Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche.

Identità, anonimato e condotte antisociali in Rete: riflessioni informatico giuridiche[1]

Raffaella Brighi, Francesco Di Tano

Abstract: Nel contesto online, dove appare molto agevole la sostituzione di persona o la creazione di false identità, si sono diffusi comportamenti antisociali e antigiuridici che si concretizzano in manifestazioni di odio, molestia e violenza interpersonali, che rendono sempre più vulnerabile l'identità digitale (e, al tempo stesso, reale) delle persone. La protezione della sfera privata dell'individuo si traduce nell'esigenza di controllare e proteggere le informazioni conservate nei dispositivi e immesse nella Rete. I metodi e gli strumenti che Internet offre per proteggere l'identità degli utenti sono innumerevoli; d'altra parte le tecnologie per la segretezza e per l'anonimato ampliano i margini di manovra di chi sfrutta la tecnologia per fini criminali e compromettono la capacità di prevenzione di condotte illecite. Il contributo riflette sul rapporto tra identità e anonimato in Rete in situazioni di conflitto tra tutela delle libertà personali, sicurezza informatica e un'effettiva azione di prevenzione del crimine.
Keywords:

1. Il contesto *online*

La rete Internet, costituita da un insieme di infrastrutture fisiche, di protocolli e di servizi informatici, crea una più complessa dimensione sociale per le attività umane a cui comunemente ci si riferisce con il termine *ciberspazio*. Benché alcuni abbiano dipinto il ciberspazio come un fenomeno meramente virtuale, non soggetto alle leggi della fisica e composto, più che da oggetti fisicamente individuabili, da semplici dati e pure informazioni[2], esso è una realtà articolata, sempre più interconnessa al mondo reale. I dati digitali comunicati nelle reti sono parte costitutiva dell'informazione e del significato che veicolano (non semplici informazioni, dunque). Gli artefatti informatici – le strutture dati, le classi, le istanze, gli algoritmi –, nel ridurre la distinzione tra ciò che è reale e la sua riproduzione digitale, non soltanto stanno ricostruendo il nostro mondo ma lo stanno «riontologizzando»[3], trasformandone la natura intrinseca. L'insieme dei significati, scambiati, integrati e aggregati da processi computazionali, costituisce la persona e tramite essa la cultura umana. Ciò conferisce ai dati digitali, alle informazioni e ai loro significati una dimensione di quasi-materialità, che va ben oltre il contesto *online,* ma controlla e dirige le azioni umane.

La ricerca giuridica ha dovuto affrontare numerose difficoltà nel qualificare queste nuove modalità del mondo reale. Internet esiste nel mondo empirico ed è percepibile dai sensi umani: i *router*, i *server*, i cavi, gli stessi computer possono essere concretamente toccati, così come i dati e le immagini visti sugli schermi e i suoni uditi. Si tratta di un mezzo interattivo che comprende tutti gli elementi basilari della comunicazione (mittente, destinatario, messaggio e canale comunicativo) e che si basa sulla commutazione di pacchetto per la condivisione delle risorse. Ai fini della sua trasmissione, ogni messaggio viene suddiviso in singoli pacchetti, ciascuno contenente una porzione del messaggio, gli indirizzi di origine e di destinazione, infor-

[1] Il saggio è frutto di un lavoro di ricerca congiunto che impegna entrambi gli autori nell'ambito del progetto PRIN 2015 "Soggetto di diritto e vulnerabilità: modelli istituzionali e concetti in trasformazione". Ai fini di questo studio, R. Brighi si è occupata dei §§. 1, 2, 3; F. Di Tano è autore dei §§ 4, 5, 6.

[2] Per un'introduzione, si vedano Wertheim 1999; Uncapher 1991; Burnstein 1996.

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

mazioni di controllo e una determinata quantità di dati con un indirizzo numerico di identificazione (Sartor 2016, 209-210). Tutto ciò che può essere digitalizzato può essere inviato come un pacchetto.

La rappresentazione in digitale e la sua comunicazione tramite Internet inducono un cambiamento nella percezione della materialità e dello spazio, con conseguente diretta o indiretta influenza sul modo di comprensione della realtà circostante e, al contempo, sui comportamenti umani. Nonostante la virtualità sia un'esperienza spazialmente ambigua, ciò che avviene *online* può essere mappato all'interno di uno spazio telematico, distribuito attraverso connessioni sempre più complesse e fluide tra i singoli nodi della Rete, sparsi nel globo.

Le qualità dello spazio *online* sono molto variabili e contraddittorie: da una parte, emergono la sua complessità, le sue apparentemente inesauribili ampiezza e velocità di movimento; dall'altra parte, le rappresentazioni attraverso le quali il ciberspazio è costruito e sperimentato sono piuttosto semplici e si avvicinano alla vita di tutti i giorni. Lontano dalle rappresentazioni astratte che abitano la visione originaria di Gibson del ciberspazio (Gibson 1984, 54), la realtà virtuale si distingue in termini di stanze, luoghi, siti, e vi si accede attraverso portali tendenti a rendere lo spazio affine agli interessi degli individui.

I nuovi media, basandosi su una comunicazione diretta punto a punto anziché su un modello *broadcasting* a grande diffusione, implicano di per sé un nuovo tipo di spazialità che si separa dall'organizzazione sociale della realtà *offline* e tende ad eluderne le relative gerarchie. La caratteristica più evidente, però, è molto probabilmente la possibilità di comunicare abbattendo le distanze spaziali e temporali, in nome di una concreta irrilevanza del momento e del luogo ai fini della comunicazione. A tutto ciò, Internet ha aggiunto l'interattività delle relazioni sociali *online*[4], con l'induzione di un particolare senso di compresenza negli utenti, in maniera similare – ma non identica, mancando il rapporto fisico – alla realtà *offline*.

Questi ambienti offerti dalla Rete possono suscitare reazioni e atteggiamenti contrastanti: da una parte, attrazione verso nuovi spazi, identità, relazioni, e dunque nuovi mondi, aperti e disponibili, fatti su misura per le proprie predilezioni individuali; dall'altra parte, diffidenza e timore per una trasformazione delle relazioni sociali e per lo smarrimento del contatto fisico, sempre più soppiantato dal *medium* elettronico.

Difatti, il volume, la portata e la varietà di dati che gli individui sono in grado di trasmettere su Internet sono enormi. Al contrario della rappresentazione analogica, quella digitale offre il vantaggio di essere direttamente elaborabile dal calcolatore e, soprattutto, di essere riproducibile infinite volte con assoluta precisione, senza detrimento della qualità o della fedeltà rispetto al dato originale. Questa facilità di riproduzione permette, al tempo stesso, una altrettanto facile distribuzione delle informazioni agli utenti localizzati in qualunque angolo del globo. La connessione a Internet è un pre-requisito fondamentale, ma l'attuale portabilità della Rete ha permesso la sua adozione anche nelle regioni più arretrate, dove le persone riescono a connettersi attraverso *smartphone* piuttosto che computer.

Internet e i suoi servizi generano una pluralità di ambienti connotati da sistemi e applicazioni anche sovrapposti, ma distinti da peculiari caratteristiche fondamentali che sembrano influenzare il comportamento degli utenti.

Il primo ambiente è senz'altro il World Wide Web, in tutte le sue evoluzioni: a partire dalla prima realizzazione di Tim Berners Lee in cui l'utente poteva navigare e usufruire, in modalità statica di una vastissima quantità di informazioni, collegate tra loro attraverso *link*, passando per il "Web partecipativo" o "Web scrivibile", in cui diventano centrali, invece, la collaborazione, la condivisione, l'interazione tra utente e sito web (il c.d. Web 2.0) per arrivare alle implementazioni più recenti focalizzate sulla formalizzazione della conoscenza (il c.d. Web Semantico) e sulla connessione intelligente tra persone e macchine.

[4] Sul punto, si veda, ad esempio Kitchin 1998.

Gli altri ambienti riguardano i servizi di comunicazione: dalla posta elettronica, oramai utilizzata in tutti i livelli, compreso quello istituzionale, ai sistemi di discussione asincrona (*forum*, *mailing list*, *newsgroup*, o la pionieristica *bullettin board*) e sincrona (essenzialmente, le *chat*), utilizzati per qualsivoglia finalità e tematica. Non si devono dimenticare, inoltre, i cosiddetti metamondi, discendenti multimediali dei primi MUD (*Multi User Dungeon*)[5], che ricreano, nella Rete, mondi virtuali attraverso immagini, video e suoni, in grado di ingenerare un notevole impatto psicologico nell'utente. Sono solitamente gli ambienti virtuali riprodotti dai videogiochi che raggiungono, da un punto di vista squisitamente grafico, livelli di aderenza alla realtà sempre più elevati. L'ultimo ambiente offerto da Internet è quello dei servizi interattivi di comunicazione audio-video in tempo reale, che hanno oramai soppiantato, per ovvi motivi, la tradizionale comunicazione telefonica.

In questo contesto, in cui le persone condividono interessi, pensieri, informazioni, collaborano, giocano ed eventualmente si aiutano vicendevolmente, la provenienza geografica perde la propria rilevanza, mentre lo scopo per il quale gli utenti si riuniscono in comunità acquisisce un ruolo preponderante nell'influenza dei comportamenti: un individuo appartenente a più gruppi, difatti, può cambiare il proprio atteggiamento da un contesto all'altro, allo stesso modo di come avviene nella realtà quotidiana.

2. Vulnerabilità dell'identità digitale

La Rete si presenta, dunque, come un complesso ecosistema governato da dinamiche proprie, emancipatesi dalla realtà *offline*, ma in fondo mai del tutto. E così anche per gli individui.

L'identità umana si forgia, *offline*, secondo meccanismi consolidati, ai quali si sono aggiunti, negli ultimi venti anni in particolare, i fattori dirompenti di Internet e delle nuove tecnologie. Il nuovo Web apre infinite possibilità di costruzione della identità personale[6], che diventa anche comunicazione e rete di collegamenti: le informazioni sono raccolte in profili diversi, ciascuno dei quali riporta un frammento di identità[7]. *Online*, l'identità può seguire direttrici differenti. Può approfondire, migliorare e completare l'individuo capace di non scindere il proprio *io* tra realtà concreta e realtà virtuale, oppure svilupparsi in maniera estrema, conducendo l'identità reale ai suoi più inesplorati confini.

Tuttavia, l'immagine di Internet come il regno dell'anonimato, dello pseudonimo e delle identità liberamente create, corrisponde poco alla realtà dei fatti (Pelliccioli 2016,11).

Sotto il profilo tecnologico, il concetto di *identità digitale* è utilizzato secondo una doppia accezione. La prima riguarda l'identità personale in Rete, intesa come definizione del proprio modo di esistere nel cibermondo (Frosini, 1981). I dati personali immessi nella Rete e liberamente (o non liberamente) accessibili, raccolti e profilati da terzi, offrono una rappresentazione delle persone che contribuisce a creare una loro identità "esterna" [8]. E sempre più questa costruzione è affidata a programmi informatici. La seconda accezione è più ristretta e riguarda le

---

[5] Per *Multi User Dungeon* si può intendere una categoria di videogiochi di ruolo, di tipo testuale, eseguiti su Internet attraverso il computer da più utenti, i quali interagiscono in tale ambiente attraverso comandi impartiti dalla tastiera.

[6] L'identità personale che sempre più pare non essere una sola, fissa e ben definita, ma esito di un processo di costruzione in continua evoluzione, diacronica e sincronica, si dilata fino a ricomprendere anche la c.d. identità digitale. In argomento, Pino (2003 e 2010); Rodotà 2012; Resta 2007; Finocchiaro 2010. Si veda anche Pozzolo e Verza 2015; Martoni, e Palmirani 2015.

[7] Rodotà la definisce "identità inconoscibile", "identità dispersa" (Rodotà 2012, 318).

[8] Fu il giusfilosofo Vittorio Frosini, come emerge dalla ricostruzione di F. Romeo in (Romeo 2106), ad introdurre per primo il concetto di "identità informatica", intesa come «l'insieme dei dati, che consentono di ricomporre l'immagine morale della sua personalità (della quale possono entrare a far parte anche elementi d'ordine biologico, come predisposizioni per malattie ereditarie, malformazioni fisiche, tare psichiche e turbe sessuali); i quali dati,

tecniche di identificazione del soggetto a mezzo di strumenti informatici, cioè la «rappresentazione informatica della corrispondenza biunivoca tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale»[9]. In questo senso l'identità può essere ad esempio un account e-mail, un profilo su un social network, un numero di carta di credito. Numerosi interventi normativi, e tra tutti il Regolamento eIDAS[10], testimoniano come il diritto abbia recepito le istanze di un maggior grado certezza nei rapporti e muova verso la definizione di nuovi strumenti tesi a creare *fiducia* nel mondo digitale. In particolare, dalle iniziative nell'ambito della strategia europea per il Digital Single Market si evince che la sicurezza informatica è sempre più concepita a protezione delle attività pubbliche e private dipendenti dall'ambiente digitale con lo scopo di incrementare il mercato del lavoro e stimolare l'innovazione[11]. L'odierna tendenza sembra dunque rifiutare il vecchio modello d'identità digitale, mascherata da pseudonimi, a favore di una maggior esposizione con la propria identità reale.

L'identità di un soggetto *rispetto* a un sistema informatico viene definita in tre passaggi: (i) l'identificazione che è il procedimento in cui si accerta l'identità di un soggetto, (ii) l'autorizzazione che è il procedimento in cui si accerta il diritto di un soggetto identificato di accedere a certe risorse o servizi informatici (e con quali limiti); e (iii) l'autenticazione, ovvero il procedimento attraverso il quale il sistema informatico *riconosce* un utente.

Quale rapporto c'è tra l'identità reale e l'identità che il soggetto assume per il sistema informatico? Alla base vi è un problema tecnico e organizzativo, specialmente nei contesti di rete: come accertare che un soggetto sia realmente chi dice di essere.

Inoltre, l'identità digitale non è in grado di tenere separata quella che è l'identità di un soggetto dalle sue caratteristiche rispetto al servizio. In informatica sono gli attributi, le proprietà, che definiscono l'identità. Nella vita reale a fronte di una sola identità personale esercitiamo una grande varietà di ruoli: lavoratore, genitore, paziente, ecc. In Rete, invece, a ciascun ruolo (consumatore, professionista, ecc.), e in relazione a ciascun servizio, corrisponde un'identità digitale.

L'identità digitale è per sua natura *vulnerabile*.

I più recenti rapporti sulla sicurezza informatica documentano l'aumento degli attacchi informatici che puntano alla violazione dei dati (*data breach*) con le finalità più varie[12]. Tra tutti, i dati più a rischio di essere esposti in caso di *data breach* sono le identità digitali che potranno servire agli attaccanti per compiere ulteriori operazioni (furto di identità). Gli attaccanti sfruttano le vulnerabilità dei sistemi (hardware e software) e le cattive configurazione dei dispositivi ma anche le vulnerabilità dei soggetti che operano in Rete con tecniche di *intelligence* su fonti di dati aperte (OSINT), ovvero raccolgono le informazioni disseminate in Rete e le sfruttano per impersonare una conoscenza reale del bersaglio e convincerlo a compiere altre operazioni a proprio vantaggio (seguire link, scaricare allegati, ecc.) con la finalità di carpirne i codici identificativi.

---

raccolti, memorizzati ed elaborati in un calcolatore elettronico, diventano – a differenza di quelli riportati su una comune scheda segnaletica – immediatamente accessibili e diffusibili». Cfr. Frosini 1981.

[9] Art. 1 lett. o) del Dpcm 24 ottobre 2014 in tema di Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

[10] Il Regolamento (UE) n.910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che fornisce una base normativa comune per le interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni.

[11] «Le reti e i sistemi informativi e i relativi servizi giocano un ruolo fondamentale nella società. La loro affidabilità e sicurezza sono essenziali per le attività economiche e sociali, e in particolare per il funzionamento del mercato interno». Considerando (1) della Direttiva UE 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Network Information Society).

[12] Per approfondimenti su statistiche, metodi e vittime si vedano ad esempio il *Data Breach Investigations Report* di Verizon (2018) e il Rapporto Clusit 2018 sulla sicurezza ICT in Italia.

Vi è la tendenza a far circolare le proprie informazioni personali in ambienti erroneamente percepiti come privati ("la mia bacheca, il mio profilo, la chat, ecc."), abbassando il livello di confidenza (Ziccardi 2015, 206) e, di contro, si rileva un indebolimento progressivo dell'adozione delle misure di sicurezza necessarie a difendere la propria identità digitale di fronte all'aumento considerevole degli attacchi informatici e alla sensazione sempre più comune che non solo i dispositivi ma anche i servizi che conservano i nostri dati personali (aziende, provider, ecc.) siano estremamente vulnerabili. I rischi potenzialmente connessi a un *data breach* di dati personali trovano una risposta giuridica nella disciplina introdotta dall'art. 33 del Regolamento generale sulla protezione dei dati (Reg. UE n. 679/2016) che impone ad ogni titolare del trattamento l'obbligo di notificare all'autorità di controllo qualsiasi violazione di sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata, entro 72 ore[13].

Il *furto di identità*, cui non corrisponde una specifica fattispecie di reato, ma è spesso il frutto di una combinazione di più norme incriminatrici[14], è uno dei comportamenti malevoli più diffusi negli ultimi anni.

Oltre a essere veicolo di truffe economiche, il furto di identità può essere adoperato per commettere reati di diffamazione e per diffondere contenuti riservati a scopo di vendetta (*revenge porn*) o di estorsione e ricatto (*sexstortion*) e atti persecutori verso individui vulnerabili (*hatespeech*, *cyberbullismo*, *cyberstalking*); condotte, queste, che hanno un forte potenziale lesivo della reputazione in virtù della persistenza delle informazioni e della loro potenziale diffusione *virale*.

In un mondo virtuale apparentemente sregolato, tanto da norme giuridiche quanto da norme sociali, gli utenti si sentono per l'appunto liberi di esplorare e di lasciar emergere angoli remoti del proprio *io*. Tra questi, molto spesso, gli istinti, l'aggressività, la violenza, l'irrazionalità. Anche quando l'aggressore non cerca la protezione dell'anonimato o di profili *fake* ma piuttosto il consenso attraverso la visibilità, aiutata da *like* e condivisioni, il mezzo informatico avvantaggia il criminale in termini di maggiore capacità offensiva (Ziccardi 2016).

A fronte della vulnerabilità dell'identità digitale che si riflette su molteplici profili - dalla determinazione dell'identità personale *on line* alla *web reputation*, dalla profilazione a forme di controllo e sorveglianza, fino ad arrivare alle condotte criminose - la protezione della sfera privata dell'individuo si traduce nell'esigenza di controllare e proteggere i dati informatici conservati nei dispositivi e immessi nella Rete, ovvero in un uso "protetto" della tecnologia, che riporti il governo dei dati in capo all'interessato.

La complessità dei nuovi paradigmi (*Cloud Computing*, *mobile* e *Internet of Things* sono gli esempi più rilevanti), l'asimmetria informativa tra chi utilizza le tecnologie e chi le governa, la mancata trasparenza delle modalità di conservazione dei dati (dove, per quanto tempo, da chi sono accessibili, ecc.) rende tuttavia estremamente complicato, oggi, raggiungere la protezione totale del dato informatico, se non attraverso strumenti progettati *ad hoc* per la sicurezza informatica e, soprattutto con l'adozione di comportamenti adeguati ai rischi correlati.

3. Anonimato apparente, anonimato assoluto e protezione dell'identità

[13] Nel caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà fondamentali delle persone fisiche, il Regolamento obbliga il titolare del trattamento a comunicare tale violazione anche a ciascun interessato, al fine di consentirgli di adottare idonee precauzioni per ridurre al minimo il potenziale danno da essa derivante.

[14] Nell'ordinamento italiano, difatti, il furto di identità commesso *online* non sempre corrisponde unicamente al reato di sostituzione di persona (art. 494 c.p.), concorrendo spesso quest'ultima figura con i reati di trattamento illecito di dati personali (art. 167 Codice Privacy), accesso abusivo a sistema informatico (art. 615-*ter* c.p.), truffa (art. 640 c.p.), frode informatica (art. 640-*ter* c.p.).

Generalmente l'anonimato in Rete è solo *apparente*. Le azioni degli utenti possono essere ricondotte ai soggetti a cui si riferiscono attraverso molteplici *tracce digitali:* l'indirizzo IP del dispositivo, i collegamenti a reti wi-fi, le autenticazioni a servizi telematici, i log dei server, ecc. Internet è un ambiente in cui tutto è tracciato, o comunque tracciabile, spazialmente e temporalmente. Una mail, ad esempio, contiene nell'*header*[15] informazioni che descrivono l'intero percorso del messaggio a partire dal computer del mittente, contrassegnato da un indirizzo IP univoco. Dall'indirizzo IP poi, in modo più o meno facile, è possibile risalire al mittente.

Il dato informatico non è in assoluto anonimo ma può essere reso anonimo in determinati contesti e per alcuni scopi. Il grado di anonimato è legato ai costi in termini di tempo, di risorse economiche e di innovazione tecnologica necessari per ricondurre le informazioni al soggetto a cui si riferiscono.

I metodi e gli strumenti che Internet offre per proteggere l'identità dei suoi utenti sono innumerevoli. Ogni livello di servizio (profilo, utente, applicativo, servizi, rete, fisico) presenta le proprie soluzioni e le proprie vulnerabilità. L'aspetto più critico riguarda tuttavia le interazioni tra i diversi livelli della catena: perché l'anonimato non crolli è necessario adottare comportamenti corretti fin dal primo passaggio, l'accesso fisico alla rete.

In tale perimetro si possono categorizzare tre forme di anonimato (Horsman 2016, 56-153). La prima è la già discussa dimensione dell'anonimato apparente, in cui l'identità si nasconde dietro a profili *fake*, false registrazioni e furti di identità. La seconda, definita "*approved anonimity*" (anonimato approvato), riguarda quei servizi di protezione dell'identità che, pur mantenendo l'anonimato degli utenti, memorizzano, in modo sicuro, i loro dati identificativi per un determinato periodo. Tali informazioni sono conservate, in special modo, nel caso in cui l'utente violi le condizioni di utilizzo o per indagini penali da parte delle autorità[16]. La terza e ultima categoria, "*full anonimity*" (anonimato completo o assoluto), concerne l'effettivo e totale anonimato fornito attraverso servizi specifici, più o meno sicuri.

La base di ogni sistema di anonimizzazione è la crittografia, una tecnica in grado di garantire anche a soggetti non esperti, se applicata correttamente, un buon livello di protezione da forme di controllo indiscriminato. La crittografia limita la conoscibilità delle informazioni a chi ne entri illegittimamente in possesso attraverso algoritmi che trasformano il testo e lo rendono incomprensibile a chi non possiede la chiave di decifratura. La sicurezza di un sistema di crittografia dipende da molti fattori tra cui i più comuni sono la debolezza della password che permette di decifrare i dati e la presenza di repliche in chiaro degli stessi dati in altri sistemi o ambienti (il backup, ad esempio).

Una nota misura di contrasto alla crittografia forte è l'imposizione di sistemi di *bypass*, ovvero *backdoor* (porte sul retro) nascoste nei codici sorgenti dei programmi che permettano a terze parti – alle forze dell'ordine, ad esempio – di aggirare i sistemi di cifratura[17]; ciò comporta tuttavia una grave compromissione della sicurezza dei sistemi stessi e una generale perdita di fiducia da parte degli utenti.

---

[15] Parte del messaggio che contiene informazioni (metadati) scritte automaticamente dal programma di posta del mittente e da ogni server nel quale transita il messaggio.

[16] Si tratta di una forma di anonimato "protetto" o "sostenibile", in cui l'esercizio della protezione dei dati personali e della riservatezza è destinato a un continuo bilanciamento con altri diritti fondamentali (Finocchiaro, e Delfini 2014, 195).

[17] Ciò avviene sostanzialmente in due modi: con la consegna al soggetto terzo di una seconda chiave crittografica (*master key*) perché possa decifrare i dati secondo necessità e con l'inserimento di difetti occulti nel codice informatico del sistema stesso per favorire intrusioni dall'esterno. In occasione della RSA Conference del 2016 alcuni tra i più grandi teorici del settore, tra cui Rivest, Shamir, Diffie, Hellman e Marlinspike, hanno unanimemente condannato l'utilizzo di simili tecnologie ritenendo l'introduzione di *master keys* nei sistemi di cifrazione un grave pregiudizio alla sicurezza degli stessi.

Per aggirare filtri e controlli della Rete e agire protetti dall'anonimato non è sufficiente mantenere segreto il contenuto della comunicazione ma occorre mascherare anche l'identità di mittente e destinatario nel caso la connessione venisse monitorata. Una delle fasi più delicate nel processo per raggiungere l'anonimato è appunto la fase di connessione. Vi sono molteplici soluzioni: sistemi (detti *proxy*) che aderendo alla logica di comunicazione client-server svolgono un ruolo di intermediario tra richieste e risposte mantenendo segreto l'indirizzo IP del client che ha effettuato la richiesta; strumenti che esibiscono sulla rete identificativi *fake*; tecnologie che creano canali di comunicazione privati per connettere, con alti standard di sicurezza, dispositivi esterni ad una infrastruttura anche attraverso ambienti non sicuri (*Virtual Private Network*, VPN) o, ancora, strumenti che consentono di amministrare e controllare da remoto *host* nascosti nella rete, agendo direttamente da questi ultimi.

La sicurezza di questi sistemi è collegata alla vulnerabilità del soggetto che sviluppa e gestisce gli strumenti a cui è affidato il processo di anonimato. Se l'anonimato è garantito da un unico soggetto, ben individuabile, questo potrà subire pressioni o attacchi mirati per invalidare l'anonimato, svelare le identità degli utenti e i contenuti delle comunicazioni[18]. È questo un limite generale dei sistemi a "codice chiuso" non direttamente verificabile e quindi di facile manomissione.

Un metodo ritenuto sicuro per creare una connessione anonima è avvalersi di *intermediari* che partecipano alla rete volontariamente mettendo a disposizione la loro connessione per trasferire il dato cifrato dal mittente al destinatario e fanno rimbalzare la comunicazione attraverso più nodi fino a arrivare a destinazione, invece di prendere una strada diretta[19]. Il circuito viene esteso un salto alla volta e il sistema negozia un nuovo insieme di chiavi crittografiche per ogni salto, così da assicurarsi che ciascun nodo non possa tracciare le connessioni durante il passaggio: l'intercettazione di un intermediario o la sua compromissione non consente dunque di collegare mittente e destinatario.

È questo il principio di funzionamento del noto sistema Tor, il software più diffuso su larga scala negli ultimi anni, utilizzato sia per navigare in maniera anonima dai propri dispositivi sia per creare servizi nascosti e momentanei (*webserver*, *chatserver*, ecc.). Funzionano in modo analogo le reti Freenet e I2P, con la differenza che esse realizzano, all'interno di Internet, reti anonime autonome e chiuse (*darknet*) da cui non è possibile accedere a siti del web pubblico, ma solo a dati e servizi specifici. Le reti chiuse possono anche essere composte unicamente da soggetti che si conoscono e di cui ci si fida.

Tor e gli altri servizi di anonimato sono strumenti capaci di fronteggiare attività investigative anche incisive. Le tecnologie per la segretezza e per l'anonimato ampliano senza dubbio i margini di manovra di chi sfrutta la tecnologia per fini criminali e compromettono la capacità di prevenzione di condotte criminose. Tuttavia, è comunque spesso possibile ricondurre l'azione criminosa al soggetto responsabile con altre strategie investigative perché il procedimento per raggiungere l'anonimato è abbastanza complesso e, piuttosto frequentemente, cade a causa di errori nell'accesso alla rete. Comportamenti che sembrano poter garantire l'anonimato, sono in realtà compromessi dall'ingresso in sistemi che identificano l'utente tramite l'indirizzo IP, tramite informazioni provenienti dalle celle telefoniche e dai satelliti o attraverso altre tracce lasciate nella rete. Spesso è l'analisi della rete sociale dei contatti a rivelare l'identità di un soggetto[20]. Anche dati rilevanti, che paiono inaccessibili perché memorizzati in dispositivi cifrati

[18] Si veda, sul punto, la ricostruzione storica di Claudio Agosti (*Vecna*), hacker e ricercatore indipendente, nell'intervista riportata in Ziccardi (2011, 236 e ss.), che rivela l'insicurezza intrinseca di certe tecnologie di anonimato.
[19] È lo stesso principio di funzionamento del *proxy*, ma si basa su una rete di volontari e unisce la crittografia forte.
[20] Narayanan e Shmatikov (2009) dimostrano che è possibile estrapolare informazioni sensibili su persone specifiche dai grafici di social-network malgrado le tecniche di "pseudonimizzazione" applicate a tali dati: i rapporti tra le diverse persone sono unici e possono essere utilizzati come identificatori.

ad esempio, possono essere ritrovati replicati altrove, in *back up*, spazi *cloud* o sincronizzati su altri dispositivi.

4. Anonimato e libertà nel mondo digitale

Benché molti servizi *online* non garantiscano l'effettivo anonimato, l'incapacità di comprendere la tecnologia sottostante spesso induce l'utente medio a credere di agire senza essere tracciato, libero di gestire la propria identità *online* e adattarla al contesto desiderato. Tale status di anonimato *percepito* permette alle persone di esprimersi in maniera più onesta, amplificandone vizi e virtù (Citron 2014), con possibili risvolti negativi e positivi.

Sotto il primo aspetto, il rischio maggiore derivante dall'anonimato è il sentimento di libertà nello sfidare le norme sociali, nel disinteressarsi da esse, in special modo quando si crede, a torto o a ragione, che le condotte non possano essere attribuite al relativo autore. Le persone tendono a ignorare le norme sociali quando si nascondono all'interno di un gruppo o dietro una maschera, secondo un processo sociale che porta all'abbassamento della soglia del normale controllo comportamentale, conosciuto in psicologia come *deindividuazione*[21].

Prima di abbandonarsi a una condotta impulsiva e aggressiva, difatti, l'individuo necessita di liberarsi del proprio modello abituale di persona responsabile con un'immagine di sé e del proprio ruolo costante nel tempo. Divenendo anonimo all'interno di un vasto gruppo o di una massa indistinta di persone, si sente scrollare di dosso le proprie responsabilità di individuo ben identificato nella società, protetto da fattori esterni che incidono sulle sue capacità di autovalutazione, di autolimitazione e di osservazione della realtà circostante, come la vergogna, il senso di colpa e il rispetto di norme comportamentali.

Sul *web* non si agisce, intenzionalmente o meno, solo in forma anonima. Nell'epoca del *web 2.0*, i contenuti sono creati direttamente dagli utenti tramite *blog*, piattaforme di *video hosting* e *social networks*, all'interno dei quali sono spesso iscritti con i propri nomi e cognomi. Nonostante la possibilità di identificazione, però, l'utente medio continua a percepirsi anonimo, come se le sue condotte *online* non siano a lui riferibili, mimetizzate e disperse tra le migliaia di altre azioni compiute *online* (Joinson 2003). L'accesso ai contenuti *online*, al contrario del reperimento materiale di una risorsa, può influenzare la percezione dell'anonimato e indurre l'utente a convincersi che delle sue azioni si siano perse le tracce (Hite et al. 2014).

A tal proposito, l'attivista John Perry Barlow, già autore della Dichiarazione d'indipendenza del Ciberspazio[22], ha osservato che il ciberspazio ha il potenziale di far sentire le persone come degli artefatti dell'informazione: se si tagliano i dati, non sanguinano, di conseguenza ognuno si sente libero di fare ciò che vuole a persone che non sono tali, ma semplicemente loro rappresentazioni.

L'anonimato e la separazione fisica tra gli utenti possono dunque rinvigorire la tendenza ad agire secondo impulsi distruttivi e a commettere in Rete atti criminali (Bartlett et al. 2016; Balfe et al. 2014; Eastwick e Gardner, 2009; Christopherson, 2007; Hayne e Rice, 1997). Quando non ricevono dai propri consociati segnali di rimprovero che rendano evidenti le loro condotte antisociali, le persone tendono a diventare più facilmente aggressive (Wallace 1999, 126), riconoscono l'altrui umanità solamente quando interagiscono dal vivo, faccia a faccia; oppure nascondono i loro veri sentimenti, covando odio fin quando non si presentino le giuste opportunità per manifestarlo (Weisband, e Atwater, 1999).

---

[21] Per deindividuazione si intende il fenomeno della perdita di autocoscienza e di apprendimento valutativo, che si verifica in situazioni di gruppo che, incoraggiando l'anonimato e allontanando l'attenzione dall'individuo, favoriscono l'adeguamento alle norme del gruppo, buone o cattive che siano. Cfr. Myers 2010; Zimbardo 1969.

[22] La Dichiarazione è consultabile all'url http://projects.eff.org/~barlow/Declaration-Final.html.

Nonostante questa preoccupante evoluzione, non si deve identificare l'anonimato come la fonte di tutti i mali. Al contrario, esso può essere essenziale, in determinati contesti, per esprimere il proprio pensiero in maniera più libera e onesta, proprio per la maggiore sicurezza – quantomeno percepita – di non essere identificati.

Abbondano esempi sull'importanza dell'anonimato per manifestare opinioni su politica, cultura e questioni sociali: dissidenti politici documentano gli abusi governativi su blog, per nascondere i loro veri nomi; adolescenti condividono su comunità online LGBT le proprie preoccupazioni sul fare *coming out* a parenti e amici; sotto la coperta dell'anonimato, alcune persone sono più disposte a confessare le difficoltà di crescere i figli, senza preoccuparsi di essere etichettate come un cattivi genitori.

Proprio per tali ragioni, Stefano Rodotà ha riconosciuto l'anonimato come una precondizione della libertà di manifestazione del pensiero ed "elemento costitutivo della versione digitale della cittadinanza, con i temperamenti resi necessari quando, ad esempio, si è di fronte alla necessità di tutelare le persone dalla diffamazione in rete" (Rodotà 2012; 2014). Secondo il giurista, solo attraverso l'anonimato "è possibile sottrarsi a interferenze nella propria vita che si traducano in aggressioni particolarmente gravi, in discriminazioni, molestie, limitazioni della libertà di espressione, esclusione da circuiti comunicativi"[23].

Si capovolge, dunque, la concezione dell'anonimato come causa delle espressioni di odio nella Rete: come una faccia della stessa medaglia, può al contrario fungere da ancora di salvezza verso una tale deriva violenta e discriminatoria.

Attraverso l'anonimato si potrebbe salvaguardare lo scambio autonomo e libero di informazioni e opinioni, nonché la costruzione volontaria di rapporti sociali, in conformità con l'intrinseca democraticità della Rete. L'individuo verrebbe protetto dai rischi di intimidazione e stigmatizzazione propri del mondo reale, consentendogli una libera manifestazione del pensiero e della propria personalità.

L'anonimato può consentire di oltrepassare i limiti dell'identità reale e avvicinarsi al (o realizzare il) sogno di creare un'identità digitale fluida, plasmata sui propri desideri e non soggiogata dai vincoli e dalle convenzioni sociali[24]. Anche i gruppi e, in special modo, le minoranze, possono dunque godere di tali benefici, potendo contare su maggiori possibilità (e minori ostacoli) per criticare, rivendicare, pretendere e organizzare mobilitazioni sempre più intense, con positive ricadute sulla partecipazione democratica alla vita politica e, conseguentemente, sulla stessa redistribuzione del potere sociale (Cuniberti 2014).

5. Condotte antisociali e antigiuridiche

Negli anni più recenti, sono proliferati, in Rete, attacchi diretti a individui singolarmente identificati, fondati sui più disparati motivi e non essenzialmente discriminatori[25]. Tali condotte destano una sempre maggiore preoccupazione all'interno degli ordinamenti degli stati democratico-liberali, poiché investono in larga parte minorenni e colpiscono gravemente la vittima nell'intimità, nell'onore e nella reputazione.

Nel panorama giuridico attuale non esiste una definizione universale del fenomeno, che può difatti assumere un'ampia varietà di forme e manifestarsi attraverso molteplici attività (De Fa-

[23] Rodotà 2012.

[24] Sul punto, per una panoramica sul tema, Resta (2014).

[25] Le motivazioni alla base di questi comportamenti possono variare da caso a caso: può trattarsi della conclusione di una relazione, di una disputa tra amici, di sentimenti perseguiti ingenuamente, oppure ancora di omofobia, intolleranza, odio, vendetta, piacere e soddisfazione personale, o anche di divertimento e scherzo. Si veda, in particolare, Hinduja, e Patchin 2015.

zio, e Sgarbi 2016). Si tratta, generalmente, di: insulti, *trolling*, *doxing*, aperte minacce, espressioni sessiste, o denigrazioni pubbliche volte a suscitare imbarazzo o umiliazione, comunicati attraverso l'invio di messaggi via e-mail, MMS, SMS, applicazioni di messaggistica istantanea (WhatsApp e Facebook), sulle *chat*, su siti *web* (tra cui, *in primis*, i *social networks*); può trattarsi, inoltre, di pubblicazione di immagini, video e informazioni false o denigratorie, recupero di informazioni private senza autorizzazione, oppure invio di virus di tipo *backdoor* o *trojan*.

A questo contesto virtuale le tradizionali fattispecie della diffamazione, dell'ingiuria, della calunnia e delle minacce risultano difficilmente applicabili e adattabili. Tali comportamenti di odio, diretti a persone specificamente individuate, sfruttano evidentemente le peculiari caratteristiche tecnologiche di Internet, distinguendosi in tal modo dalle omologhe condotte *offline*.

E così, sono facilitate azioni ossessive e ripetitive, e dunque amplificati i danni in capo alle vittime, potendo essere potenzialmente raggiunta una platea senza precedenti di persone, distanti e anche sconosciute. Sono sempre più numerose le condotte offensive rivolte a individui non conosciuti di persona, i cui dati sono reperiti attraverso la Rete, in particolar modo attraverso i *social media*. Ciò che viene pubblicato e diffuso, d'altronde, è persistente e rimane fruibile anche a distanza di anni, e specialmente le informazioni personali divengono la prima fonte di pericolo, essendo spesso sfruttate per muovere attacchi nei confronti delle vittime designate (Ziccardi 2016).

L'incidenza delle molestie *online* sta oramai superando quella delle fattispecie tradizionali (si pensi a cyberbullismo e *cyberstalking* rispetto a bullismo e *stalking*)[26], non solo da un punto di vista meramente statistico, ma anche sotto l'aspetto delle dimensioni e della gravità degli effetti prodotti alle vittime e, indirettamente, alla società.

Innanzitutto, tali attacchi prevedono solitamente minacce di violenza fisica, di stupro e di morte, che possono anche anticipare azioni di *stalking*, bullismo o reali condotte lesive (Citron 2009). Spesso includono riferimenti a indirizzi di casa e informazioni personali delle vittime, lasciando intendere una particolare familiarità da parte degli offensori e dunque inducendo un forte timore per l'incolumità personale. Come reazione, le vittime tendono a interrompere la loro frequentazione della Rete (che si tratti di *blog* personali, *chat*, *social networks*), a bloccare l'accesso ai propri siti o profili *social* privati, oppure ad adottare pseudonimi per mascherare l'identità (Nakashima 2007).

In secondo luogo, gli assalti invadono la *privacy* delle vittime. La comunicazione di informazioni, dati o materiali riservati comporta rischi immediati, come la minaccia del furto di identità, la discriminazione sul lavoro (e, in generale, in società) e danni a lungo termine, legati a un sentimento costante di perdita della sicurezza personale (Citron 2007).

Ulteriormente, gli attacchi possono essere compiuti attraverso pubbliche dichiarazioni o rivelazioni di portata diffamatoria che danneggiano la reputazione e interferiscono con la vita quotidiana e le opportunità economiche e lavorative della vittima. Si può trattare di informazioni su presunte malattie (Cohen-Almagor 2015), di fotografie ritoccate o intime, di altre informazioni lesive inviate ai datori di lavoro (Solove 2007). A certi livelli, gli aggressori giungono a manipolare i motori di ricerca in modo da far apparire più in vista tali espressioni offensive rispetto agli altri contenuti.

Il contesto cibernetico non è la causa di tali azioni, bensì l'*occasione*, o lo strumento. Ed è in grado di aggravare le conseguenze dannose sulle vittime. Com'è noto, Internet prolunga la vita di tutti i messaggi pubblicati, ivi compresi dunque quelli diffamatori e denigranti. I motori di ricerca li indicizzano con immediatezza e, soprattutto, senza alcuna scadenza, e chiunque può rinvenire informazioni o messaggi pubblicati anche a distanza di anni.

Analogamente a quanto avviene *offline*, questo genere di attacchi interpersonali *online* priva gli individui più vulnerabili del loro diritto di partecipare equamente e senza ostacoli alla vita

[26] Livingstone et al. 2014.

economica, politica e sociale, producendo altresì importanti effetti dannosi a livello psicologico.

La vittimizzazione *online* impedisce il benessere quotidiano, rappresentando un forte fattore di stress sociale (Ybarra 2004), in maniera non troppo differente rispetto a quanto avviene con gli atti subiti di persona. È stata dimostrata la loro correlazione con problemi psicologici di disadattamento sociale, come la rinuncia a frequentare altri individui, l'aumento dello stato di ansia, o una sintomatologia depressiva (Hawker, e Boulton 2000), nonché la produzione di conseguenze emotive come rabbia, tristezza, ansia, imbarazzo, paura, isteria, sensi di colpa, fino a giungere, nei casi più estremi, a tentativi di suicidio (Hinduja, e Patchin 2017). Le reazioni emotive negative diventano più frequenti quando la persecuzione è più intensa e duratura (Ortega-Ruiz et al. 2009), oppure quando si aggiungono problemi ulteriori, come la simultaneità di molestie subite *offline* (Gradinger et al. 2009). Altre ricerche hanno evidenziato come, tra i giovani studenti, siano considerate forme più gravi di aggressione *online* quelle condotte attraverso immagini o video (Slonje, e Smith 2008).-In caso di aggressioni travalicanti i confini virtuali del *web*, questo stress emotivo non può che crescere inesorabilmente e sfociare in danni e reazioni più gravi.

6. Conclusioni

Affrontare il fenomeno dell'odio e delle molestie *online* è un dovere di ciascun ordinamento giuridico costituzionale e democratico, nella consapevolezza che la libertà di espressione, pur essendo un principio sommo, non può che essere subordinata al valore della dignità della persona umana, e comunque soggetta al bilanciamento con altri diritti di pari rango costituzionale. Esprimere il pensiero è, anzi, la derivazione della personalità, costituisce la forma di manifestazione dell'essenza della persona stessa, considerata nella sua totalità (e dunque anche nella sua dignità).

A fronte di un siffatto panorama fenomenico, non si può più prescindere da una compiuta regolamentazione legislativa che disciplini puntualmente – nel rispetto del fondamentale principio di tipicità del diritto penale – ogni singola fattispecie.

Per superare i principali ostacoli critici collegati alla competenza giurisdizionale e alla efficacia ed effettività delle sanzioni, la soluzione ideale sarebbe quella dell'elaborazione e applicazione di una disciplina uniforme a livello internazionale globale, che garantirebbe certezza del diritto e della pena nei confronti dei responsabili, ovunque essi si trovino e pubblichino i contenuti illeciti. La realtà, però, è ben più complessa e articolata: le insormontabili differenze a livello costituzionale, in materia di libertà di espressione, tra ordinamenti europei e (in particolare) gli Stati Uniti[27], inducono a ritenere – quantomeno allo stato attuale – questa prospettiva una mera illusione utopistica.

Il solo precetto normativo, dunque, pur costituendo una necessaria base di indirizzo a livello domestico, non è comunque sufficiente, ed è oltretutto opportuno rendersi conto che il diritto è sempre costretto a rincorrere i fenomeni umani sociali, in particolar modo quelli che si verificano nel contesto cibernetico. Indipendentemente dalle cause di questo ritardo – che potrebbero ricondursi all'estremo dinamismo e velocità delle nuove tecnologie, nonché alla scarsa attitudine e comprensione di esse da parte dei legislatori –, sorge proprio da esso la necessità di individuare soluzioni alternative all'applicazione di norme incriminatrici.

[27] Per una panoramica e un approfondimento delle impostazioni americana ed europea, tra tutti: Post 1991, 2007 e 2009; Tsesis 2001 e 2015; Kahn 2014; Whitman 2003 e 2004.

Allo stato attuale della scienza e della tecnica, non è ancora possibile impedire preventivamente la pubblicazione di espressioni illecite. È altrettanto complesso procedere a un'automatica pronta rimozione delle stesse, in particolar modo per le piattaforme popolate da milioni di utenti, che impiegherebbero un notevole lasso di tempo per scandagliare in tempo reale tutti i contenuti pubblicati. Tale controllo, inoltre, viene compiuto non solamente da *software* sofisticati, ma anche e soprattutto da persone umane, poiché i significati del linguaggio necessitano solitamente di interpretazione e contestualizzazione. Oneri del genere, dunque, graverebbero eccezionalmente su coloro i quali forniscono servizi *online*.

Ad ogni modo, la rimozione di espressioni come i meri insulti gratuiti, eventualmente fondati su motivi razziali, etnici, religiosi, la cui portata lesiva è insindacabile, nessun pregiudizio arrecherebbe al libero scambio di idee e opinioni. Rispetto a tali fattispecie, i maggiori *content provider* si sono già organizzati attraverso complessi sistemi di monitoraggio, filtraggio e gestione delle segnalazioni degli utenti, e hanno condiviso, il 31 maggio 2016, dietro forte spinta della Commissione Europea, un codice di condotta uniforme contenente una serie di oneri e prescrizioni per combattere la diffusione dei discorsi di odio *online* in Europa[28]

Proprio in relazione a questa esigenza, una possibile soluzione a breve o medio termine può essere rappresentata dalla previsione di una forma di responsabilità dei *provider* nei casi di mancato intervento immediato (di rimozione del contenuto, di *ban* dell'utente, ecc.), a fronte di una circostanziata segnalazione, secondo il già rodato (nell'ambito del diritto d'autore) meccanismo del *notice and take down*.

Nell'adottare una tale soluzione, non potrebbe comunque prescindersi, quantomeno nel contesto italiano, da una riforma dell'ormai anacronistica disciplina europea in tema di responsabilità di Internet Service Provider: la normativa italiana che ha recepito la direttiva *e-commerce 2000/31/CE*, di oramai 19 anni fa, continua a richiedere il preliminare intervento dell'autorità competente, senza imporre all'intermediario *online* di intervenire autonomamente a fronte della segnalazione dell'utenza.

È, inoltre, pregiudiziale l'acquisizione di una elevata competenza da parte degli intermediari e, in particolare, di chi concretamente porrà in essere tale attività per conto degli stessi: che si tratti di individui che personalmente valuteranno le espressioni di odio o di programmatori che predisporranno *software* appositamente dedicati.

Non sempre, difatti, le manifestazioni di odio *online* sono facilmente identificabili. In particolar modo, le azioni persecutorie (integranti per lo più le fattispecie di *cyberstalking* e cyberbullismo) possono essere subdole e non particolarmente evidenti, se considerate singolarmente. E può accadere che i *provider*, nell'esercitare autonomamente l'attività di controllo e rimozione dei contenuti, commettano grossolani errori. Previsioni normative opportunamente precise, chiare e dettagliate indirizzerebbero senz'altro gli operatori nella loro attività di gestione delle segnalazioni. Non si deve comunque tralasciare il fatto che, nonostante i possibili interventi censori, i contenuti illeciti potrebbero ricomparire su altri spazi *web* proprio per aggirare *ban* e divieti.

Dunque, nell'affrontare questo problema che si caratterizza come essenzialmente informatico, gli intermediari della Rete hanno bisogno, nel breve e medio periodo, di un supporto altrettanto informatico[29], che vada a elidere il più possibile le lacune dei processi umani di sorveglianza e intervento sui contenuti illeciti. La programmazione di *bot* o *software* che analizzino in tempo reale i contenuti pubblicati su una determinata piattaforma è senz'altro il momento più delicato, poiché le parole assumono un significato differente in base a plurimi fattori

[28] Il documento è consultabile all'url: http://europa.eu/rapid/press-release_IP-16-1937_it.htm.

[29] I sistemi informatici possono in questo contesto restituire operatività al diritto. In completo accordo con la lettura proposta da Romeo (2016), si ritiene che tali soluzioni, assieme ad altre prospettate, vadano nella direzione di realizzare la Giuritecnica di Frosini con l'«uso della stessa tecnica per il controllo giuridico della tecnica» (Romeo 2016, 20).

(tra cui il contesto di espressione). La classificazione semantica dei termini, anche sulla base dei nuovi codici adottati dagli utenti per sfuggire ai controlli, rappresenta un primo fondamentale passo per l'elaborazione di efficaci sistemi automatici di controllo, la cui primaria utilità deve riconoscersi nella pre-identificazione dei contenuti da sottoporre al vaglio degli operatori umani.

Nuove forme di tutela possono, altresì, essere affidate agli strumenti informatici stessi, intervenendo sul loro design e sulle architetture secondo requisiti di trasparenza e neutralità. In questa linea si colloca anche il principio della *data ownership*, che riporta il governo dei dati in capo all'interessato.

Ciò significa favorire il consapevole potenziamento delle capacità e l'*empowerment* dell'utente, attraverso forme di autotutela che educhino, soprattutto le generazioni più giovani, a sviluppare un'etica comportamentale nella vita *online*, e attraverso strumenti informatici con cui definire politiche di accesso flessibili e condivise e verificare in ogni istante il grado di confidenzialità, integrità e disponibilità dei dati.

Attraverso l'educazione – famigliare, scolastica[30], generale – le persone acquisiscono conoscenza, consapevolezza e, potenzialmente, più coraggio e competenza nel reagire attivamente alle condotte di odio *online*. Le voci contrarie alle espressioni di odio potrebbero dunque emergere con maggiore frequenza, fungendo da esempio e stimolando altri utenti, prima timorosi di trovarsi in minoranza, ad esporsi in maniera concreta. Pur non essendo, allo stato, paventabile una definitiva eliminazione del fenomeno dell'*hate speech* e delle molestie *online*, non si deve rimanere inerti e accettare la sua pericolosa crescita. A difesa della dignità di ogni essere umano, la libertà di espressione *online* deve essere oggetto di rimodulazione, accurata gestione e, soprattutto, *educazione*.

Riferimenti bibliografici

Balfe, Myles, Bernard Gallagher, Helen Masson, Shane Balfe, Ruairi Brugha e Simon Hackett. 2014. "Internet Child Sex Offenders' Concerns about Online Security and their Use of Identity Protection Technologies: A Review." In *Child Abuse Review* 24 (6): 427-439.

Bartlett, Christopher P., Gentile, Douglas A. e Chelsea Chew. 2016. "Predicting cyberbullying from anonymity." In *Psychology of Popular Media Culture* 5 (2):171-180.

Burnstein, Matthew R. 1996. "Conflicts on the Net: Choice of Law in Transnational Cyberspace." In *Vanderbilt Journal of Transnational Law* 29: 75-116.

Citron, Danielle K. 2007. "Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age." In *Southern California Law Review* 80 (2): 241-297.

— 2009. "Cyber Civil Rights." In *Boston University Law Review* 89: 61-125.

— 2014. *Hate Crimes in Cyberspace*. Cambridge, MA, e Londra, UK: Harvard University Press.

Cohen-Almagor, Raphael. 2015. *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*. Cambridge, UK: Cambridge University Press.

[30] Le potenzialità della scuola, sotto il profilo dell'educazione digitale, sono ben espresse nel Piano Nazionale Scuola Digitale, che dal 2015 indirizza l'attività dell'amministrazione scolastica italiana e l'impiego di risorse a favore dell'innovazione digitale, ponendosi come obiettivi le competenze degli studenti, i loro apprendimenti, i loro risultati, e l'impatto che avranno nella società come individui, cittadini e professionisti. Per un approfondimento, si rinvia al documento pubblicato dal Ministero dell'Istruzione, dell'Università e della Ricerca alla seguente pagina web: http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf.

Christopherson, Kimberly M. 2007. “The positive and negative implications of anonymity in Internet social interactions: ‘On the Internet, Nobody Knows You’re a Dog’.” In *Computers In Human Behavior* 23 (6): 3038-3056.

Cuniberti, Marco. 2014. “Democrazie, dissenso politico e tutela dell'anonimato.” In *Diritto dell’Informazione e dell’Informatica* 2: 111-137.

De Fazio, Laura e Chiara Sgarbi. 2016. “Unwanted Online Attentions Among an Italian Students Sample.” In *European Journal on Criminal Policy and Research* 22 (2): 219-234.

Eastwick, Paul W. e Wendi L. Gardner. 2009. “Is it a game? Evidence for social influence in the virtual world.” In Social Influence 4 (1): 18-32.

Finocchiaro, Giusella e Francesco Delfini (a cura di). 2014. *Diritto dell’informatica*. San Mauro Torinese: UTET giuridica.

Finocchiaro, Giusella. 2010. “Identità personale (diritto alla).” In *Digesto delle Discipline Privatistiche*, 721-738. Torino: UTET.

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

Frosini, Vittorio. 1981. *Il diritto nella società tecnologica*, Milano: Giuffrè.

Gibson, William. 1984. *Neuromante*. Milano: Oscar Mondadori.

Gradinger, Petra, Strohmeier, Dagmar e Christiane Spiel. 2009. “Traditional bullying and cyberbullying: Identification of risk groups for adjustment problems.” In *Zeitschrift für Psychologie/Journal of Psychology* 217 (4): 205-213.

Hayne, Stephen C. e Ronald E. Rice. 1997. “Attribution accuracy when using anonymity in group support systems.” In *International Journal of Human-Computer Studies* 47 (3): 429-452.

Hawker, David S. e Michael J. Boulton. 2000. “Twenty years’’research on peer victimization and psychological maladjustment: A meta-analytic review of cross-sectional studies.” In *Journal of Child Psychology and Psychiatry* 41 (4): 441-455.

Hinduja, Sameer e Justin W. Patchin. 2015. *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.

— 2017. “Digital Self-Harm Among Adolescents.” In Journal of Adolescent Health 61: 761-766.

Hite, Dwight M., Troy Voelker e Adrian Robertson. 2014. “Measuring perceived anonimity: the development of a context independent instrument.” In *Journal of Methods and Measurement in the Social Sciences* 5 (1): 22-39.

Horsman, Graeme. 2016. “The challenges surrounding the regulation of anonymous communication provision in the United Kingdom.” In *Computers & Security* 56: 151-162.

Joinson, Adam 2003. *Understanding the Psychology of Internet Behaviour: Virtual Worlds, Real Lives*. New York, NY: Palgrave Macmillan.

Kahn, Robert A. 2014. “Why Do Europeans Ban Hate Speech? A Debate Between Karl Loewenstein and Robert Post.” In *Hofstra Law Review* 41 (3): 545-585.

Kitchin, Rob. 1998. *Cyberspace: The World in the Wires*. Chichester, UK: John Wiley & Sons.

Livingstone, Sonia, Leslie Haddon, Jane Vincent, Giovanna Mascheroni e Kjartan Ólafsson. 2014. *Net Children Go Mobile. The UK Report*. http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/NCGMUKReportfinal.pdf.

Martoni, Michele e Monica Palmirani. 2015. “Internet e identità personale.” In *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, a cura di Raffaella Brighi e Silvia Zullo, 295-308. Roma: Aracne.

Myers, David. 2010. *Social Psychology*. New York, NY: McGraw-Hill.

Narayanan, Arvind e Vitaly Shmatikov. 2009. “De-anonymizing social networks.” In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*: 173-187.

Nakashima, Ellen. 2007. “Sexual Threats Stifle Some Female Bloggers”. In *Washington Post*, 30.04.2007. http://www.washingtonpost.com/wp-dyn/content/article/2007/04/29/AR2007042901555.htm.
Ortega-Ruiz, Rosario, Paz Elipe, Joaquín A. Mora-Merchán, Juan Calmaestra ed Esther Vega. 2009. “The emotional impact on victims of traditional bullying and cyberbullying. A study of Spanish adolescents.” In *Journal of Psychology* 217 (4): 197-204.
Pelliccioli, Luca (a cura di). 2016. *La privacy nell’età dell’informazione*. Milano: L’Ornitorinco edizioni.
Pino, Giorgio. 2003*, Il diritto all’identità personale. Interpretazione costituzionale e creatività giurisprudenziale*. Bologna: Il Mulino.
— 2010. “L’identità personale.” In *Ambiti e fonti del diritto, Trattato di Biodiritto I*, a cura di Stefano Rodotà e Mariachiara Tallachini, 297-321. Milano: Giuffrè.
Pozzolo, Susanna e Annalisa Verza. 2015. *A proposito di identità. Contributi per una riflessione*. Bologna: Il Mulino.
Post, Robert C. 1991. “Racist Speech, Democracy and the First Amendment.” In *William & Mary Law Review* 32 (2): 267-327.
— 2007. “Religion and Freedom of Speech: Portraits of Muhammad.” In *Constellations* 14 (1): 72-90.
— 2009. “Hate Speech”. In *Extreme Speech and Democracy*, a cura di Ivan Hare e James Weinstein. New York, NY: Oxford University Press.
Resta, Giorgio. 2007. “Identità personale e identità digitale.” In *Il Diritto dell’informazione e dell’informatica* 3: 511-531.
— 2014. “Anonimato, responsabilità, identificazione: prospettive di diritto comparato.” In *Diritto dell’Informazione e dell’Informatica* 2: 171-205.
Rodotà, Stefano. 2012. *Il diritto di avere diritti*. Roma-Bari: Laterza.
— 2014. *Il mondo nella rete. Quali i diritti, quali i vincoli*. Roma-Bari: Laterza.
Romeo, Francesco. 2016. “Dalla giuritecnica di Vittorio Frosini alla *Privacy by Design*.” In *Informatica e diritto*, XXV: 9-23.
Sartor, Giovanni. 2016. *L’informatica giuridica e le tecnologie dell’informazione*. Torino: Giappichelli.
Slonje, Robert e Peter K Smith. 2008. “Cyberbullying: Another main type of bullying?” In *Scandinavian Journal of Psychology* 49: 147-154.
Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven, CT: Yale University Press.
Staude-Müller, Frithjof, Britta Hansen e Melanie Voss. 2012. “How stressful is online victimization? Effects of victim’s personality and properties of the incident.” In *European Journal of Developmental Psychology* 9 (2): 260-274.
Tsesis, Alexander. 2001. “Hate in Cyberspace: Regulating Hate Speech On The Internet.” In *San Diego Law Review* 38: 817-874.
— 2015. “Free Speech Constitutionalism”. In *University of Illinois Law Review* 1015-1068.
Uncapher, Williard. 1991. “Trouble in Cyberspace: Civil Liberties at Peril in the Information Age.” In *The Humanist* 51 (5): 5-14.
Wallace, Patricia. 1999. *The Psychology of the Internet*. Cambridge, UK: Cambridge University Press.
Weisband, Suzanne e Leanne Atwater. 1999. “Evaluating Self and Others in Electronic and Face-to-Face Groups.” In *Journal of Applied Psychology* 84 (4): 632-639.
Wertheim, Margaret. 1999. *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet*, New York, NY: W.W. Norton.
Whitman, James Q. 2003. *Harsh Justice: Criminal Punishment and the Widening Divide. Between America and Europe*. New York, NY: Oxford University Press.

— 2004. “The Two Western Cultures of Privacy: Dignity Versus Liberty.” In *Yale Law Journal* 113 (6): 1151-1221.
Ybarra, Michele L. 2004. “Linkages between depressive symptomatology and internet harassment among young regular internet users.” In *Cyberpsychology & Behavior* 7 (2): 247–257.
Ziccardi, Giovanni. 2011. *Hacker. Il richiamo della libertà*. Venezia: Marsilio.
— 2015. *Internet, controllo e libertà*. Milano: Raffaello Cortina Editore.
— 2016. *L’odio online. Violenza verbale e ossessioni in rete*. Milano: Raffaello Cortina Editore.
Zimbardo, Philip. 1969. “The Human Choice: Individuation, Reason, and Order versus Deindividuation, Impulse, and Chaos.” In *Nebraska Symposium on Motivation* 17: 237-307.