PER UN ALFABETO DELLA PARITÀ

2019 - IV ciclo

TECNOLOGIE, ISTITUZIONI E NUOVI SCENARI DELLA VITA UMANA

Report sugli incontri promossi dal

CRID

Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità
con il coordinamento del Prof. Gianfrancesco Zanetti (Direttore CRID)

in collaborazione con

Centro Studi e Documentazione sulla Legalità (CSDL)
Centro Documentazione Donna di Modena

Serena Vantin

(Responsabile scientifica del Report)

REPORT

SOMMARIO

CALENDARIO DEGLI INCONTRI

PRIMO INCONTRO

IL PROGETTO EQUALIST: LA PROMOZIONE DELLA PARITÀ NELL'EPOCA DELLA RETE

Giovedì 14 marzo 2019 ore 17.30-19.30

Galleria Europa | Piazza Grande 17 | Modena

Claudia Canali

CRID; Università di Modena e Reggio Emilia

Thomas Casadei

CRID; Università di Modena e Reggio Emilia

Irene Guadagnini

Comune di Modena - Assessora alle Politiche giovanili, Partecipazione e Quartieri, Pari opportunità e Relazioni internazionali, Volontariato

Serena Vantin

CRID; Università di Modena e Reggio Emilia

Coordina:

Vittorina Maestroni

Centro Documentazione Donna

(A partire dagli esiti del Progetto Horizon 2020 Equalist "Gender Equality Plans for Information Sciences and Technologies")

SECONDO INCONTRO

LE AUTO A GUIDA AUTONOMA: TRA SVILUPPO TECNOLOGICO, RUOLO DELLE ISTITUZIONI E TERZA MISSIONE DELL'UNIVERSITÀ

Venerdì 22 marzo 2019 ore 17.30-19.30

Galleria Europa | Piazza Grande 17 | Modena

Presentazione del volume "Smart roads e driverless cars. Tra diritto, tecnologie e etica pubblica", Giappichelli, Torino, 2019, collana "Diritto e vulnerabilità"

Ludovica Carla Ferrari

Comune di Modena - Assessora alle Attività produttive, Turismo e promozione della città, Smart City e Sistemi informatici e Riforma della Pubblica Amministrazione, Servizi demografici, Polizia mortuaria, Statistica

Francesco Leali

Università di Modena e Reggio Emilia

Simone Scagliarini

CRID; Università di Modena e Reggio Emilia

Coordina:

Gianfrancesco Zanetti

Direttore del CRID; Università di Modena e Reggio Emilia

(A partire dagli esiti del Progetto FAR 2015 "Il futuro dei veicoli a guida autonoma: soluzioni tecnologiche e profili etico-normativi per garantire resilienza a errori umani e attacchi cyber")

TERZO INCONTRO

LIBERTÀ RELIGIOSA, FORME DI DISCRIMINAZIONE E NUOVI PROFILI DI TUTELA DELLA LEGALITÀ COSTITUZIONALE: MONDI DELLA RETE E PRATICHE DI ODIO

Martedì 2 aprile 2019 ore 17.30-19.30

Aula S del Dipartimento di Giurisprudenza dell'Università di Modena e Reggio Emilia

Via San Geminiano 3 | Modena

Alberto Melloni

Direttore del Dipartimento di Educazione e Scienze umane - Università di Modena e Reggio Emilia

Vincenzo Pacillo

Direttore del Dipartimento di Giurisprudenza - Università di Modena e Reggio Emilia

Coordina:

Gianfrancesco Zanetti

Direttore del CRID; Università di Modena e Reggio Emilia

(Nell'ambito del Progetto "Verso l'Osservatorio sulle Migrazioni nel territorio modenese" e in collaborazione con il corso di "Didattica del diritto e media education" del Prof. Thomas Casadei)

QUARTO INCONTRO

LA SICUREZZA IN RETE: TRA RISCHI, VULNERABILITÀ E NUOVE SFIDE DI LEGALITÀ

Mercoledì 3 aprile 2019 ore 17.30-19.30

Galleria Europa | Piazza Grande 17 | Modena

Andrea Bosi

Comune di Modena - Assessore al Bilancio, Finanze, Personale, Lavoro e formazione professionale, Promozione della cultura della legalità, Centro Storico, Europa - Cooperazione

internazionale

Michele Colajanni

CRID; Università di Modena e Reggio Emilia

Introduce:

Gianfrancesco Zanetti

Direttore del CRID; Università di Modena e Reggio Emilia

Coordina:

Vincenzo Pacillo

Direttore del Dipartimento di Giurisprudenza - Università di Modena e Reggio Emilia

(A partire dagli esiti del Progetto PRIN 2015 "Soggetto di diritto e vulnerabilità: modelli istituzionali e concetti giuridici in trasformazione)

Primo incontro

IL PROGETTO EQUAL-IST: LA PROMOZIONE DELLA PARITÀ NELL'EPOCA DELLA RETE

Giovedì 14 marzo 2019, ore 17.30-19.30.

Relatori

Claudia Canali (CRID; Università di Modena e Reggio Emilia)

Thomas Casadei (CRID; Università di Modena e Reggio Emilia)

Irene Guadagnini (Comune di Modena - Assessora alle Politiche giovanili, Partecipazione e Quartieri, Pari opportunità e Relazioni internazionali, Volontariato)

Serena Vantin (CRID; Università di Modena e Reggio Emilia)

Coordinatrice

Vittorina Maestroni (Centro Documentazione Donna)

Note

Incontro svolto partendo dagli esiti del Progetto Horizon 2020 EQUAL-IST "Gender Equality Plans for Information Sciences and Technologies".

Introduzione

Negli ultimi decenni le nuove tecnologie hanno impattato profondamente le dinamiche della vita e delle relazioni umane. Per questa ragione, una branca degli studi di genere, i cd. Feminist Technologies Studies, si è proposta di riflettere sulle implicazioni che esse hanno (e avranno) sull'ineguaglianza dei generi.

Da un lato, i dati statistici mostrano l'esistenza di un "digital gender divide" quale conseguenza di già consolidate differenze socio-economiche tra i sessi (soprattutto in termini di occupazione, reddito, istruzione), che renderebbero gli strumenti tecnologici più accessibili ai soggetti in condizioni più avvantaggiate. A tal riguardo, i dati del Global Gender Gap 2017 relativi al caso italiano sono allarmanti: il nostro paese è scivolato all'ottantaduesima posizione (su un totale di 144), appena prima di Birmania, Indonesia e Kirghizistan; le discriminazioni tecnologiche andrebbero dunque lette all'interno di questo più ampio quadro di svantaggio.

Dall'altro lato, il gap sembra altresì supportato da "nuovi" stereotipi di genere, che influenzerebbero le attitudini personali dei "soggetti tecnologici", indirizzando il genere maschile verso una maggiore propensione alla tecnologia, quello femminile verso una "fuga" dalla stessa. Già Betty Friedan riconduceva le ragioni della mancata partecipazione delle donne a determinati attributi che la società impone loro: in questo senso, Martin Hilbert ha rilevato che esse si percepiscono come «technophobic», mentre gli uomini come «tech savvy». Queste attitudini generalizzate sarebbero riscontrabili sin dall'analisi dei diversi usi che ragazzi e ragazze fanno della tecnologia in età scolare: i maschi sono più interessati a scaricare videogiochi e musica, a occuparsi di on-line trading, a creare pagine web; le femmine usano internet perlopiù per instant messaging e chat-rooms.

Prospettive di ricerca

Dopo il celebre "manifesto cyborg" di Donna Haraway (1991), le nuove "sfide" che la tecnica odierna pone ai movimenti femministi, e più in generale all'intera società, possono essere collocate entro due direttrici: la (scarsa) presenza delle donne *nella* tecnologia e il rapporto tra donne *e* tecnologia.

Resta inoltre inevitabile domandarsi quali siano le vie attraverso le quali le tecnologie informatiche possano rivelarsi strumentali al contrasto delle discriminazioni di genere, ovvero se esse possano favorire uno spazio di emancipazione per le donne.

Le occasioni che essa offre, in effetti, sono potenzialmente paritarie: si pensi alle opportunità imprenditoriali a costo zero rappresentate dai canali di worldwide e-commerce o alla possibilità di utilizzo della rete nei termini del community-building.

Alcune autrici, tuttavia, non ritengono sufficiente insistere sull'"accesso" delle donne nel mondo tecnologico per come esso è oggi strutturato. Sostengono piuttosto che una più massiccia presenza del femminile nel settore tecnologico dovrà implicarne una parziale "ridefinizione".

Il Progetto EQUAL-IST

A partire da una riflessione su questi temi, l'Università di Modena e Reggio Emilia (con il coordinamento della Prof.ssa Claudia Canali) ha recentemente promosso e realizzato un Progetto HORIZON 2020 dal titolo "EQUAL-IST – Gender Equality Plans for Information Sciences and Technology Research Institutions", grazie ad una partnership con diverse Università ed enti di ricerca europei.

Il Progetto si inserisce a pieno regime nell'ambito delle direttive internazionali di gender mainstreaming e women's empowerment, mirando a ideare, e poi testare, pacchetti di azioni – potenzialmente riproducibili su altri territori e a più ampie dimensioni, in un'ottica multilivello – nel solco degli obiettivi della democrazia paritaria e della cogestione del potere, proprio a partire dal versante tecnologico.

Quest'ultimo è infatti assunto come settore strategico, "chiave" della modernizzazione delle strutture universitarie e dei programmi di insegnamento, nonché come terreno sul quale si perpetrano spirali discriminatorie che hanno spesso origine nel pregiudizio "anti-tecnologico" che colpisce le ragazze già al momento della scelta del proprio percorso di studi.

Più nel dettaglio, nell'ambito del progetto, che ha preso avvio a giugno 2016 e che si è concluso nel maggio 2019, è stata svolta innanzitutto una mappatura dei livelli di "gender balance" nelle diverse istituzioni partner, mediante la raccolta di dati disaggregati, poi comparati su scala sia nazionale sia internazionale (con riferimento all'ISCED – International Standard Classification of Education) .

In seguito, è stata messa a punto una metodologia condivisa da sperimentare nel corso di PGA – Participatory Gender Audits, i cui esiti sono stati raccolti e analizzati con strumenti quantitativi e qualitativi. Questi ultimi hanno consentito di sperimentare su piccoli gruppi forme di democrazia partecipativa e percorsi di ascolto e di dialogo "dal basso", coinvolgendo il personale a vario titolo "impiegato" nelle strutture universitarie.

Numerose proposte concrete sono state infine ideate e approvate dagli organi accademici, con il fine di supportare e sostenere buone pratiche di promozione e supporto delle donne nei percorsi di ricerca di carattere tecnologico.

Proposte operative

In collaborazione con i mondi della ricerca, le istituzioni possono assumere un ruolo attivo di promozione delle buone pratiche di inclusione delle donne nei settori tecnologici.

Linee strategiche improntate alla parità di genere e al rispetto del principio di eguaglianza in senso sostanziale, anche con riguardo allo sviluppo tecnologico e della

ricerca scientifica, sono state finanziate anche dalla Commissione Europea. A tal proposito, si pensi agli impulsi promossi a partire dalla Comunicazione "Women and Science" del 1999, da ETAN – European Technology Assessment Network Report (2000); dal Programma triennale SHE FIGURES (dal 2003); e dai Rapporti "Gender and Excellence in the Making" (2004), "Benchmarking Policy Measure for Gender Equality in Science" (2008), "The Gender Challenge in Research Funding: Assessing the European National Scenes" (2009), "Structural Change: Enhancing Excellence, Gender Equality and Efficiency in Research and Innovation" (2012), "Gendered Innovations: How Gender Analysis Contributes to Research" (2013), "Gender Equality Policies in Public Research" (2014).

A questi fini, risultano decisivi anche i contributi delle reti femminili e degli enti associativi, nell'ottica di una ricerca condivisa di strategie che possano consentire un'accelerazione verso l'accesso e la ridefinizione del ruolo delle donne rispetto alle tecnologie informatiche, secondo una logica che sia capace non solo di contrastare pregresse sacche discriminatorie ma anche di prevenirne nuove insorgenze.

Misure multilivello di promozione attiva della parità restano importanti anche sul versante del mondo occupazionale, della conciliazione tra tempi di vita e tempi di lavoro, dei servizi per la cura di bambini e anziani.

Infine, si raccomanda attenzione al sistema di comunicazione istituzionale: un canale che può favorire una circolazione mediatica di role models positivi, capaci di indurre il superamento di stereotipi discriminatori.

BIBLIOGRAFIA

Casadei, Th.

2017, *Diritto e (dis)parità. Dalla discriminazione di genere alla democrazia paritaria*, Roma, Aracne.

Cockburn C.

1992, *The Circuit of Technology: Gender, Identity and Power*, in R. Silverstone, E. Hirsch (eds.), *Consuming Technology: Media and Information in Domestic Spaces*, London, Routledge, pp. 32-47.

Drew E., Bencivenga R.

2017, *Gender in Horizon 2020: The Case of Gender Equality Plans*, in «About Gender – Rivista internazionale di studi di genere», n. 6 (12), pp. 326-355.

Hacker S.

1989, *Pleasure, Power and Technology: Some Tales of Gender, Engineering, and the Cooperative Workplace*, Boston, Unwin Hyman.

1990, *Doing It In The Hard Way: Investigations On Gender And Technology*, Boston, Unwin Hyman.

Haraway D.

1991. *Simians, Cyborgs And Women: The Reinvention Of Nature*, London-New York, Routledge.

Hilbert M.

2011, *Digital Gender Divide or Technologically Empowered Women in Developing Countries? A Typical Case of Lies, Damned Lies, and Statistics*, in «Women's Studies International Forum», n. 6, pp. 479-489.

MacKinnon C.A.

2006, *Postmodernism and Human Rights*, in C.A. MacKinnon, *Are Women Human? And Other International Dialogues*, Cambridge, MA, Harvard University Press, pp. 44-63.

Papastergiou, M.

2008, *Are Computer Science and Information Technology Still Masculine Fields? High School Students' Perceptions and Career Choices*, in «Computer & Education», n. 51, pp. 594-608.

Puente S.N.

2008, *From Cyberfeminism to Technofeminism: from an Essentialist Perspective to Social Cyberfeminism in Certain Feminist Practices in Spain*, in «Women's Studies International forum», n. 31, pp. 434-440.

Vantin S.

2015, *Digital Gender Divide e ICT. Il femminismo alla prova della rivoluzione tecnologica*, in «Il Senso della Repubblica nel XXI secolo – Quaderni di Storia e Filosofia», n. 10, pp. 9-10.

Secondo incontro

LE AUTO A GUIDA AUTONOMA: TRA SVILUPPO TECNOLOGICO, RUOLO DELLE ISTITUZIONI E TERZA MISSIONE DELL'UNIVERSITÀ

Venerdì 22 marzo 2019, ore 17.30-19.30.

Relatori

Ludovica Carla Ferrari (Comune di Modena - Assessora alle Attività produttive, Turismo e promozione della città, Smart City e Sistemi informatici e Riforma della Pubblica Amministrazione, Servizi demografici, Polizia mortuaria, Statistica)
Francesco Leali (Università di Modena e Reggio Emilia)
Simone Scagliarini (CRID; Università di Modena e Reggio Emilia)

Coordinatore

Gianfrancesco Zanetti (Direttore del CRID; Università di Modena e Reggio Emilia)

Note

Presentazione del volume "Smart roads e driverless cars. Tra diritto, tecnologie e etica pubblica", Giappichelli, Torino, 2019, collana "Diritto e vulnerabilità".
Incontro svolto nell'ambito del Progetto "Verso l'Osservatorio sulle Migrazioni nel territorio modenese" e in collaborazione con il corso di "Didattica del diritto e media education" del Prof. Thomas Casadei.

Introduzione

Le auto a guida autonoma potrebbero rivoluzionare l'intero settore automobilistico; già oggi i sistemi avanzati di assistenza alla guida rendono più sicura e agevole la guida tradizionale. La vera rivoluzione si avrà, comunque, con i veicoli che guidano autonomamente e, al livello 5, senza che sia neanche previsto l'intervento del guidatore umano. Com'è noto, infatti, si distingue fra cinque livelli di automazione:

nessuna automazione;

assistenza alla guida;

automazione parziale;

automazione condizionata;

alta automazione;

completa automazione.

I sistemi di cui al livello 1 coadiuvano il guidatore, ma non prendono il controllo del veicolo; già al livello 2 i veicoli possono prendere il controllo del veicolo anche se il guidatore rimane responsabile della guida; al livello 3, in alcune situazioni, il guidatore può affidare il controllo al veicolo; al livello 4 il veicolo può operare del tutto autonomamente anche se il guidatore può riprenderne il controllo; al livello 5 il veicolo è autonomo e non è prevista la possibilità di intervenire, per cui le persone al suo interno sono tutte passeggeri.

In Europa le automobili di livello 1 e 2 sono in vendita già da tempo, ma fra il 2020 e il 2030 si giungerà anche alla commercializzazione delle auto di livello 3 e 4.

Sviluppo tecnologico e problematiche giuridiche

Lo sviluppo tecnologico, dunque, va avanti e le istituzioni spingono anche in tal senso, poiché sistemi sicuri di guida autonoma potrebbero avere un impatto positivo sulla sicurezza stradale: la condotta di un veicolo a guida autonoma dovrebbe infatti

essere prevedibile e “a norma di legge”, o meglio del Codice della strada: ad es., l’autoveicolo dovrebbe dare la precedenza ai pedoni (e non, ad es., aggirarli), rispettare i limiti di velocità, ecc. Inoltre, gli autoveicoli a guida autonoma potrebbero essere particolarmente utili per le persone con disabilità.

I sistemi, però, non sono né saranno perfetti: percorrere le strade tradizionali comporta altresì la necessità di dover prendere decisioni anche in poche frazioni di secondo per far fronte alle modificazioni dell’ambiente circostante (dal cane che attraversa la strada repentinamente al mancato rispetto delle regole da parte di altri guidatori), talvolta dovendo decidere di sacrificare la vita dei passeggeri o di terzi: le questioni etiche sono quindi molto serie e se ne discute da diversi anni.

Inoltre, si pongono problemi di sicurezza (sistemi così complessi potrebbero essere attaccati da hacker o criminali informatici di qualsiasi tipologia, terroristi inclusi) oltreché di malfunzionamenti conseguenti ad anomalie del sistema (non solo dovuti ad anomalie meccaniche ma potenzialmente a bug dei complessi software eseguiti dal sistema informatico di ciascun veicolo a guida autonoma).

Nel caso in cui si verifichi un sinistro, sarà quindi fondamentale anche capire cosa sia realmente successo al fine di attribuire correttamente le responsabilità, soprattutto per ciò che concerne i livelli 2, 3 e 4. Al livello 5, del resto, il ruolo del guidatore umano viene meno, perché soppiantato dal sistema informatico. Prenderà dunque piede la vehicle forensics, che dovrebbe consentire di far luce su quanto realmente successo, ma in ipotesi ciò potrebbe essere molto difficile qualora non dovesse essere possibile accedere al codice eseguito da ciascun autoveicolo.

Come dimostra il recente scandalo delle emissioni, non si può sperare nella rettitudine dell’industria automobilistica ma bisogna invece imporre regole certe e stringenti, dal momento che è in gioco la sicurezza di tutti.

Anche di qui discende il ruolo fondamentale delle istituzioni nel condurre la rivoluzione in questo ambito affinché la sicurezza effettiva non venga sacrificata in nome del denaro e della necessità di conseguire ricavi sempre più elevati.

È interessante notare come diversi aspetti non siano propri unicamente di tale settore, ma coinvolgano in modo più ampio la rivoluzione della Internet of Things. Ci stiamo infatti muovendo verso una società in cui sempre più dispositivi saranno connessi a Internet, ma è nota anche l'inadeguatezza degli ordinamenti giuridici dinanzi all'avanzamento di tecnologie sviluppate, vendute e utilizzate da privati su un piano generalmente globale.

Già in merito alla sicurezza, la comune esperienza mostra che i dispositivi attuali e futuri presentano e presenteranno inevitabilmente falle di sicurezza e limitazioni, magari sconosciute al momento in cui vengono commercializzati o comunque diffusi. Difatti, non v'è dubbio che i servizi intelligenti saranno interconnessi e quindi accessibili anche a potenziali malintenzionati, soprattutto in un'ottica in cui si passa sempre più dal concetto di prodotto a quello di servizio, da Software as a Product a Software as a Service, e dal controllo dell'utilizzatore a quello del produttore (anche con conseguenze nefaste).

Le auto a guida autonoma, così, saranno pilotate da agenti intelligenti estremamente complessi, la cui architettura potrebbe essere il frutto di studi e ricerche compiuti generalmente in ambito privato, per concretizzarsi sostanzialmente in programmi che guidano il funzionamento degli autoveicoli: la loro inconoscibilità è consentita dalle varie normative in materia di proprietà intellettuale e industriale.

Proposte operative

Il ruolo delle istituzioni, e dell'università, è quindi fondamentale: prima di affrontarlo, è però opportuno evidenziare, in primo luogo, che la condotta degli agenti

intelligenti viene svolta in esecuzione di algoritmi sempre più complessi e questi possono essere in grado di prendere decisioni non previste né prevedibili dai loro produttori (ad es. grazie ai meccanismi di autoapprendimento e alla molteplicità di variabili che possono orientarne la condotta stessa), oltre che potenzialmente fatali per i passeggeri e/o i terzi. A differenza di quanto accade oggi dinanzi a scelte tanto difficili, la scelta non sarebbe compiuta in modo istintivo all'atto dell'evento tragico: sarebbe predeterminata e quindi svolta su una base razionale anziché emozionale; sulla base della ragione e non dell'istinto, di un utilitarismo che pone anche problemi di uguaglianza sostanziale (non tutti sarebbero uguali in via immediata dinanzi all'algoritmo che viene eseguito e in via mediata a chi ne ha predeterminato volontariamente le regole).

In secondo luogo, la scelta summenzionata verrebbe compiuta a priori non dal conducente del bene, nel caso di un autoveicolo (in assenza di un controllo esclusivo), bensì su scala collettiva dal produttore di ciascuno di essi. Qui emerge tutta la drammaticità della problematica e la preponderanza del potere privato su quello pubblico, poiché in esecuzione di algoritmi complessi e sconosciuti sarà una macchina a eseguire la decisione stabilita a monte, nei suoi parametri e nei suoi criteri, dal produttore del bene di cui trattasi. Inoltre, qualsiasi decisione presa potrebbe essere protetta dallo scudo dell'inconoscibilità, così come eventuali vizi o difetti del software, che potrebbero essere taciuti o nascosti.

Emergono, pertanto, problematiche giuridiche e dilemmi etici che il diritto, per le più varie motivazioni, sembra quasi rifiutarsi di affrontare e regolamentare. Eppure, la tecnologia, mediante questi sistemi, effettuerà sempre più spesso le veci dell'uomo con modalità tali che la renderanno sempre più inafferrabile anche grazie a quello schermo costituito dall'opacità del codice: bisogna quindi essere particolarmente cauti e rafforzare il ruolo del diritto.

Il legislatore ha dunque un ruolo fondamentale; accanto ad esso, si pongono diverse istituzioni che possono agevolare questo percorso molto difficile ma altrettanto stimolante. Così, le prime sperimentazioni in materia vengono svolte previa autorizzazione degli enti competenti e consentono di testare su strada questi sofisticati autoveicoli (con la presenza di una persona pronta a subentrare al sistema di guida autonoma in caso di necessità), così da acquisire preziose informazioni che le mettano alla prova.

Le istituzioni devono avere un ruolo attivo anche nello sviluppo dei predetti sistemi e un particolare rilievo assume la c.d. Terza missione dell'università, per cui le conoscenze vengono valorizzate e trasferite nello specifico contesto socio-economico di riferimento.

Da un lato, la conoscenza prodotta in ambito accademico può essere trasformata agevolmente in conoscenze utile ai fini produttivi, contestualizzandola e applicandola anche in sinergia con le aziende del territorio e non.

Dall'altro, la ricerca svolta in ambito accademico, soprattutto per ciò che concerne i profili etici e giuridici, può essere divulgata contribuendo allo sviluppo della cultura giuridica sul punto ed evidenziando le maggiori criticità che emergono.

Il tutto è dunque finalizzato, in particolare, a sottrare lo sviluppo degli autoveicoli a guida autonoma, e la rispettiva regolamentazione, al solo mercato. In tal senso, la Terza missione dell'università trova piena e compiuta realizzazione poiché l'indagine sulle questioni etiche, filosofiche e giuridiche è fondamentale per leggere criticamente l'anzidetta evoluzione e contribuire a orientarne lo sviluppo in conformità all'ordinamento giuridico.

BIBLIOGRAFIA

Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., and Ayyash M.,

2015, *Internet of things: A survey on enabling technologies, protocols, and applications*, in «IEEE Communications Surveys Tutorials», 17(4):2347-2376, Fourthquarter.

Andreolini M., Casolari S, Colajanni M,

2007, *Self-inspection mechanisms for the support of autonomic decisions in Internet-based systems*

(Third International Conference on Autonomic and Autonomous Systems - Athens, Greece - 19/06/2007) (IEEE Computer Society Washington USA), pp. 53-62, ISBN: 9780769528595.

Butti L.,

2016, *Auto a guida autonoma: sviluppo tecnologico, aspetti legali ed etici, impatto ambientale* – [*Driverless car: technological development, legal and ethical aspects, environmental impact*], in «Rivista giuridica dell'ambiente», fasc. 3-4, pp. 435-452.

Contissa G., Lagioia F., Sartor G.,

2017, *The Ethical Knob: ethically-customisable automated vehicles and the law*, in «Artificial Intelligence and Law», fasc. 3, pp. 365-378.

Costantini F., Montessoro P.,

2016, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "Smart Cars"*, in «Informatica e diritto», fasc. 1, pp. 95-115.

Dimitrakopoulos G.,

2011, *Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges*, in «ITS Telecommunications (ITST)», 2011 11th International Conference on, pp. 145-151, Aug 2011.

Gaeta M.C.,

2016, *Automazione e responsabilità civile automobilistica* – [*Automation and liability in road traffic*], in «Responsabilità civile e previdenza», fasc. 5, pp. 1718-1750.

Gerla M.,

2012, *Vehicular cloud computing*, in Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean, pp. 152-155, June 2012.

Gerla M., Lee E.-K., Pau G., Lee U.,

2014, *Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds*, in Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 241-246, March 2014.

Kumar S., Shi L., Ahmed N., Gil S., Katabi D., Rus D.,

2012, *Carspeak: A content-centric network for autonomous driving*, in Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, SIGCOMM '12, pp. 259-270, New York, NY, USA, 2012. ACM.

Lee K.C., Lee S.H., Cheung R., Lee U., and Gerla M.,
2007, *First experience with cartorrent in a real vehicular ad hoc network testbed*, in 2007 Mobile Networking for Vehicular Environments, pp. 109-114, May 2007.

Lee U., Zhou B., Gerla M., Magistretti E., Bellavista P., and Corradi A.,
2006, *Mobeyes: smart mobs for urban monitoring with a vehicular sensor network*, IEEE Wireless Communications, 13(5):52-57, October 2006.

Maurer M., Gerdes J.C., Lenz B., Winner H. (edited by),
2016, *Autonomous driving : technical, legal and social aspects*, Springer, Berlin.

Missiroli M., Pierazzi F., Colajanni M.,
2014, *Security and privacy of location-based services for in-vehicle device systems* (2014 International Conference on High Performance Computing & Simulation (HPCS 2014) – Bologna, Italia – 21-25 Giugno 2014) (Proceedings) (Institute of Electrical and Electronics Engineers (IEEE) Los Alamitos USA), pp. 841-848, ISBN: 9781479951604.

Scagliarini S. (a cura di),
2019, Smart roads *e* driverless cars: *tra diritto, tecnologie, etica pubblica*, Giappichelli, Torino.

Wang L., Wakikawa R., Kuntz R., Vuyyuru R., and Zhang L.,

2012, *Data naming in vehicle-to-vehicle communications*, in Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on, pp. 328-333, March 2012.

Whaiduzzaman Md, Sookhak M., Gani A., and Buyya R.,
2014, *A survey on vehicular cloud computing*, in «Journal of Network and Computer Applications», 40:325-344, 2014.

Yan G., Wen D., Olariu S., and Weigle M.C.,
2013, *Security challenges in vehicular cloud computing*, IEEE Transactions on Intelligent Transportation Systems, 14(1):284-294, March 2013.

Yu Y.T., Punihaole T., Gerla M., and Sanadidi M.Y., *Content routing in the vehicle cloud*, in Military Communications Conference, 2012 – MILCOM 2012, pp. 1-6, Oct 2012.

Terzo incontro

LIBERTÀ RELIGIOSA, FORME DI DISCRIMINAZIONE E NUOVI PROFILI DI TUTELA DELLA LEGALITÀ COSTITUZIONALE: MONDI DELLA RETE E PRATICHE DI ODIO

Martedì 2 aprile 2019, ore 17.30-19.30

Relatori

Alberto Melloni (Direttore del Dipartimento di Educazione e Scienze umane - Università di Modena e Reggio Emilia)

Vincenzo Pacillo (Direttore del Dipartimento di Giurisprudenza - Università di Modena e Reggio Emilia)

Coordinatore

Gianfrancesco Zanetti (Direttore del CRID; Università di Modena e Reggio Emilia).

Note

Incontro svolto nell'ambito del Progetto "Verso l'Osservatorio sulle Migrazioni nel territorio modenese" e in collaborazione con il corso di "Didattica del diritto e media education" del Prof. Thomas Casadei.

Introduzione

La libertà di manifestazione del pensiero è una fondamentale conquista che caratterizza gli stati democratici. La Rete, poi, consente una libertà di espressione senza pari: al contempo, però, si presta anche a favorire pratiche di odio a causa di una serie di fattori, fra cui l'intermediazione del dispositivo informatico che elimina il contatto fisico e, unitamente all'asincronicità delle comunicazioni, agevola la deresponsabilizzazione.

Arginare le pratiche di odio on line non è compito facile perché bisogna distinguerle dall'esercizio del diritto a manifestare liberamente il proprio pensiero: essendo un diritto fondamentale, è tutelato in massimo grado negli stati costituzionali. Allo stesso tempo, in Europa si ha comunque una certa attenzione verso le sue limitazioni anche alla luce delle esperienze totalitarie del passato e quindi si limitano quelle manifestazioni del pensiero che si concretizzano in espressioni offensive o che incitano all'odio verso singoli o gruppi in virtù delle loro convinzioni religiose, della loro razza, del loro orientamento sessuale, delle loro opinioni politiche, ecc.

Negli Stati Uniti l'approccio è diverso e meno restrittivo, con un forte privilegio del *Free Speech* rispetto a qualsiasi ipotetica limitazione.

Tuttavia, nella società dell'informazione il quadro non può che cambiare dal momento che il terreno più fecondo per la effettuazione delle suddette pratiche è da individuarsi in servizi forniti su scala globale, come social network e siti web; i relativi prestatori si trovano dunque ad operare in una molteplicità di paesi e dunque devono, o dovrebbero, rispettare le norme di ciascuno di essi.

Mondi della rete e pratiche di odio

Paradossalmente, potrebbe ritenersi – di primo acchito – che nella lotta agli hate speech, più che gli stati potrebbero essere efficaci i prestatori dei relativi servizi, i cui termini di fornitura del servizio (ossia le condizioni generali di contratto con i propri utenti) e le cui policies generalmente vietano in modo forte simili condotte. Eppure, i social network sono costantemente invasi di manifestazioni di odio e ciò è dovuto anche al fatto che le normative vigenti nei vari stati non impongono una sorveglianza dei contenuti; anche dinanzi alle segnalazioni, questi prestatori hanno ben pochi doveri e comunque una delega in tal senso verso di loro corrisponderebbe a una loro investitura praticamente formale quali censori della Rete. Inoltre, essi hanno comunque interesse a suscitare discussioni e a rendere i contenuti sempre più discussi e virali.

I social network, del resto, sono la piattaforma ideale per la effettuazione di pratiche di odio on line, poiché consentono potenzialmente di amplificare ciascun messaggio grazie alla viralità che li connota. A differenza di quanto avviene off line, i messaggi vengono inoltre memorizzati e sono persistenti; ne consegue che i loro effetti negativi si amplificano e colpiscono in modo forte le relative vittime, sovente appartenenti a gruppi sociali svantaggiati o comunque vulnerabili. In altri casi l'offesa non è diretta verso una persona determinata, o comunque un gruppo specifico, bensì verso la sensibilità religiosa di diversi soggetti; in alcuni paesi anche queste fattispecie sono previste e punite dalla legislazione vigente.

Sulla carta, dunque, le pratiche di odio sono vietate in modo più o meno forte da paese a paese, anche perché esse incidono in modo particolarmente severo sui diritti e sulla libertà delle persone che possono essere discriminate in conseguenza dello svolgimento delle suddette pratiche. Come si è detto, bisogna tuttavia comprendere viene travalicato il limite della manifestazione del proprio pensiero per giungere a una pratica di odio (e talvolta, soprattutto nel caso della satira, il confine può apparire alquanto sfumato); nel nostro ordinamento si può fare riferimento alla c.d. legge

Mancino (l. 205/93), che punisce chi incita a commettere o commette violenza o atti di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi. Ciascun caso, dunque, dovrebbe essere analizzato in modo specifico.

Bisogna però considerare che l'ambito delle pratiche di odio è più ampio di quello di cui alla legge Mancino, andando a coinvolgere anche la sfera dell'orientamento sessuale, i migranti, le donne, ecc.; si veda, in questo senso, la delibera n. 157/19/CONS dell'AGCOM del 15 maggio 2019, secondo cui le espressioni o discorso d'odio consistono nell'"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" (Regolamento recante disposizioni in materia di rispetto della dignità umana e del principio di non discriminazione e di contrasto all'hate speech; si applica, però, ai fornitori di servizi media audiovisivi e radiofonici soggetti alla giurisdizione italiana e non ai social network e alle piattaforme digitali, anche se è prevista la possibilità di concordare dei codici di condotta con i prestatori di quest'ultime).

In concreto, le pratiche di odio sono compiute costantemente e sono facilitate dalla natura immateriale e dalla facilità e rapidità di utilizzo degli strumenti informatici e delle reti telematiche, oltre che da un diffuso senso di impunità per cui on line ci si sente più liberi di insultare una persona o un gruppo che non può difendersi, o che comunque non si trova faccia a faccia con chi lo proferisce. Del resto, la viralità negativa appare molto più forte di quella positiva e molte pratiche di odio riescono nel

loro intento di suscitare non necessariamente odio verso determinati soggetti o gruppi sociali, ma anche invidia, paura, ribrezzo, ecc.

Proposte operative

La tematica è molto complessa: in linea generale, può comunque affermarsi la necessità, più che la possibilità, di cercare di arginare simili fenomeni mediante azioni sinergiche e su larga scala.

In primo luogo, dal punto di vista prettamente giuridico, e dunque nella prospettiva dell'ordinamento, sarebbe necessario non lasciare impunite le condotte più gravi per non alimentare il sopra citato senso di impunità e, comunque, per fare giustizia. La lentezza della macchina giudiziaria impone però di approntare anche delle misure che consentano di agire in modo rapido per ridurre le conseguenze negative delle pratiche di odio, ad es. mediante la disabilitazione temporanea di determinati messaggi sino alla definizione del procedimento.

In secondo luogo, i prestatori di servizi della società dell'informazione dovrebbero garantire tempi certi per la rimozione o la disabilitazione quanto meno dei messaggi certamente offensivi; un simile obbligo potrebbe essere previsto solo per i soggetti di maggiori dimensioni, ma ovviamente dovrebbe essere imposto da quei pochi soggetti che hanno un tale potere (come i grandi Stati o l'Unione europea), anche prevedendo sanzioni molto severe a scopo dissuasivo (un precedente in tal senso può rinvenirsi nel Regolamento Generale sulla Protezione dei Dati, ossia il Regolamento (UE) n. 679/2016). L'imposizione di filtri on line automatizzati appare, invece, alquanto rischiosa, poiché potrebbe comportare la censura di messaggi assolutamente leciti (e, paradossalmente, essere aggirati da chi vuole incitare all'odio ma è consapevole della presenza dei filtri stessi). Normalmente, poi, si evidenzia l'impossibilità di analizzare l'enorme flusso di messaggi e video che vengono caricati

ogni secondo sulle principali piattaforme; invero, i messaggi e i video vengono studiati, in qualche modo, dal sistema informatico che governa la piattaforma al fine di selezionare quelli da mostrare a un utente (come nel caso di Facebook) o di mostrare la pubblicità (come nel caso di YouTube); perché non dovrebbe essere possibile anche per tutelare un diritto fondamentale e proteggere individui e gruppi da insulti e discriminazioni? In questo senso, anche il recente Regolamento AGCOM menziona le piattaforme di condivisione di video e il Codice di condotta della Commissione europea per lottare contro le forme illegali di incitamento all'odio online (concluso con Facebook, Twitter, YouTube e Microsoft): a febbraio 2019, risultava rimosso in media il 72% dei contenuti notificati quali hate speech (il dato è riferito al periodo fra il 5 novembre e il 14 dicembre 2018, in cui sono state effettuate 4302 segnalazioni; in linea generale, la percentuale di rimozione è stata più elevata quando vi erano espressioni violente o minacce di morte verso gruppi specifici, mentre i messaggi asseritamente diffamatori sono stati rimossi nel 58,5% dei casi).

In terzo luogo, è necessario investire sia nella alfabetizzazione informatica che nella educazione civica digitale, rivolgendosi a tutte le fasce di età e non solo ai nativi digitali. La prima può consentire un utilizzo consapevole degli strumenti informatici, mentre la seconda è essenziale per orientarne la condotta.

In quarto luogo, è necessario ricordare che la Rete, i social network e, più in generale, gli strumenti informatici non devono essere né demonizzati né criminalizzati: il problema è l'utilizzo distorto che se ne può fare, ma che non deve far dimenticare i numerosi benefici che comportano.

BIBLIOGRAFIA

Alpa G.,

2018, *Autonomia privata, diritti fondamentali e 'linguaggio dell'odio'*, in «Contratto e impresa», fasc. 1, pp. 45-80.

Ansuátegui Roig F.J.,

2018, *Libertà d'espressione: ragione e storia* (a cura di Alessandro Di Rosa), Giappichelli, Torino.

Balkin J.M.,

2018, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, in «UC Davis Law Review», fasc. 51, pp. 1149-1210.

Belluati M.,

2018, Hate or Hateful? *L'uso del linguaggio d'offesa nelle discussioni politiche*, in «Comunicazioni politiche», fasc. 3, pp. 373-392.

Brown A.,

2015, *Hate Speech Law. A Philosophical Examination*, Routledge, New York-London.

Caruso C.,

2017, *L'*hate speech *a Strasburgo: il pluralismo militante del sistema convenzionale*, in «Quaderni costituzionali», fasc. 3, pp. 963-984.

Casadei Th.,

2019, *L'irruzione della post-verità*, in *Governare la paura*, 2019, pp. 1-18.

Claussen V.,

2018, *Fighting hate speech and fake news. The Network Enforcement Act (NetzDG) in Germany in the context of European legislation*, in «Rivista di diritto dei media», fasc. 3, pp. 110-136.

Andrea De Petris,

2018, *Libertà di religione e limiti alla tutela del pluralismo culturale. La leitkultur nella germania multiculturale*, in «Nomos», fasc. 1, pp. 35.

G. Gometz,

2017, *L'odio proibito: la repressione giuridica dello hate speech*, in «Stato, Chiese e pluralismo confessionale», fasc. 32, pp. 39.

Heinze E.,

2016, *Hate Speech and Democratic Citizenship*, Oxford, Oxford University Press.

Howard E.,

2018, *Freedom of expression and religious hate speech in Europe*, Routledge, London-New York.

Langton R.,

2018, *The Authority of Hate Speech*, in Gardner J., Green L., Leiter B. (edited by), in «Oxford Studies in Philosophy od Law», vol. 3, Oxford University Press, Oxford-New York, pp. 123-149.

Matucci G.,

2018, *Informazione online e dovere di solidarietà. Le fake news tra eduzione e responsabilità*, in «Rivista AIC», pp. 32.

Mazziotti A.,

2017, *Fake news, fake people e società della (dis)informazione: riflessioni su democrazia, informazione e libertà fondamentali al tempo dei social network*, in «I diritti dell'uomo», fasc. 1, pp. 57-58.

Moon R.,

2018, *Putting Faith in Hate. When Religion Is the Source or Target of Hate Speech*, Cambridge, Cambridge University Press.

Nardi V.,

2019, *I discorsi d'odio nell'era digitale: quale ruolo per l'*Internet service provider*?*, in «Diritto penale contemporaneo», fasc. 2.

Pitruzzella G., Pollicino O., Quintarelli S.,

2017, *Parole e potere. Libertà d'espressione, hate speech e fake news*, EGEA, Milano.

Savarese P.,

2018, *Dalla bugia alla menzogna: la postverità e l'impossibilità del diritto*, in «Nomos», fasc. 2, pp. 21.

Spigno I.,

2018, *Discorsi d'odio. Modelli costituzionali a confronto*, Giuffrè, Milano.

Waldron J.,

2012, *The harm in hate speech*, Harvard University Press, Cambridge (MA)-London.

Ziccardi G.,

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

Quarto incontro

LA SICUREZZA IN RETE: TRA RISCHI, VULNERABILITÀ E NUOVE SFIDE DI LEGALITÀ

Mercoledì 3 aprile 2019, ore 17.30-19.30.

Relatori

*Andrea Bosi (*Comune di Modena - Assessore al Bilancio, Finanze, Personale, Lavoro e formazione professionale, Promozione della cultura della legalità, Centro Storico, Europa – Cooperazione internazionale)

Michele Colajanni (CRID; Università di Modena e Reggio Emilia)

Introduzione

Gianfrancesco Zanetti (Direttore del CRID; Università di Modena e Reggio Emilia)

Coordinatore

Vincenzo Pacillo (Direttore del Dipartimento di Giurisprudenza; Università di Modena e Reggio Emilia)

Introduzione

Il tema della sicurezza in Rete è delicatissimo e lo sarà sempre più in ragione della evoluzione delle tecnologie e della loro sempre crescente pervasività, nonché della connessione perpetua alla Rete stessa. Difatti, da un lato, persone di quasi tutte le fasce di età utilizzano, direttamente e indirettamente, le nuove tecnologie, tanto che l'interazione digitale sembra talvolta preferita a quella tradizionale; dall'altro, l'*ubiquituous computing* trova una realizzazione concreta vieppiù crescente, poiché la computazione può avvenire, e sostanzialmente avviene, in qualsiasi formato, luogo (anche più o meno indefinito, come il cloud) e dispositivo (dagli smartphone agli autoveicoli, dai televisori alle lavatrici, dai dispositivi indossabili alle telecamere).

Questa evoluzione tecnologica è inarrestabile ed è guidata soprattutto da un numero relativamente modesto di grandi aziende operanti su scala mondiale: del resto, il successo della Rete è dovuto anche alla sua capillarità e all'indipendenza dalle piattaforme hardware e software.

I benefici sono noti e innumerevoli, così come i rischi. I primi e i secondi dipendono da molti fattori, fra cui la tutela della sicurezza: quando essa non è garantita, i benefici possono essere parzialmente o totalmente vanificati e i rischi crescono esponenzialmente, con conseguenze anche gravissime per i diritti e le libertà di singoli e gruppi sociali a breve, medio e lungo termine, poiché "la Rete non dimentica", o quanto meno non dimentica facilmente.

È dunque opportuno ricordare, seppur senza pretesa di esaustività in ragione della estrema ampiezza del tema di cui trattasi, quali siano i principali rischi connessi alla (in)sicurezza in Rete, distinguendo fra quelli più "tradizionali" (se così si può dire) e le nuove frontiere, per giungere poi a delineare le nuove sfide per il diritto.

Rischi e vulnerabilità

In linea generale, la rivoluzione informatica che ha portato alla nascita e allo sviluppo della "società dell'informazione" (e poi alla "società delle scatole nere" e alla "società algoritmica") comporta la necessità di garantire la sicurezza sia di ogni "strato" della Rete (fisico, logico e dei contenuti, senza addentrarsi in ulteriori suddivisioni) sia di ogni suo utente.

Da un lato, la società è sempre più "in rete" e dipende dalla infrastruttura informatica e dai dispositivi che la utilizzano, per cui bisogna proteggere le autostrade dell'informazione così come bisogna proteggere le strade "materiali" che tutti percorrono.

Dall'altro, tutte le persone, volenti o nolenti possono "finire in rete" in modo più o meno marcato (ad es., in fotografie, testi, tags, ecc.).

Tutto ciò comporta sia la nascita di nuove tipologie di rischi (che sono un portato della rivoluzione informatica) sia della evoluzione (o involuzione) tecnologica di rischi "tradizionali" (ad es., un minore può essere adescato sia off line, come in un parco, sia on line, quando utilizza un computer o uno smartphone). La realtà digitale, però, rende più subdoli alcuni attacchi: così, se una persona prova a forzare una serratura, probabilmente lascerà delle tracce fisiche; ma i costanti attacchi alle serrature immateriali potrebbero non essere percepiti da chi le subisce, e una volta forzate le serrature informatiche, è spesso possibile conoscere anche i segreti più intimi delle persone, dal momento che sono spesso custoditi in dispositivi informatici (e sovente memorizzati nel cloud, anche per impostazione predefinita dei dispositivi stessi).

Il primo rischio, si potrebbe dire, è dunque la mancanza di una adeguata alfabetizzazione informatica diffusa e di una relativa formazione permanente: le tecnologie si evolvono e i loro utilizzatori dovrebbero infatti "tenersi al passo". Ma ciò sovente non avviene e quindi si adoperano strumenti sempre più evoluti senza avere un'adeguata consapevolezza delle conseguenze del loro uso. E, come se non bastasse,

anche utenti esperti sono comunque in balìa dei fornitori di servizi e delle "scatole nere" che utilizzano, poiché non è comunque possibile avere un controllo sicuro di ciò che avviene all'interno di dispositivi tecnologici magari molto accattivanti e facili da usare, ma comunque estremamente complessi e caratterizzati da codici informatici protetti dalla normativa in materia di diritto d'autore e proprietà industriale.

Tanto premesso, si può già individuare un primo gruppo di rischi conseguenti alla insicurezza dei sistemi provocata dai rispettivi utilizzatori che non proteggono adeguatamente la propria identità informatica o dai gestori dei sistemi per falle di quest'ultimi. Si consideri, infatti, che l'immaterialità delle informazioni e l'intermediazione degli strumenti informatici agevola la sostituzione di persona e l'utilizzo, da parte di terzi, di dispositivi e servizi mediante i quali la persona opera in ambito digitale.

Un sistema informatico, infatti, riconosce un proprio utente legittimo autenticandolo attraverso qualcosa che questi conosce (ad es., nome utente e password), ha (ad es., token USB) oppure è (ad es., impronta digitale). Eppure, ancor oggi si sottovaluta l'importanza delle credenziali di autenticazione e sovente si utilizzano password deboli, come "123456" e "password", o comunque termini facilmente riconducibili all'utente; o, ancora, non le si proteggono adeguatamente, magari appuntandole su post-it attaccati sui monitor stessi; gli esempi, comunque, sono numerosissimi. Purtroppo, una condotta incauta può avere conseguenze nefaste, ma talvolta anche la massima diligenza dell'utente non basta, come nel caso di falle di sicurezza presenti nei sistemi utilizzati (o quelli comunque contenenti loro dati, indipendentemente dalla presenza di un loro account): si apre così, o quanto meno si agevola, la strada a una serie di conseguenze molto negative: l'accesso ai propri spazi digitali, che potrebbero contenere informazioni segrete e riservate la cui divulgazione potrebbe comportare discriminazioni o comunque violazioni gravissime della propria

sfera intima (ad es., foto intime o comunque dati sensibili); la commissione di truffe on line; l'esecuzione di software malevolo (ad es., i ransomware, che cifrano tutti i dati contenuti sull'hard disk dell'utente); ecc.

In secondo luogo, la questione appena accennata si connette a quella della protezione dei dati personali e alla (illusoria?) pretesa del loro controllo: in termini più ampi, alla privacy on line e off line. Difatti, il trattamento informatizzato dei dati è oramai la regola, indipendentemente dai freni che taluni legislatori cercano di imporre alle aziende private.

Dagli anni Settanta ad oggi, il numero di database è cresciuto in modo vertiginoso e questa enorme mole di informazioni è oggetto di elaborazioni sempre più sofisticate, tanto che è comune affermare che i dati costituiscono il nuovo petrolio. Si crea così una memoria digitale che, seppur frammentata in una molteplicità di database, rappresenta una versione ancora più terribile di un ipotetico *Panopticon* digitale: tutte le azioni e le parole, presenti e future, possono essere memorizzate e sottoposte a innumerevoli giudizi sia oggi sia in un futuro indefinito ed indefinibile. La sorveglianza elettronica non è oggi una semplice ed ennesima riproposizione del rapporto moderno sorvegliante – sorvegliato, poiché il controllo è oramai continuo, automatico e involontario.

Nella società dell'informazione, che diviene sempre più società della sorveglianza e del controllo, si diffondono così sistemi di videosorveglianza che sono in grado di identificare determinati soggetti o comunque di valutare le persone che si trovano di fronte; essi possono essere usati attivamente per una molteplicità di finalità, ad es. sorvegliare un negozio o un punto sensibile per individuare eventuali malintenzionati e allertare le forze dell'ordine o gli addetti alla sicurezza; rendere disponibile l'accesso a un locale, come i servizi igienici; ecc. Però essi sono spessi caratterizzati da pregiudizi e stereotipi che rischiano di colpire fasce della popolazione

già di per sé vulnerabili: così, negli Stati Uniti si è osservato un pregiudizio verso persone di colore quando questi sistemi vengono utilizzati nel contrasto alla criminalità; sistemi che consentono l'accesso a un servizio igienico a femmine o maschi discriminano le persone transessuali; ecc. A ciò si aggiunga il fatto che tutti questi sistemi elaborano dati sensibili, i cui eventuali trattamenti illeciti possono comportare rischi gravissimi per i diritti e le libertà degli interessati. Le predette tecnologie, poi, possono essere utilizzate con ancora maggiore efficacia nell'ambito di regimi totalitari.

Un terzo gruppo di rischi è, poi, conseguenza della condotta di alcune persone e colpisce soggetti esposti, di per sé, a rischi: basti pensare all'adescamento on line di minori, al cyberbullismo, al gioco d'azzardo, all'utilizzo di linguaggio violento e offensivo (giungendo all'incitamento all'odio vero e proprio), alla pedopornografia, al sexting, allo sciacallaggio on line, al *revenge porn*, ecc. Le conseguenze negative sono ovvie (ad es., un minore adescato on line potrebbe subire molestie e violenze sessuali) e in taluni casi sono aggravate dagli strumenti tecnologici, come nel caso del cyberbullismo. Difatti, gli atti di bullismo possono acquisire una diffusione amplissima (ad es., quando vengono filmati e resi disponibili on line) e la vittima può essere perseguitata sempre poiché i servizi informatici, come i social network, sono sempre disponibili (e non solo quando si trova in un determinato ambiente).

Anche l'incitamento all'odio, purtroppo, trova terreno fecondo in Rete e a farne le spese sono sovente disabili, donne, migranti, persone appartenenti a determinate etnie, ecc.; non di rado costituisce addirittura strumento – illecito – di lotta politica. Le azioni digitali, in tal senso, sono facilitate da diversi fattori, come la viralità dei social network e l'intermediazione dello strumento informatico, che in virtù della immaterialità dell'informazione digitale e della sua asincronicità agevola la deresponsabilizzazione dell'agente, unitamente alla percezione di una Rete quale Far West in cui tutto è concesso e non vi sono regole. Si giunge, in taluni casi, a una gogna

mediatica particolarmente subdola, che però non è una novità degli ultimi anni (ad es., il caso dello "Star Wars kid" risale al 2003) ma che indubbiamente può avere conseguenze sempre più gravi vista la sempre maggiore diffusione delle nuove tecnologie.

Ancora, un quarto gruppo di rischi è connesso a una evoluzione tecnologica incontrollata che può portare alla indistinzione fra realtà e virtualità: emblematico è il caso dei deepfakes, ossia delle tecniche che, a partire da fotografie o video reali, permettono di costruirne di alternativi; possono essere utilizzati, fra l'altro, in ambito politico (e generare fake news) e pornografico (spesso per danneggiare un proprio ex partner o personaggi celebri).

L'elencazione di cui sopra potrebbe continuare ancora: quanto sin qui esposto pare comunque sufficiente a introdurre un ulteriore profilo: quali sfide si pongono per il diritto nel ridurre i rischi di sicurezza soprattutto quando danneggiano ulteriormente persone già di per sé vulnerabili?

Proposte operative

Come si è visto, si può guardare alla sicurezza in Rete sia nella prospettiva dei sistemi informatici che dei loro utilizzatori. Al diritto, e dunque ai vari legislatori, spetta il difficile compito di intervenire. Tuttavia, ciascun ordinamento giuridico reagisce con estrema difficoltà alle sfide imposte dalle nuove tecnologie: la reazione è, del resto, resa più difficoltosa dalla continua commistione di aspetti informatici e non, materiali e immateriali, virtuali e reali, umani e artificiali. Essa evidenzia la complessità di un quadro in cui è necessaria una seria ed attenta opera di riflessione sulla tecnologia che la ponga quale tecnica, i cui fini non possono divenire generali: quest'ultimi, pur nella loro mutevolezza, sono stabiliti da ciascuna comunità nel rispetto dei principi e dei

valori che le danno vita e che oggi, nelle democrazie, tendono a rinvenirsi primariamente nelle loro costituzioni

La difficoltà delle sfide non deve però far rifuggire dalle stesse. Ad es., non si può condividere la prospettiva secondo cui nella società trasparente le leggi sulla privacy informatica potrebbero essere inutili poiché chi maggiormente le vìola (ricchi, potenti, forze dell'ordine, intelligence ed élite tecnologiche) avrebbe sempre un vantaggio, anche perché di norma è il diritto a rincorrere la tecnologia. Ragionando in questi termini si affermerebbe l'impotenza dei vari Stati nel tutelare il diritto alla privacy quale diritto fondamentale della persona e aumenterebbero le discriminazioni (in ragione del predetto "vantaggio"). Ciascuno Stato, invece, deve difendere la libertà "informatica", soprattutto in un'epoca in cui la cesura tra realtà materiale e virtuale si riduce progressivamente e la dimensione digitale è vissuta da un numero di persone sempre crescente; il ruolo del diritto dovrebbe essere ben più forte, al fine di guidare l'evoluzione tecnologica nel rispetto dei principi e delle libertà fondamentali.

Sono tuttavia necessari delicati interventi di regolamentazione che permettano di intervenire su alcune questioni macroscopiche: in particolare, l'attività dei prestatori dei servizi della società dell'informazione (o provider) dovrebbe essere regolata in modo specifico, abrogando normative oramai obsolete. Basti pensare che, a tutt'oggi, nell'Unione europea la responsabilità dei provider è regolata dalle leggi nazionali di recepimento della direttiva 2000/31/CE (in Italia il d.lgs, 70/2003, artt. 14-17). La tecnologia è mutata così tanto in questo periodo da imporre, più che suggerire, una modifica.

Non è questa la sede per discutere specificatamente dei contenuti di una eventuale modifica, ma sembra opportuno evidenziare una criticità specifica: la possibilità di rimuovere, in tempi rapidi e certi, determinati contenuti illeciti (es., video relativi a casi di *revenge porn*; post di incitamento all'odio; ecc.). Bisogna infatti

considerare che la sopracitata direttiva sconta una impostazione secondo cui il provider non ha mai un obbligo di monitoraggio sulle informazioni trasmesse dai destinatari del servizio, il che in linea di principio è condivisibile; tuttavia, anche se viene rimosso un contenuto illecito da un sito o servizio di hosting, questo può essere caricato successivamente da un altro utente e il provider non ha l'obbligo di impedirlo, nonostante le tecnologie odierne consentano un filtraggio efficace in alcuni casi.

Inoltre, sono necessari tempi rapidi per ottenere tutela: quelli tipici della giustizia sono del tutto inidonei. Inoltre, oggi il controllo dei contenuti viene svolto sostanzialmente dai vari prestatori, che si trovano dunque a essere i reali controllori dei contenuti stessi, ponendosi al di sopra di numerosi ordinamenti giuridici anche in forza del loro potere e della loro transnazionalità.

Vi è, dunque, una sfida delicatissima: predisporre degli strumenti efficaci che consentano di tutelare in tempi estremamente rapidi i soggetti i cui diritti vengono lesi. Non possono trascorrere mesi o anni per tutelare le vittime di cyberbullismo, diffamazione, *revenge porn*, cyberstalking, e così via, per cui è necessario studiare e implementare sistemi alternativi di risoluzione delle controversie che in tempi rapidi permettano quanto di bloccare contenuti illeciti ed evitarne la riproposizione, mentre la giustizia farà il suo (lento) corso. Non si può pensare di affidare la tutela di soggetti vulnerabili a soggetti privati, guidati dalla logica del profitto e non certo dal rispetto delle minoranze, se non quando imposto dalla legge… o dal mercato. I diritti, però, non possono essere lasciati all'arbitrio del mercato.

Quindi alcune fattispecie specifiche devono essere regolamentate in modo preciso e puntuale; non bisogna però perdere di vista l'importanza di una riflessione informatico-giuridica più ampia, finalizzata stabilire i limiti del percorso che la tecnologia e, soprattutto, l'intelligenza artificiale dovranno seguire nella loro inarrestabile opera di pervasione della società. Questa riflessione è necessaria:

l’interconnessione di prodotti e servizi intelligenti è gradualmente in crescita e pone le basi per una vera e propria rivoluzione che si realizzerà compiutamente quando le tecnologie saranno più mature e disponibili su una scala ancora più larga nei vari settori di riferimento.

Non a caso, specifici aspetti dell’evoluzione tecnologica (fra cui le possibilità di delocalizzazione del cloud computing, l’evoluzione della robotica industriale, l’accesso costante al web, l’analisi dei Big Data) suggeriscono che si possa giungere a una nuova tipologia di *enhancement* tecnologico quale potenziamento delle capacità di un individuo mediante una tecnologia portabile e diffusa, che tuttavia è anche tanto pervasiva da rendere l’individuo medesimo del tutto dipendente da essa, con una prevalenza dell’ambito artificiale su quello naturale.

BIBLIOGRAFIA

Benkler Y.,

2016, *Degrees of Freedom, Dimensions of Power*, in «Daedalus», fasc. 1, pp. 18-32.

Brighi R.,

2017, *La vulnerabilità nel cyberspazio*, in «Ars Interpretandi», fasc. 1, pp. 81-94.

Brighi R., Di Tano F.,

2019, *Identità, anonimato e condotte antisociali in Rete. Riflessioni informatico-giuridiche*, in «Rivista di filosofia del diritto», fasc. 1, pp. 183-204.

Brin D.,

1999, *The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?*, Basic Books, New York.

Casadei Th.,

2018, *La vulnerabilità in prospettiva critica*, in Giolo O., Pastore B. (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Carocci, Roma, pp. 73-99.

Durante M.,

2015, *Sicurezza e fiducia nell'età della tecnologia*, in «Filosofia politica», 2015, fasc. 3, pp. 439-458.

Fioriglio G.,

2016, *Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione*, in «Rivista elettronica di Diritto, Economia, Management», fasc. 3, pp. 22.

Orofino M., Pizzetti G.F. (a cura di),

2018, *Privacy, minori e cyberbullismo,* Giappichelli, Torino.

Lanzillo M.L.,

2018, *Lo stato della sicurezza. Costituzione e trasformazione di un concetto politico*, in «Ragion pratica», fasc. 1, pp. 9-28.

Lillà Montagnani M.,

2018, *Internet, contenuti illeciti e responsabilità degli intermediari,* EGEA, Milano.

Mayer-Schönberger V.,

2011, *Delete. The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton-Oxford.

Pasquale F.,

2015, *The Black Box Society. The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge (MA)-London.

Pizzetti F.,

2018, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino.

Rodotà S.,

2014, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari.

Sartor G.,

2016, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino.

Vantin S.,

2018, *L'eguaglianza di genere tra mutamenti sociali e nuove tecnologie. Percorsi di diritto antidiscriminatorio*, Pacini, Pisa.

Verza A.,

2017, *Aggredire attraverso l'immagine. Cristallizzazioni tecnologiche, genere e diniego di tutela nella logica disciplinante neoliberale*, in «Ragion pratica», fasc. 2, pp. 467-492.

Zanetti, G.,

2019, *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*, Carocci, Roma.

Ziccardi G.,

2015, *Internet, controllo e libertà: trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, Milano.

Ziccardi G.,

2019, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, Milano.