PRIVACY DIGITALE E GOVERNO DELLA TECNICA

FRANCESCO ROMEO
UNIVERSITÀ DI NAPOLI 'FEDERICO II'

i-lex

i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale
Rivista quadrimestrale on-line: www.i-lex.it

PRIVACY DIGITALE E GOVERNO DELLA TECNICA

Francesco Romeo

Abstract: Il lavoro affronta il tema della effettività della normative sulla privacy in un ambiente sovrastato dalle tecniche di informazione e comunicazione digitali. Un rapido excursus sulle premesse poste nella dottrina giuridica agli inizi di tali tecnologie permette di constatare il parziale fallimento dei tentativi di disciplinare le tecniche IC. Si cerca quindi di individuare le cause che hanno condotto a questo stato di ineffettività della normative basata su tecniche tradizionali di normazione. Si individuano alcune caratteristiche critiche delle tecniche IC in relazione alle caratteristiche del dato e della informazione digitali. Si evidenziano brevemente i pericoli per lo Stato di diritto posti da questi mutamenti tecnologici. Viene quindi analizzata parte del Regolamento Generale sulla Protezione dei Dati, che introduce la c.d. protezione by design. Si analizzano brevemente le condizioni entro le quail sarà possible ristabilire effettività di protezione.

Parole chiave: privacy, diritto e tecnica, privacy by design, legal protection by design

1. Una disciplina diversa: il design giuridico della tecnica

In questo scritto[1] intendo occuparmi della possibilità di superamento delle gravi problematiche di effettività[2] che hanno riguardato,

[1] Riprendo e approfondisco quanto in parte elaborato nei due articoli *Il limite dei diritti e la forza del diritto. I. La privacy mancata a vent'anni dalla legge 675/96,* e *II. Le metaregole della tecnica: Legal Protection by Design,* pubblicati su *Diritto, Economia e Tecnologie della Privacy*, rispettivamente VI, 1, 2016, p. 27 ss., e VI, 2-3, 2016, p. 139 ss.

[2] Il lemma 'effettività' è qui usato nel senso indicato da Pietro Piovani, ma anche da Hans Kelsen - peraltro citato dallo stesso Piovani -, come principio in base al quale "l'ordinamento sussiste se nel suo seno si compiono regolarmente gli atti umani, individuali, che il principio di effettività presenta come prova dell'esistenza della comunità: gli uomini ordinano l'ordinamento col loro ordinato comportamen-

Pubblicato il 3 Novembre 2017

fin dalla sua nascita in Italia, e tutt'ora riguardano, il diritto alla riservatezza o anche alla privacy. In particolare, intendo affrontare il punto dell'effettività della legge in riguardo alla tecnologia IT ed alla digitalizzazione. Proprio su questi temi il Regolamento Generale sulla Protezione dei Dati UE 2016/679 (RGPD)[3] sembra aver introdotto alcune novità di rilievo che intendo discutere.

Una corretta analisi dell'effettività non può non tener conto di un insieme complesso di aspetti di tutela del cittadino europeo, in una Unione fondata sui principi dello Stato di diritto, ma, naturalmente, l'analisi deve prendere le mosse da ciò che il regolamento stesso pone come fini da raggiungere ed interessi da proteggere.

L'effettività delle norme non è un piano di ricerca sul quale la tradizionale impostazione normativista si sia sentita coinvolta, anzi, il normativismo confina la ricerca giuridica lontano dagli orizzonti della effettività: una norma *deve essere*, la sua violazione è connaturata al suo *dover essere,* una norma priva di possibilità di violazione non sarebbe una norma giuridica, ma una legge di natura. Così, giudizi *sociologici* quali quello di adeguatezza delle regole rispetto ai fini da esse stesse posti, oppure indagini empiriche quali la verifica della consistenza rispetto alla materia da trattare, sono stati trascurati e gli effetti sono oggi palesi: la nostra privacy è scomparsa, insieme all'apparire della normativa a sua tutela. Tanto più la normativa si faceva, via via, articolata e strutturata, tanto più scompariva la nostra possibilità di serbare, mi si accetti la metafora – ma vedremo che è meno di una metafora -, noi solo per noi, o per chi da noi scelto.

Come mai abbiamo perso la nostra riservatezza? I giuristi si affannano attorno a sempre nuove ed affinate normative, ma siamo sicuri che abbiano capito il perché del fallimento delle normative pre-

---

to, che risulta dalle loro quotidiane azioni, le quali manifestano i bisogni che implicano ed alimentano le idee umane che fanno la storia". P. Piovani, voce *Effettività*, in *Enciclopedia del diritto*, XIV, Giuffrè, Milano, p. 431. Ricordo una pagina di Hans Kelsen, 'rimossa' dalla dottrina italiana, in cui l'autore indica la "desuetudine" come fonte abrogatrice di norme: H. Kelsen, *La dottrina pura del diritto*, III ed., Einaudi, 1975, p.242 s. Peraltro, per l'autore praghese un ordinamento non effettivo non esiste come ordinamento giuridico.

[3] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

cedenti? Senza questa comprensione, c'è una buona probabilità che anche la nuova normativa fallisca. Incombe lo spettro di Sisifo.

Tenuta presente la tecnica normativa del legislatore unitario, che enuncia esaurientemente fini, valori e interessi in una premessa all'articolato composta di 'considerando', la corretta interpretazione del regolamento deve collegare ad essi le singole disposizioni. I considerando sono la teleologia normativa, vale a dire l'insieme di valori sui quali misurare le regole - nonché di fini, al raggiungimento dei quali l'applicazione delle regole deve tendere. La valutazione dell'adeguatezza in relazione all'effettività della misura va quindi stimata relativamente anche ai considerando del RGPD.

Il Regolamento non è rivolto direttamente a disciplinare la privacy, la privacy non viene mai nominata nel Regolamento, la sua tutela deriva indirettamente dalla protezione del dato. Il RGPD tuttavia rinvia, nel considerando 173, alla Direttiva sulla vita privata 2002/58/CE [4].

Il Regolamento introduce al comma 1 dell'articolo 25, sotto la rubrica *"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita",* la recente categoria elaborata in dottrina ed in sede applicativa, della Privacy by Design (PbD)[5]e della più ampia Legal Protection by Design (LPbD)[6].

[4] "Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (GU L 201 del 31.7.2002, pag. 37)".

[5] Sull'origine del concetto vedi P. Hustinx, *Privacy by design: delivering the promises*, in *Identity in the Information Society*, 3, 2, p. 253 ss. Vedi inoltre: M. Langheinrich, *Privacy by Design - Principles of Privacy – Aware Ubiquitous Systems,* in *Proceedings of the 3rd International Conference on Ubiquitous Computing,* Springer, 2001, p. 273 ss.; S. Gutwirth, *Privacy and the Information Age*, Rowman&Littlefield, Lanham MD, 2002; L. Floridi, a cura di, *Protection of Information and the Right to Privacy - A New Equilibrium?*, Dordrecht, Springer, 2014; M. Hildebrandt, L.Tielemans, *Data Protection by Design and Technology Neutral Law,* in *Computer Law & Security Review,* 29, 5, 2013, p.509 ss.; B. Masiello, A. Whitten, *Engineering Privacy in an Age of Information Abundance*, in *AAAI Spring Symposium: Intelligent Information Privacy Management*, 2010, scaricabile on line.

[6] La LPbD basandosi sullo stesso principio di normazione by design, si estende ad ogni aspetto di confronto tra tutela giuridica e tecnica, così, ad esempio, al data protection.

> "1. *Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati"*

La protezione 'by design' comporta che i requisiti e le esigenze legali vengano tradotti in un requisito tecnico o operativo che realizzi l'effettività delle regole giuridiche. Nell'ultimo paragrafo approfondiremo le due categorie sopra menzionate.

È agevole notare che neppure l'art. 25 accenna direttamente alla privacy, che resta quindi uno dei tanti diritti tutelati tramite la protezione del dato, ma non posto o tutelato direttamente nel RGPD. Invece è il dato, nell'impostazione del RGPD, la chiave di volta per la tutela dei "diritti degli interessati", presumibilmente a riguardo sia degli interessi economici che della tutela della persona, ivi compresa la privacy.

Il RGPD non definisce direttamente il dato, bensì il dato personale. L'articolo 4 definisce il dato personale come un'informazione riguardante una persona fisica identificata o identificabile ("interessato")[7], proseguendo in una, culturalmente diffusa, ambiguità semantica che la teoria dell'informazione ha sin dalle origini chiarito. L'ambiguità è anche un'inutile duplicazione e consiste nell'usare in-

[7] "*Articolo 4. Definizioni. Ai fini del presente regolamento si intende per: 1) 'dato personale': qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"

differentemente i due lemmi nel medesimo significato senza differenziarli: nel regolamento il dato è un'informazione, quindi non è possibile che esistano dati che non siano anche informazione.

Non rientra in alcun modo nella definizione il ruolo del trattamento per la trasformazione dei dati in informazione. Eppure detto ruolo è di primaria importanza ed il Regolamento stesso si preoccupa di disciplinarlo. Nella realtà, il trattamento dei dati li trasforma, da esso nasce qualcosa che non è contenuta direttamente nella molteplicità isolata dei dati: l'informazione è il frutto del trattamento dei dati e dal tipo di trattamento dipende la valutazione dell'azione di colui che tratta i dati ai fini della determinazione della eventuale responsabilità. A supporto e dimostrazione di quanto detto sta la articolata normativa del Regolamento in merito ai tipi di trattamento ed ai soggetti titolari o responsabili di esso.

Nonostante la definizione normativa, nell'uso fattone dal Regolamento il lemma 'dato' assume sempre il significato di *entità da trattare per ottenere informazione*. In parte, e tacitamente nei fatti, abbiamo un avvicinamento alle definizioni di dato ed informazione elaborate in ambito di teoria dell'informazione ed in informatica[8]. Forse proprio per questo uso del lemma, nonostante la definizione, nel Regolamento può essere ravvisato il primo *statuto europeo dell'informazione,* una regolamentazione completa della circolazione dei dati e della creazione, protezione e sfruttamento dell'informazione.

Il Regolamento enuncia anzitutto nei considerando, ed alle volte nell'articolato stesso, un ordine di scopi, valori, interessi e limiti volti a chiarire interpretativamente il significato delle disposizioni. Un'analisi quantitativa del peso digitale dei considerando rispetto all'articolato può forse convincere sulla loro non inutilità: gli articoli ed i considerando non si discostano di molto come peso digitale. Il

[8] La definizione venne proposta da C. E. Shannon, ma l'accoglienza in ambito filosofico non fu delle migliori, e la portata della proposta venne limitata all'ambito informatico; oggi è divenuta il punto di riferimento in ogni campo che studi il fenomeno dello scambio o della redazione di messaggi. A partire dalla definizione di Shannon, e sulla sua base, sono state avanzate diverse proposte di definizione valida in ogni disciplina, vedi per tutti: R. M. Losee, *A Discipline Independent Definition of Information*, in *J. of the American Society for Information Science*, 48, 3, 1997, p. 254 ss. vedi F. Romeo, *Lezioni di logica ed informatica giuridica*, Giappichelli, 2012, p. 39 ss.

RGPD si suddivide in 173 considerando e 99 articoli, in un file .txt i considerando pesano 170.251 byte, formati da 24.023 parole, 145.221 caratteri spazi esclusi e gli articoli pesano 206.851 byte, formati da 30.608 parole composte da 174.720 caratteri spazi esclusi.

Dato il peso dei considerando, si può affermare con buona probabilità di successo, che quanto escluso da essi non rientri nell'ordine valoriale del Regolamento.

I considerando sono in parte costituiti da enunciati descrittivi, non normativi, rappresentando a mo' di saggio scientifico non tanto le possibili fattispecie concrete ma la realtà che richiede l'intervento normativo ancor prima di quello applicativo. Agli enunciati descrittivi sono collegati alle volte enunciati quasi-normativi, che, invece di obblighi, pongono semplici auspici, con gli aggettivi "auspicabile" o "opportuno", come, in via esemplificativa, nei considerando 7, 9, 14, 19, 20, 22, 24, 26. Gli enunciati quasi-normativi pongono, invece di regole, apprezzamenti di valore, stabilendo gradazioni di preferenze verso le quali deve indirizzarsi l'interpretazione delle regole nella loro valutazione teleologica; in modo oggi un poco desueto in dottrina, questi enunciati potrebbero venire ascritti a quella che nell'articolo 12 delle nostre disposizioni preliminari viene anche chiamata "intenzione del legislatore".

I primi due considerando mettono subito in evidenza il perno della normativa, la sua teleologia giuridica, e gli interessi in conflitto:

> *"(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. [...]*
>
> *(2) [...] Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche".*

I due poli tra i quali si sviluppa la dialettica sono costituiti dal diritto fondamentale alla tutela della persona per ciò che riguarda i dati

personali[9], da una parte, e dalla libertà economica in quanto fonte di progresso economico e sociale, dall'altra. Il Regolamento non sembra porre le due istanze su di un medesimo piano. Piuttosto, la protezione della persona, con riguardo al trattamento dei dati di carattere personale, appare essere il centro verso il quale non può non rivolgersi la teleologia dei principi e delle norme poste a tutela della libertà economica, dei relativi diritti e libertà fondamentali, in particolare del diritto alla protezione dei dati personali, realizzando *"uno spazio di libertà, sicurezza e giustizia"* e *"un'unione economica"*, contribuendo *"al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche"*.

Questa teleologia delinea il campo, o meglio traccia i confini entro i quali deve realizzarsi la tutela suddetta, confini lungo i quali avvengono il confronto degli interessi ed i possibili conflitti. Nel nostro caso, ferma restando la tutela della persona, lo spazio entro il quale essa deve realizzarsi è determinato da un lato dalle *libertà fondamentali* dell'individuo e dall'altro dal *progresso economico-sociale*, dal *rafforzamento economico* e dalla *convergenza delle economie nel mercato interno.* È di tutta evidenza che la libertà di iniziativa economica si trova a confrontarsi non solo con la tutela della persona fisica, ma anche con gli interessi dell'intero gruppo sociale.

Questa è una linea di possibile grave attrito: gli interessi economici, specialmente se qualificati a livello sociale e con una direzione di crescita ed espansione - ma su questo occorrerà tornare -, non sempre potranno trovarsi in accordo con gli interessi individuali alla tutela delle libertà fondamentali individuali e realizzazione delle istanze inalienabili di sicurezza e giustizia. Anzi, spesso, le esigenze sociali di rafforzamento economico potranno fungere da soppressore delle libertà, anche economiche, individuali. In particolare, i cambiamenti introdotti dalla informatizzazione e dalla digitalizzazione dell'ambiente sociale umano hanno introdotto nuove tipologie di comportamenti e nuovi beni, in cui si manifesta, o viene facilitata, in modo spesso subdolo o nascosto, tale soppressione.

[9] Citando, come normativa di riferimento l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea.

La posizione di limiti giuridici al trattamento dei dati presuppone la possibilità del trattamento - che resta quindi lecito per default -, inoltre la tutela del dato personale, impostata nell'orizzonte di una tutela degli interessi economici pubblici verso la crescita economica, si contrappone alla possibilità giuridica di separazione definitiva di uno spazio dell'individuo escluso dal rapporto con l'altro, richiedendo invece una continua commisurazione di interessi pubblici con interessi individuali. La tutela della persona in riguardo ai dati personali trova quindi in questi due punti una forte limitazione. Del resto, su questo il RGPD non fa altro che continuare sulla linea dei precedenti regolamenti e direttive. Il diritto ad essere lasciati soli non è, fin dall'impostazione di Warren e Brandeis[10], il diritto alla solitudine, alla non socialità, non riguarda l'individuo fisicamente inteso, ma la sua rappresentazione, l'informazione su di esso, meglio, la regolamentazione della circolazione dell'informazione su di esso: dato, informazione e privacy sono indissolubilmente connessi, ma non nella persona fisica, quanto piuttosto nella sua rappresentazione culturale e sociale.

Sembra quindi ripetersi l'impostazione data alla normativa negli anni Ottanta, anche se, rileggendo le discussioni di quegli anni, era proprio una società come l'attuale ed una mancanza di privacy come l'attuale ciò contro cui si intendeva rivolgere tale normativa. Gli scudi della riservatezza e della privacy vennero alzati proprio contro gli attuali esiti della libertà di trattamento dei dati. Certamente, se all'epoca ci fossimo immaginati una società come l'attuale, avremmo pensato ad una normativa diversa, capace di mantenere il livello di privacy dell'epoca. Sarebbe però stato necessario immaginare lo sviluppo tecnologico, che all'epoca non era prevedibile, e sarebbe stato necessario comprendere appieno la realtà digitale. Così non è stato, pur tuttavia, anche se il regolamento sembra perseverare in alcuni errori di fondo, l'articolo 25 inserisce un importante cambiamento, che sarà destinato senza dubbio a notevoli applicazioni giurisprudenziali, prevedendo nuovi tipi di responsabilità per le imprese IT e non solo.

L'articolo 25 introduce l'obbligo, a carico del titolare del trattamento, di verificare la *adeguatezza* ed *efficacia* delle misure adottate,

[10]S. D. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 4, 5. 1890, p. 193 ss.

facendo sì che tali misure prevedano la protezione fin dal momento della determinazione dei mezzi del trattamento. Pur con tutte le limitazioni previste nell'articolo, l'obbligo fa sorgere una responsabilità nei casi in cui il titolare stesso non si sia preoccupato di curare gli aspetti di adeguatezza ed efficacia in relazione allo stato della tecnica. Sembra risolversi così il problema dei continui cambiamenti tecnici elusivi di normative puntuali, demandando al titolare del trattamento stesso l'obbligo di aggiornamento tecnico in ragione della adeguatezza ed efficacia della protezione.

L'articolo 25 è una norma elastica, destinata, in futuro, ad una prima applicazione probabilmente restrittiva ed in seguito a fungere da perno per l'introduzione nell'ordinamento dell'Unione del principio della LPbD; ci troviamo quindi ad analizzare un passaggio dalle garanzie procedurali giuridiche a quelle tecniche giuridicamente supervisionate.

Non si tratta di un passaggio di consegne diretto a trasferire forza normativa dalla tutela giuridica a quella tecnica, quanto, piuttosto, leggendo l'articolo 25 nell'insieme delle disposizioni del RGPD, di un abbandono di alcuni presupposti teorici di separatezza tra regole di diritto e regole tecniche[11]. Il pur cauto cambiamento di orientamento va accolto con ampio favore, essendo possibile individuare all'interno della tradizionale impostazione normativista, come già evidenziato, una delle principali cause della scarsa effettività raggiunta dalle regole giuridiche nel rapporto tra IT e privacy.

2. La metamorfosi: dallo Habeas Data alla persona digitale

Il diritto alla riservatezza è un diritto di recente acquisizione nel nostro ordinamento, viene introdotto nell'ultimo quarto del ventesimo secolo, ma la sua storia è forse tra le più frequentate in ambito giuridico. Rammento brevemente alcuni passi importanti per la successiva analisi.

[11] R. D'Orazio, *Protezione dei dati by default e by design*, in S. Sica, V. D'Antonio, G.M. Riccio, (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver, 2016, p.108.

Ancora nel 1963 con il 'caso Petacci' la Corte di Cassazione ribadiva l'assenza di un autonomo diritto alla riservatezza nell'ordinamento italiano [12], sebbene, questa volta, sentendo "l'esigenza" di una tutela, la Suprema Corte superava lo scoglio dogmatico con un artifizio interpretativo, configurandola come tutela delle modalità di esplicazione, "manifestazione concreta" del diritto assoluto di personalità[13].

Nel 1978 scriveva Stefano Rodotà: "ai dipendenti di un'impresa romana di costruzioni è stato sottoposto un elenco di 502 domande. Vi si domanda, tra l'altro, se credono in Dio, soffrono di stitichezza, fanno sogni di argomento sessuale, temono d'essere spiati, sono attratti dalla carriera militare, hanno letto con piacere la storia di Cappuccetto rosso. I sindacati e il partito radicale hanno protestato, chiedendo alla magistratura di far cessare questa indagine lesiva della personalità dei dipendenti e contraria allo statuto dei lavoratori[14]". Proprio lo statuto dei lavoratori introduceva per primo [15], nell'ordinamento italiano, una esplicita previsione riguardante la riservatezza, siamo nel 1970 e con la legge 20/05/70 n. 300 all'articolo 8 viene sancito il divieto di indagini sulle opinioni politiche sindacali o religiose del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

La norma fu anche un utile grimaldello per scardinare definitivamente l'impianto dommatico della tipicità dei diritti della personalità e nel 1975 la Corte di Cassazione, nella cd. 'sentenza Soraya', seguendo le istanze presentate in gran numero dalla giurisprudenza di merito, riconosceva definitivamente il diritto alla riservatezza come consistente "nella tutela di quelle situazioni e vicende strettamente

[12] "Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto *erga omnes* alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza."Cass. 20, 04, 1963, n. 990, in *Foro It.* 1963, I, c. 877 e c. 1298, con nota di A. De Cupis, dal significativo titolo *Riconoscimento sostanziale, ma non verbale, del diritto alla riservatezza*.

[13] Vedi in merito G. Giampiccolo, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1958, p. 458 ss.

[14] S. Rodotà, *Alla ricerca delle libertà*, Il Mulino, 1978, p. 99.

[15] L'osservazione è dello stesso Rodotà, *ivi*, p. 101.

personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti".

È degno di nota il fatto che un diritto dallo sviluppo normativo così impetuoso, nasca dall'opera della giurisprudenza e non da quella del legislatore. Ancor più degno di nota è il fatto che, per introdurre una tutela giuridica a casi fino ad allora non rilevanti per l'ordinamento, i giudici della Suprema Corte abbiano fatto ricorso ad un tipo di interpretazione che ha nettamente trascurato il dato letterale: "*Scire leges non est verba earum tenere, sed vim ac potestatem*"[16].

Da quel momento la tutela della riservatezza seguirà una continua ed esponenziale crescita, sia giurisprudenziale che istituzionale e legislativa.

È lecito interrogarsi sulle cause di un simile cambiamento di orientamento: ciò che si riteneva non giuridicamente tutelabile, improvvisamente diviene uno dei settori di maggior intervento giuridico.

All'epoca della sentenza Soraya era cambiato molto nella tecnologia, ad esempio con l'introduzione dei teleobiettivi zoom in fotografia e dei registratori portatili; contemporaneamente, la diffusione dei mass-media, quali ad esempio la televisione, permetteva una diffusione della notizia a gruppi sempre più estesi di individui, è proprio la Corte di Cassazione che rileva il cambiamento delle relazioni sociali in seguito al mutamento tecnologico. Ma è con la diffusione capillare dei computer, con la riproduzione-rappresentazione di tutta la realtà e della cultura stessa in formato digitale che la tutela della riservatezza, minacciata dalla raccolta di dati personali in sempre più capienti banche dati, si allarga alla tutela del dato personale, e trova la grande sfida della tecnologia al diritto. La riservatezza diviene un interesse da tutelare giuridicamente nel momento in cui la tecnologia distrugge i limiti naturali all'irrompere sociale nella vita degli individui. Molto doveva cambiare, ci si trovava all'alba di un cambiamento epocale

[16] Citazione, in riferimento a Celso, L 17 Dig. de leg., della Cass. 27, 05, 1975, n. 2129 detta *sentenza Soraya* in *Foro It.*, 1976, I, c. 2904. Una interessante indagine teorica sarebbe offerta dall'approfondimento degli argomenti della Corte, che appaiono di tipo analogico, anche se la Corte stessa lo nega recisamente.

che solo pochi giuristi all'epoca intravidero, seppur ammantato dalle nebbie del futuro.

È infatti con l'introduzione di sistemi artificiali che elaborano anche autonomamente i dati ed intervengono su di essi e sulla realtà, trasformandoli e generando informazioni sugli individui, che le banche dati si trasformano in banche di significati a riguardo della vita e della personalità degli individui, oramai conosciuti ben oltre i limiti dell'ingenuo questionario dell'azienda romana degli anni settanta. È con l'introduzione di Internet che le possibilità di controllo della vita privata dell'individuo, spionaggio ed intromissione nelle personalità individuali, perde i limiti spaziali del vicinato, valicando ogni luogo ed ogni confine.

Espongo schematicamente i fenomeni principali dei quali occorre tener conto nella indagine; di questi tre riguardano lo sviluppo socio-tecnico, tre le caratteristiche inerenti al rapporto diritto-tecnologia digitale, quattro i fenomeni strettamente giuridici e tre quelli sociali.

In merito ai primi tre, essi caratterizzano lo sviluppo socio-tecnico negli ultimi venti anni. Il primo è costituito dalla potenzialmente totale capacità riproduttiva della realtà, in ambiente virtuale, offerta dalle tecniche basate su dati digitali, ivi compresa la realtà attinente alla persona, il secondo è costituito dal gigantesco aumento della raccolta dati personali, ed il terzo è costituito dall'aumento e diffusione della possibilità di comunicazione di detti dati. Al grandissimo aumento della possibilità di comunicazione e interazione tra individui corrisponde l'annullamento della distanza, ogni minaccia alla riservatezza diventa potenzialmente compresente.

Le tappe della tecnologia informatica segnarono anche le tappe della progressiva perdita di controllo dell'individuo sulla circolazione delle informazioni a riguardo della propria vita privata e della propria persona. Può lasciar sorridere, ma oggi qualsiasi cittadino, per quanto 'borghese piccolo piccolo' possa essere, è conosciuto globalmente, profilato, consigliato, controllato. Già è così, ma la tecnologia informatica è destinata ad ampliare questa possibilità di vita sociale per l'essere umano. Fin dall'inizio dell'era digitale si discuteva di questa che, allora, appariva solo come una possibilità, particolarmente con-

siderando gli Stati ed i sistemi di intelligence[17], e con il progredire delle discussioni si affermava il motto 'sicurezza richiede sorveglianza'. In seguito la possibilità divenne realtà[18]. Oggi la sorveglianza è amplificata ed ingigantita, ma siamo solo alle porte di quel cambiamento che, si prevede, muterà alcune delle più radicate abitudini della socialità umana, l'introduzione dello Internet of Things (IoT). Stiamo entrando in una società in cui non solo gli esseri umani comunicheranno tra loro, ma anche le cose, raccogliendo dati processandoli e comunicandoli. Qui, l'ubiquitarietà della raccolta dati e della sorveglianza travalica ogni possibilità di controllo ed esclusione da parte dell'individuo. Diventa pressoché impossibile isolarsi, distinguere la propria vita privata da quella pubblica, separare i propri frammenti di vita da quelli degli altri. Gli onnipresenti sensori degli oggetti rileveranno e processeranno continuamente i dati dell'individuo in ogni suo momento della giornata[19]. Il collegamento Internet e cloud permette

[17] Per la discussione a livello politico-legislativo si possono consultare gli istruttivi *Congressional Records Senate: The Computer and Individual Privacy*, 113, Special Print, 8 marzo, 1967; *Computers and Individual Privacy*, 115, Special Print, 10 novembre, 1969; *Computers, Data Banks and Constitutional Rights*, 116, Special Print, 3 Febbraio, 1970, nonché la Note della *Harvard Law Review, Privacy and Efficient Government: Proposals for a National Data Center*, 82, 1968, p. 400 ss., con il punto della situazione a quella data ed una esauriente indagine di dottrina; in letteratura all'origine della discussione sulla sorveglianza e computers vedi D. N. Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, The George Washington Law Review, 33, 1964, p. 270 ss.; W. F. Murphy, *Wiretapping on Trial: A Case Study in the Judicial Process*, 1965; A. F. Westin, *Science, Privacy and Freedom: Issues and Proposals for the 1970's*, Part I, *The Current Impact of Surveillance on Privacy*, *Columbia Law Review*, 66, 1966, p.1003 ss.; A. F. Westin, *Science, Privacy and Freedom: Issues and Proposals for the l970's*, *Part II Balancing the Conflicting Demands of Privacy, Disclosure and Surveillance*, p.1205 ss.; A. R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, in *Michigan Law Review*, 16, 1969, p. 1901 ss.; J. M. Rosenberg, *The Death of Privacy*, 1969; A. F. Westin, *Information Technology in a Democracy,* Cambridge Mass., 1971.

[18] Tra le moltissime pubblicazioni in materia vedi on-line D. Lyon, *The World Wide Web of surveillance: The Internet and off-world power-flows*, in *Information Communication and Society*, 1998, p.32 ss.; di David Lyon tradotto in italiano vedi: *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Milano, 2002.

[19] Vedi lo studio *Don't Panic. Making Progress on the 'Going Dark' Debate* del Berkman Center for Internet & Society at Harvard University, 1, 2, 2016. In questo studio si paragona l'attuale offerta di hardware con possibilità di comunicazione criptata, in modo da renderne impossibile l'intercettazione (going dark) con la

l'operare 'smart' dell'apparecchio dotato di sensori. Esso è indispensabile per le grandi capacità di calcolo e memoria, necessarie per realizzare le prestazioni 'smart', infatti, perché questo avvenga, i dati devono essere trasferiti, o meglio, duplicati, in un elaboratore con capacità di calcolo adeguate. Lo IoT entra nelle case e, direi, nei vestiti del cittadino, ne registra le conversazioni e le comunica in rete, ne verifica i movimenti quotidiani, le 'cose' potranno ascoltare i problemi dell'utente, consigliarlo, dirigerlo, insomma facilitargli la vita. Certo, siamo alle prime applicazioni, ma già ne abbiamo parecchie[20].

Saranno vite senza privacy quelle dei cittadini comuni e una vita di poco valore quella del 'borghese piccolo piccolo': sulla via del consumo, definitivamente soggiogato dalla lavapiatti.

Nonostante il grande influsso in dottrina dell'articolo di Warren e Brandeis[21], e nonostante il fatto che in esso veniva da subito correttamente evidenziato il legame tra perdita della privacy e possibilità di riproduzione e comunicazione dell'informazione, tale rapporto viene spesso mal compreso; ad esempio, si tende a generalizzare l'influsso a tutta la tecnologia[22], mentre la chiave di volta del cambiamento è

possibilità di sorveglianza offerta dallo IoT: "A plethora of networked sensors are now embedded in every day objects. These are prime mechanisms for surveillance: alternative vectors for information-gathering that could more than fill many of the gaps left behind by sources that have gone dark – so much so that they raise troubling questions about how exposed to eavesdropping the general public is poised to become." op.ult. cit. p. 13.

[20] "In February 2015, stories surfaced that Samsung smart televisions were listening to conversations through an on board microphone and relaying them back to Samsung to automatically discern whether owners were attempting to give instructions to the TV. A statement published in Samsung's privacy policy instructed users to "be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of the Voice Recognition. (Samsung, Samsung Privacy Policy – SmartTV Supplement, http://www.samsung.com/sg/info/privacy/smarttv.html" Tratto da *Going Dark* cit. p.14.

[21] S. D. Warren, L. D. Brandeis, *The Right to Privacy*, cit.

[22] Qui di seguito un esempio di questa posizione piuttosto superficiale proveniente da un autorevole studioso: "the history of privacy is deeply intertwined with the history of technology. A wealth of scholarly literature tracks and demonstrates how privacy as a normative concept has evolved in light of new information and communication tecnologies since the early modern period, when face-to-face interactions were challenged by urbanization and the rise of mass communication. In the beginning of the nineteenth century, a combination of societal changes, institu-

stata l'evoluzione delle tecniche di riproduzione e comunicazione dell'informazione, alle quali si aggiunge oggi la possibilità di riduzione ad informazione di tutta la mente umana.

Tre caratteristiche *tecnologiche* essenziali delineano i contorni del problema giuridico-informatico.

La prima riguarda il potenziale diffusivo del dato digitale, trasmissibile a qualsiasi distanza, identico in ogni sua riproduzione, fruibile senza essere consumato o distrutto, facilmente occultabile: queste caratteristiche sono anche quelle della informazione e dei significati da esso o tramite esso descritti, memorizzati ed elaborati. La digitalizzazione rende evanescente il confine, tracciato dalle sentenze dell'ultima metà del secolo scorso, tra notizia riguardante la vita privata e notizia di rilevante interesse pubblico. Il destinatario della informazione non è più colui che viene designato come tale da chi dà l'informazione, ma chiunque, anche chi, assolutamente estraneo, non è neppure spazialmente né temporalmente presente;

La seconda caratteristica riguarda la possibilità di cumulare enormi quantità di dati trasformandoli in informazioni complesse, riproducibili in infiniti esemplari identici e conservabili all'infinito, che significa anche 'presenza continua', possibilità di essere usati in ogni momento. È una possibilità conseguente alla immaterialità del dato digitale ed alla tecnologia digitale, limitabile ma non eliminabile dall'intervento giuridico, se non eliminando o cambiando la tecnica informatica;

La terza caratteristica riguarda la possibilità di generare informazione nuova dalla combinazione di altra informazione: ogni elaborazione di dati digitali genera informazione che a sua volta può essere elaborata in ulteriore informazione. Tutto il mondo digitale è autocompatibile, e componibile in una continua elaborazione di nuove informazioni, con soli procedimenti di calcolo e combinazione.

---

tional developments, and technological advancements gave birth to a series of new threats to privacy. At the time, innovative technologies – including telegraph communications and portable cameras – were among the key drivers (interacting with other factors, such as in create literacy rates) that led to growing concerns about privacy protection." U. Gasser, *Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy*, in *Harv. L. Rev. F.,* 130, 2016, p. 61; vedi anche D. Vincent, *Privacy: a Short History*, Polity, 2016.

La maggior parte dei cambiamenti sociali avvenuti dopo l'avvento dell'era digitale sono conseguenza diretta della digitalizzazione. Così è per la globalizzazione, ad esempio, ma così è anche per la progressiva perdita di controllo dello Stato sulle attività giuridicamente rilevanti sul suo territorio sovrano. È stata la mancanza di territorialità di Internet a generare una perdita del potere di controllo dello Stato[23]. Internet non ha territorialità in senso stretto o in senso giuridico, è una relazione tra computer dislocati in tutto il mondo. Pur non avendo territorialità è uno spazio in cui si incontrano le menti individuali, i pensieri e le volontà degli individui. Questa mancanza di confini territoriali[24] segnerà, dalla nascita di Internet in poi, tutta la questione della effettività delle normative statali a tutela della privacy ed anche le *ratio* delle molte successive normazioni. Alla perdita del potere di controllo statale sulla circolazione delle informazioni si è aggiunta la crescita delle autorità private. L'esempio di Stefano Rodotà, prima riportato, diventa diffusa ed incontrollata realtà: oggi la profilazione degli utenti è attività diffusa, la conoscenza delle nostre preferenze, ben oltre la storia di Cappuccetto rosso, rientra nel patrimonio di numerose imprese. L'uomo connesso è un uomo profilato, ha un suo profilo digitale, non, semplicemente, più o meno corrispondente alla espressione comportamentale della sua persona. Il profilo digitale contiene informazioni relative alle preferenze individuali, natura genetico-biologica, opinioni, insomma tutto ciò che è necessario per avere la rappresentazione di una persona. È un sapere che non domanda e non richiede la sincerità di una risposta, non teme la menzogna, è un sapere che viene costruito scientificamente sulla osservazione di comportamenti, avvenimenti e fatti e per questo permette persino uno sguardo sul futuro della persona. Le informazioni vengono raccolte direttamente, non accogliendo l'intento di comunicarle, bensì osservando nascostamente comportamenti ed abitudini con l'opera di oc-

[23] Vedi N. Irti, *Norme e luoghi – Problemi di geo-diritto*, 2006, nonché dello stesso autore, *Un diritto incalcolabile*, 2016, p. 151 ss.

[24] Se si volesse porre un confine territoriale ad Internet si negherebbe Internet per definizione, perché, in qualità di rete che unisce tutte le reti, esiste, come tale, solo tutto ciò che è in questa connessione globale. Possono pensarsi, e possono essere costruite, altre reti, ma non equivarrebbero a questo 'insieme di tutti gli insiemi'. Tuttavia, pur costruendo altre reti, non si ovvierebbe ai problemi posti dalla digitalizzazione e dalla natura immateriale del dato digitale.

culti 'raccoglitori-agenti informatici'. Così è possibile costruire un duplicato immateriale della persona, preciso, puntuale, ma è possibile anche costruire una errata rappresentazione.

Quanta strada dalla ditta di costruzioni romana che tanto clamore suscitò con i suoi questionari, e quanta privacy perduta! E questa privacy perduta non è dissolta a causa dei vincoli di un contratto, che si limita a legare tra loro un numero determinato di soggetti conosciuti; piuttosto è ora nell'agire quotidiano, sociale o privato, casalingo ed affettivo, il momento in cui l'individuo vede esposta la propria personalità all'ingresso degli sguardi, indagatori ed accaparratori, di una moltitudine di soggetti, perlopiù sconosciuti e neppure conoscibili. Alla perdita di riservatezza non è corrisposta una inerzia normativa, direi anzi il contrario, tutto ciò è accaduto nonostante gli interventi del legislatore e della giurisprudenza, tanto da lasciar supporre - ma giunti a questo punto la supposizione si tramuta in ipotesi - che i continui sforzi normativi celino proprio una qualche inadeguatezza degli strumenti usati.

I quattro fenomeni che destano interesse nel campo strettamente *giuridico* sono:

1. La moltiplicazione ed espansione della normativa sulla privacy è evidenza della presenza di conflitti di interessi sui quali deve intervenire il diritto;

2. I continui cambiamenti e ripensamenti normativi sono evidenza di mancati raggiungimenti di stabili prospettive regolative dovuti a molteplici fattori che vanno profondamente discussi ed analizzati su di un piano empirico;

3. La condivisione dei due fenomeni accennati nei due punti precedenti a livello globale è evidenza che la scelta tra l'intervento ed il non intervento normativo esula, allo stato attuale, dalle possibilità del legislatore statale;

4. L'ingresso della normativa a riguardo della riservatezza nelle costituzioni è evidenza della particolare sensibilità dei problemi di regolazione, che riguardano non solo l'individuo, ma la persona.

Alle sopraccennate problematiche occorre aggiungere i cambiamenti indotti nei rapporti sociali che hanno un rilievo giuridico pubblico. L'annullamento della sfera di riservatezza privata rileva, qui, non solo per l'individuo interessato, ma per l'intero gruppo sociale. È possibile affermare che al diritto alla privacy corrisponda non solo un

interesse privato ma anche un interesse pubblico, se si tengono presenti le possibilità di intervento sulle e direzione delle scelte politiche individuali a dipendenza delle informazioni raccolte, detenute e processate sugli individui profilati. Ma, oltre al fenomeno della profilazione individuale, quello della facilità di clonazione di banche dati accomuna individui ed enti nella stessa tipologia di attività. Anche un ente privato o pubblico e perfino gli apparati statali, possono venire spiati e le loro informazioni più segrete possono venire utilizzate per i più diversi scopi[25]. Le caratteristiche del dato digitale rendono possibile questa realtà. Queste nuove possibilità generano nuovi centri di raccolta delle informazioni e nuovi centri privati di potere, che da economico tende inesorabilmente a conquistare spazi politici. Verso questi centri di potere si rivolgono gli individui, e particolarmente i giovani, nella costruzione ed esplicazione della loro socialità. La dimensione territoriale, ed il controllo del territorio, già punto distintivo del potere statale, che lo sovra ordinava rispetto ad altri poteri, diviene una limitazione, lo Stato appare lentamente delegittimato dal volgersi altrove dei suoi cittadini, la territorialità costituisce ora il limite più distaccante, giacché lo sguardo amicale, il circolo di amici, le relazioni quotidiane si svolgono spesso in una simil-compresenza digitale che altera i confini affettivi ed emozionali dell'individuo, distaccandoli dalla vicinanza territoriale. La socialità comune e la condivisione culturale non si costruiscono più nelle comunità intermedie, sull'importanza delle quali tanta parte della dottrina civilistica e costi-

[25] Questo è forse il fenomeno più innovativo, più interessante ed anche più preoccupante: la possibilità che vengano sottratte e rese pubbliche informazioni riguardanti chiunque ed a qualsiasi livello sociale ed istituzionale. Dai capi si Stato, ai papi, ai segreti di Stato, non c'è banca dati irresistibile, né vita non osservabile, cito, ad esempio, i fenomeni conosciuti come Wikileaks, Vatileaks, oppure il caso Schrems. Questo cambia i rapporti tra cittadini e Stato, ma anche i rapporti di forza tra Stati, sempre più sovranità ed informazione si intrecciano strettamente. In effetti, l'altra faccia del cybercrime è il cyberwarfare, in cui l'atto viene compiuto non da privati ma da istituzioni sovrane. Il confine però, nel 'liquido' ambiente dell'informazione, è quantomai evanescente. Vedi: O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, *Yale Law School FacultyScholarship Series, Paper 3852, 2012:*
http://digitalcommons.law.yale.edu/fss_papers/3852.

tuzionalistica ha insistito[26], esse travalicano i confini statali e nazionali, in una globalizzazione i cui effetti sulla geografia politica mondiale sono ancora lontani dal poter essere considerati scientificamente, ma stanno costruendosi.

A ciò si aggiunga la apparente adesione alla cessione di informazioni sulla propria persona e la sottovalutazione della importanza del comportamento. Sempre prendendo a paragone l'esempio di Rodotà, all'epoca - certo non era un torno d'anni neoliberista - ci fu una generale alzata di scudi contro la ditta di costruzioni romana. Da sindacati ad esponenti politici, ad insigni giuristi, giornalisti e uomini di spettacolo, tutti stigmatizzarono l'attacco alla persona del lavoratore perpetrato con la somministrazione del questionario. Oggi, che la raccolta dati è assai più penetrante, invasiva e quotidiana, non si assiste ad una pari levata di scudi. Il tutto trascorre silentemente, con la sensazione dell'inevitabilità. Mentre gli anni Settanta vedevano un attento intervento politico e sociale, oggi il diffuso sentire appare essere un generalizzato 'mi vendo', o 'così fan tutte', in cambio di servizi informatici. L'individuo cede l'uso dei propri dati in cambio di prestazioni informatiche quali l'accesso a siti web, tariffe telefoniche agevolate, ricerche sul web e via discorrendo. Oppure è l'individuo stesso, di sua volontà, che compila il questionario - sempre nell'esempio di Rodotà - esponendo la propria vita privata sulla pubblica piazza dei social networks. L'impostazione politica, questa volta, è liberista ed antipaternalista, non protegge l'individuo, lo lascia libero di 'scegliere' come lasciarsi soggiogare. A questo riguardo la presenza di una normativa articolata, come quella sulla privacy, è anche controproducente a livello psicologico, lasciando supporre all'individuo una effettiva protezione da parte dello Stato, deresponsabilizzandolo. A ben guardare si tratta di una finta scelta, è un caso evidente di paradosso di Arrow, in cui ciò che si vuole è legato, per volontà della controparte, ad una serie di eventi o indesiderati o che non si conoscono affatto. L'uso del motore di ricerca Google obbliga alla cessione dei propri dati personali di navigazione e la cessione equivale ad una perdita del controllo su di essi. Non c'è alcuna alternativa possibile, ad esempio un prezzo in denaro, non è possibile scegliere tra il navigare a pagamento, senza

[26] Nelle belle, ma anche discusse, pagine giuridiche scritte all'epoca, vedi: P. Rescigno, *Le società intermedie*, in *Il Mulino*, 1958; C. Mortati, *Istituzioni di diritto pubblico*, II, VIII ed., Cedam, 1989, p. 1049 ss.

essere tracciato, ed il navigare con 'fidelity card', gratuitamente ma con tracciamento. Da sola, la caratteristica della raccolta dati di navigazione dovrebbe viziare l'accordo. Si aggiunga il fatto che, oramai, la propria presenza sul web è una modalità essenziale ed imprescindibile per la piena esplicazione della propria personalità, per una vita sociale pienamente partecipativa[27]. La domanda dell'individuo non è volta ad ottenere servizi informatici superflui o ludici o voluttuari, bensì, nella maggior parte dei casi, a scambiare informazione essenziale alla esplicazione della propria vita sociale e di relazione. La tutela di questo diritto costituzionalmente garantito ha portato la giurisprudenza ed il legislatore alla normazione sulla privacy, in un momento in cui le minacce erano molto inferiori, se paragonate all'oggi direi quasi risibili. Quel che si paventava[28], e si adduceva a motivazione dell'intervento normativo, si sta verificando, accade quotidianamente. Eppure, nessuno alza più scudi oggi, né tanto meno barricate: ci si accontenta di una normazione-paravento, ineffettiva e, non di rado, velleitaria, ridondante, pleonastica ed elusiva, ma, soprattutto, abbozzata per principi o demandata alla contrattazione o autoregolamentazione o, ancor peggio, condannata al purgatorio di retorici, o mai realizzati, codici etici[29].

Per altro verso, l'intera realtà digitale, rappresentazione dell'agire umano, stimola, in modo fino ad ora mai realizzato, la naturale predisposizione all'imitazione. Cambia molto nell'agire sociale degli individui, dal senso del pudore a quello di empatia o simpateticità. Questi cambiamenti sono una sfida per i sistemi morali e religiosi, convocando la loro infaticabile ermeneutica ad una gigantesca opera di adeguamento, ma questo cambiamento non è ininfluente per i sistemi giuridici, laddove basati sulla condivisione morale o sociale di opinioni.

---

[27] Anche il diritto di accesso ad Internet sta trovando una sua protezione costituzionale come mezzo irrinunciabile per la realizzazione della persona nei suoi diritti fondamentali, vedi M. Pietrangelo, a cura di, *Il diritto di accesso ad Internet*, ESI, 2011.

[28] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973, p. 91 ss.

[29] Basti l'esempio del fallimento dell'articolo 140 della L.196/03 sul "Codice di deontologia e di buona condotta" relativamente al marketing diretto, il campo più piratesco e redditizio della raccolta dati.

Evidenziamo quindi almeno tre fenomeni *sociali* che destano interesse nel campo giuridico, causati dalla digitalizzazione:

1. Globalizzazione, trasferimento e privatizzazione dei centri del potere e di sovranità;

2. Diversa costruzione della socialità e della morale, verso confini del tutto nuovi dell'essere umano, per i quali scorgere ora, razionalmente, una regolazione è pressoché impossibile; solo l'immaginazione letteraria può qui soccorrere il giurista;

3. Possibilità di influire, quasi determinare in modo nascosto le scelte individuali, non solo di consumo o economiche ma anche politiche e sociali, sicché la radice nel principio di libertà del diritto alla riservatezza, evidenziata dai costituzionalisti nel secolo scorso, si mostra qui in tutti i suoi minacciati contorni.

La perdita della riservatezza potrebbe significare una diminuzione o perdita della possibilità di autodeterminazione degli individui e quindi il venir meno di spazi politici democratici e di libera scelta. Anche l'idea stessa di democrazia viene messa in discussione dalla digitalizzazione, ma non discussa in dottrina, visto che la mancanza di libertà nella formazione delle opinioni e decisioni individuali non viene stigmatizzata e neppure discussa, ma accettata o rimossa.

Qui, più che in qualsiasi altro campo, le tradizionali tecniche di normazione sono inadeguate, dobbiamo oramai avere l'onestà intellettuale di ammetterlo, ma occorre indicare vie alternative, e non appare facile.

I giuristi italiani, con qualche pregiata ma isolata eccezione, si accorgono tardi dell'importanza e pervasività del cambiamento tecnologico[30]. Il rapporto tra privacy e computers stenta a venir discusso in

[30] Per una panoramica sul diritto privato negli anni settanta vedi: L. Nivarra, a cura di, *Gli anni settanta del diritto privato*, Giuffrè, 2008; molti autori evidenziavano già la insufficienza della normativa in merito ai diritti della personalità per proteggere la riservatezza del cittadino, sempre più minacciata dalle innovazioni tecnologiche, ma le peculiarità del fenomeno informatico non vennero messe a fuoco fin da subito. Come scritti italiani pionieri vedi: V. Frosini, *Cibernetica, diritto e società*, 1968; G. Conso, *L'informatica e la libertà del cittadino*, in *Temi*, 1971; S. Rodotà, *Elaboratori elettronici e controllo sociale*, Il Mulino, 1973; M. Bessone, *Politica dell'informazione e strategie di 'Datenschutz'*, in *Pol. Dir.*, 1974, p. 107 ss.; *Atti del colloquio internazionale su Informatica e diritto: efficienza dei sistemi automatici di informazione nella difesa sociale e garanzie dei diritti individuali*, Pavia, 15-17 settembre 1972,1974; M. G. Losano, *La protezione dei dati individua-*

sede giuridica, da un lato per la scarsa comprensione della tecnologia informatica, da altro lato per la mancanza di una normativa o comunque di una tradizione giuridica sulla privacy, ed ancora da altro lato per la mancanza di confronto con la dottrina statunitense[31]. Mentre negli Stati Uniti, - nei quali originano sia l'istituto, che le nozioni di dato digitale ed informazione che i personal computer, che Internet, e via dicendo - la discussione di dottrina inizia già nei primi anni Sessanta, e negli anni Settanta sarà in pieno svolgimento, in Italia si dovrà attendere più di un decennio. In effetti, si dovrà attendere che il diritto alla riservatezza faccia il proprio ingresso definitivo nell'ordinamento, con la 'sentenza Soraya'[32], sospinto dalle sempre più irruente innovazioni tecnologiche.

Il ritardo è condiviso con - o forse cagionato da - la speculazione filosofica in campo giuridico, legata ad una visione dualista ed isolazionista delle 'scienze dello spirito' rispetto alle 'scienze della natura'. È questa, purtroppo, una posizione che tutt'ora impedisce lo studio e la piena comprensione dei nuovi fenomeni, imprigionando i giovani ricercatori in impostazioni incapaci di slegarsi da un passato

li, in *Civiltà delle macchine*, XXVI, 1977, n. 3-4, p. 39 ss.; G. Alpa, *Privacy e statuto dell'informazione (Il Privacy Act, 1974 e la Loi relative à l'informatique, aux fichiers et aux libertés n.78-17 del 1978)*, in *Riv. dir. civ.* 1979, 1, parte I, p.65 ss.

[31] Il confronto ancora manca, vale sempre, nella maggior parte dei giuristi italiani, l'argomento vetero-positivista che chiude il giurista nei limiti di interprete del diritto positivo statuale. L'argomento, nell'ambito della tutela del dato e dell'informazione, mostra, oserei dire, la sua fallacia. L'interprete del diritto non è solo interprete del posto ma anche di ciò che è 'dato' naturalmente, non sono solo le proprietà formali del testo, a determinare il risultato finale della sua opera, ma anche quelle sostanziali che derivano dalla realtà interpretata. Nella teoria giusnaturalista, da questo punto di vista più esplicativa, si fa riferimento alla 'natura delle cose', L. Lombardi Vallauri, voce *Diritto Naturale*, in *Digesto delle discipline privatistiche, sez. civ.*, VI, Utet, 1990, p.314 ss.

[32] I primi ad evidenziare i possibili problemi relativi alla privacy derivanti da una raccolta dati veloce ed economica operata dagli elaboratori furono gli informatici, in particolare Bernard S. Benson, nel 1961. Nel 1962 lo Special Committee on Science and Law of the Association of the Bar of the City of New York, dà luogo ad un'inchiesta sull'impatto sulla privacy delle nuove tecnologie, particolarmente elettroniche. L'inchiesta fu diretta da Alan F. Westin, che divenne in seguito il punto di riferimento statunitense nel rapporto tra computer e privacy. Nel 1964 Vance-Packard pubblica *The Naked Society*, David McKay Co., 1964. Per un approfondimento vedi G. GonzálezFuster, *The Emergence of Personal Data Protectionas a Fundamental Right of the EU*, Springer International pub., 2014.

culturale importante, sì, ma non estensibile ermeneuticamente oltre i confini temporali della prima metà del secolo scorso. Affrontiamo un mutamento che coinvolge la filosofia risalendo fino alle sue origini, l'uomo non è più il solo a pensare razionalmente, a sentire e percepire, a ragionare. Chi dialoga con l'uomo sono oggi dei sistemi cognitivi artificiali, creati dall'uomo, gli stessi oggetti sembrano dialogare tra loro nello IoT, e comunque sono collegati in modo del tutto nuovo con gli esseri umani. Molte premesse di tutti i sistemi filosofici sono messe in discussione e la vecchia abitudine di riportare il presente al passato e di svolgere ermeneuticamente il passato nel presente è ora fuorviante. La modernità non è più nella contemporaneità digitale. Estendere analogicamente i concetti elaborati filosoficamente per un uomo e per una realtà così diversi è un'operazione densa di incognite e minacce, per i risultati sociali ai quali essa può condurre. Questa denuncia va pronunciata ad alta voce e continuamente ripetuta, infatti spetta al giurista, in quanto studioso della normatività, e tecnico di sistemi normativi, disegnare il funzionamento di mondi futuri, razionalizzare l'emozionalità umana nei limiti di un possibile convivere sociale. È nostro compito, quindi, conoscere ciò che si annuncia come portatore di cambiamenti, per regolarli. La miscomprensione della realtà porta a errate regolazioni sociali e queste sono il danno più grande che l'umanità possa ricevere. Oggi più che mai, di fronte ad una realtà nuovissima e diversissima, dobbiamo trovare il coraggio di cercare nuove forme di convivenza politica e sociale.

Uno degli errori più comuni, nella maggior parte dei giuristi degli anni settanta del secolo scorso, fu l'assimilazione degli elaboratori elettronici a tutti gli altri prodotti tecnologici quali, ad esempio, i televisori, le lavatrici o le fotocopiatrici. Pochi colsero il fatto che gli elaboratori, partendo da dati, usano e creano informazione, e lo fanno tramite calcoli logici, gli stessi che utilizza l'uomo quando ragiona. Non è il lavoro manuale che viene replicato, ma quello intellettuale, cioè l'ultimo baluardo che separa la tecnica dall'uomo.

Come precedentemente esposto, nel Novecento cambia il concetto di informazione; ingegneri ed informatici la definiscono in modo rigoroso, come risultato di un processo di trasformazione di dati; su questa definizione si costruisce la relativa scienza della informazione automatica, cioè dell'informatica. La definizione ingegneristica non si sovrappone né sostituisce una definizione filosofica, perché

quest'ultima è mancata. rispetto all'uso comune ed anche giuridico. Oggi questi nuovi significati sono spesso ben compresi ed alquanto diffusi, ma negli anni settanta essi erano nel patrimonio lessicale di informatici ma non di filosofi, letterati e giuristi: la teoria dell'informazione si origina in ambito scientifico, mentre la filosofia ha per millenni mancato l'oggetto nelle sue speculazioni, concentrandosi, piuttosto, sulla teoria del significato. Il ritardo filosofico si percepisce tutt'ora nelle difficoltà verso la comprensione della tecnica in generale oltre che della informazione in particolare. I giuristi, almeno gli italiani ma non da soli, vennero quindi colti impreparati, ma al generale disinteresse si oppose invece l'interesse di pochi ricercatori e della magistratura, che subito centrarono il problema[33], inquadrando il diritto alla riservatezza nel più ampio diritto alla tutela della persona in tutto l'ambito relazionale e sociale e non solo come diritto di esclusione del pubblico dal proprio ambito privato.

La chiave del problema venne individuata, dopo una riflessione quasi decennale, nel rapporto tra dati informatici e persona, venendo a delineare prima uno *Habeas Scriptum*[34], poi uno *Habeas Mentem*[35] ed uno *Habeas Data*[36]. Quest'ultimo ha trovato la sua positività, come principio, nelle costituzioni sudamericane.

Circa un decennio trascorse prima di riuscire ad astrarre completamente il concetto di dato ed informazione da quello di scritto o enunciato.

La paternità del salto, da scritto a dato che riguarda la persona, è generalmente attribuita al filosofo del diritto, nonché uno dei fondatori dell'informatica giuridica italiana, Vittorio Frosini. Per il filosofo italiano lo *Habeas Data* va pensato come il diritto del cittadino di disporre dei propri dati personali, così come gli viene riconosciuto il diritto di disporre liberamente del proprio corpo. Ma, oltre l'intuizione

---

[33] Vedi G. Marini, *La responsabilità civile,* in *Gli anni settanta del diritto privato*, a cura di L. Nivarra, cit., p. 252 ss.; S. Rodotà, *Elaboratori elettronici cit.*; S. Rodotà, *La privacy fra individuo e collettività*, in *Pol. Dir.* 1974, 545 ss.; G. Alpa, *Privacy e statuto dell'informazione cit*.

[34] S. Rodotà, *Elaboratori elettronici cit*., p. 121.

[35] S. Rodotà, *Progresso tecnico e problemi istituzionali nella gestione delle informazioni*, in *Privacy e banche dati*, a cura di N. Mateucci, 1981, p. 131.

[36] V. Frosini, *La protezione della riservatezza nella società informatica*, in: N. Matteucci, a cura di, *Privacy e banche di dati*, cit., p. 44. anche in *Informatica e diritto*, 1, 1981, pp. 9 e 10, come citato nella letteratura latino americana.

del filosofo, è da sottolineare l'importanza che essa ha avuto nella posizione del principio nelle costituzioni del Sudamerica[37]. Negli autori che hanno discusso ed elaborato i testi è sempre presente il riferimento al filosofo italiano, anche se la discussione sui temi in questione è di molto precedente, infatti, negli Stati Uniti la prima origine sembra doversi attribuire a Steven Weber[38].

L'impostazione del giurista più attento, da subito, alle problematiche giuridiche dell'informatica, Stefano Rodotà, prende le mosse dall'interno del dibattito politico italiano dell'ultimo quarto del Novecento ed in questo quadro argomentativo. Richiamo alla memoria di sfuggita l'intervento al convegno sull'uso alternativo del diritto che fu il momento in cui il ruolo della posizione politica nell'interpretazione del diritto venne rilevato ed ampiamente discusso in dottrina[39]. Nonostante ciò, non è, quella di Rodotà, una posizione di rottura rispetto alla teoria giuridica, che rivendica al diritto, composto di norme, la direzione del comportamento umano. Neppure è un'impostazione ingenua o trascurata nei riguardi delle tecnologie informatiche. Da subito il giurista ne coglie i pericoli per l'individuo ed il libero sviluppo della persona e dedica se non la sua intera opera di giurista, almeno la maggior parte alla salvaguardia della riservatezza.

È proprio in questo tentativo, che non ha risparmiato forze ed intelletto, che si può misurare l'insufficienza, in questo ambito, di una concezione del diritto che limita il proprio intervento a ciò che avverrà dopo che un determinato fatto sia accaduto, accompagnata dalla pretesa che, per la tutela giuridica, sia sufficiente la rivendicazione e posizione della norma che qualifichi il comportamento giuridicamente. Nel mondo digitale l'accaduto è spesso una nuova incancellabile realtà, determinata dalle caratteristiche del dato digitale: clonabilità, inconsumabilità e ubiquitarietà. Non adeguare la richiesta di diritto o

[37]F. Morales Prats, *La tutela penal de la intimidad: 'privacy e informatica'*, Ediciones Destino, 1984, p.47; José Afonso Da Silva, *Curso de Direito Constitucional Positivo*, Malheiros Editores, 1984, p. 458 nota 73.

[38]S. J. Weber, *Habeas Data: The Right of Privacy versus computer surveillance*, *University of San Francisco Law Reports*, vol. 5, 1971, p. 358 ss.

[39]S. Rodotà, *Funzione politica del diritto dell'economia e valutazione degli interessi realizzati dall'intervento pubblico*, in P. Barcellona (a cura di), *L'uso alternativo del diritto*, vol. I, 1973, 229 ss. Merita ricordare che negli Stati Uniti, nello stesso torno d'anni, il dibattito sulla politicità della decisione del giudice veniva affrontato con studi empirici di giurimetrica.

la previsione normativa a queste caratteristiche significa, nel nostro caso, vanificare ogni protezione, talché la norma giuridica diventa solo una statuizione di principio, valida indipendentemente dalla sua efficacia ed effettività, ma non una regola.

La problematicità della impostazione qui in esame sta proprio nel non riuscire a trasformare una rivendicazione politica, anche finemente argomentata dal punto di vista giuridico e condivisibile da quello scientifico, in una normativa applicabile che raggiunga lo scopo per il quale è stata posta. La scelta normativa rivolta ai principi piuttosto che alle regole fu condivisa dai pochi che all'epoca si dedicarono alla materia. Scrive Guido Alpa in riferimento ad una tesi di Stefano Rodotà: "[...] trova conferma la tesi che in materia di informatica e di tutela della privacy non è consigliabile introdurre modelli molto dettagliati e rigidi, ma è preferibile ricorrere ad una legislazione per princípi"[40]. Se all'epoca l'opinione e la scelta potevano essere condivisibili, a causa della novità della materia e del progresso tecnologico, che non rendevano conoscibile appieno la problematica, oggi così non è più e la drammaticità e pericolosità dell'assenza dello Stato è palese.

Ma portiamo qualche esempio. Che dire delle norme sul divieto di esportazione di dati in paesi in cui il livello di protezione assicurato non è paragonabile a quello europeo? L'esempio più imponente è rappresentato dagli Stati Uniti, per i quali, fino ad ora, sono valse le regole cosiddette degli accordi di Safe Harbor, nei quali le imprese autonomamente si impegnavano a garantire tale livello di protezione. Ma il dato digitale non è controllabile nella sua duplicazione e diffusione e dunque in quali banche dati saranno ora i dati esportati negli Stati Uniti con gli accordi di Safe Harbor? E come verranno utilizzati? Non lo possiamo sapere, l'interessato non può neppure immaginare chi, come e dove stia detenendo informazioni a suo riguardo e che uso ne stia facendo. Sono informazioni che possono toccare anche governi, autorità e poteri statali, il controllo e l'uso di queste informazioni è, quindi, di grande rilievo per il mantenimento di forme di governo democratiche dello Stato. La posizione della regola nulla ha potuto, e nulla possono neppure le nuove regole, in sostituzione degli

[40]G. Alpa, *Privacy e statuto dell'informazione* cit., p.119, in riferimento a S. Rodotà, *Elaboratori elettronici* cit. p. 91 ss.

accordi di Safe Harbor. Eppure la teleologia di quelle regole era apparentemente tutta protesa verso l'impedire il verificarsi di questi comportamenti, al fine di garantire la libertà della persona. È chiarissimo, in questo esempio, che una volta che il comportamento lesivo si sia verificato, il danno non sarà più eliminabile, e questo danno riguarda la persona e lo Stato, non già il mercato, il consumatore, le cose o i dati.

Negli anni successivi il dibattito giuridico portò ad una divaricazione normativa. Da un lato si approfondirono i percorsi dai principi all'interpretazione e viceversa[41], dall'altro si ampliò a dismisura tutta la normazione tecnica, contenuta in discipline di settore assai specializzate. Il principio di *Habeas Data* venne introdotto in molte costituzioni sudamericane, come azione volta alla richiesta di dati, ridimensionando l'idea originaria di Vittorio Frosini. L'elaborazione-rivendicazione di principi generali di derivazione costituzionale avrebbe dovuto ispirare la normazione tecnica, ma così non fu. Le regole tecniche, oggetto spesso di trattativa tra legislatori e centri di potere privato, non rispecchiarono, se non in modo nominalistico, i nuovi principi elaborati a tutela della persona.

Mentre i principi generali, da soli, sono assai deboli in riguardo alla loro cogenza generale, affidandosi piuttosto alla ponderazione di contrastanti principi ogni volta singolarmente operata in via interpretativa, le regole tecniche costringono, lasciando uno spazio pressoché nullo all'interprete. Il principio opera spesso solo come controllo della interpretazione, ma non dell'applicazione e la risultante sociale è stata quanto precedentemente descritto. L'impostazione basata sulla rivendicazione di diritti non solo come semplice posizione di norme, ma anche come derivazione ermeneutico-costituzionale trascura l'*enforcement* del diritto.

Un altro rilievo riguarda proprio l'*enforcement*, in quanto le caratteristiche peculiari del dato digitale fanno sì che non basti più la tecnica della descrizione di fattispecie punitive, infatti la perseguibilità della violazione è assai aleatoria, mentre il danno prodotto è spesso irreparabile ma anche incontrollabile, ed il nesso di causalità difficilmente dimostrabile. È esemplare il caso Mosley vs. Google, in cui nel

[41] Il diritto civile scoprì i principi costituzionali e si dedicò all'adeguamento delle interpretazioni delle leggi civili ai principi costituzionali, vedi P. Perlingieri, *Il diritto civile nella legalità costituzionale*, ESI, 1984.

2008 l'attore vedeva violata la sua privacy, prima dalla pubblicazione su un giornale scandalistico di alcune foto a riguardo di suoi incontri privati, poi dalla pubblicazione di tali foto in Internet. Il motore di ricerca Google fungeva da tramite per il reperimento delle foto da parte di ognuno, ogni volta che si digitassero le opportune chiavi di ricerca. Il procedimento si è chiuso nel 2015 in via transattiva, con accordo tenuto segreto dalle parti. Tuttavia, pur nell'ignoranza dell'accordo, alcune cose devono essere evidenziate. Anzitutto i files con le foto esistono e non è possibile in alcun modo, allo stato attuale della tecnica, trovarli tutti e distruggerli, questi possono in ogni momento tornare ad essere visibili. La lunga procedura giudiziaria, fino alla transazione, ha visto l'attore ogni volta farsi carico del reperimento delle immagini e della richiesta al motore di ricerca di cancellazione di quell'indirizzo, ma non del file. Il motore di ricerca ha sempre negato la possibilità tecnica di oscuramento di tutte le foto compromettenti presenti in rete, sicché per Mosley si rendeva necessaria una continua, estenuante ed economicamente impegnativa attività di controllo. La segretezza dell'accordo suscita, inoltre, grandi perplessità: certamente, per il 'borghese piccolo piccolo' sarebbe impossibile seguire la medesima via.

È quindi quanto mai necessaria una cooperazione del diritto con la tecnologia per una tecnica giuridica che sia anche tecnica del reale. Il diritto deve essere costruito dentro alla tecnica stessa, per evitare l'attuale stato di ineffettività di tante statuizioni ed inapplicabilità di tante interpretazioni.

Come si è già accennato, è significativo il fatto che le peculiarità della digitalizzazione siano state, fin dall'origine, non pienamente comprese dal giurista. I fondatori ed inventori dei computers e dell'informatica, come Alan Turing o Claude Shannon, intendevano riprodurre con essi le capacità mentali umane, interamente intese, non solo limitatamente alle capacità di calcolo[42]. Lo studioso di 'scienze

[42] Iniziando da Alan Turing, tutti gli studiosi di Intelligenza Artificiale, a qualsiasi corrente o ramo di ricerca appartenessero, si riconoscevano nel compito di riuscire a riprodurre artificialmente la mente umana. Così, ad esempio, fu anche per Marvin Minsky, per Jerry Fodor e per Terrence Sejnowsky. Anche per gli studiosi di cibernetica e successivamente di robotica ed in genere di *machine learning* la sfida di ricerca fu la riproduzione delle attività cognitive umane. Non si trattava di costruire potenti 'macchine di calcolo', né 'macchine stupide', al contrario, si in-

umane', invece, si è sempre rivolto ai nuovi strumenti come a macchine calcolatrici, o, tuttalpiù, come a macchine da scrivere, certamente non come a riproduzioni dell'attività mentale umana. L'impostazione giuridica risente tutt'ora di quella prima posizione culturale[43]. Neppure si è compresa la rivoluzionaria impostazione culturale sottostante ai concetti di dato ed informazione elaborati da Claude Shannon nella nuova scienza dell'informazione e che in seguito diventeranno il suo cardine concettuale[44]. Proprio il dato digitale, e la sua trasformazione in informazione tramite l'applicazione di operazioni algebriche, costruisce le rappresentazioni della IT, nonché la simulazione del pensiero umano e della sua azione, in una parola, della sua mente.

Tramite la elaborazione algebrica e algoritmica di dati digitali, con l'ausilio di tecniche che provengono dalle scienze che studiano l'uomo, si giunge alla riproduzione virtuale della 'mente' dell'uomo, di tutto quell'insieme culturale e biologico che ne imposta la sua presenza ed agire nel mondo. Questa 'persona virtuale' esiste sotto forma di bit e di questi ne conserva le proprietà: clonabilità, immaterialità, ubiquitarietà. Mentre la persona fisica è, direi quasi, prigioniera della sua fisicità, il duplicato virtuale può essere in ogni luogo contemporaneamente.

---

tendevano costruire 'sistemi cognitivi intelligenti'. È tuttora così. Se gli attuali personal computer sono delle 'macchine stupide', anche se sempre meno, è perché essi incorporano solo alcuni risultati parziali di questi studi. Un attuale robot intelligente, invece, ha le capacità cognitive e mentali medie di un animale di affezione, e, alle volte, paragonabili a quelle di un bambino. Vedi per tutti A.M. Turing, *Computing machinery and intelligence*, in *Mind*, 59, 1950, p. 433 ss., consultabile, insieme a tutto il materiale del padre fondatore dell'intelligenza artificiale su: http://www.turingarchive.org/.

[43] Esiste una responsabilità culturale? Oppure ogni ideologia ed ogni filosofia è libera di presentare la propria visione del mondo senza dover dar conto degli esiti passati? Nel campo che stiamo analizzando ci sono dei colpevoli, ed andrebbero evidenziati. Quale credibilità si può concedere a filosofie che hanno mancato di vedere una così imponente realtà all'orizzonte? Nessuna, ed un utile lavoro potrebbe essere svolto nell'evidenziare gli errori, piuttosto che le corrette impostazioni, o le previsioni esatte, di dette teorie, v. F. Romeo, *Sulla chiusura della rivista i-lex*, in *i-lex, rivista di scienze giuridiche, scienze cognitive ed intelligenza artificiale (www.i-lex.it)*, 22, 2015, p. 8 ss.

[44] Vedi supra nota 8.

Ma esistono veramente questi nostri duplicati virtuali? Per l'ordinamento giuridico italiano è sufficiente la risposta che sia *possibile che esistano* per esigere un intervento normativo non proveniente da autorità private, né extra-statuali, ma formulazione diretta dei principi costituzionali a protezione della persona e della sua libertà e dignità, senza alcun riguardo prioritario alla libertà di iniziativa economica e prescindendo da qualsiasi considerazione socio-economica sulle necessità della economia globalizzata. La globalizzazione è una tendenza economico-culturale dei nostri tempi, certamente non destinata a durare, il controllo della mente delle persone, invece, è un'attività criminale che mette in pericolo il fondamento stesso dello Stato di diritto e delle democrazie occidentali: vale a dire la libertà della persona.

L'informatica mutua dalla teologia induista il lemma 'Avatar', indicando con esso la rappresentazione virtuale grafica di un individuo, in genere di un partecipante ad un gioco. Ma la tecnica digitale è andata ben oltre il trastullo della grafica, duplicando digitalmente quell'insieme di informazioni che nel passato si racchiudevano all'interno dell'individuo. Gli Avatar grafici ricevono ora una mente digitale. Quelle informazioni, che un tempo non uscivano dal segreto del 'modo d'essere' di ciascun individuo, incontrano nell'Avatar digitale la condivisione sociale della immagine e rappresentazione dell'individuo. Ne risulta una rappresentazione che non è più semplicemente dell'individuo, ma della persona e per essa, per la sua vita di relazione, potenzialmente devastante.

Questo è adesso il punto di partenza per comprendere come debba essere impostata la normativa che regola l'intera realtà IT dal punto di vista della realtà da regolare e dell'effettività: una volta che si sia compreso cosa sia e quali caratteristiche abbia il dato digitale, ed a cosa serva nelle tecniche ICT, è possibile comprendere quale normativa sia quella più adatta alla sua regolazione.

Non ci troviamo in un *cul de sac*, anzi, le caratteristiche sopra esposte ci permettono, di delineare una possibile soluzione, laddove, non trascurando la posizione di norme di principio, tali norme vengano poste già pensando al loro *enforcement* nella specifica tecnica normata ed in tutti i suoi possibili sviluppi. Si potrebbe pensare, ad esempio, ad una norma generale di responsabilità che disponga non su specifiche tecniche ma *sulla tecnica stessa*, e che quindi riesca a

tipizzare la mutevolezza dell'ambiente in cui si trova ad operare a cagione della tecnica.

La creazione della regola giuridica in quest'ottica richiede una stretta collaborazione tra diversi settori di ricerca, sia giuridici che informatici che economici e, certamente, la concezione che il giurista ha del diritto uscirà mutata da quest'opera di adeguamento[45]. Forse il diritto non si trova più da solo nell'opera di definizione e statuizione dei possibili futuri umani, ma certo la sua opera normativa, con e sulla tecnica, è imprescindibile se l'orizzonte sociale umano intende comprendersi nei confini dello Stato di diritto.

In tutte le epoche storiche di grande transizione, il giurista ha cercato nuove basi o diversi fondamenti alla sua opera di composizione sociale. Il pendolo teorico ha oscillato tra diritto scritto e diritto naturale nelle varie epoche, accompagnando nascite di nuove potenze e tramonti di vecchi regimi. Ogni volta la tecnica giuridica è stata in grado di inventare nuovi strumenti concettuali adatti al dire diritto e quindi a chiudere controversie. Forse può essere riletto in questa chiave l'attuale apertura delle ricerche di teoria generale del diritto verso strumenti di analisi propri delle ricerche sul diritto naturale. Il giusnaturalismo ha capacità nomopoietiche che il positivismo si nega. Ogni epoca storica, in cui ciò che viene reputato diritto affronta una crisi dei fondamenti, si volge verso il diritto naturale, e la più volte annunciata 'crisi del diritto' è probabilmente solo una crisi di certo positivismo. Ci troviamo ad affrontare una crisi sul piano della teoria quindi, ma non c'è motivo di dubitare che anche l'odierna crisi, che i vecchi strumenti e concetti giuridici stanno affrontando[46], non possa venir risolta con nuovi strumenti, sta a noi giuristi, però, l'essere capaci di farlo, sta a noi innovare senza distruggere, così come nella migliore tradizione giuridica.

---

[45] Vedi sul punto ampiamente M. Hildebrandt, *Smart Technologies and the End(s) of Law*, Elgar, 2016; M. Hildebrandt, K. De Vries a cura di, *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, 2013.

[46] N. Irti, *La crisi della fattispecie*, in *Riv. Dir. Proc*., 2014, 1, 36 ss.; le riflessioni avanzate in quell'articolo vengono ampliate ed approfondite in: N. Irti, *Un diritto incalcolabile*, Giappichelli, 2016; A. Andronico, *Viaggio al termine del diritto. Saggio sulla Governance*, Giappichelli, 2012.

3. Uno sguardo al futuro: Il governo della tecnica digitale e la *Legal Protection by Design*

Il Regolamento rivendica finalmente, in diversi luoghi, quel ruolo di governo della tecnica che tanto è stato discusso a livello teorico[47].

Governare la tecnica significa conoscere le sue regole e disegnare regole giuridiche in grado di interagire con esse per orientarne i risultati verso gli scopi posti dal diritto stesso. Una parte del problema dell'effettività si annida proprio nell'adeguatezza della regola giuridica in riguardo alla tecnica che intende regolare per il raggiungimento dei fini posti nella normativa giuridica.

Se la regola tecnica stabilisce i comportamenti umani necessari al raggiungimento di una certa trasformazione del mondo, la regola giuridica li qualifica giuridicamente. Anche la regola giuridica, come quella tecnica, è rivolta a dirigere comportamenti umani, in vista di un qualche cambiamento del mondo circostante. Le due regole hanno il medesimo fine ultimo, ma la funzione della prima trova la sua ragione nella socialità umana, ed è volta a strutturare l'azione dell'individuo in funzione di quella. La funzione della seconda, invece, si struttura sul mondo naturale, ed in ragione di questo dirige l'azione dell'individuo. Il raggiungimento del risultato voluto, di trasformazione del mondo, è la risultante dell'operare di entrambe le regole.

Il rapporto tra diritto e tecnica è profondo ed intrecciato nei secoli, è tuttavia evidente che le tecniche di informazione e comunicazione siano all'origine di questo rapporto. L'unione è così stretta da riuscire a mettere in luce gli aspetti problematici, a livello teorico generale, nella individuazione e definizione dello stesso concetto di diritto[48]. Risiede in questo stretto legame la necessità, in un ambiente sociotecnico, di disegnare le norme direttamente sulla loro possibile effettività, per poter assicurare effettività alle norme giuridiche stesse. Nel settore delle IT questo aspetto è amplificato in conseguenza di molteplici fattori attinenti soprattutto alle caratteristiche del dato digitale,

[47] La discussione in sede di teoria del diritto inizia con N. Irti, E. Severino,*Dialogo su diritto e tecnica*, Laterza, 2001, ma prosegue tutt'oggi.

[48] Non è questo il luogo di approfondimento di questa problematica, ma sul punto v. F. Romeo, *Antropologia giuridica. Un percorso evoluzionista verso l'origine della relazione giuridica*, Giappichelli, 2012.

su cui si intende intervenire normativamente, oltre che alle caratteristiche del tipo di intervento normativo.

In riguardo alle caratteristiche peculiari del dato digitale, alle quali abbiamo accennato precedentemente, esse portano direttamente alla difficile perseguibilità della violazione di una norma, giacché il nesso di causalità tra azione e danno è difficilmente dimostrabile, l'individuazione dell'elemento soggettivo, o del soggetto responsabile, è pressoché impossibile, oppure, nella maggior parte delle volte, possibile a pena della violazione di altre norme, quali quelle sulla libertà di manifestazione del pensiero o di informazione. Questo costante contrasto di valori fondamentali ed interessi da proteggere è ciò che il diritto dovrebbe regolare, ma la valutazione giuridica compiuta attraverso la ponderazione giudiziale di principi e valori, non è in grado di valutare le molteplici conseguenze della decisone, dovute alla interazione con essa delle tecniche dell'IT, rischiando spesso di creare ulteriori conflitti e violazioni. In parte per la sostanziale incomprensione o ignoranza dell'interprete delle tecniche IT, ed in parte per la continua velocissima innovazione di dette tecniche.

A tutto ciò si aggiunge la irreparabilità del danno prodotto, che si dirige principalmente alla persona, più che al patrimonio, e, perdurando nel tempo, è di difficile calcolabilità e quantificazione. Ciò rende insufficiente la tradizionale tecnica normativa di descrizione di fattispecie punitive: la semplice minaccia dell'uso della forza non coglie il bersaglio digitale, l'intervento successivo alla commissione dell'illecito è spesso inutile o inadeguato rispetto ad un danno che coinvolge incalcolabilmente l'intera persona e la sua intera vita di relazione futura. Spesso ci si trova a fronteggiare danni per l'intera vita di relazione del soggetto, paragonabili ai danni biologici, ma che riguardano la sua immagine sociale e reputazione.

Il giudizio giuridico attuale appare, quindi, inerme ed inadeguato, nella sua mastodontica lentezza, nei confronti di una tecnologia proteiforme, che agilmente e rapidamente muta e si adatta ai cambiamenti normativi non tanto in esecuzione di una richiesta normativa, quanto in elusione dei suoi scopi. La normazione, tramite standard oppure per principi, è troppo lenta, oppure incerta e costosa per trovare effettività nei confronti di questa tecnologia, teoricamente incompresa, che sta pervadendo rapidamente ogni ambito della vita privata dell'individuo.

Una ulteriore caratteristica riguarda l'apparente esiguità della lesione immediata, è anche per questo motivo che l'individuo leso difficilmente giunge ad affrontare l'iter interpretativo-giudiziario. Invece, assai spesso, tali esigue lesioni alla persona, una volta raggiunto il bacino di dati raccolti su di essa, si trasformano, tramite tecniche di profilazione, nell'irreparabile danno alla vita di relazione. L'individuo è generalmente all'oscuro dell'operare di dette tecniche sui suoi dati, né conosce i risultati.

La normazione per principi non individua direttamente fattispecie di responsabilità tipiche e, pur permettendo una più flessibile applicazione ad una realtà mutevole, pur tuttavia non riesce ugualmente ad essere effettiva qualora la realtà sia velocemente mutevole. D'altro lato, però, la regolazione per standard tecnici di specifiche tecniche è troppo rigida per trovare applicazione ad una tecnologia in rapidissimo mutamento.

Ciò conduce all'attuale insoddisfacente situazione: se si cerca di regolare le tecniche IT singolarmente, esse saranno sì impostate già prima della implementazione o dell'uso commerciale secondo la regola giuridica, ma rapidamente muteranno eludendo la norma. Nel caso opposto, in cui si normi per principi, essi andranno adattati ai molteplici casi concreti ed alle diverse tecniche nel momento giudiziale, lasciando al cittadino leso la scelta sulla opportunità di chiedere una risposta giuridica e contemporaneamente lasciando ampia libertà di scelta all'interprete nel valutare ogni singolo caso. Così si abbandona la prassi giuridica alla variabilità ed incertezza del risultato e la persona alla libera appropriazione di molteplici centri di interesse.

L'introduzione delle Autorità Garanti ha in parte alleviato il male ma non risolto il problema. Proprio sulla privacy si trova la casistica più numerosa di fallimenti normativi. Così è, ad esempio, per la firma apposta, o per il click, di accettazione al trattamento dei dati, oramai ridotta a pura formalità.

Alcuni contributi alla discussione scientifica in questi ultimi anni hanno elaborato un approccio alla tecnologia nuovo rispetto al normativismo classico, dapprima enucleando la categoria delle *Privacy-Enhancing Technologies (PETs)*[49], in seguito quella della *Privacy by*

[49]Le Privacy-Enhancing Technologies sono discusse da parecchi anni: "The idea of shaping technology according to privacy principles has been discussed since many years, addressing among other the principles of data minimisation, anonymi-

Design (PbD)[50], generalizzata oggi alla *Legal Protection by Design (LPbD)*.

La LPbD non limita il suo campo alla Privacy, ma si estende ad ogni aspetto di confronto tra tutela giuridica e tecnica, così, ad esempio, al data protection.

LPbD "[…] entails that legal conditions are translated into a technical requirement to sustain the force of law. The bottom line is that where computational infrastructures implicate the substance of fundamental rights they must (1) engage democratic participationas to the default they constitute; (2) be engineered and designed in a way that makes them 'resistable'; and (3) be made 'contestible' in a court of law"[51].

Questi sono i tre principi cardine della LPbD sulla tecnica: *partecipazione democratica*, *resistibilità* e *contestabilità* avanti ad un tribunale, principi che quindi, come detto sopra, si estendono alle PETs ed alla PbD.

La LPbD differenzia tra tecniche che non incorporano in loro stesse la possibilità di queste garanzie giuridiche e tecniche che verificano, nel senso di rendere vere, queste possibili realtà giuridiche. Nel secondo caso la realtà giuridica, la sua normatività, viene ad essere incorporata nella tecnica. Questa modalità di regolazione si differenzia su questo punto dalla semplice posizione nell'enunciato normativo di un dover essere giuridico.

Qui sta la nuova importante svolta del legislatore unitario all'artinolo 25 del RGPD: l'utilizzazione di una tecnica non privacy

---

sation and pseudonymisation. This led to the term Privacy Enhancing Technologies (PETs), which covers the broader range of technologies that are designed for supporting privacy and data protection." È quanto si trova sul sito dell'agenzia europea ENISA, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies. Vedi R. Hes, J. Borking, a cura di, *Privacy-enhancing Technologies: the path to anonymity*, Registratiekamer, The Hague 2000, on line: http://govdocs.ourontario.ca/node/14782; P. Agre, M. Rotenberg, a cura di, *Technology and Privacy, The New Landscape*, MIT Press, 1998. Presso l'università di Stanford sono in rete alcune pagine intese a mettere a disposizione degli utenti le informazioni necessarie sulle PETs per migliorare il controllo sui propri dati da parte dell'utilizzatore di Internet: http://cyberlaw.stanford.edu/wiki/index.php/PET .

[50] Vedi nota 5.

[51] M. Hildebrandt,*Smart Technologies*, cit. p. 263.

enhancing oppure che non permette una protezione secondo i tre principi innanzi enunciati genera responsabilità.

Il primo requisito, quello della *partecipazione democratica*, richiede una partecipazione sociale, del legislatore e di altri attori sociali, alla elaborazione del design tecnico: privilegiando lo sviluppo e l'implementazione di alcune tecniche rispetto ad altre si assicura la compatibilità di queste con l'ordinamento giuridico e con gli scopi sociali da questo perseguiti.

Il requisito della *resistibilità* si riferisce alla possibilità, effettivamente realizzabile, per l'individuo, di impedire l'uso della specifica tecnica nei confronti dei suoi dati, o di modificare gli stessi, possibilità che presuppone la effettiva conoscenza di ogni singolo trattamento.

Infine la *contestabilità* avanti ad un tribunale, si riferisce alla possibilità di azione giudiziaria e probatoria nei confronti dell'uso di tale tecnica.

Appare chiaro che la maggior parte delle tecniche di raccolta dati attualmente praticate non soddisfano queste tre caratteristiche.

La protezione by Design, è senz'altro la più recente invenzione giuridica, promettente seppur non priva di interrogativi, per affrontare il sempre più celere progresso tecnico, in particolar modo riguardo le tecnologie IT. "[…] without LPbD we face the end of law asweknowit, though - paradoxically - engaging with LPbD will inevitably end the hegemony of modern law as we knowit. There is no way back, we can only move forward.

However, wehave different options; either law turns into administration or techno-regulation, or it re-asserts ist 'regime of veridiction' in novel ways."[52]

Ormai la nuova strada è aperta, se il richiamo alla legge e gli strumenti del positivismo novecentesco sono insufficienti, ancor di più manifestano i segni dell'età oltremodo avanzata i richiami a valori trascendenti o a nuove quanto traballanti etiche[53]. Un rinnovato con-

[52]M. Hildebrandt, *Smart Technologies, cit. p.114.*

[53] Anche il campo dell'etica si trova sconvolto dalle ICT. Si pensi solo al mutamento della morale sessuale che si è accompagnato alla diffusione di Internet. Anzi, proprio il campo dell'etica, ancor più del diritto, si trova impreparato ad affrontare il cambiamento, e questo è conseguenza della negazione teorica della possibilità di riprodurre la mente dell'uomo artificialmente. Già nel 2002 rilevavo questa mancanza, e da allora non sono stati fatti grandi passi in avanti, v. F. Romeo, *Il*

fronto del diritto con le tecnologie del digitale tramite queste vecchie tecniche giuridiche risulterebbe inadeguato e velleitario, non più in grado di garantire effettività, non solo, a causa delle novità tecniche. Si aggiunge ad esse un nuovo, e forse più grave e per ora imperscrutabile, ambito di criticità: il cambiamento cagionato nell'essere umano, sia a livello sociale e relazionale che a livello biologico. Il cambiamento biologico viene in considerazione sia direttamente, per il diverso sviluppo delle connessioni cerebrali nell'interazione del giovane con la realtà virtuale[54], sia per il possibile aumento delle capacità cognitive individuali tramite le tecniche di 'realtà aumentata' e la ibridazione uomo-computer[55].

Il giurista, e per il suo tramite il diritto, deve prendere coscienza che l'uomo per il quale dice diritto non è più lo stesso uomo, cadono tante premesse sottintese dai giuristi, non esplicitate ma condivise, e con esse cadono tanti argomenti entimematici che costruiscono il ragionamento giuridico. Per il giurista cambia un punto di riferimento da millenni immutato e ritenuto immutabile, che la teoria del diritto giusnaturalista ha teorizzato come una delle tre 'radici del diritto': la 'natura umana' [56]. Le tecniche digitali e l'ICT sono tecniche dell'umano: ne simulano la mente, interagiscono con essa e la modificano. Non è questo il luogo per approfondire questo tema, mi limito a sottolineare un punto. La 'natura umana' è sempre stata il fulcro o il baricentro della normatività, del dover essere del diritto, che in ragione di questa è stato determinante nella interpretazione-applicazione del diritto positivo. Si pensi, a titolo di esempio, alla forza dell'argomento sulla natura umana nella enucleazione, determinazione e definizione novecentesca dei diritti fondamentali, dei diritti umani e del concetto di persona. Ora questo punto di riferimento cade. Quali nuovi orizzonti si aprano al giurista è difficile dire; anche questa nuova, e per ora imperscrutabile, situazione, è una delle cause

diritto artificiale, Giappichelli, 2002, p.155 s. Quando il giurista parla di "superamento della natura umana" difficilmente pensa al lato informatico-digitale, quanto, piuttosto, agli aspetti biologici attinenti alla morte, alla riproduzione, alla modificazione genetica.

[54]B. Volpi, *Gli adolescenti e la Rete*, Carocci, 2014.

[55] Il cambiamento a livello biologico ha condotto taluni a seriamente teorizzare la transizione ad uno stadio umano diverso, vedi: N. Bostrom, *A History of Transhumanist Thought*, in *Journal of Evolution and Technology*, 14, 1, 2005, p. 1 ss.;

[56]L. Lombardi Vallauri, voce *Diritto Naturale*, cit., p.314 ss.

dell'ineffettività della normativa a tutela della persona nei confronti delle IT.

Su quanto sin'ora esposto, il nuovo Regolamento Generale sulla Protezione dei Dati, accoglie cautamente, all'articolo 25, i principi della LPbD, che potrebbero servire al giurista per elaborare nuove tecniche normative e nuovi tipi di intervento. Occorre tuttavia notare che ancora non è avvertita appieno, a livello politico, la forza del cambiamento nell'ambiente tecnologico umano e nell'uomo stesso. La realtà va spesso oltre la verità, e sottrae quel velo culturale oscurante che si deposita col tempo sulle cose, distruggendo miti, dissacrando misteri, falsificando teorie, ma rischiarando percorsi futuri. Una impostazione empirista, come quella qui adottata, non può trascurare questa funzione rivelatrice e chiarificatrice del fatto. Porto quindi un'immagine, diffusa sulla stampa qualche mese fa, come esempio di re nudo: quella di Mark Zuckerberg davanti al suo computer, nel quale era evidente la striscia di scotch nero, ed oscurante, accuratamente installato sopra la webcam del laptop. Quella telecamera è un esempio di non-PET, di tecnica elaborata non in vista di una protezione dei dati personali, bensì in vista della captazione e dell'appropriamento di dati personali. In molti elaboratori la telecamera è azionabile via software: alcuni software proprietari, con codice sorgente segreto, permettono l'attivazione della telecamera da remoto, indipendentemente dalla volontà dell'utente. Nell'esempio, l'illustre utente, esperto di modi di processamento di dati personali, utilizzando lo scotch oscurante, ha messo in atto una tecnica che permetteva la protezione dei suoi dati, perdendo, però, la piena funzionalità dell'apparato. I profili di illiceità delle non-PETs, in relazione all'art. 25 RGPD sono molteplici. L'utente è generalmente all'oscuro dell'esistenza della possibilità di essere spiati da webcam[57], ma, anche conoscendola, non ha altre agevoli possibilità di agire che il manuale oscuramento della webcam, impedendosi così il normale utilizzo del mezzo, o esponendolo al rischio di danneggiamento. La tecnica, in questo caso, non soddisfa il requisito della *resistibilità* da parte dell'utente.

[57] Sono in realtà molteplici le tecniche di spionaggio da remoto presenti sui nostri computer, non solo la webcam ma anche il microfono è un hardware diretto verso l'esterno, con la possibilità di captare dati dall'esterno indipendentemente dal controllo dell'utente.

La tutela risarcitoria contrattuale ha qui molteplici possibilità di intervenire, dalla vendita di prodotto difettoso, al vizio occulto, ai numerosi profili relativi alla corretta informativa da dare al consumatore. Ma non è solo la responsabilità contrattuale il possibile aggancio normativo. Lo strumento informatico non-PET, o non-DPET [58] è anch'esso esposto ad intrusione da parte di terzi, se connesso ad una rete. Qui le fattispecie illecite o criminose si moltiplicano, in numero e varietà, con l'aumento delle possibilità di intrusione nel sistema informatico e con l'aumento del numero dei soggetti coinvolti, per arrivare a coinvolgere, in casi estremi ma possibili, la sicurezza nazionale. Difficile escludere, in tutti questi casi, la responsabilità dell'impresa per la vendita di prodotti informatici non-DPET. L'esclusione di questo insieme di responsabilità dell'impresa nell'uso di dati informatici diventa, con la introduzione della LPbD, un fatto ideologico, non più una ineluttabile conseguenza di mutamenti tecnici. Il legislatore ha operato una scelta e posto una norma a sua esplicazione.

Il dibattito sulla opportunità di inserimento di dispositivi che permettessero il controllo della identità dell'utente di un computer e del relativo flusso di dati, risale agli anni Novanta del secolo scorso; estesamente si rilevava l'opportunità del controllo a fini di sicurezza, sorveglianza e prevenzione dei reati[59]. Si è creata così in dottrina la bipartizione tra interesse degli Stati alla sorveglianza ed interesse individuale alla 'opacità'. Oggi è più facile disegnare la rete di interessi che si tesse attorno ai dati informatici, personali o meno. Di questa rete fanno parte, come protagonisti, soprattutto le imprese dell'IT, per le quali il dato è il bene economico sul quale si costruisce la loro attività d'impresa. L'interesse al controllo, più che quello alla trasparenza, è quindi diversamente ripartito tra diversi attori economici e politici[60]. Resta aperto, quindi, il campo, vasto ed interessantissimo, della

[58] Data Protection Enhancing Technology.

[59] Le fattispecie criminose che più venivano proposte come necessitanti l'intervento erano quelle relative ai reati attinenti ad atti terroristici ed alla pedofilia.

[60] Vedi sul punto P. De Hert, S. Gutwirth, *Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power*, in E. Claes, A. Duff, S. Gutwirth, a cura di, *Privacy and the Criminal Law*, 2006 p. 61 ss.; R. D'Orazio, *Dati personali in rete aperta*, in V. Cuffaro, V. Ricciuto, *Il trattamento dei dati personali. II. Profili applicativi*, Giappichelli, 1999, p. 277ss.

discussione sociale e della implementazione delle tecniche trascurate dalle imprese perché non favorevoli ai loro interessi di mercato. Un campo nuovo per l'informatica giuridica del diritto pubblico e costituzionale, che arriva fino a coinvolgere temi relativi allo Stato di diritto ed alla costruzione di una società democratica nella realtà digitale. In particolare, la LPbD in uno 'smart environment', quale sarà, prevedibilmente, l'ambiente socio-tecnico in cui dovremo interagire nei prossimi anni, sarà pervasivamente presente in ogni strumento digitale disponibile, questa sarà la condizione prima per la costruzione delle future democrazie digitali, qualora si trovi la forza per costruirle.

"È giunto il tempo d'armarsi e di dar ordini", sono le parole di Richmond nel Riccardo III di Shakespeare, parole che hanno espresso la decisione che aprì la strada alla modernità inglese. Molte sono le armi digitali, molti i campi di battaglia e molti gli aspiranti sovrani. Esiste un nuovo lemma che individua questa realtà e sul quale il giurista deve riflettere: *cyberwarfare.* Il lemma definisce ogni tipo di utilizzazione dell'informazione in un atto di guerra. Colui che si potrà armare e dar ordini sarà colui che possiederà le armi, colui che possiederà informazione.