"Annali online della Didattica e della Formazione Docente"
Vol. 9, n. 13/2017, pp. 302-305 – ISSN 2038-1034

E. Maestri, *Lex informatica. Diritto, persona e potere nell'età del cyberspazio*, Napoli, Edizioni Scientifiche Italiane, 2015, pp. 144, € 15.00

Le tecnologie informatiche forniscono quella che può essere definita una "nuova dimensione della realtà" poiché, aggregando e combinando (e quindi creando) dati informatici, trasformano la realtà e riducono la distinzione tra essa e la rappresentazione digitale. Tale trasformazione si articola in due direzioni: da un lato il dato reale per essere *trasdotto* in una sequenza di bit manipolabili dal calcolatore deve in qualche modo essere concettualizzato; d'altro canto ogni rappresentazione informatica ha necessariamente un impatto (*feedback*) sulla realtà che dipende da molte e successive elaborazioni informatiche.

Il rapporto tra costruzione del dato informatico e ordinamento giuridico può dunque configurarsi come rapporto tra due forme di normazione – la *Lex informatica* da un lato e la legge giuridica dall'altro – dell'azione individuale e collettiva.

Delineare la modalità in forza della quale il *software* e l'*hardware* dei sistemi informativi vincolano il comportamento umano è l'obiettivo che anima il saggio di Maestri, oggetto della presente recensione.

Storicamente la legge e i regolamenti governativi hanno stabilito le principali regole della politica dell'informazione, incluse le regole costituzionali sulla libertà di espressione e sul diritto di proprietà. Tuttavia, se si fa riferimento al web, a Internet e in generale alla società dell'informazione, le leggi e i regolamenti non sono la sola e unica fonte del diritto. Le capacità tecnologiche e la progettazione dei sistemi impongono regole ai partecipanti. La creazione e lo sviluppo di politiche dell'informazione sono incorporati oggi nella progettazione e negli standard della Rete tanto quanto nei sistemi di configurazione. L'insieme di regole per il flusso delle informazioni è imposto soprattutto dalla tecnologia e dalla programmazione informatica (pp. 9-10).

La *Lex informatica* – nodo centrale attorno al quale si articola l'intera struttura del contributo dell'Autore – è un'espressione che si riferisce all'insieme delle scelte tecniche che impongono dei comportamenti (p. 10). Il diritto in Internet è veicolato attraverso il mezzo tecnico: il divieto di legge diventa il divieto dal punto di vista tecnico; ciò che non *deve essere* fatto non *deve poter essere* fatto. La *Lex informatica* permette sia di stabilire norme specifiche per i flussi di informazioni veicolati sulla Rete sia di imporre le politiche generali dei flussi e dell'automazione delle informazioni digitali. Attraverso le architetture tecnologiche (si pensi ai protocolli PICS) la *Lex informatica* può vietare alcune azioni, quali l'accesso, sulla Rete e può imporre alcuni flussi informazionali, quali il conferimento obbligatorio di dati di *routing* per l'invio dei messaggi elettronici (p. 28).

Nessuno degli strumenti alternativi di *governance* (convenzioni internazionali, autoregolazioni, soft law, licenze, contratti, *Lex informatica* ecc.) può essere considerato di per sé sufficiente a regolare il cyberspazio, ma tutti possono e devono concorrere, in un dialogo internormativo, in una osmosi e in una circolazione di modelli, a costruire un apparato flessibile e adeguato alle esigenze delle reti globali.

Nel caso delle tecnologie informatiche, la relazione tra azioni umane e diritto si dispiegherebbe attraverso logiche *bottom up*, aggregative e comunitarie tipiche del web: leggerezza di vincoli, legami orizzontali tra le persone, dimensione paritaria, lotta al *Digital divide*. La dislocazione spaziale e non territoriale della comunicazione digitale trasforma la società in un modello organizzativo che presenta la forma di una rete globale. Internet è uno spazio che stimola una forte spinta alla libertà e alla conoscenza. Gli attori della Rete divengono plurilogici, adattativi e comunitari al tempo stesso, virtualmente migranti ed aperti alle differenze e al pluralismo culturale (p. 27).

Non di meno, in contrapposizione con questa potenzialità inclusiva, aperta ed interattiva della rete di Internet, l'altra faccia dell'era dell'informazione è caratterizzata da una lotta per il dominio della Rete, attuata attraverso la gestione ed il controllo di Internet da parte di una "corporate governance multi-stakeholder", diretta, di fatto, da un *network* delle multinazionali della comunicazione informatica e telematica. La Rete, dominata da attori non statali della globalizzazione tecnologica e della competizione economica, diventa al tempo stesso centralizzata e decentrata, si adatta e si ripolarizza in una variazione infinita, eludendo il territorio, strutturando confinamenti immateriali dello spazio globale e producendo un insieme di norme, mascherate da politiche di trasparenza, di protezione e di promozione dei diritti umani, da un lato, e implementata da un'architettura tecnologica di filtraggio, di etichettatura e di valutazione dei contenuti web dall'altro (p. 28).

Un esempio emblematico di ciò è il caso *Mattel vs. Cphack*, approfondito dall'Autore nel capitolo I, dal quale si evidenzia l'emersione di problemi legati alla giurisdizione, al diritto d'accesso ad Internet, ai concetti di *fair use* e di *commons*.

Ad avviso di Maestri, l'esempio del caso *Mattel vs. Cphack* dimostra come il software censorio (*Cyber Patrol*) ideato dalla Mattel presentasse una architettura di filtraggio – la cui funzione è impedire l'apertura delle pagine dei siti ritenuti inadatti sul personal computer degli utenti – che estendeva arbitrariamente i limiti costituzionali del *copyright*, aggirando le garanzie approntate dal Primo emendamento e rendendo, perciò, vana la salvaguardia della *fair use clause*. Se la legge sul *copyright* deve proteggere il materiale sotto *copyright* e, al contempo, anche il *fair use*, ne consegue che le leggi poste a tutela della *Lex informatica* (ad esempio la clausola antielusione prevista dal *Digital Millenium Copyright Act*), a sua volta preposto alla protezione del materiale sotto *copyright*, dovrebbero lasciare spazio al *fair use* (pp. 17-22).

In questo senso, il code (il software e l'architettura tecnologica di protezione del materiale informatico) non è una legge, non è soggetto ai limiti costituzionali, ma ha la copertura della legge e funziona come una legge, anzi a volte con maggiore efficacia. Il code (codici sorgente, protocolli informatici, ecc.) è una delle forme inedite attraverso le quali si esprime il soft law: una serie di atti, non omogenei quanto a origine e natura, che, benché privi di effetti giuridici vincolanti, risultano comunque, in vario modo, giuridicamente rilevanti. È così che il code diventa legge. I controlli inseriti nelle tecnologie di protezione e di regolazione dell'accesso in Rete divengono una regola la cui violazione è altresì una violazione della legge (p. 23, 28, 35).

La concorrenza (*co-regulation*), se non addirittura la prevalenza (*self-regulation*) della *Lex informatica* sulla normazione giuridica dell'ecosistema digitale apre al giurista, e in particolare

al filosofo del diritto che si interroga sulle precomprensioni, i pregiudizi o le attese circa l'ordinamento giuridico, problemi in parte inediti, sia di tipo teorico (in che modo concepire l'ordinamento delle fonti? Come intendere l'identità personale nel mondo digitale? Come si trasforma l'istituto della proprietà intellettuale?) sia di tipo politico-morale (come garantire la privacy rispetto alla possibilità, nient'affatto teorica come dimostra il caso Snowden, di programmi di sorveglianza di massa tramite la raccolta di metadati (*data protection and data retention*)? Come evitare che multinazionali dell'informatica rendano la Rete un'area planetaria privatizzata sulla quale esercitare un monopolio, se non di diritto certamente di fatto?). La monografia di Maestri ci aiuta a orientarci in questa massa intricata di questioni lungo un percorso argomentativo diviso in sei capitoli.

Dopo il primo capitolo dedicato al caso *Mattel vs. Cphack* e il successivo capitolo dedicato a chiarire la natura tecnocratica e privatistica della *Lex informatica*, dei quali abbiamo già dato cenno, l'Autore evidenzia come nella Rete si possono formare dei *Leviatani digitali* che attraverso una forma di "contratto sociale 2.0" offrono agli *users* la possibilità di utilizzare un mezzo tecnologico a patto che si rinunci a esercitare il dominio sui propri dati personali inseriti nel sistema informatico. Si realizza quindi una forma di socialità digitale sotto però l'egida, minacciosa, dei Big Data che possono immagazzinare e rielaborare tali dati fuori dal controllo della persona che ne è legittima proprietaria, ma che, d'altra parte, volontariamente se ne aliena per potere fruire dell'esperienza della socialità digitale (p. 40).

Il terzo capitolo presenta quindi i caratteri della *persona digitale* intesa come "l'insieme di tutte le informazioni inserite dalla persona nella Rete, dalle tracce digitali lasciate dalla sua navigazione e dai documenti prodotti dall'interazione con l'ambiente web in cui si trova" (p. 51). La *persona digitale* subisce, però, continui rischi di manipolazione della sua identità, di intromissione nella sua privacy, o di sottrazione di informazioni. A tal proposito l'Autore si sofferma sulla formazione del c.d. diritto all'oblio e chiarisce le differenze tra un approccio europeo e uno statunitense rispetto alla pretesa dei soggetti di vedere cancellate dalla rete informazioni riguardanti la propria vita personale, facendo notare i lati negativi, in termini di bilanciamento tra diritto all'informazione e diritto all'oblio, della recente pronuncia C-131-12 del 13 maggio 2014 della Corte di Giustizia dell'Unione europea sul diritto di ogni cittadino a chiedere ai motori di ricerca la deindicizzazione di un contenuto che lo riguardi.

Il quarto capitolo presenta un interessante parallelismo tra il *Panopticon* di Bentham e un modello di sorveglianza digitale chiamato *Synopticon*, in cui ciascun soggetto volontariamente entra in una relazione di mutua sorveglianza (p. 85). Si realizza così il completamento dell'ideale benthamiano del massimo di controllo con il minimo del costo. Mentre nel *Panopticon* ciascun recluso non sapendo quando è sorvegliato finisce per sorvegliare se stesso (p. 86), nella socialità digitale invece il principio della massima trasparenza si perfeziona. Mentre il prigioniero di Bentham è solo ed è soggetto suo malgrado a sorveglianza, nelle odierne pratiche di sorveglianza globale invece l'azione si perfeziona esattamente nel momento in cui ciascuno si auto-illumina volendo entrare in contatto con gli altri utenti. La sorveglianza inizia non nella sfera pubblica, ma in quella privata, ed è messa in azione non da un ente esterno, il sorvegliante, ma dal soggetto stesso che entra nei social network e condivide con altri *users* informazioni personali (foto, video, dati sensibili ecc.) senza averne tuttavia il controllo, che ri-

mane nelle mani delle *media corporations* le quali possono utilizzarlo per fini commerciali o peggio per condividerlo con enti governativi. Si passa così al *Synopticon*: "un modello di sorveglianza nel quale molti soggetti osservano i pochi" (p. 85).

Il quinto capitolo affronta le implicazioni di teoria e filosofia del diritto provocate dall'affermarsi della *Lex informatica* e dalla diffusione delle pratiche di sorveglianza digitale. In primo luogo l'Autore efficacemente confronta il modello di regolazione tramite diritto e il modello di regolazione tramite *Lex informatica*. Mentre il primo ha una giurisdizione statale e territoriale, la seconda ha un ambito di applicazione virtualmente globale; mentre il primo ha come contenuto norme e sentenze, la seconda ha come contenuto norme e tecniche che permettono la realizzazione di talune funzioni; mentre il primo ha come fonte un legislatore e i suoi atti, la seconda ha come fonte i programmatori informatici che costituiscono i codici di accesso alla Rete e l'uso dei *software*. Infine l'efficacia del diritto dipende dall'applicazione di esso da parte di operatori giuridici spesso stimolati dall'istanza di parte mentre, al contrario, la *Lex informatica* è auto-esecutiva: ad essa non si può disobbedire e se non si consente a configurazioni già preimpostate dai programmatori informatici e a clausole vessatorie unilaterali non si può neppure entrare nella Rete o utilizzarne il *software* (pp. 93-95).

Nell'ultimo capitolo l'Autore sottolinea come sia necessario riportare l'attenzione sul bilanciamento dei diritti e come si debba considerare lo spazio pubblico di Internet un *commons*, un bene comune, indispensabile per avere il riconoscimento dei diritti fondamentali, così da permettere alla creatività umana di esprimersi secondo regole deliberate democraticamente in una cornice costituzionale entro la quale il cyberspazio viene considerato un *medium* di organizzazione e di mobilitazione delle relazioni faccia a faccia. Sottratto alla continua mercificazione, la "costituzionalizzazione del cyberspazio" permetterebbe di ripensare la sfera pubblica digitale (si pensi ai *blog*) come un modo per rivitalizzare le discussioni aperte e diffuse tra cittadini che alimentano le radici delle società democratiche.

Enrica Martinelli