann*, trad. it., Torino, Einaudi, 1990).

[77] Così, J. RIFKIN, *La civiltà dell'empatia. La corsa verso la coscienza globale nel mondo in crisi*, trad. it., Milano, Mondadori, 2011, p. 537.

[78] Cfr. F. COLOMBO, *Di cosa parliamo quando parliamo di social media*, in ID., *Il potere socievole*, cit., pp. 38-39.

[79] *Ibidem*.

[80] "[…] la principale trasformazione nelle società complesse si è verificata attraverso la sostituzione delle comunità spaziali con i network come forme prime di socialità" (cfr. M. CASTELLS, *Comunità virtuali o società in rete?*, in ID., *Galassia Internet*, cit., p. 117).

buito ad avvicinare la nostra vita quotidiana al cyberspazio [81], generando un nuovo ed inedito spazio, quello dell'*inter-realtà* [82]: un ambiente sociale ibrido, contraddistinto dalla commistione e dalla sovrapposizione di esperienze reali (offline) e di esperienze digitali (online).

Si assiste così – *ed è questa la più significativa novità dei social!* – al passaggio dalla comunità tradizionalmente intesa (radicata nel territorio) [83] alla Rete [84], o meglio ai nuovi network che, invece, sono del tutto affrancati dalla dimensione spaziale [85]. Inedite forme di aggregazione sociale, che – con Castells – possiamo definire comunità *specializzate* e/o *di scelta*, occasionate dalle preferenze, dalle necessità e dalle strategie degli utenti e degli attori sociali [86]. Comunità sempre *in fieri*, all'interno delle quali la parola d'ordine è *flessibilità* e in cui i legami sono, sì, meno impegnativi e più liberi, ma, al contempo, si fanno anche più fragili ed incerti.

---

[81] Vd. G. RIVA, *I social network*, cit., p. 14.

[82] Circa la nozione di inter-realtà, cfr. J. VAN KOKSWIJK, *Hum@n, Telecoms & Internet as interface to interreality*, Hoogwoud, Bergboek, 2003; G. RIVA, *Interreality. A new paradigm for e-health*, in *Studies in Health Technology and Informatics*, 144, 209, pp. 3-7; ID., *Irrealtà. Reti fisiche e digitali e post-verità*, in Il Mulino, 2/2017, pp. 326-334.

[83] A proposito della comunità di luogo (e, in modo particolare, del rapporto e del distinguo fra comunità e società), d'obbligo il rinvio alla nota teoria elaborata da F. TÖNNIES, *Comunità e società*, trad. it., Roma-Bari, Laterza, 1963, pp. 45-46.

[84] Sul passaggio dalla comunità alla Rete e sulla differenza che si dà fra le due dimensioni, meritano d'esser qui ricordate le osservazioni di Bauman: "[…] appartenere a una comunità è una condizione molto più sicura e affidabile che far parte di una rete, anche se comporta sicuramente più vincoli e più obblighi. La comunità ti osserva da vicino e ti lascia poco spazio di manovra (può metterti al bando e spedirti in esilio, ma non ti consente di uscirne di tua iniziativa), mentre la rete può non preoccuparsi minimamente che tu obbedisca alle sue norme […], e dunque ti lascerà le briglie molto più lente e, soprattutto, se te ne vai non ti penalizzerà" (Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, cit., p. 25).

[85] In particolare – come sottolinea LÉVY – i nuovi media "[…] non sono più legati ad una zona geografica, ma ad una comunità virtuale di ascoltatori, spettatori o lettori che possono abitare ovunque nel mondo" (P. LÉVY, *Cyberdemocrazia*, cit., p. 48).

[86] M. CASTELLS, *Comunità virtuali o società in rete?*, in ID., *Galassia Internet*, cit., p. 130.

Si noti, questa sorta di "transizione" dalla comunità al network suggerisce anche due possibili considerazioni. La prima è che, con i social network sembra realizzarsi quella particolare forma di *sociazione* che – per Simmel – è rappresentata dalla *socievolezza*. Una singolare modalità d'interazione, nell'ambito della quale il processo di associazione integra un valore *in sé*: una relazione sviluppata nella modalità del gioco, che si contraddistingue per l'assenza di tutte quelle tensioni che, invece, sono proprie dei rapporti e dei vincoli politici, economici e giuridici. In base alla ricostruzione del celebre sociologo tedesco, infatti, la socievolezza sarebbe il frutto della *libera interdipendenza degli individui* che interagiscono fra di loro, mossi unicamente dal *desiderio di stare insieme*, senza contenuti o obiettivi ulteriori [87].

La seconda considerazione è che, contrariamente alle finalità per le quali sono stati pensati (*semplificare le comunicazioni e i contatti fra gli utenti ed agevolare la condivisione di contenuti e informazioni*), i social stanno diventando sempre più autoreferenziali [88], determinando lo sviluppo di vere e proprie comunità *personalizzate* e *io-centriche* modellate sui gusti e sulle preferenze dell'individuo [89].

Di qui, come avvertono in molti [90], il pericolo che si assista ad

---

[87] G. SIMMEL, *Socievolezza*, trad. it., Milano, Armando Editore, 1997.

[88] Come Lévy evidenziava già alcuni anni fa: "l'evoluzione contemporanea della libertà di espressione nel cyberspazio, come l'esplosione quantitativa e qualitativa del Web, sembra portarci verso una situazione dove tutte le istituzioni, le imprese, i gruppi, le équipe e gli individui diventeranno mass media di loro stessi e gestiranno la loro comunità virtuale che corrisponde alla loro zona di influenza sociale" (P. LÉVY, *Cyberdemocrazia*, cit., p. 52).

[89] "I nuovi sviluppi tecnologici sembrano accrescere le possibilità che l'individualismo in rete diventi la nuova forma dominante di socialità". Assistiamo, invero, allo sviluppo e all'aumento di un networking sempre più personalizzato per un'ampia gamma di situazioni sociali. "[…] tendenze che equivalgono al trionfo dell'individualismo" (M. CASTELLS, *Comunità virtuali o società in rete?*, in ID., *Galassia Internet*, cit., pp. 130-131).

[90] Sulla nascita di comunità incentrate sul singolo, cfr. M. CORNEY, *Sustaining the New Economy. Work, Family and Community in the Information Age*, Cambridge, Cambridge University Press, 2000; R. PUTNAM, *Bowling Alone. The Collapse and Revival of American Community*, New York, Simon & Schuster, 2000; M. CASTELLS, *La nascita della società in rete*, trad. it., Milano, Egea, 2002.

una sorta di reviviscenza dell'individualismo [91], sotto forma di individualismo *in e/o di rete* [92]. Non di rado, infatti, i network si conformano ai valori, agli interessi, ai desideri e ai progetti dei singoli. Inclinazioni che, tra l'altro, vengono poi adoperate per mettere a punto strategie commerciali [93], per orientare i comportamenti [94] e, non da ultimo, anche per condizionare le scelte politiche [95]. E, sempre di qui, anche tutta una serie di rischi che possono investire proprio l'individuo e, in maniera particolare, la sua percezione del mondo, le relazioni con gli altri e le sue stesse condizioni psico-fisiche [96].

Entro questa cornice, si inseriscono quello che può essere considerato come *il paradosso dei social network*, ovvero: l'emergere di forme di isolamento sociale [97] o – per dirla con Anders – di *ere-*

---

[91] A proposito dei riverberi dell'individualismo, cfr. A.C. AMATO MANGIAMELI, *Tra pensiero moderno e diritto. Oltre l'individualismo possessivo*, in L. CONGIUNTI, A. NDRECA, G. FORMICA (a cura di), *Oltre l'individualismo. Relazioni e relazionalità per ripensare l'identità*, Roma, Urbaniana University Press, 2017, in part. pp. 101-113. Inoltre, per un'agile ricostruzione vd. M.N. CAMPAGNOLI, *Ragionando oltre l'individualismo. Appunti e riflessioni a partire da una lettura*, in *Rivista di Filosofia del Diritto*, 1/2019, pp. 205-219.

[92] In tal senso, cfr. B. WELLMAN, *Physical place and cyberspace: the rise of networked individualism*, in *International Journal of Urban and Regional Research*, 1/2001.

[93] "[…] in un mondo commerciale che strumentalizza in maniera crescente le tendenze narcisistiche e voyeuristiche, Internet" e i social network diventano "uno strumento imbattibile per trasformare in merce ogni ambito della vita" (J. RIFKIN, *La civiltà dell'empatia*, cit., pp. 537-538).

[94] Come spiega AMATO MANGIAMELI, *infra*, *Prima Parte*.

[95] Particolarmente interessanti, sul punto, le recenti riflessioni di G. ZICCARDI, *L'uso delle nuove tecnologie in politica*, in ID., *Tecnologie per il potere*, Milano, Raffaello Cortina, 2019, in part., pp. 15-50.

[96] Fra i più noti disturbi conseguenti all'uso (e all'abuso) dei social network: la *cyberdipendenza* (molto simile a quella creata dall'assunzione di alcool o di sostanze psicotrope) e l'incapacità di controllare il tempo trascorso on-line; il *multitasking* che, a lungo andare, incrementa la propensione alla distrazione e riduce la capacità di immagazzinare informazioni; la *sindrome da vibrazione fantasma* che porta al controllo ossessivo e continuo dello smartphone e/o del tablet; l'*insonnia digitale*, ovvero l'alterazione dei ritmi circadiani e lo sviluppo di forme; la *depressione digitale*, la perdita di interesse per la vita reale e di qualsiasi forma di empatia verso gli altri (cfr. M. SPITZER, *Solitudine digitale*, cit., in particolare, pp. 153-176 e pp. 279-290).

[97] Si veda quanto osservato all'inizio in merito alla sindrome da hikikomori, *infra*, paragrafo 1.

miti di massa [98] e la conseguente diffusione di forme di rifiuto della vita reale [99]. Un rifiuto analogo a quello dei turisti giapponesi affetti dalla c.d. *sindrome di Parigi* [100], che, una volta arrivati nella capitale francese e vedendo disattesa la loro percezione idealizzata e romanzata della città, manifestano condizioni di disagio.

Abituati alle opportunità e agli scenari ottimizzati proposti dal mondo virtuale e dai social, nel momento in cui ritorniamo alla dimensione reale, decisamente meno piacevole ed accattivante [101], avvertiamo una sorta di malessere [102] che ci porta a rifugiarci nella vita offertaci dallo schermo [103]. Un po' come accade agli *i-Gen*, l'attuale generazione di nativi digitali iperconnessi: ragazzi del tutto incapaci di concepire un mondo senza Internet, e che – rispetto alle esperienze reali – prediligono di gran lunga quelle digitali [104], più semplici e più gratificanti.

---

[98] V.d. G. ANDERS, *Il mondo dopo l'uomo. Tecnica e violenza*, trad. it., Milano, Mimesis, 2008, p. 93.

[99] Cfr. B.-C. HAN, *Nello sciame. Visioni del digitale*, trad. it., Milano, Nottetempo, 2015.

[100] Sulla sindrome di Parigi, vd.: P. ADAM, *Le Syndrome de Paris*, Parigi, Inventaire, 2005; A. VIALA, H. OTA, M.N. VACHERON, P. MARTIN, F. CAROLI, *Les japonais en voyage pathologique à Paris: un modèle original de prise en charge transculturelle*, in *Nervure de journal Psychiatrie*, 5/2004, pp. 31-34.

[101] Non a caso, con una pittoresca – ma efficace – metafora Siva Vaidhyanathan sottolinea che i social (l'autore, per il vero, parla in modo particolare di Facebook) ci attirano attraverso un meccanismo simile a quello delle patatine fritte, facendoci assaporare piccoli ma frequenti piaceri ai quali ci assuefacciamo presto. Gratificazioni che – fra le altre cose – non implicano, né particolari capacità critiche, né men che meno un'analisi approfondita dell'esperienza che stiamo facendo (S. VAIDHYANATHAN, *Anti-Social Media*, New York, Oxford University Press, 2018, p. 35).

[102] Cfr. C. BROD, *Technostress. The Human Cost of the Computer Revolution*, Reading MA, Addison-Wesley, 1984; T.S. RAGU-NATHAN, M. TARAFDAR, B.S. RAGU-NATHAN, Q. TU, *The consequences of technostress for the users in organizations. Conceptual development and empirical validation*, in *Information Systems Research*, 19, 2008, pp. 417-433; Q.E. BOOKER, C.M. JR. REBMAN, F.L. KITCHENS, *A model for testing technostress in the online education environment. An exploratoty study*, in *Issues in Information Systems*, 15, 2015, pp. 214-222.

[103] Espressione con la quale rinvio alle ricostruzioni di TURKLE (*La vita sullo schermo*, cit.), che, più di vent'anni fa – e tra i primi – si interrogava sui riverberi legati all'avvento di Internet.

[104] Vd. J.M. TWENGE, *Iperconnessi. Perché i ragazzi oggi crescono meno ribelli, più tolleranti, meno felici e del tutto impreparati a diventare adulti*, trad. it., Torino, Einaudi, 2018.

5. Conclusioni

È innegabile: con le loro interfacce intuitive e decisamente *friendly*, i social, non ci offrono semplicemente occasioni di svago, o spensierate digressioni dalla realtà, ma ci accompagnano e ci agevolano quotidianamente anche nello svolgimento delle attività personali, così come di quelle professionali. È sufficiente pensare alla frequenza e all'estrema facilità con la quale – in qualsiasi momento e da qualunque luogo – possiamo, ad esempio: controllare l'account di lavoro restando aggiornati in tempo reale; condividere documenti con tecniche che hanno soppiantato il vecchio e lento fax (WhatsApp, Google Drive, Dropbox,…); prendere parte a una conference call risparmiandoci viaggi e perdite di tempo (Skype, GoToMeeting, Cisco Webex Meetings,…); gestire la rete domestica e gli elettrodomestici di casa (Smart Living, Neurio, MyVirtuoso Home,…); oppure monitorare il nostro stato di salute (iFarmaci, Laboratory Gear Medical, PubMedClip,…).

Supporti irrinunciabili ai quali fanno, però, da contrappeso anche tutta una serie di criticità, che vanno dagli atteggiamenti scorretti e/o disfunzionali, sino ai c.d. *cyber crimes* [105]. Un ampio e variegato ventaglio di fattispecie, fra le quali spiccano condotte come: la diffusione di *fake news* [106]; il *furto d'identità* [107]; il *cy-*

[105] Comportamenti che – come osserva AMATO MANGIAMELI – aumentano di pari passo con lo sviluppo delle tecnologie (*infra*, *Prima Parte*).

[106] Notizie che vengono diffuse da bots programmati per fingersi umani e per trarre in inganno la platea degli utenti, allo scopo di creare tensioni o di orientare le decisioni politiche. Fenomeno che è stato già oggetto d'attenzione da parte del legislatore, come testimonia il D.D.L. 2688 del 2017 "*Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica*", che prevede l'introduzione di una contravvenzione (art. 656 *bis*) e di due nuove fattispecie criminose (artt. 265 *bis* e 265 *ter*); ed il D.D.L. 3001 del 2017 "*Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news*", che mira a "responsabilizzare i fornitori dei servizi di social network sui contenuti veicolati attraverso le proprie piattaforme, tutelare gli utenti da notizie costruite intenzionalmente per trarli in inganno e contrastare la commissione di reati attraverso la rete".

[107] Di cui Zao è solo l'ultima minaccia in ordine di tempo. App virale, che affascina gli utenti consentendo di scambiare i loro volti con quelli dei personaggi cinematografici e/o televisivi, e che – avendo accesso alle loro immagini – può facilmente aprire il varco a pericolose violazioni e sottra-

berstalking [108]; il *cyberbulling* [109]; il *troll* [110]; l'*hate speech* [111]; il *sexting* [112]; oppure la *sextortion* [113]. Comportamenti lesivi che, non di rado, si annidano tra le pieghe dei social e che, per certi versi, sono incentivati dalla struttura e dalle caratteristiche proprie dei network.

Il motivo è presto detto: la virtualità, sommata alla semplicità di accesso e di utilizzo, fa sì che i social vengano percepiti alla stregua di ambienti prettamente ludici e privi di conseguenze. Si sviluppa, così, l'illusione di operare in una sorta di *Far West giu-*

---

zioni (cfr. G. SCORZA, *Arriva Zao e di nuovo la privacy va in fumo per una risata,* in *L'Espresso*, 3 settembre 2019).

[108] Per uno specifico approfondimento G. ZICCARDI, *Cyberstalking e molestie portate con strumenti elettronici: aspetti informatico-giuridici*, in *Rassegna italiana di criminologia*, 3/2012, pp. 160-173.

[109] A contrasto del quale è intervenuta la l. n. 71 del 2017 "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*". Per un'interessante analisi della fattispecie cfr., fra gli altri, F. TONIONI, *Cyberbullismo*, Milano, Mondadori, 2014; M.L. GENTA, A. BRIGHI, A. GUARINI, *Bullismo elettronico: fattori di rischio connessi alle nuove tecnologie*, Roma, Carocci, 2009.

[110] Particolare comportamento che prevede la creazione di pagine e/o di gruppi volutamente provocatori, polemici e incitanti alla violenza (ex. "non vogliamo le persone di colore"; "tutti contro i musulmani"; "no a down"; ecc.), che hanno lo scopo di scatenare discussioni e litigi online. Cfr. D. FACCHINI, *Trolls Inc. Il volto autoritario della rete tra libertà d'insulto, pubblicità e privacy*, Milano, Altreconomia, 2015.

[111] E, cioè, la diffusione di espressioni d'odio e discriminatorie. Condotta sulla quale si segnala la recente Delibera dell'Autorità per le Garanzie nelle Comunicazioni (AGCOM) del 15 maggio 2019, con la quale è stato approvato il "*Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech*" (cfr. *Materiali normativi a supporto – Parte Seconda*).

[112] Vale a dire, l'invio di testi o immagini sessualmente esplicite tramite Internet o telefono cellulare. Vd., fra gli altri, F. CURRÒ, *Il sexting*, in *I Profili dell'abuso. Profiling*, 2/2017; S. SHARIFF, *Sexiting e cyberbullismo. Quali limiti per i ragazzi sempre connessi?*, trad. it., Milano, Edra, 2016.

[113] Attività estorsiva a sfondo sessuale (ricatto sessuale), che, in una prima fase, si avvale degli strumenti e dei canali informatici per contattare le vittime e per indurle a pratiche sessuali (invio di foto, video, testi espliciti); mentre, nella seconda fase, implica l'estorsione. La vittima viene, infatti, costretta al pagamento di una somma di denaro in cambio della mancata divulgazione del materiale compromettente precedentemente condiviso. Con specifico riferimento alla condotta agita nei confronti dei minori, cfr. EUROPOL, *Online Sexual Coercion and Extortion as a Form of Crime Affecting Children: A Law Enforcement Perspective*, 2017.

ridico [114], dove ci si crede facoltizzati ad utilizzare un eloquio più anticonformista e diretto [115], e ad adottare atteggiamenti più disinvolti e spregiudicati. Un'illusione, che nasce da un duplice fraintendimento di fondo e, nello specifico, da una visione distorta del virtuale e della Rete.

Per un verso, si crede che il virtuale si contrapponga al reale e che tutto ciò che accade online (in quanto, per l'appunto, *non-reale*) non possa determinare né ricadute sociali, né, men che meno, conseguenze e/o sanzioni di tipo giuridico. Quando, invece – derivando dal latino *virtus* e avendo la sua radice etimologica in *vis-roboris* (forza, potenza) – il virtuale è il contrario dell'attuale [116] e rappresenta ciò che "non-è-ancora", ma "è-in-potenza". Una dimensione che, contrariamente a quello che si può supporre, comporta dei riverberi assolutamente concreti (*e reali*) sulla vita offline.

Per un altro verso, si pensa che in Rete (e, dunque, anche nei social) regni l'anonimato più assoluto, tanto che – riprendendo il celebre fumetto Steiner [117] – si potrebbe dire: *on the Internet nobody knows you're a dog!* Una falsa credenza, che induce alla perdita (o comunque alla riduzione) del controllo sociale [118]. Si

---

[114] Riprendo, qui, l'efficace espressione utilizzata da G. ZICCARDI, *Social media. Uso sicuro di web, messaggistica, chat e social network*, Milano, "Corriere della Sera", 2017, pp. 7-12.

[115] A tal proposito, è interessante ricordare che negli anni si è sviluppata la *netiquette*: un insieme di regole che disciplinano il comportamento che gli utenti dovrebbero tenere in Rete. Un Galateo per il Web che non è disciplinato da leggi *ad hoc*, ma che si fonda su una serie di pratiche e di convenzioni generali e condivise. Regole che, tuttavia, vengono spesso richiamate all'interno dei contratti di fornitura di servizi di accesso da parte dei Provider e, delle quali, il mancato rispetto comporta una generale disapprovazione da parte degli altri utenti e, nei casi più gravi, sono punite tramite *ban*.

[116] "Il virtuale […] non si contrappone al reale ma all'attuale. Contrariamente al possibile, statico e già costituito, il virtuale è come un complesso problematico, il nodo di tendenze e di forze che accompagna una situazione, un evento, un oggetto o un'entità qualsiasi, e che richiede un processo di trasformazione: l'attualizzazione" (P. LÉVY, *Il virtuale*, cit., p. 6).

[117] Stringa pubblicata sul *New Yorker* il 5 luglio del 1993.

[118] Così Riva: "Nonostante siano nati proprio per evitare il problema dell'anonimato, la loro progressiva trasformazione da reti chiuse in reti aperte consente nuovamente agli utenti di nascondere facilmente la propria identità. E come mostrato da decine di studi su questi temi, non potendo riconoscere l'identità del soggetto si riduce il controllo sociale e, quindi, gli utenti tendono a comportarsi in maniera più disinibita" (G. RIVA, *I social network*, cit., p. 139).

sviluppa, così, un meccanismo che, *mutatis mutandis*, sembra ricordare quello evidenziato da Stanley Milgram nel suo *Obbedienza all'autorità*. Con la differenza che – mentre negli esperimenti condotti dallo psicologo statunitense l'anonimato garantiva e rafforzava l'obbedienza all'autorità – in Rete e sui social, l'anonimato diventa un incentivo a violare qualsiasi genere di regola.

Fraintendimenti ed errate letture, in cui – nonostante i diversi provvedimenti normativi europei [119] e nazionali [120] – in molti, tuttora, incorrono spesso, in particolar modo fra i più giovani [121]. Difatti, pur essendo nati e cresciuti assieme ad Internet e ai nuovi media ed avvalendosene di continuo, i nativi digitali non sono sempre adeguatamente alfabetizzati al loro uso corretto e, anzi, sono fra le categorie più esposte ai *cyber crimes*, dei quali, non di rado, oltre che vittime, diventano attori inconsapevoli [122].

---

[119] Tantissimi i provvedimenti adottati in ambito europeo, fra i più noti ed importanti: la *Direttiva del Parlamento e del Consiglio d'Europa n. 46 del 1995* (in tema di tutela dei dati personali); la *Convenzione di Budapest del Consiglio d'Europa* del 23 novembre del 2001 (sulla criminalità informatica); la *Risoluzione legislativa del Parlamento europeo sulla proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale* del 26 marzo 2019.

[120] A livello nazionale, si possono ricordare: la *Legge n. 547 del 1993* ("*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*"); la *Legge n. 675 del 1996* ("*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*"); il *D.Lgs. 196 del 2003* ("*Codice in materia di protezione dei dati personali*"); il *D.Lgs. n. 82 del 2005* ("*Codice della Pubblica amministrazione digitale*"); la *Legge n. 38 del 2006* ("*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet*"); la *Legge 48 del 2008* ("*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica*"); la *Legge 38 del 2009* ("*Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori*").

[121] Di qui, l'importanza e l'utilità delle tante campagne di informazione e delle iniziative realizzate nell'ambito del Progetto SIC (Generazioni Connesse). Progetto finanziato dalla Commissione Europea, coordinato dal Ministero dell'Istruzione, dell'Università e della Ricerca, e realizzato in collaborazione con l'Agenzia Generale per l'Infanzia e l'adolescenza, con la Polizia Postale e delle Comunicazioni, nonché, con Save the Children, Telefono Azzurro, e con il Movimento in Difesa del Cittadino (cfr. *https://www.generazioni connesse.it/site/it/home-page/*).

[122] Cfr. L. Di Mele, E. Isatto, *Se la competenza digitale non contrasta il*

Ed è proprio ai giovani che il diritto *dei/nei* social oggi guarda con particolare interesse e prudenza, come è stato recentemente dimostrato dal General Data Protection Regulation (GDPR) che, all'art. 8, disciplina il consenso al trattamento dei dati prestato dai minori durante l'accesso ai servizi della società dell'informazione [123]. Disposizione con la quale il Regolamento (UE) 679/2016 ha cercato di contemperare il diritto del minore ad usufruire delle straordinarie opportunità offerte dai nuovi media (che se utilizzati in maniera appropriata possono anche supportare lo sviluppo degli adolescenti [124]), con la necessità di tutelarne i dati e di scongiurare il pericolo di violazioni ed abusi [125]. Un tentativo, quello dell'art. 8, dettato dalla consapevolezza che – al di là delle criticità e dei possibili rischi – i social network (così come il Web in generale), per noi uomini, sono un po' come il mare descritto da Baudelaire ne *Les Fleurs du mal*: forza ignota, talvolta pericolo, ma anche, richiamo irresistibile, attrazione affascinante, spazio fecondo portatore di nuove opportunità e di ricchezze e, perché no, anche occasione di libertà:

"*Homme libre, toujours tu chériras la mer!*
La mer est ton miroir; tu contemples ton âme
Dans le déroulement infini de sa lame,
Et ton esprit n'est pas un gouffre moins amer.

---

cyber-bullismo, in *Media Education. Studi, ricerche e buone pratiche*, IX, 1/2019, pp. 146-160.

[123] Così, l'art. 8, comma 1: "[…] per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni". E, proprio con riferimento alla possibilità che gli Stati membri di stabilire un'età inferiore a quella prevista dal GDPR, è interessante ricordare che il d.lgs. 101 del 2018, con l'art. 2 *quinques*, ha previsto un limite di 14 anni.

[124] Cfr. H. Jenkins, *Culture partecipative e competenze digitali. Media education per il XXI secolo*, Milano, Feltrinelli, 2010; P.G. Lange, M. Ito, Creative production, in M. Ito et. al. (a cura di), *Hanging Out, Messing Around, and Geeking Out: Kids Living and Learning with New Media*, Boston, MIT Press, 2010, pp. 243-293.

[125] Vd. G. Riva, *Social network*, cit., p. 169; R. Trinchero, *Io non ho paura. Capire e affrontare il bullismo*, Milano, Franco Angeli, 2013.

Tu te plains à plonger au sein de ton image;
Tu l'embrasses des yeux et des bras, et ton cour
Se distrait quelques fois de sa propre rumeur
Au bruit de cette plainte indomptable et sauvage.
Vous êtes tous les deux ténébreux et discrets:
Homme, nul n'a sondé le fond de tes abîmes;
O mer, nul ne connaît tes richesses intimes,
Tant vous êtes jaloux de garder vos secrets!
Et cependant voilà des siècles innombrables
Que vous vous combattez sans pitié ni remord,
Tellement vous aimez le carnage et la mort,
O lutteurs éternels, o frères implacables!" [126].

[126] C. BAUDELAIRE, *Les Fleurs du Mal*, Gallimard, 2015.

III

NUOVE PROSPETTIVE DIDATTICHE: EDUCAZIONE E SCUOLA DIGITALE

Sommario

1. Brevi cenni introduttivi

Era il 1997 quando Pierre Lévy, tra i primi, avvertiva che lo sviluppo delle reti digitali, sommato alla sempre maggiore diffusione delle ICT, avrebbe modificato il nostro modo di pensare, producendo un'intelligenza collettiva, virtualizzata, planetaria e condivisa [1]. Dalla profezia del filosofo francese ci separano poco più di vent'anni. Un lasso temporale che potrebbe sembrare limitato, ma che, se posto in relazione con la straordinaria rapidità di avanzamento e di trasformazione propria della rivoluzione digitale [2], appare notevole e, comunque, sufficiente a far sì che quel presagio si sia – quantomeno per certi versi – tramutato in realtà.

Il recente progresso tecnologico ha, infatti, determinato il profilarsi di una nuova concezione di sapere: agile, facilmente fruibi-

[1] *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milano, Raffaello Cortina, 1996.

[2] Fra i tanti, cfr., P. CELLINI, *La rivoluzione digitale*, Roma, Luiss University Press, 2018.

le, interattiva, inclusiva e comunitaria [3]. Da un lato, la linea di demarcazione fra la nozione di informazione e quella di conoscenza [4] è diventata via via sempre più labile ed evanescente, dall'altro, si è assistito alla diffusione di inediti e non-convenzionali canali di divulgazione e di apprendimento [5]. Fenomeni questi, che, come è intuitivo, oltre a comportare tantissimi vantaggi in termini di semplicità, prossimità, rapidità e diffusione, hanno sollevato anche parecchie questioni. Basti pensare che, nell'opulenza della società tecnologica, tra flussi di dati, informazioni indistinte e device sempre connessi, l'acquisizione delle competenze digitali rischia di essere considerata più importante – e molto più utile – di quella dei contenuti e la conoscenza rischia di essere soppiantata da un mero nozionismo acritico [6].

La ragione è presto detta. Il fatto che la memoria sia ormai esterna e online e che tutti i più diversi contenuti possano essere reperiti in Rete – in ogni momento e senza troppi sforzi – favorisce un approccio frettoloso e superficiale alle informazioni [7]. Un approccio che difetta proprio di quella capacità di ricer-

---

[3] Si pensi a quanto osservato da Bauman: "[…] gli stimoli viaggiano indipendentemente dalle loro cause: anche se le cause sono locali, la portata delle loro ispirazioni è globale. […] Intrappolati nel world-wide-web, i modelli di imitazione volano in uno spazio extraterritoriale quasi a caso" (Z. BAUMAN, *Conversazione sull'educazione*, Trento, Erickson, 2012, in part., pp. 135-136).

[4] Sul passaggio dalla conoscenza all'informazione cfr. A.C. AMATO MANGIAMELI, *infra*, *Parte Prima*.

[5] Basti pensare ai tutorial, ai forum di discussione e alle tantissime piattaforme di condivisione che affollano il Web e alle quali, almeno una volta, ognuno di noi si è rivolto per ottenere delucidazioni (una definizione veloce e/o una spiegazione immediata) o per ricevere istruzioni su come fare qualcosa (scaricare un'app, editare o convertire dei *files*, acquisire e gestire spazi di memoria, avviare *backup*, configurare un pc, un *tablet* o uno *smartphone*, sincronizzare dispositivi, condividere documenti…).

[6] Sulla perdita di capacità critica, particolarmente interessanti le osservazioni di GÜNTHER ANDERS (*Il mondo dopo l'uomo. Tecnica e violenza*, trad. it., Milano, Mimesis, 2008, in part. p. 92).

[7] Un approccio che potremmo definire liquido (Z. BAUMAN, *Modernità liquida*, trad. it., Roma-Bari, Laterza, 2002) e che, a ben vedere, si inscrive perfettamente nella cultura consumistica del *take away* e dell'*usa e getta* (T. CANTELMI, *Tecnoliquidità. La psicologia ai tempi di internet: la mente tecnoliquida*, Cinisello Balsamo, San Paolo, 2013, in part. p. 10).

ca e di quel discernimento attivo e ponderato [8], che sono i prerequisiti della conoscenza [9].

Di qui, l'esigenza di riflettere e di interrogarsi sui riverberi che le nuove tecnologie possono avere sull'istruzione e, più precisamente, sull'educazione e sull'attività didattica. E sempre di qui la necessità – anche alla luce degli obiettivi della *Strategia dell'Unione europea per la gioventù* (2019-2027) [10] – di accostarsi al digitale, non solo percependone le mancanze e guardandosi dalle possibili minacce, ma anche riconoscendone i pregi e le potenzialità. Nella consapevolezza che, se è vero che già nel *Fedro* di Platone vengono posti in evidenza i rischi legati all'introduzione della scrittura e al mancato esercizio della memoria [11], è altrettanto vero che "la cultura è un coltello affondato nel futuro" [12], una "rivoluzione permanente" [13], e che nessun sapere può chiudersi completamente all'uso delle nuove tecnologie.

---

[8] Cfr., fra gli altri, R. TRINCHERO, *Contro la guerra cognitiva. Educare allo scetticismo attivo*, in *Media Education. Studi, ricerche, buone pratiche*, Vol. 9, 1/2018, pp. 17-36.

[9] Sull'importanza di sviluppare capacità che consentano di reperire, vagliare e rielaborare i contenuti disponibili in rete, particolarmente interessanti le osservazioni di ADRIANO FABRIS (*Introduzione*, in A. FABRIS [a cura di], *Scuola e digitale*, "Paradoxa", 3/2018).

[10] Adottata con la *Risoluzione del Consiglio (2018/C 456/01)* del 18 dicembre 2018, tale Strategia mira a: 1) collegare l'UE e i giovani; 2) favorire la parità di genere; 3) costruire società inclusive; 4) incentivare e assicurare l'informazione e il dialogo costruttivo; 5) salvaguardare la salute mentale e il benessere, 6) sostenere i giovani delle aree rurali; 7) garantire lavori di qualità per tutti; 8) promuovere un apprendimento di qualità; 9) assicurare uno spazio di partecipazione per tutti; 10) sviluppare un'Europa verde e sostenibile; 11) promuovere le organizzazioni giovanili e i progetti europei.

[11] Così, Socrate: "questa scoperta infatti, per la mancanza di esercizio della memoria, produrrà nell'anima di coloro che la impareranno la dimenticanza, perché fidandosi della scrittura ricorderanno dal di fuori mediante caratteri estranei, non dal di dentro e da se stessi".

[12] G. SANTYANA, *The Life of Reason, or the Phase of Human Progress, Introduction and Reason in common sense*, New York, The MIT Press, 1905.

[13] Z. BAUMAN, K. TESTER, *Società, etica, politica. Conversazioni con Zigmunt Bauman*, Milano, Raffaello Cortina, 2002.

2. Educazione e/o istruzione. Definizioni, caratteristiche e principali fonti normative

Ancor prima di domandarsi in che modo le nuove tecnologie possano incidere sull'istruzione e sull'educazione, è utile chiarire a cosa si allude con queste due espressioni. Difatti, nonostante siano spesso utilizzati alla stregua di sinonimi, tali termini, in realtà, rinviano ad ambiti e a livelli formativi fra loro molto differenti (per modalità, ampiezza e finalità). E proprio a partire dalla comprensione e dalla riaffermazione di tale differenza, può risultare più semplice riflettere sulle ICT, così da coglierne i pregi e i limiti, e da individuarne l'uso più opportuno e funzionale allo scopo che – di volta in volta e a seconda delle circostanze – si intende raggiungere: sia esso quello di istruire oppure quello di educare.

Come spesso accade, anche in questo caso, l'etimologia si rivela una valida alleata in quanto, facendo luce sui significati e sulle valenze linguistiche, indirettamente contribuisce a dipanare e a chiarire anche alcune importanti questioni di merito.

In prima battuta, è utile sottolineare che il verbo "educare" (dal latino *educere*, letteralmente: "tirare fuori", "condurre fuori") ha come primo significato quello di "portare in superficie", nel senso di indurre "a maturazione", ovvero, di portare "a compimento" ciò che di per sé è già contenuto e insito in un determinato soggetto e che, grazie all'educazione, viene semplicemente esternato. Diversamente, il verbo "istruire" (che trae origine dal latino *instruere*, nella triplice accezione: "preparare", "costruire" e "insegnare") prevede l'indottrinamento del soggetto, che – proprio attraverso l'istruzione – apprende *ex novo* contenuti e competenze di cui se no sarebbe sprovvisto.

Altrimenti detto ed in breve, l'educazione presuppone un processo maieutico di ricerca, comprensione, estrazione e valorizzazione, invece, l'istruzione implica l'apprendimento di nozioni e l'acquisizione di nuove capacità, come avviene nel caso della lettura, della scrittura o del calcolo.

Come è intuitivo, tali differenze condizionano anche il rapporto che i due diversi ambiti hanno con le nuove tecnologie. In particolare, l'istruzione, riguardando prevalentemente la trasmissione e la condivisione di concetti e contenuti, può svolgersi senza particolari difficoltà anche in ambienti digitali e attra-

verso piattaforme tecnologiche, come del resto avviene con l'*e-learning* [14].

Al contrario, l'educazione, travalicando la mera acquisizione di cognizioni ed avendo a che vedere con la formazione e con lo sviluppo delle funzioni mentali [15] e dei valori morali [16] dell'individuo, pur potendosi avvalere delle ICT, richiede sempre un intervento di indirizzo, di controllo e – laddove necessario – anche di correzione.

Sin qui, il distinguo fra istruzione ed educazione. Un distinguo che, però, anche a livello giuridico, è stato spesso sottovalutato, dando origine ad un'equivoca sovrapposizione di piani in cui il diritto-dovere all'educazione ha spesso ceduto il passo al diritto-dovere all'istruzione, concorrendo – seppur involontariamente ed indirettamente – ad un uso improprio e poco consapevole delle nuove tecnologie. Un veloce *excursus* normativo potrà meglio chiarire i termini della questione.

Guardando al diritto internazionale, va detto subito che il pri-

---

[14] A proposito dell'*e-learning* e – più correttamente – dell'istruzione nell'*infosfera*, FLORIDI osserva che le ICT possono "favorire l'affermazione di un livello di didattica personalizzata […] in contesti non elitari" permettendo "a milioni di individui di accedere ad un'esperienza […] ritagliata sulle proprie esigenze" (*La quarta rivoluzione*, cit., pp. 89-97, in part. p. 93). In argomento, particolarmente interessanti le osservazioni di MALDONADO che riflette sul più generale concetto di apprendimento a distanza (*Teledidattica come telelavoro*, in T. MALDONADO, *Critica della ragione informatica*, trad. it., Milano 2006, p 126). Per ulteriori approfondimenti, poi, si vedano, fra gli altri, anche: A. DE PIANO, *Telematica e didattica*, in P. FRIGNANI, L. GALLIANI [a cura di], *Atti del convegno Expo e-learning*, Ferrara 2004; S. DOWNES, *E-learning 2.0*, in *eLearn Magazine*, 10/2005; A. DE PIANO, *Dalla trasmissione di informazioni alla condivisione di conoscenze*, in *Il Giornale dell'E-Learning*, 3/2008; A. LAMANDINI, *L'evoluzione dell'e-learning ed e-learning in evoluzione. Ricerche di Pedagogia Didattica*, in *Journal of Theories and Research in Education*, 1/2009).

[15] Vd. F. RAVAGLIOLI, *Educazione occidentale*, Roma, Armando Editore, 1988, vol. III, pp. 354-359.

[16] È interessante ricordare che Socrate – sostenitore della *παιδεία* – è il primo a mettere in luce la correlazione fra educazione e morale, sottolineando che l'*ἀρετή*, oltre ad essere virtù pratica, è anche virtù etica, e che l'educazione non può prescindere dalla conoscenza del bene e, in ultima analisi, dalla filosofia (per un'agile ricostruzione del pensiero del filosofo greco, cfr., fra gli altri, A. STAVRU, *La nuova paideia di Socrate*, in P. MANGANARO, E. VIMERCATI [a cura di], *Formare e tras-formare l'uomo. Per una storia della filosofia come paideia*, Pisa, ETS, 2017, pp. 31-49).

mo richiamo legislativo all'educazione/istruzione risale al 1948 e si rintraccia nell'art. 26 della *Dichiarazione Universale dei Diritti dell'Uomo*. Dove, nonostante si faccia riferimento allo sviluppo della personalità umana e alla formazione culturale, morale, civile e politica dell'individuo [17] – anziché di diritto all'educazione – si parla esclusivamente di diritto all'istruzione.

Un'inversione ed una sostituzione concettuale tutt'altro che marginale, che si riscontra anche nell'art. 13 del *Patto Internazionale sui Diritti Economici, Sociali e Culturali* del 1966, in cui – riprendendo pressoché fedelmente la formulazione della Dichiarazione Universale – non si fa alcun cenno al diritto all'educazione, limitando la trattazione al solo diritto all'istruzione e, di fatto, andando a ripiegare e ad appiattire il primo (e ben più rilevante ed ampio diritto) sul secondo.

Decisamente unico è, invece, l'approccio adottato dalla *Convenzione sull'eliminazione di tutte le forme di discriminazione nei confronti delle donne* del 1979, nella quale, all'art. 10, il diritto fondamentale all'educazione assurge a prerequisito di non discriminazione, uguaglianza e parità, in ogni ambito: scolastico, familiare, lavorativo e socio-politico.

Un discorso a parte deve, poi, essere riservato alla *Convenzione sui diritti del fanciullo* del 1989: primo e più importante provvedimento di respiro internazionale che adotta un approccio completo e integrato al diritto all'educazione. Un approccio con il quale si dà simultaneamente conto del diritto fondamentale del bambino all'educazione, dei corrispondenti doveri dei genitori e, non da ultimo, anche delle diverse responsabilità assunte dagli Stati aderenti [18]. E non è tutto. Infatti, tratteggiando le finalità alle quali deve tendere l'educazione [19], la Convenzione mette bene in

---

[17] Così, l'art. 26: "[…] L'istruzione deve essere indirizzata al pieno sviluppo della personalità umana ed al rafforzamento del rispetto dei diritti umani e delle libertà fondamentali. Essa deve promuovere la comprensione, la tolleranza, l'amicizia fra tutte le nazioni, i gruppi razziali e religiosi, e deve favorire l'opera delle Nazioni Unite per il mantenimento della pace. […]".

[18] Sul punto, si vedano, gli artt. 18, 24 e 28.

[19] Queste, nel dettaglio, le finalità dell'educazione così come individuate dall'art. 29: "[…] l'educazione del fanciullo deve avere come finalità: a) favorire lo sviluppo della personalità […] delle […] facoltà e delle […] attitudini mentali e fisiche, in tutta la loro potenzialità; b) sviluppare nel fanciullo il rispetto dei diritti dell'uomo e delle libertà fondamentali e dei principi con-

evidenza anche il particolare rapporto di *genus* ad *species* che lega il diritto all'educazione e il diritto all'istruzione.

Infine, con specifico riferimento al legame fra diritto all'educazione ed educazione ai diritti umani, oltre ovviamente ai diversi rapporti dell'Unesco [20], non si può non rammentare la *Dichiarazione delle Nazioni Unite sull'educazione e la formazione ai diritti umani* del 2011. Dichiarazione nella quale l'educazione personale-individuale viene posta in relazione con quella politico-sociale e i diritti umani vengono prospettati come il *trait d'union* che congiunge le due dimensioni [21].

Analogamente alla normativa internazionale, anche quella europea si richiama con maggiore frequenza all'istruzione anziché all'educazione. Esemplari, da questo punto di vista, le formulazioni adottate dall'art. 14 della *Carta dei Diritti fondamentali dell'Unione Europea* (dedicato per l'appunto all'istruzione) [22], così co-

---

sacrati nella Carta delle Nazioni Unite; c) sviluppare nel fanciullo il rispetto dei suoi genitori, della sua identità, della sua lingua e dei suoi valori culturali, nonché il rispetto dei valori nazionali del paese nel quale vive, del paese di cui può essere originario e delle civiltà diverse dalla sua; d) preparare il fanciullo ad assumere le responsabilità della vita in una società libera, in uno spirito di comprensione, di pace, di tolleranza, di uguaglianza tra i sessi e di amicizia tra tutti i popoli e gruppi etnici, nazionali e religiosi, e delle persone di origine autoctona; e) sviluppare nel fanciullo il rispetto dell'ambiente naturale. […]".

[20] Si ricordino: il *Rapporto Faure "Apprendere ad essere"* del 1972 (in cui l'educazione è vista come una responsabilità della società – comunità educante – e dove, per la prima volta, viene introdotta la nozione di educazione permanente); il *Rapporto Delors "Nell'educazione un tesoro"* del 1996 (che individua i quattro pilastri dell'educazione:1) imparare a conoscere; 2) imparare a fare; 3) imparare a vivere insieme; 4) imparare a essere); nonché il più recente *Rapporto Education for All "Reaching the Marginalized"* del 2010 (che sottolinea e denuncia i problemi educativi dei paesi in via di sviluppo).

[21] In tal senso, merita d'essere qui richiamato l'art. 2, nel quale si legge: "[…] L'educazione e la formazione ai diritti umani comprende tutte le attività di educazione, formazione, informazione, coscientizzazione e apprendimento intese a promuovere l'universale rispetto e [l'] osservanza di tutti i diritti umani e [delle] libertà […]".

[22] In cui si legge: "1. Ogni individuo ha diritto all'istruzione e all'accesso alla formazione professionale e continua. 2. Questo diritto comporta la facoltà di accedere gratuitamente all'istruzione obbligatoria. 3. La libertà di creare istituti di insegnamento nel rispetto dei principi democratici, così come il diritto dei genitori di provvedere all'educazione e all'istruzione dei loro figli secondo le loro convinzioni religiose, filosofiche e pedagogiche, sono rispettati secondo le leggi nazionali che ne disciplinano l'esercizio".

me quelle che si ritrovano nel Rapporto *Crescita, competitività occupazione. Le sfide e le vie da percorrere per entrare nel XXI secolo* del 1993, nel Rapporto *Insegnare e apprendere. Verso una società cognitiva* del 1995 e – non da ultimo – nelle Conclusioni del Consiglio del 12 maggio 2009 su *Un quadro strategico per la cooperazione europea nel settore dell'istruzione e della formazione* "ET 2020". Conclusioni che, individuando i quattro obiettivi strategici [23] diretti a promuovere la realizzazione dei cittadini europei e a contribuire alla prosperità economica sostenibile, si incentrano in maniera prevalente sull'istruzione.

Passando a considerare la normativa nazionale, va detto subito che il nostro legislatore (esattamente come quello internazionale ed europeo) sembra fare un uso abbastanza disinvolto ed esteso dell'espressione istruzione, alla quale ricorre anche quando, in realtà, nei contenuti, rinvia alla dimensione educativa. Va altresì detto che, all'interno del nostro ordinamento, i riferimenti espliciti all'educazione non sono molti. Ad esempio, nella Costituzione – ad eccezione degli artt. 2 e 3 che, con riguardo allo sviluppo e alla piena realizzazione della persona, indirettamente rimandano alla sfera educativa – il diritto all'educazione non viene praticamente mai menzionato. E persino negli artt. 33 e 34 si parla unicamente di istruzione, come se, quest'ultima, implicitamente abbracciasse anche la ben più ampia e composita sfera educativa.

Un certo mutamento di prospettiva si registra, invece, nel Codice Civile che, nell'art. 147, fra gli obblighi dei genitori, annovera sia l'istruzione che l'educazione. Ambiti che – in questo caso – il legislatore non tratta, né come sinonimi, né men che meno come endiadi, ma che, in questa sede, richiama congiuntamente nel chiaro intento di ricomprenderli entrambi fra i doveri nei confronti dei figli.

Sempre guardando al nostro Codice Civile, non si può fare a

---

[23] Questi, in sintesi gli obiettivi individuati: 1) l'apprendimento permanente e la mobilità devono diventare una realtà; 2) la qualità e l'efficacia dell'istruzione e della formazione devono essere migliorate; 3) l'equità, la coesione sociale e la cittadinanza attiva devono essere promosse; 4) la creatività, l'innovazione, l'imprenditorialità e l'acquisizione delle competenze digitali dovrebbero essere incoraggiate e promosse (per una descrizione più ampia e dettagliata rinvio al testo delle *Conclusioni*, disponibile in rete all'indirizzo *https://archivio.pubblica.istruzione.it/buongiorno_europa/allegati/conclusioni_et.pdf*, pp. 18-20).

meno di ricordare l'art. 2048, che introduce e disciplina la c.d. *culpa in educando*: ovverosia, la responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte per gli eventuali danni cagionati dai figli minori non emancipati, dalle persone soggette a tutela, dagli allievi oppure dagli apprendisti. Come è evidente, si tratta di una disposizione alquanto significativa che – a fronte dell'utilizzo sempre più diffuso e pervasivo delle nuove tecnologie da parte dei minori – assume un rilievo del tutto particolare. Si pensi, ad esempio, al fenomeno del *cyberbulling* e alla responsabilità di cui sono investiti i genitori, gli educatori e – in taluni casi – persino gli istituti scolastici [24].

Da ultimo, e sempre con riferimento alla normativa nazionale, si segnalano la l. n. 107 del 13 luglio 2015 (*Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti*) [25] e il successivo d.lgs. n. 65 del 13 aprile 2017 [26] (*Istituzione del sistema integrato di educazione e di istruzione dalla nascita sino a sei anni*) [27]. Provvedimenti che sono volti ad assicurare un uniforme ed adeguato livello di coordinamento pedagogico su tutto il territorio nazionale e che – oltre ad allinearsi con gli obiettivi individuati dall'Unione Europea (vale a dire: rendere più coerenti ed efficaci gli interventi nazionali,

---

[24] Nel dettaglio, la l. n. 71 del 29 maggio 2017 – recante *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo* – prevede che, nel caso in cui il soggetto che realizza atti di cyberbullismo sia un minore di quattordici anni, non si configurerà una responsabilità penale e, tuttavia, i genitori del cyberbullo potranno comunque essere tenuti a risarcire la vittima per presunta *culpa in educando*. Risarcimento al quale – in base al combinato disposto del summenzionato art. 2048 e dell'art. 61 della l. n. 312 dell'11 luglio 1980, che disciplina la responsabilità patrimoniale del personale direttivo, docente, educativo e non docente – oltre ai genitori, possono essere chiamati anche gli insegnanti.

[25] Legge recante la disciplina su *La buona scuola*, *infra* nota 10.

[26] Adottato in risposta alla Raccomandazione della Commissione europea n. 112 del 20 febbraio 2013 (*Investire nell'infanzia per spezzare il circolo vizioso dello svantaggio sociale*), il Sistema integrato per l'istruzione e l'educazione ha come prima finalità quella di garantire alle bambine e ai bambini pari opportunità di educazione, istruzione, cura, relazione e gioco, superando i divari territoriali, economici, etnici e culturali. Fra le sue peculiarità, anche quella di individuare dei livelli essenziali – o più correttamente – dei livelli standard, vale a dire, quelle prestazioni minime che, come tali, devono essere garantite a tutti senza che si diano distinzioni.

[27] *Infra*, nota 10.

coordinare ed agevolare i processi di condivisione, e migliorare i sistemi di istruzione e di formazione)[28] – si dimostrano particolarmente attenti tanto al diritto all'istruzione quanto al diritto all'educazione[29].

Sin qui, al di là degli usi e degli abusi linguistici, l'effettiva portata dei due ambiti formativi e, assieme ad essa, anche le ragioni che giustificano il loro diverso rapporto con le tecnologie: funzionale e tutto sommato lineare quello dell'istruzione; ben più articolato e controverso quello dell'educazione.

3. Tecnologie digitali e modelli educativi

Già da diversi anni siamo immersi in una dimensione del tutto particolare, quella della *tecnosfera* e dell'*infosfera*[30]. Una dimensione nuova, che è frutto del connubio fra tecnica, attività umana ed informazione e, nella quale, il digitale sostituisce l'analogico, mentre il virtuale[31] sembra destinato a soppiantare il reale. Anche per questo motivo, ci troviamo a far di conto con una serie di questioni che – oltre alla *biosfera*, sempre più orientata alla manipolazione e alla ricodificazione della vita biologica[32] – riguardano anche la *noosfera*. Questioni che incidono sulle nostre strutture

[28] D'obbligo, il rinvio alla Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni (*Mobilitare, collegare e responsabilizzare i giovani: una nuova strategia dell'UE per la gioventù*) del 22 maggio 2018; nonché alla successiva Risoluzione del Consiglio dell'Unione Europea e dei rappresentanti dei governi degli Stati membri, riuniti in sede di Consiglio, su un quadro di cooperazione europea in materia di gioventù (*Strategia dell'Unione europea per la gioventù 2019-2027*) del 18 dicembre 2018.

[29] Con riguardo alla l. n. 107 del 13 luglio 2015, particolarmente significativi, i riferimenti all'educazione alla cittadinanza attiva, alla pace, ad un approccio interculturale, alla parità e allo sport.

[30] Sull'*infosfera*, cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, cit., pp. 27-65.

[31] D'obbligo, il richiamo alle riflessioni di P. LÉVY, *Il virtuale*, trad. it, Milano, Cortina Editore, 1997.

[32] Sull'affascinante e, al contempo, controverso rapporto fra il corpo e le nuove tecnologie e – in particolar modo – sulla ricodificazione della nostra identità antropologica e sul possibile ricorso alle c.d. biofabbriche cfr. A.C. AMATO MANGIAMELI, *Corpi docili Corpi gloriosi*, Torino, Giappichelli, 2007.

mentali [33] e che modificano il nostro stesso modo di pensare [34]. Ciononostante, la relazione fra tecnologie, digitale e educazione – lungi dall'essere risolta – suscita ancora tutta una serie di incomprensioni, timori e diffidenze.

Terreno di dibattito e di confronto, l'educazione digitale non divide solo insegnanti ed educatori, ma anche giuristi, informatici e sociologi che, fra minacce e vantaggi, provano in vario modo ad orientarsi. Da un lato, coloro che guardano alla tecnologia con sospetto e che ne percepiscono soltanto i pericoli [35]. Dall'altro, quelli che adottano un approccio ottimistico ed entusiastico [36] e che, per questo motivo, sottostimano o ignorano rischi e criticità. Due distinte interpretazioni e due polarità che, in un'alternanza pressoché ininterrotta, si succedono dividendosi il primato. Talvolta, a prevalere è una chiusura cieca e sterile, talaltra, invece, è un'apertura acritica e indiscriminata.

Di qui, la necessità e l'urgenza di un approccio ponderato, bilanciato ed equilibrato, che sappia contemperare prospettive ed esigenze differenti. Solo in questo modo, infatti, la dimensione educativa potrà effettivamente giovarsi dell'irrinunciabile supporto delle ICT: sfruttandone appieno la memoria e le capacità [37],

---

[33] In merito all'incidenza che le nuove tecnologie hanno sulla mente, si vedano, fra gli altri: T. CANTELMI, C. DEL MIGLIO, M. TALLI, A. D'ANDREA, *La mente in Internet: psicopatologie delle condotte online*, Padova, Piccin, 2000; S. CANNIZZARO, F. DI MARIA, *Reti telematiche e trame psicologiche*, Milano, Mondadori, 2001; V. CARRETTI, D. LA BARBERA, *Psicopoatologia delle realtà virtuali*, Milano, Mondadori, 2001; P. PANCHERI, A. SIRACUSANO (a cura di), *Psichiatria e mass media*, Roma, CIC, 2002.

[34] Sul punto, particolarmente significative ed efficaci le osservazioni di CANTELMI: "il digitale cattura, avanza inarrestabile, esalta ed eccita. La rivoluzione digitale, inaugurando affascinanti universi di conoscenza e di esperienza, ha già […] modificato il registro delle nostre possibilità mentali e sensoriali, contribuendo a plasmare una nuova cultura e differenti forme e modalità di sentire il rapporto con se stessi, con gli altri e con il mondo" (T. CANTELMI, *Homo tecno-digitalicus 2.0*, in ID., *Tecnoliquidità*, cit., pp. 11-36, in part., p. 25).

[35] Come, ad esempio, VIRILIO che, non a caso, introduce un parallelismo fra la c.d. bomba informatica e quella atomica (P. VIRILIO, *La bomba informatica*, trad. it., Milano, Raffaello Cortina, 2000).

[36] Esemplare, in tal senso, la visione prospettata da LÉVY (*L'intelligenza collettiva*, cit.).

[37] Fra gli altri, si vedano: F. CIOTTI, G. RONCAGLI, *Il mondo digitale. Introduzione ai nuovi media*, Roma-Bari, Laterza, 2000; A. CALVANI, *Che cos'è la*

senza tuttavia correre il rischio di snaturarsi, riducendosi ad un mero "passa parola" di informazioni indistinte e prive di controllo [38].

Un primo ed essenziale passo in questa direzione può essere compiuto a partire dalla consapevolezza che l'educazione, oltre ad essere un diritto fondamentale (il diritto di ciascun bambino alla costruzione delle proprie strutture mentali e dei propri principi morali [39]), è anche un dovere: familiare, sociale e intergenerazionale. Un obbligo al quale, si può adempiere solo a condizione di non compiere l'errore – oggi per il vero alquanto diffuso – di delegare *sic et simpliciter* ogni compito alla tecnologia e ai suoi mezzi, omettendo di vigilare sui linguaggi, sulle modalità di divulgazione, di fruizione e, ovviamente, anche sui contenuti.

Il rischio è quello di passare dai modelli pedagogico-educativi tradizionali (normativo-autoritari e/o affettivo-protettivi) a quelli commerciali e seduttivi. Modelli, questi, che si basano su un approccio *peer-to-peer* e "social" e che rischiano di mettere in secondo piano e di non tener adeguatamente conto delle finalità dell'educazione. Un rischio al quale se ne aggiungono altri, come, ad esempio: la maggiore difficoltà di comunicazione fra giovani e adulti ed il possibile incremento del *digital devide intergenerazionale* [40], oppure la diffusione di nozioni de-centralizzate e de-gerarchizzate, che si rivelano del tutto prive di autorevolezza [41] e di credibilità [42].

---

tecnologia nell'educazione, Roma, Carocci, 2004; D. PERSICO, V. MIDORO (a cura di), *Pedagogia nell'era digitale*, Ortona, Menabò, 2013; L. MESSINA, M. DE ROSSI, *Tecnologie, formazione e didattica*, Roma, Carocci, 2015.

[38] Un "passa parola" che – a ben vedere – nella società dell'opulenza informativa si incontra spesso (vd. V. MAYER-SCHÖNBERGER, K.N. CUKIER, *Big data. Una rivoluzione che sta trasformando il nostro modo di vivere e già minaccia la nostra libertà*, Milano, Garzanti, 2013, in part., pp. 18, 20, 22).

[39] J. PIAGET, *Il diritto all'educazione nel mondo attuale*, trad. it., Milano, Edizioni di Comunità, 1951.

[40] Vd. P. FERRI, *Nativi digitali*, Milano, Mondadori, 2011.

[41] Cfr. quanto osservato da D. LA BARBERA, S. CANNIZZARO, S. LA BARBERA, C. LA CASCIA, *Le dipendenze tecnologiche in adolescenza. Aspetti tecnici e dati della ricerca*, in V. CARETTI, D. LA BARBERA (a cura di), *Addiction. Aspetti biologici e di ricerca*, Milano, Raffaello Cortina, 2010, pp. 183-195.

[42] Noto, da questo punto di vista, il fenomeno delle *fake news* (cfr. M. ADINOLFI, *Hanno tutti ragione? Post-verità, fake news, big data e democrazia*, Salerno, Astrolabio, 2019).

Si consideri però: se è vero che la percezione di questi pericoli rappresenta un freno alla diffusione delle tecnologie digitali; è altrettanto vero che si tratta di pericoli che possono essere evitati e ridimensionati grazie ad alcune accortezze come quella di accompagnare e di monitorare l'accesso alle ICT da parte dei minori, ricorrendo – laddove necessario – a filtri, limitazioni e interventi correttivi. A costituire una minaccia, infatti, non è tanto la possibilità che l'educazione possa aprirsi alle tecnologie digitali, ma quella che, così facendo, essa possa (o intenda) abdicare a quelle particolari funzioni pedagogiche che – da sempre – le sono proprie e la individuano [43].

Contrariamente a quanto si tende a pensare, il connubio fra educazione e tecnologia digitale non solo non può essere ritenuto di per se stesso un azzardo ma non rappresenta nemmeno una novità in senso proprio. Non è una novità perché la storia dell'educazione è sempre stata costellata da incursioni tecnologiche (dall'invenzione della stampa all'uso del limografo, dal ciclostile al videoproiettore, sino ad arrivare al più recente impiego della lavagna interattiva multimediale, la c.d. LIM [44]) e non è neppure un azzardo perché i pericoli legati all'uso improprio dei mezzi e delle strumentazioni possono concretizzarsi solo nel caso in cui l'educatore venga meno al suo ruolo, costringendo il minore ad un *empowerment* precoce [45]. Un empowerment che lo tramuta in un "piccolo adulto" e che – abbandonandolo in un universo di stimoli e di interazioni che non tengono conto della sua età e delle sue fragilità [46] – può metterne a repentaglio (e com-

---

[43] Sintetiche ma, al contempo, particolarmente significative ed efficaci le osservazioni del Presidente di Indire, GIOVANNI BIONDI (*Scuola digitale, perché è un connubio necessario e come esorcizzare la paura*, in *Agenda Digitale*, 9 febbraio 2018).

[44] Vd. A. DE PIANO, *La Lavagna Interattiva Multimediale. I risultati di una ricerca esplorativa*, in *Prospettiva Persona*, 88, 2014, pp. 49-54; S. PENGE, *Introduzione. Dallo smartphone alla LIM: la parentela delle interfacce*, in V. ZAGAMI, *Fare scuola nella classe digitale. Tecnologia e didattica attiva fra teoria e pratiche d'uso innovative*, Torino, Loescher, 2013, p. 5 ss.

[45] Sul punto, D. LA BARBERA, S. CANNIZZARO, S. LA BARBERA, C. LA CASCIA, *Le dipendenze tecnologiche in adolescenza*, cit.

[46] Tantissimi i pericoli ai quali i minori possono trovarsi esposti in assenza di una "mediazione" dell'adulto-educatore: dalla possibilità di essere oggetto di adescamento (il c.d. *grooming*, di cui all'art. 609 *undicies* c.p.) e di cadere vittime di violenze a sfondo sessuale (e di condotte illecite quali la

prometterne del tutto) il fondamentale diritto all'infanzia [47].

La via da percorrere è, dunque, assolutamente chiara. Non si tratta né di promuovere un accesso spregiudicato ed acritico alle tecnologie digitali, né di rifuggirle in maniera aprioristica e ottusa; al contrario, si tratta di accompagnare, orientare e regolamentare la loro diffusione [48].

Se così, è evidente che occorre operare un cambio di prospettiva che muova da alcuni essenziali punti fermi:

i) in primo luogo, è necessario tenere a mente che, al di là delle sollecitazioni e delle trasformazioni, l'educazione ha sempre avuto un obiettivo costante e primario: quello di formare teste che, oltre ad essere "piene" (ossia edotte e istruite), fossero anche "ben fatte" [49], in quanto autonome e dotate di discernimento;

ii) in secondo luogo, bisogna avvedersi del fatto che la tecnologia e la cultura non sono dimensioni antagoniste ma sfere correlate che si implicano e si accrescono reciprocamente. Infatti, la cultura è il motore dell'innovazione tecnologica [50] e la tecnologia, influenzando il sistema sociale, alimenta e diffonde nuova cultura [51];

iii) in terzo luogo, si deve capire che oggi l'educazione e, con essa, anche l'attività didattica e la scuola non sono chiamate solo ad *accostarsi al digitale* (come un qualsiasi mezzo [52]), ma de-

---

pedopornografia, il *sexting* e la *sextortion*, artt. 600 *ter* e 609 *undicies* c.p.), al rischio si subire pericolose vessazioni (come avviene nel caso del *cyberbullismo*, disciplinato di recente dalla l. n. 71 del 18 maggio 2017) e manipolazioni psicologiche (come nel caso, del tutto particolare, in cui il minore venga istigato alla magrezza estrema e all'adozione di atteggiamenti anoressici e/o bulimici, art. 580 *bis* c.p.).

[47] D'obbligo il richiamo a J. PIAGET, *Il linguaggio del fanciullo*, trad. it., Firenze, Giunti, 1962 e E.H. ERIKSON, *Gioventù e crisi dell'identità*, trad. it., Roma, Armando Editore, 1974.

[48] Con riferimento al rapporto fra nuove tecnologie e diritto, e a proposito dell'importanza di una regolamentazione rispettosa ed efficace, cfr. AMATO MANGIAMELI, *infra*, *Parte Prima*.

[49] Si veda E. MORIN, *La testa ben fatta*. *Riforma dell'insegnamento e riforma del pensiero*, trad. it., Milano, Raffaello Cortina, 2000.

[50] In tal senso, L. GUERRA (a cura di), *Tecnologie dell'educazione e innovazione didattica*, Parma, Junior, 2010, in part. p. 15.

[51] Benché non recentissime, si ricordino le osservazioni di R. CERRI MUSSO, *Tecnologie educative*, Genova, La Scuola, 1995, p. 22.

[52] In tal senso la "sfida" del digitale non sta nel suo uso, ma nella sua "funzionalizzazione didattica" (M. MUSCARÀ, *Il dialogo possibile tra scuola e*

vono *farsi esse stesse digitali*, lasciandosi permeare, contaminare ed estendere dalle tecnologie [53]. Ad esempio: sperimentando nuovi canali, prospettando nuovi ambienti, privilegiando nuovi linguaggi, individuando nuovi metodi e adottando nuove strategie.

4. La nuova scuola

L'impatto che le nuove tecnologie possono avere ed hanno sulla didattica è davvero considerevole, e parecchi sono i segnali della trasformazione strutturale che in questi anni sta interessando – e in buona parte ha già interessato – il nostro sistema scolastico: sempre più digitale, multimediale e, in una parola, sempre più *open source*. Fra gli indizi più significativi e paradigmatici di questa transizione:

i) l'*eTwinning*, la community europea – lanciata con il *Programma eLearning* [54] e poi integrata in *Erasmus Plus* (2014-2020) [55] – pensata per il personale (docente, dirigente e bibliotecario) e per gli studenti delle scuole degli stati membri aderenti, fra cui l'Italia. Una piattaforma gratuita e sicura [56], gestita dal consorzio internazionale *European Schoolnet*, grazie alla quale – oltre a comunicare, a collaborare, a sviluppare progetti e a condividere idee [57] – è

nuove tecnologie nella formazione degli insegnanti, in *Pedagogia oggi*, 2/2016, pp. 222-235).

[53] Come sottolinea anche GUERRA, le tecnologie "[…] devono essere apprese e utilizzate strutturalmente all'interno di modelli tecnologici dell'educazione" (*Tecnologie dell'educazione e innovazione didattica*, cit., p. 19). Da questo punto di vista, è importante chiarire che il docente non deve tramutarsi in un tecnico, ma deve operare scelte didattico-educative consapevoli e funzionali, che contemplino l'inclusione delle nuove tecnologie nel processo di insegnamento-apprendimento.

[54] Iniziativa biennale (2004-2006) della Commissione europea per l'integrazione effettiva delle ICT nei sistemi di istruzione e formazione in Europa.

[55] *Programma europeo per l'istruzione, la formazione, la gioventù e lo sport*, approvato con il *Regolamento (UE) 2013/1288*.

[56] La consultazione dei progetti, ad esempio, è riservata agli insegnanti che vi partecipano e può essere consentita agli studenti soltanto dietro invito.

[57] Basti pensare che – accedendo gratuitamente ad *eTwinning Portal* (attualmente disponibile in 28 lingue) – gli insegnanti possono entrare a far parte dei *Gruppi eTwinning*, spazi virtuali in cui i docenti si incontrano e discutono di temi specifici. Ben 14 i gruppi al momento attivi: "*Coding at*

possibile ricevere supporto tecnologico e avvalersi di strumenti e di servizi fra i quali l'*App eTwinning Live* (pensata per i dispositivi mobili) e lo *School Education Gateway* (specificatamente rivolto agli insegnanti, ai dirigenti scolastici, ai politici, agli esperti di settore e, in generale, a tutti coloro che operano nel campo dell'istruzione scolastica);

ii) la *Città educante*, un progetto quadriennale avviato nel 2014 e cofinanziato dal MIUR, articolato in tre macro-aree tematiche: 1) scuola; 2) società; 3) tecnologia. Teso a innovare l'approccio educativo, a favorire la connessione scuola-aziende-territorio, e ad incentivare la ricerca in tema di *cloud computing*, *collaborative sourcing*, *social networks, big data analysis* e *robotica*, il progetto *Città educante* ha permesso la sperimentazione di nuovi modelli di insegnamento e di apprendimento orientati allo sviluppo e all'inclusione sociale [58];

iii) il *life-long-learning* (LLL), un particolare processo di auto-orientamento e auto-educazione che si inserisce in *Erasmus Plus* (2014-2020) e che si sviluppa lungo tutto l'arco della vita della persona. Un percorso di formazione continua che, giovandosi delle ICT, è calibrato sulle specifiche esigenze del singolo. Oggetto d'interesse da parte dell'Unione Europea già in occasione del Consiglio Europeo di Lisbona del 2000, il *life-long-learning* si propone il raggiungimento di tre importanti obiettivi strategici, ossia: 1) migliorare la qualità e l'efficacia dei sistemi di istruzione e di formazione; 2) facilitare l'accesso di tutti gli individui (senza che si diano distinzioni di sorta) ai sistemi di istruzione e di formazione; 3) aprire (anche grazie all'apporto delle nuove tecnologie) i sistemi di istruzione e di formazione al mondo esterno;

iv) la *flipped classroom* (o anche *flipped lesson*), ossia la c.d. classe capovolta. Sperimentata per la prima volta nel 2007 dagli americani Jonathan Bergmann e Aaron Sams nella Woodland

---

schools"; "English as a Second Language"; "Entrepreneurship in education"; "Bringing eSafety into eTwinning projects"; "French as a Second Language"; "STEM"; "Sustainable Schools Network"; "Game-based classroom"; "Inclusive Education"; "Creative Classroom"; "Virgilio-Your eTwinning Guide"; "Gender-Know How to Stop Stereotypes"; "Integrating Migrant Students at School"; "School Leadership".

[58] Maggiori dettagli sono disponibili online sul portale del progetto (*http://www.cittaeducante.it/SitePages/sito/progetto.html*).

Park High School del Colorado, la *flipped classroom* è l'emblema di una didattica che, sfrutta le potenzialità offerte dalla tecnologia, per cambiare volto. Ribaltando ed invertendo completamente le modalità e la scansione temporale tipiche della lezione tradizionale (in cui alla spiegazione in aula segue lo studio individuale a casa e, successivamente, un momento di verifica sempre in aula), la *flipped lesson* si basa, invece, su episodi di apprendimento situati online (EAS) [59], che vengono caricati in forma di video-tutorial sulle varie piattaforme *e-learning*. Videolezioni accessibili in qualsiasi momento, che possono essere visualizzate dallo studente finché non ne abbia appreso tutti i contenuti. Autentico modello di connubio virtuoso fra scuola e nuove tecnologie, la *flipped classroom* – oltre a rispondere pienamente ed efficacemente alle finalità didattiche, consentendo a tutti gli studenti di apprendere i contenuti proposti, indipendentemente da quelle che possono essere le loro differenti propensioni e le loro capacità – contribuisce anche a rendere più produttivo e funzionale il tempo trascorso a scuola, che viene impiegato per prospettare questioni ulteriori e più complesse o per affrontare e approfondire tematiche ancor più specifiche [60].

Ovviamente, quelli qui menzionati sono semplicemente alcuni dei tantissimi esempi di una scuola che sta cambiando. Una scuola che – anche giovandosi di nuove piattaforme e di software

---

[59] Nel dettaglio, gli EAS prevedono tre diverse fasi: I) il *momento preparatorio* in cui il docente seleziona e assegna agli studenti risorse multimediali relative all'argomento in oggetto; II) il *momento operatorio*, cioè la fase in cui gli studenti svolgono un compito o creano prodotti volti a dimostrare il loro apprendimento; III) il *momento ristrutturativo* e *conclusivo* in cui il docente valuta e corregge i prodotti elaborati dagli studenti, fissa i nodi concettuali emersi e accompagna la classe verso una rielaborazione ulteriore di quanto è stato appreso. (Per un approfondimento sugli EAS, imprescindibile il rinvio ai lavori di P.C. RIVOLTELLA che, da diversi anni, si occupa del tema e i cui studi rappresentano un importante punto di riferimento. In modo particolare, si vedano: *Che cos'è un EAS? L'idea, il metodo, la didattica*, Milano 2016; *Didattica inclusiva con gli EAS*, Brescia 2015; *Fare didattica con gli EAS. Episodi di Apprendimento Situato*, Brescia 2013).

[60] A proposito della *flipped classroom*, cfr., fra gli altri: M. MAGLIONI, F. BISCARO, *La classe capovolta. Innovare la didattica con il flipped classroom*, Trento, EDS, 2014, p. 20 ss.; M. MAGLIONI, *Capovolgiamo la scuola*, Trento, Erickson, 2018, pp. 37-41).

cloud (come *Dropbox* [61], *Evernote* [62], *iCloud* [63], *OneDrive* [64]) – acquista un *appeal* maggiore e incrementa la qualità e l'efficacia della sua *performance* didattico-educativa.

Diffusa [65], inclusiva, partecipata e al contempo differenziata, la scuola digitale si apre e attinge alle ICT, sia per avvicinare, incentivare e formare gli studenti, sia per cercare di rispondere ai *Disturbi Specifici dell'Apprendimento* [66] (dislessia [67], disgrafia [68], discalculia [69], comorbilità [70]) e ai *Bisogni Educativi Specia-*

---

[61] Programma che – attraverso dispositivi mobili di qualsiasi natura – permette di condividere rapidamente file di qualsiasi tipo con altri utenti.

[62] Database virtuale che trasforma il proprio dispositivo mobile in un'agenda elettronica sincronizzata; consente di ordinare note e appunti, organizzare appuntamenti e calendari.

[63] Servizio di *cloud storage* offerto da *Apple*, che permette agli utenti di *iPhone*, *iPad*, *Mac* e anche *Windows* di creare *backup* dei propri file su un *hard disk virtuale* (*iCloud Drive*), sincronizzando tutti i dispositivi.

[64] Servizio di *cloud storage* offerto da *Microsoft*, che permette di salvare i dati personali e condividere foto e file con i propri contatti attraverso smartphone, tablet o computer.

[65] Affascinante e particolare, l'idea di *scuola diffusa*, coniuga la riflessione didattica con quella architettonica. L'auspicio è che la scuola, da luogo chiuso, fatto di barriere – strutturali e concettuali – si tramuti in uno spazio arioso, aperto, privo di limiti e di pregiudizi, in cui i giovani possano svilupparsi in piena libertà (P. MOTTANA, G. CAMPAGNOLI, *La città educante. Manifesto dell'educazione diffusa. Come oltrepassare la scuola*, Trieste, Asterios, 2017, in part. pp. 9-32).

[66] Si tratta dei cosiddetti "DAS", così come individuati dalle *Linee Guida per il diritto allo studio degli alunni e degli studenti con disturbi specifici dell'apprendimento* allegate al Decreto Ministeriale. n. 5669 del 12 luglio 2012. Per un approfondimento sui disturbi dell'apprendimento cfr.: F. FOGAROLO, *Il computer di sostegno*, Trento, Erickson, 2013; C. SCAPIN, F. FOGAROLO, *Competenze compensative: tecnologie e strategie per l'autonomia scolastica per gli alunni con dislessia e altri DSA*, Trento, Erickson, 2010.

[67] Disturbo fra i più frequenti, che si traduce in una minore correttezza ed in una minore velocità nella lettura a voce alta rispetto a quanto ci si attenderebbe in base all'età, alla classe frequentata o all'istruzione ricevuta.

[68] DAS che coinvolge la scrittura e, in modo particolare, la grafia. Nel caso in cui, invece, il disturbo determini un disordine nella codifica del testo scritto e comprometta l'ortografia – anziché di disgrafia – si parla di disortografia.

[69] Difficoltà specifica che coinvolge l'abilità di calcolo, riverberando negativamente sia sull'organizzazione della cognizione numerica (ossia sull'intelligenza numerica basale), sia sull'esecuzione delle procedure di calcolo.

[70] Espressione peculiare con la quale ci indica la compresenza di due o più DAS. Si tratta, in pratica, di un'associazione di disturbi che riverbera in maniera ancor profonda ed incisiva sulle abilità complessive del soggetto.

li[71] (disabilità motoria, sensoriale e/o intellettiva, disagi neuropsichiatrici, disturbi dello spettro autistico[72]). Del resto si sa – con le loro tante soluzioni compensative, abilitative e/o riabilitative[73] – le tecnologie rappresentano un prezioso sussidio all'attività didattica[74], un supporto irrinunciabile e funzionale a garantire il diritto allo studio[75].

Svecchiata e sotto molti aspetti completamente ridisegnata dalla Legge 107 del 2015[76], dal *Piano Nazionale Scuola Digitale (PNSD)*[77] e dal d.lgs. n. 65 del 2017[78], la scuola mostra un volto

---

[71] Meglio noti con la sigla "BES", sui quali – oltre, ovviamente alla l. n. 104 del 1992 e alla l. n. 17 del 1999 – si deve ricordare la Direttiva Ministeriale del 27 dicembre 2012, recante *Strumenti d'intervento per gli alunni con Bisogni Educativi Speciali e organizzazione scolastica*, come pure, la Circolare Ministeriale del 6 marzo 2013 e, da ultimo, anche la nota del MIUR del 3 aprile 2019. (Per ulteriori approfondimenti cfr.: F. ZAMBOTTI, *Tecnologie come risorsa inclusiva*, in D. IANES, S. CRAMEROTTI, *Alunni con BES. Bisogni educativi speciali*, Trento, Erickson, 2013, pp. 289-300).

[72] Emblematica la sperimentazione avviata dall'Università di Stanford e volta all'uso dei *Google Glass* per permettere a chi presenta disturbi dello spettro autistico di riconoscere le emozioni (cfr. M. TONELLI, *La nuova vita dei Google Glass: aiutare i bambini con autismo a riconoscere le emozioni*, in *La Stampa*, 11 agosto 2019).

[73] Sui risvolti biogiuridici legati all'impiego della tecnologia per sopperire ai limiti del corpo e per tentare di superarne la caducità, imprescindibile il rinvio a A.C. AMATO MANGIAMELI, *Corpi docili Corpi gloriosi*, cit. e ID., *Natur@, Appunti di Biogiuridica*, Torino Giappichelli, 2020 (in corso di stampa).

[74] Per una panoramica dei supporti e dei servizi tecnologici offerti si invita alla consultazione del portale *Handitecno* a cura dell'*Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa (INDIRE)*.

[75] Costituzionalmente garantito dagli artt. 3 e 34 della nostra Carta Fondamentale, il diritto allo studio si colora di nuance ulteriori quando interessa persone con disabilità. Su questo specifico tema – e dunque sul diritto allo studio dei disabili – rinvio, fra i tanti, al lavoro F. BLANDO, *Soggetti disabili e istruzione. La lotta per il diritto*, in *Federalismi.it*, 10/2017, pp. 2-17.

[76] Legge recante la *Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti*. Provvedimento meglio noto con la dicitura *La buona scuola*.

[77] Piano che dedica ampio spazio al ruolo abilitante delle tecnologie e che insiste sull'importanza della scuola digitale (testo disponibile in rete: *http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf*, in part. pp.7-9).

[78] Decreto con il quale – a norma dell'art. 1, commi 180 e 181, lett. *e*), della l. n. 107 del 2015 – si è provveduto all'istituzione del sistema integrato di educazione e di istruzione dalla nascita sino a sei anni.

diverso. Un volto tecnologico di cui i tratti più rivoluzionari e salienti sono stati efficacemente messi a fuoco dal MIUR nel 2018 con i *Dieci punti per l'uso dei dispositivi mobili a scuola* (*Bring your own device – BYOD*) ai quali ha poi fatto seguito il *Sillabo per l'educazione civica digitale*.

Alquanto controversi e discussi, soprattutto all'indomani della loro adozione, i *Dieci punti per l'uso dei dispositivi mobili a scuola* sono stati inizialmente visti come una sorta di "liberalizzazione" dell'uso del cellulare, destinata a riverberare in maniera negativa sull'attenzione degli studenti e a disturbare e intralciare l'attività didattica. Una prima frettolosa lettura questa, che però è stata presto abbandonata, anche perché non teneva conto di due fattori, ovvero del fatto che:

i) l'apertura al BYOD – e cioè a politiche che prevedessero l'utilizzo dei dispositivi elettronici personali durante l'attività didattica e che fossero basate sulla collaborazione fra scuola digitale, famiglie e enti locali – era già stata precedentemente prevista dal Piano Nazionale Scuola Digitale che la annoverava fra le sue azioni (*#azione 6*) [79];

ii) il termine inglese device, oltre allo smartphone, indica tutti i diversi tipi di strumenti (tool) digitali, come il pc, il tablet o l'e-book reader.

Ben lungi dal costituire uno "sdoganamento" del cellulare, invece, il BYOD permette di introdurre nel contesto scolastico quei device (o meglio quei tool) che possono rivelarsi utili e funzionali all'apprendimento, ma dei quali non tutti gli istituti sono provvisti o – se ne sono dotati – non sempre posseggono in numero congruo a soddisfare le esigenze degli studenti. L'introduzione e l'utilizzo dello strumento personale, poi, è sottoposta al controllo del docente e deve rispettare quanto previsto dalla "Politica d'uso accettabile e sicura della rete" (PUA) della singola struttura.

Ricco di contenuti, ma al contempo di agile lettura e immediata comprensione, il BYOD rappresenta lo specchio e l'archi-

[79] È importante sottolineare che è proprio a tale azione del PNSD che si deve il superamento della Direttiva del Ministro del 15 marzo 2007 – recante *Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica* – che, invece, vietava completamente l'uso di qualsiasi *device* personale.

trave della nuova scuola. Una scuola che: *favorisce le condizioni strutturali per l'uso delle tecnologie digitali* (punto 3); *accoglie e promuove lo sviluppo del digitale nella didattica* (punto 4); *usa i dispositivi come mezzi e non fine* (punto 5); *si avvale dei tool per incentivare l'autonomia delle studentesse e degli studenti* (punto 6); *trasforma gli ambienti di apprendimento, favorendo la collaborazione e la condivisione* (punto 8); *rafforza la comunità scolastica, migliora la didattica e favorisce l'alleanza educativa con le famiglie* (punto 9); *forma i futuri cittadini digitali* (punto 10) [80].

Si tratta di una scuola che – con David Jonassen – potremmo definire *mindtools*, nel senso di *mind+tools*, all'interno della quale si predispongono le condizioni per sviluppare un connubio sinergico e virtuoso fra mente e tecnologie, dove gli studenti non apprendono *dalle* ma *con le* ICT (*not to learn from but to learn with*) [81].

5. Un interrogativo e un auspicio

Non molto tempo fa Nicholas Carr [82] si chiedeva se *Google ci avrebbe reso stupidi*. Riflettendo sul delicato rapporto fra ICT, educazione e scuola, questa stessa domanda sembra riproporsi e suonare pressappoco così: *l'introduzione delle nuove tecnologie negli ambienti didattici e formativi ci renderà più stupidi?* Alla luce del percorso sin qui svolto, si possono abbozzare due risposte assolutamente differenti.

I) *Sì, ma soltanto qualora*, attraverso l'uso delle tecnologie, anziché la conoscenza si insegua semplicemente un'ipermnesia, accumulando informazioni, particolari e dettagli senza procedere né a una selezione né ad una rielaborazione critica degli stessi. Scelta, questa, che rischierebbe di tramutarci in tanti Irneo

[80] In realtà, ogni punto del BYOD meriterebbe d'esser qui richiamato integralmente. Per consentire la visione completa del provvedimento si è scelto di inserirlo fra i materiali normativi che corredano la seconda parte del volume (cfr., *infra*, *Materiali normativi*).

[81] D.H. JONASSEN, *Computers in the Classroom: Mindtools for Critical Thinking*, New Jersey, Englewood Cliffs, 1996.

[82] *Internet ci rende stupidi? Come la rete sta cambiando il nostro cervello*, trad. it., Milano, Raffaello Cortina, 2011.

Funes, l'*idiot savant* di cui narra Borges in uno dei suoi più noti racconti [83], che si contraddistingueva per la memoria prodigiosa, ma non certo per intelligenza o capacità.

II) *No, a patto che* l'approccio alle ICT e la loro introduzione all'interno del contesto didattico-educativo, attraverso la previsione dell'educazione e della scuola digitale, non divenga sinonimo di "sostituzione" o, peggio ancora, di "deresponsabilizzazione", quanto piuttosto di "aggiornamento" e di "efficientamento". In altri termini, si tratta di ampliare le risorse, incrementare gli strumenti, migliorare e svecchiare i metodi [84], senza mai perdere di vista quelli che sono gli obiettivi (formare menti autonome, dotate di conoscenze e di capacità critica). In altre parole, le ICT devono essere usate ragionevolmente – o, meglio, *ragionevolmente* – come un supporto ed uno stimolo per la mente e per la creatività umana [85] e non per sostituirsi ad essa. La via, in questo senso, è bene indicata da Himanen, che nel suo *L'etica hacker e lo spirito dell'età dell'informazione* – a partire dall'osservazione del *modus operandi* degli sviluppatori di Linux – tratteggia il c.d. "modello hacker di apprendimento". Ovverosia, un modello: *i*) aperto alla libera circolazione delle idee; *ii*) contraddistinto dall'accesso universale in cui il codice sorgente è pubblico (open source); *iii*) basato sulla condivisione dei problemi, delle soluzioni e delle procedure; *iv*) pronto allo scambio, alla condivisione, al dialogo e al confronto. Un modello di apprendimento aperto, plurale e – al contempo – critico.

Estremamente capaci e competenti, ma, anche, creativi, curiosi, pronti a sperimentare nuovi percorsi e a misurarsi con nuovi

---

[83] J.L. BORGES, *Finzioni*, trad. it., Torino, Adelphi, 2014.

[84] Ed è proprio in tal senso che – come osservava alcuni anni fa Galimberti – la scuola dovrebbe farsi più vicina agli studenti, più accattivante e anche più *erotica*: "[…] bisognerebbe che i professori, oltre a sapere la loro materia, fossero anche in grado di comunicarla e di affascinare. Perché l'apprendimento, lo dice Platone, avviene per via erotica" (U. GALIMBERTI, in *WiseSociety*, 11 settembre 2011).

[85] Noti, sul punto, i lavori di Ken ROBINSON ai quali si rinvia (*Scuola creativa. Manifesto per una nuova educazione*, trad. it. Trento, Erickson, 2016; *Fuori di testa. Perché la scuola uccide la creatività*, trad. it., Trento, Erickson, 2015; *The element. Trova il tuo elemento cambia la tua vita*, trad. it., Milano, Feltrinelli, 2012).

problemi, gli hacker[86] dominano la Rete senza scopi malevoli, solo per amore della conoscenza. *Pirati-gentiluomini*, gli hacker sono la dimostrazione concreta di come le ICT possano fungere da *leva cognitiva*[87]. Una leva che può – e deve – essere maneggiata e padroneggiata anche dall'educazione e dalla scuola.

[86] Sulla figura dell'hacker e sulla sua differenza dal cracker, interessanti ed esaustive le osservazioni di AMATO MANGIAMELI, *infra*, *Parte Prima*.

[87] Sull'uso delle tecnologie e di Internet come "leva cognitiva", cfr. M. ARCANGELI, *Prefazione*, in D. DE KERCKHOVE, *La rete ci renderà stupidi?*, trad. it., Roma, Castelvecchi, 2016, p. 8.

Educare
con
le nuove tecnologie

Mappe di sintesi

Nuovi paradigmi
Il cloud

Concetti e passaggi-chiave

- Risorsa di archiviazione e di gestione dei dati e delle informazioni
- Forme-struttura (privato, pubblico, ibrido)
- Servizi (IaaS, PaaS, DaaS, DraaS, BaaS, StaaS, SECaaS, NaaS)
- Soggetti (provider, consumer, carrier, auditor, broker)
- Volano di cambiamento o *Vulnus* per la sicurezza?
- Il GDPR: più sicurezza?

CISPE.cloud

General Data Protection Regulation

Nuovi media

I social network

Concetti e passaggi-chiave

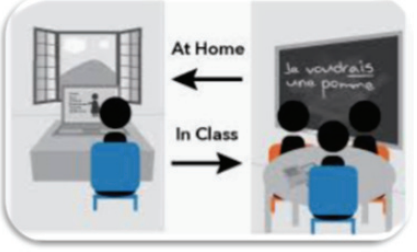
- Social e World Wide Web
- Network: tra comunicazione, relazionalità e nuove identità
- Mezzi di comunicazione *di massa* e mezzi di comunicazione *per la massa* (YouTube, Facebook, Instagram, Pinterest, Linkdln, Twitter, Skype, Messenger, Viber, Telegram, Signal, Snapchat e WhatsApp)
- Dalla *società confessionale* agli *eremiti di massa*
- Social e Far West Giuridico?
- Conseguenze *reali* dei comportamenti *virtuali* (grooming, cyberstalking, cyberbulling, sextortion)

Nuove prospettive didattiche

Educazione e scuola digitale

Concetti e passaggi-chiave

- Istruire e educare: diritti e doveri fondamentali
- La tecnologia è d'aiuto?
- Cultura come rivoluzione permanente
- Tecnologia e didattica (eTwinning, Città educante, life-long-learning, flipped classroom)
- BES e DAS
- No a teste piene! Sì a teste ben fatte!



Materiali normativi

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio 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 (Regolamento generale per la protezione dei dati – GDPR) [1]

Il Parlamento europeo e il Consiglio dell'Unione europea,
visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,
vista la proposta della Commissione europea,
previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,
visto il parere del Comitato economico e sociale europeo,
visto il parere del Comitato delle regioni,
deliberando secondo la procedura legislativa ordinaria,
considerando quanto segue:
(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergen-

[1] Adottato il 27 aprile 2016.

za delle economie nel mercato interno e al benessere delle persone fisiche.
(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.
(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.
(5) L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.
(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.
(7) Tale evoluzione richiede un quadro più solido e coerente in ma-

teria di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

(9) Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. […].

(10) Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

(11) Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per con-

trollare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.
[…]
(14) È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.
[…]
[…]
[…]
(38) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.
(39) Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e

precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

(40) Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

(41) Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la "Corte di giustizia") e della Corte europea dei diritti dell'uomo.

(42) Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai

fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

(43) Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

(44) Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

(45) È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del tratta-

mento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale.

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

(47) I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Co-

stituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.
(48) I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.
(49) Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.
(50) Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri

per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.
Ove l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del titolare del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere.
(51) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane di-

stinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.
[…]
(53) Le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica. Pertanto il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da

persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

(54) Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di «sanità pubblica» dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio (1): tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.

(55) Inoltre, è effettuato per motivi di interesse pubblico il trattamento di dati personali a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute.

[…]

[…]

(58) Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia dif-

ficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

(59) È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

(60) I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli. Tali informazioni possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

(61) L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti,

dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Qualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale.
[…]
(63) Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.
(64) Il titolare del trattamento dovrebbe adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online. Il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste.
(65) Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il "diritto all'oblio" se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali so-

no stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

(66) Per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.

(67) Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

[…]
[…]
[…]

(72) La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati. Il comitato europeo per la protezione dei dati istituito dal presente regolamento ("comitato") dovrebbe poter emanare orientamenti in tale contesto.
(73) Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, le attività di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, o di violazioni della deontologia professionale, per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, tra cui un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale, per l'ulteriore trattamento di dati personali archiviati al fine di fornire informazioni specifiche connesse al comportamento politico sotto precedenti regimi statali totalitari o per la tutela dell'interessato o dei diritti e delle libertà altrui, compresi la protezione sociale, la sanità pubblica e gli scopi umanitari. Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.
[…]
(78) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati

personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

(79) La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

(80) Quando un titolare del trattamento o un responsabile del trattamento non stabilito nell'Unione tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi a tali interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, o al controllo del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione, è opportuno che tale titolare del trattamento o responsabile del trattamento designi un rappresentante, tranne se il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati personali o il trattamento di dati personali relativi alle condanne penali e ai reati, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento, o se il titolare del trattamento è un'autorità pubblica o un organismo pubblico. Il rappresentante dovrebbe agire per conto del titolare del trattamento o del responsabile del trattamento e può essere interpellato da qualsiasi autorità di controllo. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del titolare del trattamento o del responsabile del trattamento ad agire per con-

to di questi ultimi con riguardo agli obblighi che a questi derivano dal presente regolamento. La designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal titolare del trattamento o dal responsabile del trattamento, anche per quanto riguarda la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del presente regolamento. Il rappresentante designato dovrebbe essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento o del responsabile del trattamento.
[…]
(82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.
Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
[…]
[…]
[…]
(85) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla re-

putazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

(86) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

(87) È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

[…]

(89) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.
(90) In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.
[…]
[…]
[…]
(101) I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamen-

to. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

(102) Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati.

(103) La Commissione può decidere, con effetto nell'intera Unione, che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti del paese terzo o dell'organizzazione internazionale che si ritiene offra tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una dichiarazione completa che illustra le motivazioni al paese terzo o all'organizzazione internazionale, di revocare una tale decisione.

(104) In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili.

[…]

[…]

(107) La Commissione può riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione dei dati. Di conseguenza il trasferimento di dati personali verso tale paese terzo od organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui al presente regolamento relativamente ai trasferimenti sottoposti a garanzie adeguate, comprese norme vincolanti d'impresa, e a deroghe per situazioni particolari. In tal caso è opportuno prevedere consultazioni tra la Commissione e detti paesi terzi o organizzazioni internazionali. La Commissione dovrebbe informare tempestivamente il paese terzo o l'organizzazione internazionale dei motivi e avviare consultazioni con questi al fine di risolvere la situazione.
[…]
[…]
[…]
(116) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento.
(117) L'istituzione di autorità di controllo a cui è conferito il potere di eseguire i loro compiti ed esercitare i loro poteri in totale indipendenza in ciascuno Stato membro è un elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali. Gli Stati membri dovrebbero poter istituire più

di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa.
[…]
[…]
(129) Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento. Tali poteri dovrebbero includere anche il potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. Gli Stati membri possono precisare altri compiti connessi alla protezione dei dati personali ai sensi del presente regolamento. È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole. In particolare ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso, rispettare il diritto di ogni persona di essere ascoltata prima che nei suoi confronti sia adottato un provvedimento individuale che le rechi pregiudizio ed evitare costi superflui ed eccessivi disagi per le persone interessate. I poteri di indagine per quanto riguarda l'accesso ai locali dovrebbero essere esercitati nel rispetto dei requisiti specifici previsti dal diritto processuale degli Stati membri, quale l'obbligo di ottenere un'autorizzazione giudiziaria preliminare. Ogni misura giuridicamente vincolante dell'autorità di controllo dovrebbe avere forma scritta, essere chiara e univoca, riportare l'autorità di controllo che ha adottato la misura e la relativa data di adozione, recare la firma del responsabile o di un membro dell'autorità di controllo da lui autorizzata, precisare i motivi della misura e fare riferimento al diritto a un ricorso effettivo. Ciò non dovrebbe precludere requisiti supplementari ai sensi del diritto processuale degli Stati membri. L'adozione di una decisione giuridicamente vincolante implica che essa può essere soggetta a controllo giurisdizionale nello Stato membro dell'autorità di controllo che ha adottato la decisione.
[…]

[…]
[…]
(135) È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un'autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. Tale meccanismo non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati.
(136) In applicazione del meccanismo di coerenza il comitato dovrebbe emettere un parere entro un termine determinato, se i suoi membri lo decidono a maggioranza o se a richiederlo è un'autorità di controllo interessata o la Commissione. Il comitato dovrebbe altresì avere il potere di adottare decisioni giuridicamente vincolanti qualora insorgano controversie tra autorità di controllo. A tal fine, dovrebbe adottare, in linea di principio a maggioranza dei due terzi dei suoi membri, decisioni giuridicamente vincolanti in casi chiaramente determinati in cui vi siano pareri divergenti tra le autorità di controllo segnatamente nell'ambito del meccanismo di cooperazione tra l'autorità di controllo capofila e le autorità di controllo interessate sul merito del caso, in particolare sulla sussistenza di una violazione del presente regolamento.
[…]
[…]
[…]
(148) Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in

cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

(149) Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia.

(150) Alfine di rafforzare e armonizzare le sanzioni amministrative applicabili per violazione del presente regolamento, ogni autorità di controllo dovrebbe poter imporre sanzioni amministrative pecuniarie. Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 TFUE a tali fini. Se le sanzioni amministrative sono inflitte a persone che non sono imprese, l'autorità di controllo dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. Imporre una sanzione amministrativa pecuniaria o dare un avvertimento non incide sull'applicazione di altri poteri delle autorità di controllo o di altre sanzioni a norma del regolamento.

[…]
(152) Se il presente regolamento non armonizza le sanzioni amministrative o se necessario in altri casi, ad esempio in caso di gravi violazioni del regolamento, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri.
(153) Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo, negli archivi stampa e nelle emeroteche. È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali. Gli Stati membri dovrebbero adottare tali esenzioni e deroghe con riferimento alle disposizioni riguardanti i principi generali, i diritti dell'interessato, il titolare del trattamento e il responsabile del trattamento, il trasferimento di dati personali verso paesi terzi o a organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza nonché situazioni di trattamento dei dati specifiche. Qualora tali esenzioni o deroghe differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto dello Stato membro cui è soggetto il titolare del trattamento. Per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo.
[…]
(156) Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie dovrebbero assicurare che siano state predisposte misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o

storica o a fini statistici è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati personali). Gli Stati membri dovrebbero prevedere garanzie adeguate per il trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Le condizioni e le garanzie in questione possono comprendere procedure specifiche per l'esercizio di tali diritti da parte degli interessati, qualora ciò sia appropriato alla luce delle finalità previste dallo specifico trattamento, oltre a misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità. Il trattamento dei dati personali per finalità scientifiche dovrebbe rispettare anche altre normative pertinenti, ad esempio quelle sulle sperimentazioni cliniche.

[…]

[…]

(166) Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE. In particolare, dovrebbero essere adottati atti delegati riguardanti i criteri e i requisiti dei meccanismi di certificazione, le informazioni da presentare sotto forma di icone standardizzate e le procedure per fornire tali icone. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.

(167) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione

competenze di esecuzione ove previsto dal presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio. A tal fine, la Commissione dovrebbe contemplare misure specifiche per le micro, piccole e medie imprese.
[…]
[…]
[…]
(170) Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
(171) Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.
[…]
[…]

Hanno adottato il presente regolamento

Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 2
Ambito di applicazione materiale

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento non si applica ai trattamenti di dati personali:
a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.
4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Articolo 3
Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamen-

to nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.
2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Articolo 4
Definizioni

Ai fini del presente regolamento s'intende per:
1) ***dato personale***: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) ***trattamento***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
[…]
4) ***profilazione***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) ***pseudonimizzazione***: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
[…]
7) ***titolare del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) ***responsabile del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) ***destinatario***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
10) ***terzo***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) ***consenso dell'interessato***: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) ***violazione dei dati personali***: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
[…]
[…]

Articolo 5
Principi applicabili al trattamento di dati personali

1. I dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (***liceità, correttezza e trasparenza***);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali (***limitazione della finalità***);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (***minimizzazione dei dati***);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (***esattezza***);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (***limitazione della conservazione***);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (***integrità e riservatezza***).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (***responsabilizzazione***).

Articolo 6
Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
[…]
2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.
3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:
a) dal diritto dell'Unione; o
b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.
[…]
4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure

se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7
Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8
Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.
[…]
[…]

Articolo 12
Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.
2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.
3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.
4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un

mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:
a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.
Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.
7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Articolo 13
Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14
Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.
5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

Articolo 15
Diritto di accesso dell'interessato

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.
3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

Articolo 16
Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 17
Diritto alla cancellazione ("diritto all'oblio")

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.
2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:
a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
[…]
[…]

Articolo 19
Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 20
Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei da-

ti a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Articolo 21
Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, sal-

vo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
[…]
[…]

Articolo 24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
[…]
[…]

Articolo 28
Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del di-

ritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. […]

[…]

Articolo 30
Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.
[…]
[…]

Articolo 32
Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. […]

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. […]

Articolo 34
Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). […]
[…]
[…]

Articolo 39
Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati perso-

nali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Articolo 40
Codici di condotta

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.
2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento.
[…]
[…]

Articolo 44
Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate

al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 45
Trasferimento sulla base di una decisione di adeguatezza

1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.
[…]
[…]

Articolo 48
Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.
[…]

Articolo 50
Cooperazione internazionale per la protezione dei dati personali

In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per:
a) sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali;
b) prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;

c) coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;
d) promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.
[…]
[…]
[…]

Articolo 63
Meccanismo di coerenza

Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione.
[…]
[…]

Articolo 68
Comitato europeo per la protezione dei dati

1. Il comitato europeo per la protezione dei dati ("comitato") è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.
2. Il comitato è rappresentato dal suo presidente.
3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.
4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.
5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.
6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento.
[…]
[…]

Articolo 83
Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.
2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa […].
[…]
9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

Articolo 84
Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.
2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.
[…]
[…]

Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo (Legge n. 71 del 2017) [2]

La Camera dei deputati ed il Senato della Repubblica hanno approvato;
Il Presidente della Repubblica
Promulga
la seguente legge:

Art. 1
Finalità e definizioni

1. La presente legge si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di età nell'ambito delle istituzioni scolastiche.
2. Ai fini della presente legge, per "cyberbullismo" si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.
3. Ai fini della presente legge, per "gestore del sito internet" si intende il prestatore di servizi della società dell'informazione, diverso da quelli di cui agli articoli 14, 15 e 16 del decreto legislativo 9 aprile 2003, n. 70, che, sulla rete internet, cura la gestione dei contenuti di un sito in cui si possono riscontrare le condotte di cui al comma 2.

Art. 2
Tutela della dignità del minore

1. Ciascun minore ultraquattordicenne, nonché ciascun genitore o soggetto esercente la responsabilità del minore che abbia subito ta-

[2] Legge del 29 maggio 2017.

luno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, da identificare espressamente tramite relativo URL (Uniform resource locator), non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici.

2. Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto responsabile non abbia comunicato di avere assunto l'incarico di provvedere all'oscuramento, alla rimozione o al blocco richiesto, ed entro quarantotto ore non vi abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento o il gestore del sito internet o del social media, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento della richiesta, provvede ai sensi degli articoli 143 e 144 del citato decreto legislativo 30 giugno 2003, n. 196.

Art. 3
Piano di azione integrato

1. Con decreto del Presidente del Consiglio dei ministri, da adottare entro trenta giorni dalla data di entrata in vigore della presente legge, è istituito presso la Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica, il tavolo tecnico per la prevenzione e il contrasto del cyberbullismo, del quale fanno parte rappresentanti del Ministero dell'interno, del Ministero dell'istruzione, dell'università e della ricerca, del Ministero del lavoro e delle politiche sociali, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero della salute, della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, dell'Autorità per le garanzie nelle comunicazioni, del Garante per l'infanzia e l'adolescenza, del Comitato di applicazione del codice di autoregolamentazione media e minori, del Garante per la protezione dei dati personali, di associazioni con comprovata esperienza nella promozione dei diritti dei minori e degli adolescenti e nelle tematiche di genere, degli operatori che forniscono servizi di social networking e degli altri operatori della rete internet, una rappresentanza delle associazioni studentesche e dei genitori e una rap-

presentanza delle associazioni attive nel contrasto del bullismo e del cyberbullismo. Ai soggetti che partecipano ai lavori del tavolo non è corrisposto alcun compenso, indennità, gettone di presenza, rimborso spese o emolumento comunque denominato.
2. Il tavolo tecnico di cui al comma 1, coordinato dal Ministero dell'istruzione, dell'università e della ricerca, redige, entro sessanta giorni dal suo insediamento, un piano di azione integrato per il contrasto e la prevenzione del cyberbullismo, nel rispetto delle direttive europee in materia e nell'ambito del programma pluriennale dell'Unione europea di cui alla decisione 1351/2008/CE del Parlamento europeo e del Consiglio, del 16 dicembre 2008, e realizza un sistema di raccolta di dati finalizzato al monitoraggio dell'evoluzione dei fenomeni e, anche avvalendosi della collaborazione con la Polizia postale e delle comunicazioni e con altre Forze di polizia, al controllo dei contenuti per la tutela dei minori.
3. Il piano di cui al comma 2 è integrato, entro il termine previsto dal medesimo comma, con il codice di coregolamentazione per la prevenzione e il contrasto del cyberbullismo, a cui devono attenersi gli operatori che forniscono servizi di social networking e gli altri operatori della rete internet. Con il predetto codice è istituito un comitato di monitoraggio al quale è assegnato il compito di identificare procedure e formati standard per l'istanza di cui all'articolo 2, comma 1, nonché di aggiornare periodicamente, sulla base delle evoluzioni tecnologiche e dei dati raccolti dal tavolo tecnico di cui al comma 1 del presente articolo, la tipologia dei soggetti ai quali è possibile inoltrare la medesima istanza secondo modalità disciplinate con il decreto di cui al medesimo comma 1. Ai soggetti che partecipano ai lavori del comitato di monitoraggio non è corrisposto alcun compenso, indennità, gettone di presenza, rimborso spese o emolumento comunque denominato.
4. Il piano di cui al comma 2 stabilisce, altresì, le iniziative di informazione e di prevenzione del fenomeno del cyberbullismo rivolte ai cittadini, coinvolgendo primariamente i servizi socio-educativi presenti sul territorio in sinergia con le scuole.
5. Nell'ambito del piano di cui al comma 2 la Presidenza del Consiglio dei ministri, in collaborazione con il Ministero dell'istruzione, dell'università e della ricerca e con l'Autorità per le garanzie nelle comunicazioni, predispone, nei limiti delle risorse di cui al comma 7, primo periodo, periodiche campagne informative di prevenzione e di sensibilizzazione sul fenomeno del cyberbullismo, avvalendosi dei principali media, nonché degli organi di comunicazione e di stampa e di soggetti privati.

6. A decorrere dall'anno successivo a quello di entrata in vigore della presente legge, il Ministro dell'istruzione, dell'università e della ricerca trasmette alle Camere, entro il 31 dicembre di ogni anno, una relazione sugli esiti delle attività svolte dal tavolo tecnico per la prevenzione e il contrasto del cyberbullismo, di cui al comma 1.
7. Ai fini dell'attuazione delle disposizioni di cui al comma 5, è autorizzata la spesa di euro 50.000 annui a decorrere dall'anno 2017. Al relativo onere si provvede mediante corrispondente riduzione, per gli anni 2017, 2018 e 2019, dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2017-2019, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2017, allo scopo parzialmente utilizzando l'accantonamento relativo al medesimo Ministero.
8. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 4
Linee di orientamento per la prevenzione e il contrasto in ambito scolastico

1. Per l'attuazione delle finalità di cui all'articolo 1, comma 1, il Ministero dell'istruzione, dell'università e della ricerca, sentito il Ministero della giustizia – Dipartimento per la giustizia minorile e di comunità, entro trenta giorni dalla data di entrata in vigore della presente legge adotta linee di orientamento per la prevenzione e il contrasto del cyberbullismo nelle scuole, anche avvalendosi della collaborazione della Polizia postale e delle comunicazioni, e provvede al loro aggiornamento con cadenza biennale.
2. Le linee di orientamento di cui al comma 1, conformemente a quanto previsto alla lettera l) del comma 7 dell'articolo 1 della legge 13 luglio 2015, n. 107, includono per il triennio 2017-2019: la formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica; la promozione di un ruolo attivo degli studenti, nonché di ex studenti che abbiano già operato all'interno dell'istituto scolastico in attività di peer education, nella prevenzione e nel contrasto del cyberbullismo nelle scuole; la previsione di misure di sostegno e rieducazione dei minori coinvolti; un efficace sistema di governance diretto dal Ministero dell'istruzione, dell'università e della ricerca. Dall'adozione delle linee di orientamento non devono derivare nuovi o maggiori oneri per la finanza pubblica.
3. Ogni istituto scolastico, nell'ambito della propria autonomia, in-

dividua fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi della collaborazione delle Forze di polizia nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.
4. Gli uffici scolastici regionali promuovono la pubblicazione di bandi per il finanziamento di progetti di particolare interesse elaborati da reti di scuole, in collaborazione con i servizi minorili dell'Amministrazione della giustizia, le prefetture – Uffici territoriali del Governo, gli enti locali, i servizi territoriali, le Forze di polizia nonché associazioni ed enti, per promuovere sul territorio azioni integrate di contrasto del cyberbullismo e l'educazione alla legalità al fine di favorire nei ragazzi comportamenti di salvaguardia e di contrasto, agevolando e valorizzando il coinvolgimento di ogni altra istituzione competente, ente o associazione, operante a livello nazionale o territoriale, nell'ambito delle attività di formazione e sensibilizzazione. I bandi per accedere ai finanziamenti, l'entità dei singoli finanziamenti erogati, i soggetti beneficiari e i dettagli relativi ai progetti finanziati sono pubblicati nel sito internet istituzionale degli uffici scolastici regionali, nel rispetto della trasparenza e dell'evidenza pubblica.
5. Conformemente a quanto previsto dalla lettera h) del comma 7 dell'articolo 1 della legge 13 luglio 2015, n. 107, le istituzioni scolastiche di ogni ordine e grado, nell'ambito della propria autonomia e nell'ambito delle risorse disponibili a legislazione vigente, promuovono l'educazione all'uso consapevole della rete internet e ai diritti e doveri connessi all'utilizzo delle tecnologie informatiche, quale elemento trasversale alle diverse discipline curricolari, anche mediante la realizzazione di apposite attività progettuali aventi carattere di continuità tra i diversi gradi di istruzione o di progetti elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, organi di polizia, associazioni ed enti.
6. I servizi territoriali, con l'ausilio delle associazioni e degli altri enti che perseguono le finalità della presente legge, promuovono, nell'ambito delle risorse disponibili, specifici progetti personalizzati volti a sostenere i minori vittime di atti di cyberbullismo nonché a rieducare, anche attraverso l'esercizio di attività riparatorie o di utilità sociale, i minori artefici di tali condotte.

Art. 5
Informativa alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero

1. Salvo che il fatto costituisca reato, in applicazione della normativa vigente e delle disposizioni di cui al comma 2, il dirigente sco-

lastico che venga a conoscenza di atti di cyberbullismo ne informa tempestivamente i soggetti esercenti la responsabilità genitoriale ovvero i tutori dei minori coinvolti e attiva adeguate azioni di carattere educativo.
2. I regolamenti delle istituzioni scolastiche di cui all'articolo 4, comma 1, del regolamento di cui al decreto del Presidente della Repubblica 24 giugno 1998, n. 249, e successive modificazioni, e il patto educativo di corresponsabilità di cui all'articolo 5-bis del citato decreto n. 249 del 1998 sono integrati con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

Art. 6
Rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48

1. La Polizia postale e delle comunicazioni relaziona con cadenza annuale al tavolo tecnico di cui all'articolo 3, comma 1, sugli esiti delle misure di contrasto al fenomeno del cyberbullismo. La relazione è pubblicata in formato di tipo aperto ai sensi dell'articolo 68, comma 3, lettera a), del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82.
2. Per le esigenze connesse allo svolgimento delle attività di formazione in ambito scolastico e territoriale finalizzate alla sicurezza dell'utilizzo della rete internet e alla prevenzione e al contrasto del cyberbullismo sono stanziate ulteriori risorse pari a 203.000 euro per ciascuno degli anni 2017, 2018 e 2019, in favore del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48.
3. Agli oneri derivanti dal comma 2 del presente articolo, pari a 203.000 euro per ciascuno degli anni 2017, 2018 e 2019, si provvede mediante corrispondente riduzione dello stanziamento del fondo speciale di parte corrente iscritto, ai fini del bilancio triennale 2017-2019, nell'ambito del programma "Fondi di riserva e speciali" della missione "Fondi da ripartire" dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2017, allo scopo parzialmente utilizzando l'accantonamento relativo al medesimo Ministero.
4. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

Art. 7
Ammonimento

1. Fino a quando non è proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594, 595 e 612 del co-

dice penale e all'articolo 167 del codice per la protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento di cui all'articolo 8, commi 1 e 2, del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, e successive modificazioni.
2. Ai fini dell'ammonimento, il questore convoca il minore, unitamente ad almeno un genitore o ad altra persona esercente la responsabilità genitoriale.
3. Gli effetti dell'ammonimento di cui al comma 1 cessano al compimento della maggiore età.
La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Dieci punti per l'uso dei dispositivi mobili a scuola
BYOD – *Bring your own device* [3]

1.
Ogni novità comporta cambiamenti

Ogni cambiamento deve servire per migliorare l'apprendimento e il benessere delle studentesse e degli studenti e più in generale dell'intera comunità scolastica.

2.
I cambiamenti non vanno rifiutati, ma compresi e utilizzati per il raggiungimento dei propri scopi

Bisogna insegnare a usare bene e integrare nella didattica quotidiana i dispositivi, anche attraverso una loro regolamentazione. Proibire l'uso dei dispositivi a scuola non è la soluzione.
A questo proposito ogni scuola adotta una Politica di Uso Accettabile (PUA) delle tecnologie digitali.

3.
La scuola promuove le condizioni strutturali per l'uso delle tecnologie digitali

Fornisce, per quanto possibile, i necessari servizi e l'indispensabile connettività, favorendo un uso responsabile dei dispositivi personali (BYOD).
Le tecnologie digitali sono uno dei modi per sostenere il rinnovamento della scuola.

4.
La scuola accoglie e promuove lo sviluppo del digitale nella didattica

La presenza delle tecnologie digitali costituisce una sfida e un'opportunità per la didattica e per la cultura scolastica. Dirigenti e insegnanti attivi in questi campi sono il motore dell'innovazione. Occorre coinvolgere l'intera comunità scolastica anche attraverso la formazione e lo sviluppo professionale.

---

[3] Testo adottato il 19 gennaio 2018.

5.
I dispositivi devono essere un mezzo, non un fine

È la didattica che guida l'uso competente e responsabile dei dispositivi.
Non basta sviluppare le abilità tecniche, ma occorre sostenere lo sviluppo di una capacità critica e creativa.

6.
L'uso dei dispositivi promuove l'autonomia delle studentesse e degli studenti

È in atto una graduale transizione verso situazioni di apprendimento che valorizzano lo spirito d'iniziativa e la responsabilità di studentesse e gli studenti. Bisogna sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione, anche in vista di un apprendimento lungo tutto l'arco della vita.

7.
Il digitale nella didattica è una scelta: sta ai docenti introdurla e condurla in classe

L'uso dei dispositivi in aula, siano essi analogici o digitali, è promosso dai docenti, nei modi e nei tempi che ritengono più opportuni.

8.
Il digitale trasforma gli ambienti di apprendimento

Le possibilità di apprendere sono ampliate, sia per la frequentazione di ambienti digitali e condivisi, sia per l'accesso alle informazioni, e grazie alla connessione continua con la classe. Occorre regolamentare le modalità e i tempi dell'uso e del non uso, anche per imparare a riconoscere e a mantenere separate le dimensioni del privato e del pubblico.

9.
Rafforzare la comunità scolastica e l'alleanza educativa con le famiglie

È necessario che l'alleanza educativa tra scuola e famiglia si estenda alle questioni relative all'uso dei dispositivi personali. Le tecnologie digitali devono essere funzionali a questa collaborazione.
Lo scopo condiviso è promuovere la crescita di cittadini autonomi e responsabili.

10.

Educare alla cittadinanza digitale è un dovere per la scuola

Formare i futuri cittadini della società della conoscenza significa educare alla partecipazione responsabile, all'uso critico delle tecnologie, alla consapevolezza e alla costruzione delle proprie competenze in un mondo sempre più connesso.

Delibera N. 157/19/CONS – Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'*hate speech* [4]

L'Autorità

Nella riunione del Consiglio del 15 maggio 2019;

Vista la legge 31 luglio 1997, n. 249, recante "*Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo*";

Visto il decreto legislativo 31 luglio 2005, n. 177, recante "Testo unico dei servizi di media audiovisivi e radiofonici", di seguito denominato Testo unico;

Vista la delibera n. 25/19/CONS, del 22 gennaio 2019, recante "Consultazione pubblica sullo schema di regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di on discriminazione e di contrasto all'hate speech";

Visto l'art. 7 della Dichiarazione universale dei diritti umani delle Nazioni Unite del 1948 secondo il quale "Tutti sono eguali dinanzi alla legge e hanno diritto, senza alcuna discriminazione, ad una eguale tutela da parte della legge. Tutti hanno diritto ad una eguale tutela contro ogni discriminazione che violi la presente Dichiarazione come contro qualsiasi incitamento a tale discriminazione";

Visto l'art. 1 della Convenzione internazionale sull'eliminazione di ogni forma di discriminazione razziale delle Nazioni Unite del 1965, ratificata con legge 13 ottobre 1975, n. 654, secondo cui "l'espressione 'discriminazione razziale' sta ad indicare ogni distinzione, esclusione, restrizione o preferenza basata sulla razza, il colore, l'ascendenza o l'origine nazionale o etnica, che abbia lo scopo o l'effetto di distruggere o di compromettere il riconoscimento, il godimento o l'esercizio, in condizioni di parità, dei diritti dell'uomo e delle libertà fondamentali in campo politico, economico, sociale e culturale o in ogni altro settore della vita pubblica";

Visto l'art. 4 della Convenzione internazionale sull'eliminazione di ogni forma di discriminazione che prevede che "gli Stati contraenti condannano ogni propaganda ed ogni organizzazione che s'ispiri a concetti ed a teorie basate sulla superiorità di una razza o di un

[4] Testo adottato il 15 maggio 2019.

gruppo di individui di un certo colore o di una certa origine etnica, o che pretendano di giustificare o di incoraggiare ogni forma di odio e di discriminazione razziale, e si impegnano ad adottare immediatamente misure efficaci per eliminare ogni incitamento ad una tale discriminazione od ogni atto discriminatorio, tenendo conto, a tale scopo, dei principi formulati nella Dichiarazione universale dei diritti dell'uomo e dei diritti chiaramente enunciati *nell'articolo 5 della presente* Convenzione". Tra queste misure lo stesso art. 4 prevede esplicitamente quelle finalizzate a "non permettere né alle pubbliche autorità, né alle pubbliche istituzioni, nazionali o locali, l'incitamento o l'incoraggiamento alla discriminazione razziale";
Visto l'art. 1 della Convenzione sull'eliminazione di tutte le forme di discriminazione contro le donne delle Nazioni Unite del 1979, ratificata con legge 14 marzo 1985, n. 132, secondo il quale "la discriminazione contro le donne sta ad indicare ogni distinzione o limitazione basata sul sesso, che abbia l'effetto o lo scopo di compromettere o annullare il riconoscimento, il godimento o l'esercizio da parte delle donne, indipendentemente dal loro stato matrimoniale e in condizioni di uguaglianza fra uomini e donne, dei diritti umani e delle libertà fondamentali in campo politico, economico, culturale, civile, o in qualsiasi altro campo";
Vista la Raccomandazione di politica generale n. 15 della ECRI (Commissione Europea contro il Razzismo e l'Intolleranza del Consiglio d'Europa), relativa alla lotta contro il discorso dell'odio adottata l'8 dicembre 2015 che stimola gli Stati ad agire concretamente affinché ogni forma di discriminazione etnica sia contrastata ed eliminata, coerentemente con il diritto internazionale che tutela i diritti umani;
Visto l'art. 17 della Convenzione sui diritti dell'infanzia e dell'adolescenza delle Nazioni Unite del 1989, ratificata con legge 27 maggio 1991, n. 176, secondo il quale: "Gli Stati parti riconoscono l'importanza della funzione esercitata dai mass media e vigilano affinché il fanciullo possa accedere ad una informazione ed a materiali provenienti da fonti nazionali e internazionali varie, soprattutto se finalizzati a promuovere il suo benessere sociale, spirituale e morale nonché la sua salute fisica e mentale. A tal fine, gli Stati parti: a) incoraggiano i mass media a divulgare informazioni e materiali che hanno una utilità sociale e culturale per il fanciullo e corrispondono allo spirito dell'art. 29 [...]";
Visto l'art. 29 della Convenzione sui diritti dell'infanzia e dell'adolescenza delle Nazioni Unite del 1989, ratificata con legge 27 maggio 1991, n. 176, secondo il quale "Gli Stati parti convengono che

l'educazione del fanciullo deve avere come finalità: a) favorire lo sviluppo della personalità del fanciullo nonché lo sviluppo delle sue facoltà e delle sue attitudini mentali e fisiche, in tutta la loro potenzialità; b) sviluppare nel fanciullo il rispetto dei diritti dell'uomo e delle libertà fondamentali e dei principi consacrati nella Carta delle Nazioni Unite; c) sviluppare nel fanciullo il rispetto dei suoi genitori, della sua identità, della sua lingua e dei suoi valori culturali, nonché il rispetto dei valori nazionali del paese nel quale vive, del paese di cui può essere originario e delle civiltà diverse dalla sua; d) preparare il fanciullo ad assumere le responsabilità della vita in una società libera, in uno spirito di comprensione, di pace, di tolleranza, di uguaglianza tra i sessi e di amicizia tra tutti i popoli e gruppi etnici, nazionali e religiosi e delle persone di origine autoctona [...]";
Visto il preambolo (lettera h) della Convenzione sui diritti delle persone con disabilità delle Nazioni Unite del 2006, ratificata con legge 3 marzo 2009 n. 18, in cui si riconosce che "la discriminazione contro qualsiasi persona sulla base della disabilità costituisce una violazione della dignità inerente e del valore della persona umana";
Visto l'art. 3 della Convenzione sui diritti delle persone con disabilità delle Nazioni Unite del 2006, ratificata con legge 3 marzo 2009, n. 18, che pone tra i principi della Convenzione stessa la non discriminazione;
Visto l'art. 21 (Non discriminazione) della Carta dei diritti fondamentali dell'Unione Europea del 2000 e in particolare il comma 1, secondo il quale "È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, gli handicap, l'età o le tendenze sessuali";
Visto l'art. 22 (Diversità culturale, religiosa e linguistica) della Carta dei diritti fondamentali dell'Unione Europea del 2000 secondo il quale "L'Unione rispetta la diversità culturale, religiosa e linguistica";
Visto l'art. 3 della Costituzione Italiana secondo cui "Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese";

Vista la direttiva n. 2000/43/CE del Consiglio dell'Unione Europea, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica;
Visto l'art. 3-ter della direttiva n. 2007/65/CE del Parlamento europeo e del Consiglio, dell'11 dicembre 2007, che modifica la direttiva 89/552/CEE del Consiglio relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti l'esercizio delle attività televisive secondo il quale "Gli Stati membri assicurano, con misure adeguate, che i servizi di media audiovisivi forniti dai fornitori di servizi di media soggetti alla loro giurisdizione non contengano alcun incitamento all'odio basato su razza, sesso, religione o nazionalità";
Visto l'art. 6 della Direttiva (UE) 2018/1808 pubblicata nella Gazzetta ufficiale dell'Unione europea del 28 novembre 2018; 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi) come modificato
Considerato quanto specificamente previsto in materia dal ***Testo unico*** e, in particolare, dagli articoli:
3 a norma del quale "Sono principi fondamentali del sistema dei servizi di media audiovisivi e della radiofonia la garanzia della libertà e del pluralismo dei mezzi di comunicazione radiotelevisiva, la tutela della libertà di espressione di ogni individuo, inclusa la libertà di opinione e quella di ricevere o di comunicare informazioni o idee senza limiti di frontiere, l'obiettività, la completezza, la lealtà e l'imparzialità dell'informazione, la tutela dei diritti d'autore e di proprietà intellettuale, l'apertura alle diverse opinioni e tendenze politiche, sociali, culturali e religiose e la salvaguardia delle diversità etniche e del patrimonio culturale, artistico e ambientale, a livello nazionale e locale, nel rispetto delle libertà e dei diritti, in particolare della dignità della persona, della promozione e tutela del benessere, della salute e dell'armonico sviluppo fisico, psichico e morale del minore, garantiti dalla Costituzione, dal diritto dell'Unione europea, dalle norme internazionali vigenti nell'ordinamento italiano e dalle leggi statali e regionali";
– 7, comma 2, ***lett. a)***, secondo il quale "La disciplina dell'informazione radiotelevisiva, comunque, garantisce: a) la presentazione veritiera dei fatti e degli avvenimenti, in modo tale da favorire la libera formazione delle opinioni". La medesima norma precisa che l'Autorità stabilisce ulteriori regole per le emittenti per rendere effettiva

l'osservanza dei principi ivi contenuti nei programmi di informazione;
– 10, comma 1, secondo il quale "L'Autorità, nell'esercizio dei compiti ad essa affidati dalla legge, assicura il rispetto dei diritti fondamentali della persona nel settore delle comunicazioni, anche mediante servizi di media audiovisivi o radiofonici";
– 32, comma 5, secondo il quale "I servizi di media audiovisivi prestati dai fornitori di servizi di media soggetti alla giurisdizione italiana rispettano la dignità umana e non contengono alcun incitamento all'odio basato su razza, sesso, religione o nazionalità";
Vista la delibera n. 13/08/CSP, del 31 gennaio 2008, recante "Atto di indirizzo sulle corrette modalità di rappresentazione dei procedimenti giudiziari nelle trasmissioni radiotelevisive";
Vista la delibera n. 424/16/CONS, del 16 settembre 2016, recante "Atto di indirizzo sul rispetto della dignità umana e del principio di non discriminazione nei programmi di informazione, di approfondimento informativo e di intrattenimento", avente valore di indirizzo interpretativo delle disposizioni contenute negli artt. 3, 32, comma 5, e 34 del Testo unico in cui è previsto che i programmi radiotelevisivi nella diffusione di notizie devono "uniformarsi a criteri-verità, limitando connotazioni di razza, religione o orientamento sessuale non pertinenti ai fini di cronaca ed evitando espressioni fondate sull'odio o sulla discriminazione, che incitino alla violenza fisica o verbale ovvero offendano la dignità umana e la sensibilità degli utenti contribuendo in tal modo a creare un clima culturale e sociale caratterizzato da pregiudizi oppure interferendo con l'armonico sviluppo psichico e morale dei minori", nonché devono "rivolgere particolare attenzione alla modalità di diffusione di notizie e di immagini sugli argomenti di attualità trattati avendo cura di procedere ad una veritiera e oggettiva rappresentazione dei flussi migratori, mirando a sensibilizzare l'opinione pubblica sul fenomeno dell'hate speech, contrastando il razzismo e la discriminazione nelle loro espressioni mediatiche";
Vista la delibera n. 442/17/CONS, del 24 novembre 2017, recante "Raccomandazione sulla corretta rappresentazione dell'immagine della donna nei programmi di informazione e di intrattenimento" avente valore di indirizzo interpretativo delle disposizioni contenute negli artt. 3, 7, comma 2, lett. a), 10, comma 1, e 32, comma 5, del Testo unico con particolare riferimento al tema delle molestie a sfondo sessuale il quale "se non affrontato adeguatamente – rischia di perdere connotati informativi per scadere, in alcuni casi, nella colpevolizzazione della vittima che denuncia episodi risalenti nel tempo e in un

indiretto attacco alla sua credibilità come persona e come professionista" rischiando così da un lato "di alimentare immagini stereotipate della figura femminile" e dall'altro di generare al contrario, "la gogna mediatica [...] in processi e ostracizzazioni [...] rispetto a episodi nei quali si confondono, in un calderone fuori controllo, violenze, molestie e approcci comunque inadeguati";
Vista la delibera n. 46/18/CONS, del 6 febbraio 2018, recante "Richiamo al rispetto della dignità umana e alla prevenzione dell'incitamento all'odio" con la quale l'Autorità ha richiamato "i fornitori di servizi media audiovisivi a garantire nei programmi di informazione e comunicazione il rispetto della dignità umana e a prevenire forme dirette o indirette di incitamento all'odio, basato su etnia, sesso, religione o nazionalità" alla luce dei dati di monitoraggio sul pluralismo politico/istituzionale relativi al periodo 29 gennaio-4 febbraio 2018 dai quali la trattazione di casi di cronaca relativi a reati commessi da immigrati appariva "orientata, in maniera strumentale, ad evidenziare un nesso di causalità tra immigrazione, criminalità e situazioni di disagio sociale e ad alimentare forme di pregiudizio razziale nei confronti dei cittadini stranieri immigrati in Italia, contravvenendo ai principi di non discriminazione e di tutela delle diversità etniche e culturali che i fornitori di servizi media audiovisivi sono tenuti ad osservare nell'esercizio dell'attività di diffusione radiotelevisiva";
Visto il "Codice di autoregolamentazione delle trasmissioni di commento degli avvenimenti sportivi" denominato "Codice media e sport", recepito con il Decreto del Ministero delle comunicazioni del 21 gennaio 2008 n. 36;
Visto l'art. 2 della legge 3 febbraio 1963, n. 69 secondo il quale "È diritto insopprimibile dei giornalisti la libertà di informazione e di critica, limitata dall'osservanza delle norme di legge dettate a tutela della personalità altrui ed è loro obbligo inderogabile il rispetto della verità sostanziale dei fatti, osservati sempre i doveri imposti dalla lealtà e dalla buona fede. Devono essere rettificate le notizie che risultino inesatte, e riparati gli eventuali errori [...]";
Visto il "Testo unico dei doveri del giornalista", approvato dal Consiglio Nazionale dei giornalisti nella riunione del 27 gennaio 2016 che stabilisce che "il giornalista rispetta i diritti fondamentali delle persone e osserva le norme di legge poste a loro salvaguardia; [...] applica i principi deontologici nell'uso di tutti gli strumenti di comunicazione, compresi i social network";
Visto, in particolare l'art. 9 del "Codice deontologico relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica",

allegato al "Testo unico dei doveri del giornalista" sopra citato, che stabilisce che "nell'esercitare il diritto-dovere di cronaca, il giornalista è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali;
Vista la carta dei servizi per il superamento delle barriere comunicative approvata dal Tavolo permanente di confronto CNU-AGCOM-Associazioni persone con disabilità istituito il 16 aprile 2012;
Visto il Contratto nazionale di servizio tra il Ministero dello sviluppo economico e la Rai-Radiotelevisione italiana S.p.A. 2018-2022;
Vista la delibera n. 410/14/CONS, del 29 luglio 2014, recante "Regolamento di procedura in materia di sanzioni amministrative e impegni e Consultazione pubblica sul documento recante Linee guida sulla quantificazione delle sanzioni amministrative pecuniarie irrogate dall'Autorità per le garanzie nelle comunicazioni" come modificata, da ultimo, dalla delibera n. 581/15/CONS, del 16 ottobre 2015;
Considerato che la delibera n. 403/18/CONS, del 25 luglio 2018, recante "Avvio del procedimento per l'adozione di un regolamento in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech e all'istigazione all'odio" ha inteso avviare un percorso per l'attuazione del precetto sancito nel citato art. 32, comma 5, del Testo unico;
Tenuto conto che una quota significativa dei contenuti messi a disposizione sui servizi di piattaforma per la condivisione di video non è sotto la responsabilità editoriale del fornitore di piattaforme per la condivisione di video e che tali fornitori, tuttavia, in genere determinano l'organizzazione dei contenuti, ossia programmi, video generati dagli utenti e comunicazioni commerciali audiovisive, anche in modo automatizzato o con algoritmi.
Considerato che fornitori di piattaforme per condivisione di video, pertanto, dovrebbero essere tenuti ad adottare le misure appropriate per tutelare il grande pubblico dai contenuti che istigano alla violenza o all'odio nei confronti di un gruppo o di un membro di un gruppo per uno dei motivi di cui all'art. 21 della Carta dei diritti fondamentali dell'Unione europea;
Considerato che, alla luce delle disposizioni normative vigenti, i principi fondamentali del sistema dei servizi di media audiovisivi e della radiofonia rappresentati dalla libertà di espressione, di opinione e di ricevere e comunicare informazioni – comprensivi anche dei diritti di cronaca, di critica e di satira – devono conciliarsi con il rispetto della dignità della persona, dell'armonico sviluppo fisico, psichico e morale del minore, nonché con l'apertura alle diverse opinioni e ten-

denze politiche, sociali, culturali e religiose e con la salvaguardia delle diversità etniche e del patrimonio culturale, artistico e ambientale, a livello nazionale e locale;

Considerato che con il termine *"hate speech"* si intende l'utilizzo strategico di contenuti o espressioni mirati a diffondere, propagandare o fomentare l'odio, la discriminazione e la violenza per motivi etnici, nazionali, religiosi, ovvero fondati sull'identità di genere, sull'orientamento sessuale, sulla disabilità, o sulle condizioni personali e sociali, attraverso la diffusione e la distribuzione di scritti, immagini o altro materiale anche mediante la rete *internet*, i *social network* o altre piattaforme telematiche;

Considerato che l'Organizzazione per la Sicurezza e la Cooperazione in Europa (OSCE), nel dicembre 2009, prendendo atto del rapporto *"Hate Crimes in the OSCE Region – Incidents and Responses"* dell'Ufficio per le Istituzioni Democratiche e i Diritti Umani (ODIHR), ha ritenuto di impegnarsi ed impegnare gli Stati membri dell'organizzazione, tra cui l'Italia, nella lotta contro i crimini d'odio (Decision No. 9/09 *"Combating Hate Crimes"*) invitando gli Stati membri dell'organizzazione anche ad indagare il potenziale legame tra un uso sempre crescente di *internet* e la diffusione di opinioni che possano costituire un incitamento, motivato da pregiudizio, alla violenza ovvero a crimini generati dall'odio, meglio noti con il termine di *"hate crimes"*, e a sensibilizzare la società civile e l'opinione pubblica sul tema, al fine di garantire un approccio globale alla lotta contro questa tipologia di crimine;

Considerato che gli argomenti trattati nei programmi informativi e di intrattenimento diffusi dai servizi di media audiovisivi e radiofonici diventano sempre più di frequente oggetto di attenzione, discussione, polarizzazione ed estremizzazione nei *social media*, che rappresentano forme significative, talvolta prevalenti per alcune fasce della popolazione, di accesso alle informazioni, nonché di espressione, formazione e sedimentazione dell'opinione pubblica, spesso alimentando artate strategie di disinformazione finalizzate a sostenere discorsi d'odio o comunque a diffondere rappresentazioni strumentali, falsate e discriminatorie dei complessi fenomeni osservati;

Considerato che l'esigenza informativa è assolta primariamente dai mezzi di comunicazione di massa che, a norma dell'art. 21 della Costituzione come interpretato dalla giurisprudenza costituzionale e ordinaria, devono concorrere a fornire alla pubblica opinione un'informazione completa, obiettiva, imparziale e pluralistica e che l'esercizio del diritto di critica e di cronaca deve essere improntato a criteri di verità, di essenzialità e continenza, a partire dalla corretta

rappresentazione dei fatti e dalla diffusione di dati verificati e di comparazioni statisticamente significative;
Rilevata l'esigenza di garantire, in particolare nei programmi di informazione e intrattenimento, effettività alla tutela dei diritti fondamentali della persona, nel rispetto del principio di non discriminazione e di tutela della diversità etniche, culturali, religiose e connesse a peculiari condizioni soggettive, fisiche, mentali e sociali. In particolare, nel rispetto della libertà editoriale e del diritto di libera manifestazione del pensiero e di cronaca, ciascun fornitore di servizi media deve garantire la completezza dell'informazione e l'assenza di discorsi d'odio: la Corte europea dei diritti dell'uomo si è soffermata più volte sulla distinzione tra forme di discorso pubblico tollerato in una società democratica e discorso che deve essere limitato e sanzionato al fine di proteggere il diritto di individui e gruppi di non essere discriminati, o discorso che può portare alla violenza, ai disordini pubblici e alla criminalità;
Ritenuta, pertanto, la necessità di fornire una regolamentazione di dettaglio del precetto contenuto nel citato art. 32, comma 5, del *Testo unico* affinché nei servizi di media audiovisivi e radiofonici sia assicurato l'effettivo rispetto dei diritti fondamentali a garanzia degli utenti, *sub specie* di dignità della persona e del principio di non discriminazione, oltre che il divieto di incitamento all'odio basato su etnia, sesso, religione e nazionalità, procedendo a tal fine ad una specifica attività di monitoraggio;
Ritenuto nelle more del recepimento nel nostro ordinamento della nuova direttiva 2018/1808 pubblicata nella *Gazzetta ufficiale* dell'Unione europea del 28 novembre 2018, di prevedere l'avvio di procedure di co-regolamentazione affinché non solo i fornitori di servizi di media audiovisivi, ma anche le piattaforme per la condivisione di video predispongano codici di condotta recanti misure idonee a prevenire e contrastare ogni forma di istigazione all'odio e di violazione dei principi sanciti a tutela della dignità umana;
Ritenuto per l'effetto di procedere all'individuazione dell'ambito delle fattispecie riconducibili al dettato normativo, soggette al potere di vigilanza e sanzionatorio dell'Autorità, secondo gli indirizzi ed orientamenti giurisprudenziali in materia, in particolar modo della Corte europea dei diritti dell'uomo;
Ritenuto che ai fini della valutazione delle fattispecie oggetto del presente provvedimento il contesto in cui l'evento si è prodotto, la relazione media tradizionali e *social network*, i mezzi per la diffusione del messaggio acquisiscono una particolare rilevanza. Infatti, il contenuto diffuso sul servizio di media audiovisivo o radiofonico

può essere oggetto di ulteriori estremizzazioni o polarizzazione attraverso la circolazione in rete;
Espletata la consultazione pubblica prevista dalla delibera n. 25/19/CONS;
Visti i contributi pervenuti nell'ambito della consultazione pubblica da parte della Presidenza del Consiglio (Dipartimento per le Pari Opportunità – UNAR) (prot. n. 116718 del 18 marzo 2019), del Consiglio Nazionale dell'Ordine dei giornalisti (prot. n. 122569 del 20 marzo 2019), dell'Associazione culturale UPRE Roma (prot. 129239 del 25 marzo 2019), dell'Associazione Articolo 19 (prot. n. 155904 del 9 aprile 2019) e delle seguenti società: Rai-Radiotelevisione italiana S.p.A. (prot. 125991 del 22 marzo 2019); R.T.I. S.p.A. Reti televisive italiane (prot. n. 128369 del 25 marzo 2019); La7 S.p.A. (prot. n. 126634 del 22 marzo 2019); Sky Italia S.r.l. (prot. n. 141462 del 1° aprile 2019);
Sentite le osservazioni formulate nel corso delle audizioni dei seguenti soggetti che ne hanno fatto richiesta: Aeranti Corallo (in data 9 aprile 2019); Confindustria Radio e Tv (in data 9 aprile 2019); R.T.I. Reti Televisive Italiane S.p.A. (in data 9 aprile 2019); La7 S.p.A. (9 aprile 2019);
Considerato quanto segue:
1) Con riferimento alle competenze attribuite all'Autorità in materia di tutela del rispetto della libertà umana e di dignità della persona e di contrasto all'incitamento all'odio basato su razza, sesso religione o nazionalità, deve farsi riferimento agli artt. 3, 7, 10 e 32, comma 5, del *Testo unico*. Alla luce di quanto previsto da tali norme, non forma materia di dibattito la competenza dell'Autorità a emanare disposizioni regolamentari per garantire il rispetto dei principi sopra richiamati da parte dei fornitori dei servizi di media audiovisivi e radiofonici. Invero, tali disposizioni rappresentano il fondamento del potere regolamentare dell'Autorità e le consentono di fissare regole, quali quelle contenute nel Regolamento allegato, volte ad assicurare il rispetto dei diritti fondamentali della persona nel settore delle comunicazioni.
2) Con riferimento a quanto emerso nell'ambito della consultazione pubblica sullo schema di regolamento, in particolar modo in ordine alle definizioni, al campo di applicazione nonché ai profili procedurali, si riportano di seguito le principali osservazioni svolte dai partecipanti, unitamente alle conclusive valutazioni, motivate, dell'Autorità:

Posizioni principali dei soggetti intervenuti

Osservazioni di carattere generale

I partecipanti alla consultazione, hanno condiviso gli obiettivi generali di tutela della dignità umana, del principio di non discriminazione e di contrasto all'*hate speech*.
La maggior parte dei partecipanti ha tuttavia evidenziato che le espressioni o discorsi d'odio (*hate speech*), sono di regola diffuse non sui media tradizionali (tv, radio, carta stampata), ma tramite il *web*, spesso a causa di notizie diffuse senza la intermediazione operata dai giornalisti (il pubblico è raggiunto da ogni genere di notizia attraverso *social*, *blog* e siti).
In quest'ottica è stato evidenziato come alcune norme risultino eccessivamente gravose per i fornitori di servizi di media audiovisivi, mentre nessuna disposizione cogente viene rivolta alle piattaforme o ai social e, in generale, a quanto diffuso *on line*.
Un soggetto ritiene che lo schema di regolamento sottoposto a consultazione rappresenti *"un intervento particolarmente pervasivo nei confronti dei broadcaster tradizionali, nonostante la questione dell'hate speech trovi la sua massima espressione e diffusione sulle piattaforme social, che hanno, ad oggi, pochi limiti e sfuggono al controllo e al potere sanzionatorio dell'Autorità"*. Inoltre, due soggetti propongono che lo strumento della co-regolamentazione sia adottato anche per i fornitori di servizi media audiovisivi e radiofonici. Un soggetto chiede di voler rinviare l'emanazione della delibera oggetto di consultazione, all'esito di un intervento del legislatore complessivo e di sistema che disciplini l'intero comparto, ivi inclusi gli operatori OTT. Infine, alcuni soggetti chiedono che sia riconsiderata l'opportunità di adottare il regolamento medesimo.

Osservazioni dell'Autorità

La consultazione ha evidenziato la condivisione da parte dei soggetti intervenuti delle finalità dello schema di regolamento di tutela delle dignità umana e di contrasto all'*hate speech*. Tuttavia, alcuni partecipanti alla consultazione hanno chiesto che sia riconsiderata l'opportunità di adottare il regolamento medesimo e che, in ogni caso, la materia sia oggetto di co-regolamentazione anche per i fornitori di servizi media audiovisivi e radiofonici. L'Autorità ritiene necessario fornire una regolamentazione di dettaglio del precetto contenuto nel citato art. 32, comma 5, del *Testo unico* affinché nei servizi di media audiovisivi e radiofonici sia assicurato l'effettivo rispet-

to dei diritti fondamentali a garanzia degli utenti, con particolare riferimento alla dignità della persona e al principio di non discriminazione.
In quest'ottica, nell'intento di promuovere la cultura dell'integrazione come strumento di contrasto ad ogni forma di discriminazione, il regolamento è destinato ad assolvere una funzione propositiva e proattiva per l'adozione non solo sui media tradizionali di linguaggi di comunicazione rispettosi della dignità umana.

Capo I

Disposizioni generali

Art. 1 (Definizioni)

Posizioni principali dei soggetti intervenuti

Un soggetto non condivide la definizione di *"espressioni d'odio"* contenuta nella *lett. n)* dell'art. 1 in quanto le alternative riportate nello schema di regolamento contengono definizioni molto ampie con significativi margini di indeterminatezza e propone di fare riferimento a quanto previsto dall'art. 604-*bis*, cod. pen. che punisce *"chi propaganda idee fondate sulla superiorità o sull'odio razziale o etnico, ovvero istiga a commettere o commette atti di discriminazione per motivi razziali, etnici, nazionali o religiosi"*.
Un altro soggetto rileva come la delibera non possa eccedere i limiti contenuti nell'art. 32, comma 5, del *Testo unico* che si riferisce esclusivamente ai contenuti che ledono la dignità delle persone e incitano all'odio basato su razza, sesso, religione o nazionalità. Pertanto, ritiene che il Regolamento dovrebbe limitarsi a sanzionare le forme di espresso incitamento all'odio o di propaganda di idee discriminatorie. Un partecipante chiede di definire in modo più puntuale il reato di incitamento all'odio e il possibile contenuto discriminatorio al fine di salvaguardare il diritto ad informare e ad essere informati.
Un soggetto propone di aggiungere, nell'ambito dell'art. 1, la definizione di giornalista.
Un altro propone di eliminare il termine "razziale" ritenendo preferibile il riferimento al concetto di origine etnica in quanto assume una valenza più ampia rispetto al concetto di razza includendo gli aspetti legati a fattori culturali e linguistici. Richiede inoltre che, i fattori di discriminazione, siano integrati con l'identità di genere.
Infine, un soggetto richiede che sia inserito, nell'ambito dell'elen-

cazione delle forme di odio basate sull'intolleranza, anche la parola "*antiziganismo*".

Osservazioni dell'Autorità

Per quanto attiene ai diversi rilievi formulati in relazione alla definizione di "*espressioni o discorso d'odio*", tenuto conto della esigenza di disporre di una formulazione univoca e certa, si ritiene di adottare, tra le diverse definizioni proposte nello schema di regolamento, la seguente: "espressioni o discorso d'odio (*hate speech*)", l'utilizzo di contenuti o espressioni suscettibili di diffondere, propagandare o fomentare l'odio e, la discriminazione e istigare alla violenza nei confronti di un determinato insieme di persone 'target', attraverso stereotipi relativi a caratteristiche di gruppo, etniche, di provenienza territoriale, di credo religioso, d'identità di genere, di orientamento sessuale, di disabilità, di condizioni personali e sociali, attraverso la diffusione e la distribuzione di scritti, immagini o altro materiale, anche mediante la rete *internet*, i *social network* o altre piattaforme telematiche.

Art. 2
(Ambito di applicazione)

Posizioni principali dei soggetti intervenuti

Un soggetto propone di evidenziare le attribuzioni disciplinari dell'Ordine dei giornalisti.

Osservazioni dell'Autorità

L'art. 2 definisce la portata applicativa del regolamento avuto riguardo al profilo soggettivo e oggettivo. si riferisce ai principi e alle disposizioni cui devono adeguarsi i fornitori di servizi.
Si è ritenuto di inserire, al comma 2, il riferimento alle attribuzioni dell'Ordine dei giornalisti di cui al combinato disposto della legge n. 69/1963 e del D.P.R. n. 137/2012, relativamente ai propri iscritti.

Capo II

Fornitori di media audiovisivi e radiofonici

Il Capo II è stato completamente riformulato per tenere conto delle osservazioni svolte dai soggetti partecipanti alla consultazione pubblica. In particolare, il Capo ora si compone di 6 articoli (artt. 3-8),

dedicati ai principi generali, ai principi specifici di contrasto all'*hate speech*, alle iniziative di contrasto, ai procedimenti sanzionatori, alla violazione dei principi e infine alla pubblicazione dei provvedimenti. Di seguito si dà conto dei principali rilievi svolti dai partecipanti e delle conseguenti valutazioni dell'Autorità.

Posizioni principali dei soggetti intervenuti

Un partecipante non condivide il riferimento alla categoria dei "*soggetti a rischio di discriminazione*" cui è legata, nell'ambito dello schema di regolamento, l'introduzione di una serie di cautele e di obblighi preventivi dei fornitori di servizi di media audiovisivi e radiofonici in quanto ogni individuazione di soggetti a rischio di discriminazione risulterebbe arbitraria atteso che qualunque gruppo umano, definito in base al genere, alle preferenze sessuali, alla posizione sociale, alla fede religiosa, alle caratteristiche etniche, è parimenti suscettibile di discriminazione.
Numerosi soggetti hanno espresso perplessità sulla formulazione originaria dell'art. 5 ritenendo le previsioni in esso contenute potenzialmente in contrasto con la libertà editoriale delle emittenti e con la libertà di cronaca e come tali idonee a ledere la libertà di espressione e l'indipendenza delle emittenti e dei giornalisti, e al contempo di difficile attuazione concreta.
Il sindacato dell'Autorità rischia di incidere su scelte editoriali delle emittenti (e dei loro giornalisti), limitando, in alcuni casi, la libertà di scelta sui contenuti. Inoltre, esporrebbe le emittenti – e la stessa Autorità – a innumerevoli esposti da parte di soggetti terzi che ritenessero di essere stati lesi dalla diffusione di notizie, immagini e ogni altro contenuto. Pressoché ogni "contenuto" è "suscettibile anche solo di alimentare pregiudizi".
Inoltre, è stato evidenziato come nella trattazione di temi che coinvolgono soggetti a rischio di discriminazione il criterio di valutazione è soggettivo con conseguente difficoltà di individuare il confine che separa una narrazione discriminatoria da una narrazione completa e coerente con i principi costituzionali. È stato altresì sottolineato che per le emittenti televisive la disciplina in materia già esiste. Un ulteriore strumento di regolamentazione, ad avviso di un partecipante, rischierebbe di appesantire il lavoro giornalistico, richiedendo l'adozione di artifici dialettici nella narrazione delle notizie.
Un soggetto ritiene che lo schema di regolamento di fatto realizza una sostanziale equiparazione tra emittenti private e concessionaria. È stato anche rilevato che il potere sanzionatorio dell'Autorità riconosciuto dal regolamento sottoposto a consultazione non abbia

una base normativa e si ponga in contrasto con i principi generali dell'ordinamento e con lo stesso Tusmar.
Quanto al monitoraggio è stato osservato come i criteri individuati nello schema rischiano di introdurre un controllo minuzioso, discrezionale, non regolato parametri certi e predeterminati, sui contenuti e sulle modalità di realizzazione dei programmi. Taluni elementi potrebbero rivelarsi troppo poco determinati e consentire un sindacato eccessivo (la finalità e la motivazione dell'espressione, il tono utilizzato), altri si riferiscono ad elementi che non sono per loro natura controllati e controllabili (come il pubblico).
Infine, perplessità sono state sollevate con specifico riferimento ai profili procedurali e, in particolare, al potere di segnalazione per il rischio di aprire a segnalazioni di ogni tipo e provenienza. Pertanto, è stato suggerito di limitare la legittimazione alle segnalazioni alle associazioni ed enti statutariamente impegnate nella lotta alle discriminazioni e al razzismo.

Osservazioni dell'Autorità

Per ciò che riguarda i criteri cui i fornitori di servizi di media audiovisivi devono attenersi al fine di assicurare il rispetto dei principi di non discriminazione e di contrasto all'*hate speech*, l'Autorità, nell'ambito dello schema di regolamento, aveva ritenuto opportuno esemplificare una serie di parametri al fine di rendere più trasparente la propria attività di vigilanza.
Tuttavia, esaminate le osservazioni sollevato, si ritiene condivisibile la proposta della maggior parte dei soggetti intervenuti di adottare previsioni di carattere più generale nelle quali sono chiaramente rappresentate le finalità del provvedimento in relazione ai valori e principi che, in attuazione del dettato costituzionale e legislativo, l'Autorità intende tutelare.
Si è pertanto ritenuto di eliminare l'art. 5 del Regolamento, così da incentrare la disciplina degli obblighi gravanti sui fornitori di servizi di media audiovisivi in tema di contrasto all'*hate speech*, su quanto previsto dagli artt. 3 *(Principi generali)* e 4 *(Principi di non discriminazione e contrasto all'hate speech)*. Considerazioni analoghe valgono in relazione all'art. 7 dello schema sottoposto a consultazione nel quale erano individuati i criteri di monitoraggio. Anche in questo caso, nel prendere atto delle perplessità manifestate dai soggetti intervenuti, si è ritenuto di non esplicitare nel provvedimento degli elementi che possono essere considerati ai fini del monitoraggio.
Tale modifica, unitamente all'eliminazione dei dettagliati criteri pre-

visti dall'art. 5, assicura il pieno rispetto della libertà editoriale dei fornitori di servizi media.
L'art. 5, premesso il rango costituzionale della tutela della dignità umana, intende promuovere iniziative volte a creare una consapevolezza anche culturale di tale diritto attraverso il contributo dei mezzi di informazione. Se la finalità è comune e condivisa, è indubbio che sulla concessionaria pubblica, in ragione della missione di cui è portatrice e del contratto di servizio, grava una maggiore responsabilità anche etica a promuovere i valori sottesi al presente provvedimento.
In merito alle osservazioni con cui si rileva la possibile violazione del principio di legalità, in ragione della mancata espressa previsione nell'ambito dell'art. 51 del Tusmar, di sanzioni per la violazione dell'art. 32, comma 5, si rileva che la sanzione amministrativa prevista dall'art. 9 (divenuto art. 7 a seguito dell'eliminazione degli artt. 5 e 7) trova la sua base legale nell'art. 1, comma 31, legge n. 249 del 1997, che assoggetta a sanzione amministrativa pecuniaria "*i soggetti che non ottemperano agli ordini e alle diffide dell'Autorità, impartite ai sensi della presente legge*".
Tale norma fa senz'altro riferimento anche alle prescrizioni di contenuto ordinatorio contenute negli atti di regolazione, quale quelle previste dal comma 2 dell'art. 9 (divenuto comma 3 dell'art. 7) del Regolamento. In altri termini, l'art. 1, comma 31, della legge n. 249 del 1997 prevede una sanzione per l'inosservanza degli ordini impartiti dall'Autorità ai sensi della stessa legge e, quindi, anche per la violazione delle misure ordinatorie impartite nell'esercizio delle funzioni regolatorie che la legge attribuisce all'Autorità e di cui il regolamento sottoposto a consultazione è certamente espressione.
Si condivide il suggerimento emerso nel corso della consultazione in merito la legittimazione alle segnalazioni soltanto per le associazioni ed enti statutariamente impegnate nella lotta alla discriminazione, fermo restando il potere dell'Autorità di agire d'ufficio per la verifica delle violazioni del regolamento.
Viene introdotto, al comma 1 dell'art. 6 *(Procedimenti sanzionatori)* il riferimento alla natura sistematica o episodica delle violazioni in quanto tale elemento diviene rilevante nella graduazione delle conseguenze previste dal successivo art. 7 *(Violazione dei principi)*.
A tal riguardo, si evidenzia che, nel caso di violazioni episodiche dei principi previsti dal regolamento, l'Autorità, previo contraddittorio, invia una comunicazione alla Società dandone comunicazione sul proprio sito. Qualora si tratti di violazioni sistematiche o particolarmente gravi, l'Autorità avvia un procedimento sanzionatorio, e in caso di violazioni, diffida il fornitore di servizi di media audiovisivi a non reiterare la condotta illecita.

Capo III

Fornitori di piattaforme per la condivisione di video

Art. 11
(Discriminazione e discorsi di incitamento all'odio diffusi sulle piattaforme per la condivisione di video)

Posizioni principali dei soggetti intervenuti

Per quanto riguarda i fornitori di piattaforme per la condivisione di video, l'art. 11 promuove procedure di co-regolamentazione: a giudizio di alcuni partecipanti, non sembrano misure equilibrate se paragonate al coacervo di norme a carico dell'emittenza nazionale evidenziando dunque la disparità di trattamento tra le piattaforme, oggetto di un generico invito alla coregolamentazione, e i media tradizionali, destinatari di obblighi, controlli e sanzioni.

Osservazioni dell'Autorità

Deve rilevarsi che le norme primarie che delimitano l'area di competenza dell'Autorità non consentono, allo stato, interventi regolatori aventi ad oggetto i contenuti diffusi sulle piattaforme per la condivisione di video. L'Autorità può pertanto promuovere, mediante procedure di coregolamentazione, l'adozione di misure appropriate per tutelare il grande pubblico dai contenuti che istigano alla violenza o all'odio nei confronti di un gruppo o di un membro di un gruppo per uno dei motivi di cui all'art. 21 della Carta dei diritti fondamentali dell'Unione europea. Ciò anche sulla scorta di quanto previsto dalle Direttive europee sui servizi di media audiovisivi.
Si ritiene pertanto di non apportare modifiche all'art. 11 (art. 9 nella nuova formulazione del Regolamento) se non l'introduzione del comma 5 laddove si prevede che l'Autorità si riserva di rivedere il presente regolamento alla luce di eventuali codici condotta o misure autonomamente adottate anche dai fornitori di servizi di media audiovisivi che sono pertanto invitati a promuovere iniziative di questo genere.

Capo IV

Disposizioni finali

Art. 12
(Comitato Consultivo)

Posizioni principali dei soggetti intervenuti

Sull'art. 12 sono intervenute osservazioni di vario tenore. La posizio-

ne espressa dagli editori televisivi converge nel ritenere non condivisibile la scelta di istituire un Comitato posto che ogni decisione e valutazione spetta all'Autorità cui, dunque, il Comitato non può sostituirsi. Laddove l'Autorità ritenga comunque necessario mantenere la previsione, il Comitato dovrebbe essere necessariamente integrato con i rappresentanti del settore radiotelevisivo.
Un soggetto intervenuto propone di prevedere la nomina, nell'ambito del Comitato consultivo, del Presidente del Consiglio nazionale dell'Ordine nazionale dei giornalisti. Due soggetti evidenziano che il comitato consultivo di esperti non prevede la presenza di un rappresentante degli operatori. Un altro soggetto non condivide l'istituzione di un Comitato di esperti.

Osservazioni dell'Autorità

L'Autorità, pur sottolineando come la previsione di istituire un Comitato di esperti fosse strumentale all'esigenza di valutare e verificare l'impatto applicativo del regolamento anche al fine di rivederne la formulazione dopo una prima fase attuativa attraverso l'ausilio di esperti appartenenti a categorie diverse per assicurare una lettura integrata e trasversale delle questioni sottese al provvedimento, ritiene di accogliere le osservazioni svolte da alcuni partecipanti e di eliminare la previsione del Comitato consultivo.
Si considera tuttavia necessario prevedere un coinvolgimento del Consiglio Nazionale dell'Ordine dei giornalisti allorquando nella fattispecie oggetto di esame da parte dell'Autorità sia coinvolto un giornalista. L'Ordine, infatti, nell'esprimere apprezzamento per la scelta dell'Autorità di intervenire in questa delicata materia, ha sottolineato la costante attività di vigilanza svolta per evitare e prevenire simili fenomeni, manifestando al contempo la necessità di essere coinvolto laddove il caso sia imputabile o comunque coinvolga un giornalista. Tale scelta appare condivisibile soprattutto ove si consideri che il provvedimento dell'Autorità può rivolgersi solo all'emittente;
Rilevata l'esigenza di garantire, in particolare nei programmi di informazione e intrattenimento, effettività alla tutela dei diritti fondamentali della persona, nel rispetto del principio di non discriminazione e di tutela della diversità etniche, culturali, religiose e connesse a peculiari condizioni soggettive, fisiche, mentali e sociali. In particolare, nel rispetto della libertà editoriale e del diritto di libera manifestazione del pensiero, ciascun fornitore di servizi media deve garantire la completezza dell'informazione e l'assenza di discorsi d'odio: la Corte europea dei diritti dell'uomo si è soffermata più volte sulla distinzione tra forme di discorso pubblico tollerato in una società

democratica e discorso che deve essere limitato e sanzionato al fine di proteggere il diritto di individui e gruppi di non essere discriminati, o discorso che può portare alla violenza, ai disordini pubblici e alla criminalità;
Ritenuto che i criteri di cui l'Autorità può conto, in caso di violazioni dei principi di non discriminazione e di contrasto all'*hate speech*, nella valutazione della condotta dei fornitori di servizi di media audiovisivi sono i seguenti:

a) utilizzo di espressioni, immagini, suoni, elementi grafici – quali i titoli e i sottopancia utilizzati per la sintesi di contenuti delle trasmissioni e tutti gli altri contenuti, anche quelli tratti dai *social networks* o dai messaggi SMS inviati dagli utenti e mandati in onda in sovrimpressione – che possano, in maniera indiretta o diretta, diffondere, incitare, promuovere o giustificare l'odio o forme di discriminazione e intolleranza, offendere la dignità umana o, in casi estremi, che possano portare alla violenza, al disordine e al crimine nei confronti di una persona o di gruppi di persone per motivi di genere, età, orientamento sessuale, classe, etnia, lingua, nazionalità, colore della pelle, origine sociale, credenze religiose, istruzione, affiliazione politica, *status* personale e familiare, disabilità fisiche e mentali, condizioni di salute e per ogni altro motivo che possa costituire una lesione dei diritti della persona;

b) diffusione di dati relativi alla sfera privata delle persone non rilevanti e pertinenti ai fini della cronaca, per prevenire e combattere fenomeni di discriminazione, che possono essere alimentati da notizie inesatte, tendenziose o non veritiere;

c) diffusione di immagini e informazioni imprecise, sommarie, fuorvianti e tendenziose, che possano suscitare anche allarmi ingiustificati, e non sorretti dai dati e dalle informazioni effettivamente disponibili, nei confronti di persone o gruppi di persone, e ingenerare suggestione o confusione nel telespettatore con nocumento dei principi di lealtà, obiettività e buona fede nella corretta ricostruzione degli avvenimenti;

d) improprie associazioni di notizie o fenomeni che sembrano stabilire un nesso tra caratteristiche o eventi specifici ad un determinato gruppo di persone, e spettacolarizzazione e generalizzazione di vicende, tali da alimentare e diffondere rappresentazioni strumentali, falsate, stereotipate e discriminatorie;

e) mancata tempestiva correzione di eventuali errori o inesattezze intervenuti nella diffusione di notizie e nella trattazione di temi che possano riguardare soggetti a rischio di discriminazione al fine di garantire una informazione completa e imparziale, assicurando altresì la facoltà di replica;

f) mancato rispetto, nei programmi, dei criteri di correttezza del linguaggio e del comportamento dei partecipanti, in particolar modo se si tratta di rappresentanti politici e istituzionali o altri personaggi di rilevanza pubblica, e riproposizione di modelli verbali e comportamentali caratterizzati da volgarità, rappresentazione di violenza fisica o verbale, aggressività, pregiudizi e allusioni che possano offendere la dignità umana e contrastare con l'esigenza di garantire effettività alla tutela dei diritti fondamentali della persona;

g) nel caso di violazioni dei principi di non discriminazione e contrasto all'*hate speech* realizzatesi nel corso di trasmissioni radiofoniche o televisive diffuse in diretta da ospiti, membri del pubblico, interlocutori telefonici o via *internet* o in collegamento, mancata presa di posizione del conduttore o del giornalista in merito al proprio contrario avviso rispetto a quanto accaduto per ricondurre il programma entro i binari della correttezza e del rispetto dei principi sopra richiamati;

h) nel caso di trasmissioni registrate, mancata adozione di ogni più utile accorgimento per prevenire e / o evitare la diffusione di contenuti lesivi della dignità della persona;

Ritenuta, pertanto, la necessità di fornire una regolamentazione di dettaglio del precetto contenuto nel citato art. 32, comma 5, del *Testo unico* affinché nei servizi di media audiovisivi e radiofonici sia assicurato l'effettivo rispetto dei diritti fondamentali a garanzia degli utenti, *sub specie* di dignità della persona e del principio di non discriminazione, oltre che il divieto di incitamento all'odio basato su etnia, sesso, religione e nazionalità, procedendo a tal fine ad una specifica attività di monitoraggio;
Ritenuto per l'effetto di procedere all'individuazione dell'ambito delle fattispecie riconducibili al dettato normativo, soggette al potere di vigilanza e sanzionatorio dell'Autorità, secondo gli indirizzi ed orientamenti giurisprudenziali in materia, in particolar modo della Corte europea dei diritti dell'uomo;
Ritenuto che ai fini della valutazione delle fattispecie oggetto del presente provvedimento il contesto in cui l'evento si è prodotto, la relazione media tradizionali e *social network*, i mezzi per la diffu-

sione del messaggio acquisiscono una particolare rilevanza. Infatti, il contenuto diffuso sul servizio di media audiovisivo o radiofonico può essere oggetto di ulteriori estremizzazioni o polarizzazione attraverso la circolazione in rete;
Rilevata pertanto l'opportunità di promuovere l'elaborazione e l'adozione di codici di autoregolamentazione da parte delle piattaforme digitali per il contrasto ai discorsi d'odio;
Udita la relazione del Commissario Antonio Nicita, relatore ai sensi dell'art. 31 del *Regolamento concernente l'organizzazione ed il funzionamento dell'Autorità*;

Delibera

Art. 1

È approvato il *Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech* unitamente alla relativa relazione introduttiva, come riportati rispettivamente negli Allegati A e B alla presente delibera che ne costituiscono parte integrante.
La presente delibera può essere impugnata entro sessanta giorni dalla sua pubblicazione innanzi al Tar del Lazio.
La presente delibera è pubblicata sul sito *web* dell'Autorità ed entra in vigore il giorno successivo a quello della sua pubblicazione.

Roma, 15 maggio 2019

IL PRESIDENTE
Angelo Marcello Cardani

IL COMMISSARIO RELATORE
Antonio Nicita

Per attestazione di conformità a quanto deliberato
IL SEGRETARIO GENERALE
Riccardo Capecchi

Recta Ratio

Testi e Studi di Filosofia del Diritto

Volumi pubblicati

Prima serie:

1. V. MATHIEU, *Luci ed ombre del giusnaturalismo,* 1989, pp. 328.
2. D. CAMPANALE, *Il diritto naturale tra metafisica e storia. Leibniz e Vico, I. Leibniz*, 1988, pp. 180.
3. F. D'AGOSTINO, *La sanzione nell'esperienza giuridica*, terza edizione, 1993, pp. 200.
4. F. VIOLA, *Diritti dell'uomo diritto naturale etica contemporanea*, 1989, pp. 220.
5. S. COTTA, *Diritto persona mondo umano*, 1989, pp. II-322.
6. B. MONTANARI, *Fenomeni sociali e lettura giuridica*, 1989, pp. 300.
7. C. BRUAIRE, *La forza dello spirito e lo spirito del diritto*, a cura di PIERFRANCO VENTURA, 1990, pp. XVIII-166.
8. B. PASTORE, *Tradizione e diritto*, Prefazione di Enrico Opocher, 1990, pp. 308.
9. G. FIASCHI, *Il desiderio di nulla. Compimento rivoluzionario e sessualità moderna*, 1990, pp. 120.
10. S. AMATO, *Il soggetto e il soggetto di diritto*, 1990, pp. 280.
11. A. DAL BROLLO, *La giustizia rivoluzionaria*, 1990, pp. 172.
12. H. KELSEN, *La pace attraverso il diritto*, a cura di LUIGI CIAURRO, 1990, pp. 180.
13. B. CELANO, *Dover essere e intenzionalità. Una critica all'ultimo Kelsen*, 1990, pp. 344.
14. G. ZACCARIA (a cura), *Diritto positivo e positività del diritto*, 1991, pp. XIV-366.
15. P. AMSELEK (a cura), *Teoria degli atti linguistici etica e diritto*, ed. it. a cura di Angiola Filipponio, 1991, pp. 300.
16. F. TODESCAN, *Itinerari critici dell'esperienza giuridica*, 1991, pp. 156.
17. F. D'AGOSTINO, *Il diritto come problema teologico*, 1992, pp. 232.
18. V. VILLA, *Conoscenza giuridica e concetto di diritto positivo. Lezioni di filosofia del diritto*, 1993, pp. 372.
19. B. MONTANARI (a cura), *La norma subita,* 1993, pp. 216.
20. R. MENEGHELLI, *Frammenti di filosofia minima*, 1993, pp. 140.

Seconda serie:

1. N. BOBBIO, *Teoria generale del diritto*, 1993, pp. X-302.
2. F. D'AGOSTINO, *Filosofia del diritto*, seconda edizione ampliata, 1996, pp. VIII-280.
3. G. COSI, *Il Logos del diritto*, 1993, pp. X-430.
4. O. HÖFFE, *Persino un popolo di diavoli ha bisogno dello Stato. Contributi filosofici per un'etica del diritto e dello Stato*, a cura di AGATA C. AMATO MANGIAMELI, 1993, pp. 194.
5. L. TRIOLO, *La norma ignota. Metateoria e teoria del diritto in Kelsen*, 1993, pp. X-410.
6. A. ARGIROFFI, *Valori, prassi, ermeneutica. Emilio Betti a confronto con Nicolai Hartmann e Hans Georg Gadamer*, 1994, pp. XII-236.
7. E. FRAENKEL, *La componente rappresentativa e plebiscitaria nello Stato costituzionale democratico*, a cura di LUIGI CIAURRO e CLEMENTE FORTE, 1994, pp. 98.

8. AA.VV., *Ermeneutica e filosofia analitica. Due concezioni del diritto a confronto*, a cura di MARIO JORI, 1994, pp. 274.
9. F. D'AGOSTINO, *Il diritto come problema teologico ed altri saggi di filosofia e teologia del diritto*, 1994, pp. 274.
10. AA.VV., *Ontologia e fenomenologia del giuridico, Studi in onore di Sergio Cotta*, a cura di FRANCESCO D'AGOSTINO, 1995, pp. VIII-356.
11. F. D'AGOSTINO, *La sanzione nell'esperienza giuridica, quarta edizione*, ristampa anastatica del 1995, pp. 200.
12. M. CASCAVILLA, *Colpa e infelicità. Giustizia e pena in Rosmini*, 1995, pp. VIII-176.
13. C. SARZOTTI, *Jean Domat. Fondamento e metodo della scienza giuridica*, 1995, pp. XII-332.
14. J.M. FINNIS, *Legge naturale e diritti naturali*, a cura di FRANCESCO VIOLA, 1996, pp. XXXII-476.
15. AA.VV., *Pluralità delle culture e universalità dei diritti*, a cura di FRANCESCO D'AGOSTINO, 1996, pp. 382.
16. P. SAVARESE, *Schelling filosofo del diritto. Introduzione alla lettura e commento di testi fondamentali*, 1996, pp. 238.
17. A.C. AMATO MANGIAMELI, «*Desiderai essere un cittadino*». *Oltre il retaggio simbolico della moderna sov*ranità, 1996, pp. 198.
18. L. TRIOLO, *Primato del diritto e giustizia*, 1996, pp. VIII-296.
19. L. PALAZZANI, *Il concetto di persona tra bioetica e diritto*, 1996, pp. VIII-304.
20. M. TALLACCHINI, *Diritto per la natura. Ecologia e filosofia del diritto*, 1996, pp. X-414.

Terza serie

1. F. D'AGOSTINO, *Bioetica nella prospettiva della filosofia del diritto, terza edizione ampliata*, 1998, pp. X-358.
2. N. BOBBIO, *Il positivismo giuridico*, 1996, pp. X-262.
3. E. PARIOTTI, *Individuo, comunità, diritti tra liberalismo, comunitarismo ed ermeneutica*, 1997, pp. 284.
4. F. D'AGOSTINO, *Il diritto come problema teologico ed altri saggi di filosofia del diritto*, terza edizione riveduta ed ampliata, 1997, pp. 322.
5. F. D'AGOSTINO (a cura di), *Ius divinum. Fondamentalismo religioso ed esperienza giuridica*, 1998, pp. VI-402.
6. I. TRUJILLO PÉREZ, *Francisco de Vitoria. Il diritto alla comunicazione e i confini della socialità umana*, 1997, pp. 214.
7. F. CONIGLIARO, *Dominium terrae. L'uomo nel mondo della natura*, 1998, pp. 256.
8. A. OLLERO-TASSARA, *Diritto "positivo" e diritti umani*, a cura di ISABEL TRUJILLO PÉREZ, 1998, pp. VI-210.
9. L. PALAZZANI, *Diritto naturale ed etica matrimoniale in Christian Thomasius. La questione del concubinato*, 1998, pp. VIII-348.
10. G. COSI, *La responsabilità del giurista. Etica e professione legale*, 1998, pp. XVI-452.
11. S. BERLINGÒ, *L'ultimo diritto. Tensioni escatologiche nell'ordine dei sistemi*, 1998, pp. VIII-266.
12. F. D'AGOSTINO, *La sanzione nell'esperienza giuridica*, quinta edizione, 1999, pp. XII-220.
13. M.F. RABAGLIETTI, *Diritto e legge nell'intramontabile mito di Antigone e Creonte*, 2000, pp. VI-154.
14. A.C. AMATO MANGIAMELI, *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, 2000, pp. VIII-292.
15. V. MATHIEU, *L'uomo animale ermeneutico*, 2000, pp. VI-282.
16. F. D'AGOSTINO, *Filosofia del diritto*, terza edizione ampliata, 2000, pp. VIII-296.

17. D. FALCIONI, *Natura e libertà in Kant. Un'interpretazione del progetto. Per la pace perpetua* (1795), *Presentazione di* Reinhard Brandt, 2000, pp. VIII-172.
18. L. TRIOLO, *Legalismo e legalità*, 2000, pp. VIII-192.
19. D. CANALE, *La costituzione delle differenze. Giusnaturalismo e codificazione del diritto civile nella Prussia del '700*, 2000, pp. 310.
20. E. PARIOTTI, *La comunità interpretativa nell'applicazione del diritto*, 2000, pp. 232.

Quarta serie

1. F. VIOLA, *Etica e metaetica dei diritti umani*, 2000, pp. XII-232.
2. F. CONIGLIARO, *La libertà. Estasi e tormento*, 2001, pp. VIII-328.
3. S. AMATO, *Coazione, coesistenza, compassione*, 2002, pp. VI-230.
4. F. D'AGOSTINO (a cura di), *La sterilizzazione come problema biogiuridico*, 2002, pp. VI-158.
5. V. BELLVER CAPELLA, *Clonare? Etica e diritto di fronte alla clonazione umana*, 2002, pp. XX-244.
6. A. ARGIROFFI, *Identità personale, giustizia ed effettività. Martin Heidegger e Paul Ricoeur*, 2002, pp. XVI-212.
7. I.T. MUCCICONI, «*Matrimonio di fatto*» *e pensiero giuridico*, 2002, pp. VIII-276.
8. M. GENTILE, *Giustizia e desiderio. La verità della vittima nel pensiero di René Girard*, 2003, pp. XIV-274.
9. I. TRUJILLO, *Imparzialità*, 2003, pp. XII-324.
10. F. BIONDO, *Benessere, giustizia e diritti umani nel pensiero di Amartya Sen*, 2003, pp. VI-256.
11. M. CASCAVILLA, *Il diritto insufficiente e necessario*, 2003, pp. XIV-214.
12. F. D'AGOSTINO-P.A. AMODIO (a cura di), *Le libertà religiose e di culto. Contenuto e limiti*, 2003, pp. XIV-130.
13. B. PASTORE, *Per un'ermeneutica dei diritti umani*, 2003, pp. VIII-184.
14. F. D'AGOSTINO, *Parole di bioetica,* 2004, pp. VIII-236.
15. V. VILLA, *Il positivismo giuridico: metodi, teorie e giudizi di valore. Lezioni di filosofia del diritto,* 2004, pp. X-326.
16. G. SADUN BORDONI, *L'ordine infranto. Il declino dello Stato nazionale tra diritto e politica,* 2004, pp. VIII-264.
17. P. MORO, *I diritti indisponibili. Presupposti moderni e fondamento classico nella legislazione e nella giurisprudenza,* 2004, pp. XII-292.
18. E. PARIOTTI, *La giustizia oltre lo stato: forme e problemi,* 2004, pp. 240.
19. V. MATHIEU, Privacy *e dignità dell'uomo. Una teoria della persona,* 2004, pp. X-146.
20. A.C. AMATO MANGIAMELI, *Stati postmoderni e diritto dei popoli*, 2004, pp. XII-216.

Quinta serie

1. G. SOLARI, *Il problema del diritto e dello Stato nella filosofia del diritto di Giorgio Guglielmo Federico Hegel,* a cura di F. D'Agostino, 2005, pp. XVIII-126.
2. E. BLOCH, *Diritto naturale e dignità umana*, 2005, pp. XIV-338.
3. F. MACIOCE, *La lealtà. Una filosofia del comportamento processuale*, 2005, pp. VI-274.
4. G. SARACENI, *Il Profeta e la legge. Riflessioni bergsoniane di filosofia per il diritto*, 2005, pp. VI-130.
5. M.A. FODDAI, *Sulle tracce della responsabilità. Idee e norme dell'agire responsabile*, 2005, pp. XVIII-414.
6. S. BAUZON, *La persona biogiuridica*, 2005, pp. XIV-138.
7. F. D'AGOSTINO, *Filosofia del diritto*, quarta edizione riveduta e ampliata, 2005, pp. VIII-308.

8. F. D'AGOSTINO, *Parole di giustizia*, 2006, pp. X-150.
9. F. D'AGOSTINO, *Lezioni di Teoria del Diritto*, 2006, pp. X-206.
10. F. D'AGOSTINO, *Lezioni di Filosofia del Diritto*, 2006, pp. XVI-280.
11. M. BORRELLO, *Diritto e forza. La questione della regola come limite all'arbitrio giuridico*, 2006, pp. X-366.
12. M. CASCAVILLA, *Diritto e morale nell'età dell'Illuminismo*, 2006, pp. X-250.
13. S. AMATO, *Biogiurisprudenza. Dal mercato genetico al* self-service *normativo*, 2006, pp. XII-188.
14. D. ANSELMO, *Shari'a e diritti umani*, 2007, pp. XXIV-332.
15. A.C. AMATO MANGIAMELI, *Corpi docili. Corpi gloriosi*, 2007, pp. XVIII-172.
16. G.R. MORCHON, *Teoria del diritto. Fondamenti di Teoria comunicazionale del diritto*, vol. I, a cura di G. Zaccaria, 2007, pp. XXVI-426.
17. F. MACIOCE, *Una filosofia della laicità*, 2007, pp. X-202.
18. L. CORSO, *Giustizia senza toga. La giuria e il senso comune*, 2008, pp. 248.
19. M. VOGLIOTTI (a cura di), *Il tramonto della modernità giuridica. Un percorso interdisciplinare*, 2008, pp. XVI-360.
20. M. MANGINI-F. VIOLA, *Diritto naturale e liberalismo. Dialogo o conflitto?,* 2009, pp. XIV-194.

Sesta serie:

101. A.C. AMATO MANGIAMELI, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, seconda edizione riveduta e aggiornata, 2015, pp. XII-348.
102. F. MACIOCE, *Ordine pubblico e autodeterminazione*, 2010, pp. X-202.
103. C. SARTEA, *Deontologia. Filosofia del lavoro professionale*, 2010, pp. XVIII-294.
104. F. D'AGOSTINO, *Bioetica e biopolitica. Ventuno voci fondamentali*, 2011, pp. XII-248.
105. P. GOMARASCA, *Comunità e partecipazione. L'idea di democrazia in Pier Luigi Zampetti*, 2011, pp. XX-228.
106. F. VIOLA, *Rule of Law. Il governo della legge ieri ed oggi*, 2011, pp. XII-172.
107. F. ZINI, *Il dono nella prospettiva della filosofia del diritto*, 2011, pp. XIV-190.
108. G. SADUN BORDONI, *Diritto e politica. Studi sull'epoca post-globale*, 2011, pp. X-266.
109. L. PALAZZANI, *Sex/gender: gli equivoci dell'uguaglianza*, 2011, pp. X-214.
110. F. D'AGOSTINO, *Corso breve di filosofia del diritto*, 2011, pp. 168.
111. S. AMATO, *Eutanasie. Il diritto di fronte alla fine della vita*, edizione riveduta e ampliata, 2015, pp. XIV-234.
112. F. D'AGOSTINO, *Jus quia justum. Lezioni di filosofia del diritto e della religione*, 2012, pp. XVI-168.
113. F. BIONDO, *Disobbedienza civile e teoria del diritto. I conflitti presi sul serio*, 2012, pp. XXII-250.
114. M. MANGINI, *Il ragionamento giuridico tra formalismo e retorica*, 2012, pp. XII-212.
115. C. SARTEA, *Biodiritto. Fragilità e giustizia*, 2012, pp. X-174.
116. G. SOLARI, *Il problema della giustizia e dello Stato nell'antichità classica*, a cura di A. Votrico, 2013, pp. XII-200.
117. G. TUZET, *Filosofia della prova giuridica*, 2013, pp. XIV-322.
118. F. MACIOCE, *Il nuovo noi. La migrazione e l'integrazione come problemi di giustizia*, 2014, pp. X-222.
119. S. BAUZON, *Il divenire umano. Riflessioni etiche sui fini della natura*, 2014, pp. XII-124.
120. V. SALA, *Italo Mancini. Filosofo del diritto*, 2014, pp. VIII-128.

121. F. D'AGOSTINO, *Sessualità. Premesse teoriche di una riflessione giuridica*, 2014, pp. XX-160.

122. L. PALAZZANI, *Il potenziamento umano. Tecnoscienza, etica e diritto*, 2015, pp. XII-172.

123. E. ANCONA, G. DE ANNA (a cura di), *Il tomismo giuridico del XX secolo. Antologia di autori e testi*, 2015, pp. XXIV-344.

124. M.G. BERNARDINI, *Disabilità, giustizia, diritto. Itinerari tra filosofia del diritto e Disability Studies*, 2016, pp. XXXIV-286.

125. L. PALAZZANI, *La filosofia* per *il diritto. Teorie, concetti, applicazioni*, 2016, pp. X-254.

126. L. CORSO, *I due volti del diritto. Élite e uomo comune nel costituzionalismo americano*, 2016, pp. XVI-272.

127. L. DI CARLO, *Teoria istituzionale e ragionamento giuridico*, 2017, pp. XII-364.

128. L. NEPI, *Violenza sessuale e soggettività sessuata*, 2017, pp. XII-140.

129. L. PALAZZANI, *Dalla bio-etica alla tecno-etica: nuove sfide al diritto*, 2017, pp. XII-404.

130. C. SARTEA, *Diritti umani. Un'introduzione critica*, 2018, pp. X-158.

Settima serie:

131. M. POMPEI, *Abuso del diritto. Un approccio tra filosofia e teoria*. Prefazione di F. D'Agostino, 2019, pp. XVI-248.

132. C. SARTEA, *Bioetica e biogiuridica. Itinerari, incontri e scontri*. Premessa di F. D'Agostino, 2019, pp. XVI-200.

133. M. KRIENKE, *Ripensare il diritto naturale e la dignità umana. Tradizione e attualità di due* topoi *etico-giuridici*, 2020, pp. X-358.

134. A.C. AMATO MANGIAMELI, M.N. CAMPAGNOLI, *Strategie digitali. #diritto_educazione_tecnologie*, 2020, pp. XIV-394.