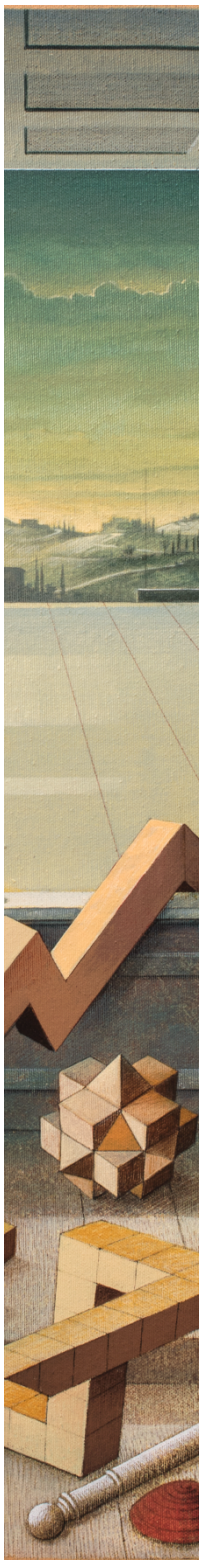
Cultura giuridica e diritto vivente
Rivista on line del Dipartimento di Giurisprudenza
Università di Urbino Carlo Bo
Note e Commenti



COME SI GOVERNA LA TECNOLOGIA DIGITALE?

Licia Califano

Abstract
[How to govern digital technology?] Digital technology has brought big advantages for people's everyday life. Yet, digital world creates many risks for fundamental rights and freedom. The Author analyses the nature and characteristics of those risks, with a special focus on the traditional definition of sovereignty and democracy and the protection of individual liberties and rights, in particular the right to political participation, right to health and to the protection of personal data.

Key Words:
Constitution, Sovereignty, Data protection, Technology, Rights

Vol. 8 (2021)

Come si governa la tecnologia digitale?

Licia Califano [*]

1. Lo sviluppo tecnologico prosegue inarrestabile e, con esso, il trionfo della tecnica sulla vita dell'uomo.

Al fondo vi è la condivisibile convinzione di migliorare la vita di ciascuno di noi, aumentando la qualità e la quantità dei beni e dei servizi che ci vengono offerti quali utenti/consumatori.

Ma, se i vantaggi non possono certo essere negati, occorre al contempo capire e spiegare che il mondo così profondamente mutato non è esente da rischi che hanno inevitabilmente una ricaduta sulla vita delle persone, sui diritti e sulle libertà: rischi e pericoli di cui dobbiamo essere consapevoli.

Oggi la produzione, la memorizzazione e l'utilizzo delle informazioni**,** che noi stessi generiamo nel vissuto di una tecnologia digitale che sempre più ci accompagna nelle azioni quotidiane, sono generate in modo automatico da una molteplicità di sistemi a costo zero che rendono disponibili le informazioni personali di una moltitudine di individui; informazioni che si prestano ad una infinità di utilizzi - aziendale, economico, sociale e, come vedremo, anche politico - e in molti settori che dal commercio via via si estendono al turismo, ai trasporti e che sempre più trovano spazi nel mondo della sicurezza e della sanità.

Non a caso si è sottolineato come non sia eccessivo affermare che le informazioni, oltre ad accompagnare e migliorare gli scambi economici e le transazioni tradizionali, diventano un fattore di produzione al pari della terra, del capitale e del lavoro[1].

Un tema che oggi acquista una particolare e rinnovata attualità perché il momento storico che viviamo, di emergenza sanitaria globale, ha prodotto una ulteriore forte accelerazione nell'utilizzo della tecnologia digitale. Le misure di contenimento della pandemia adottate dai governi di tutto il mondo hanno costretto le pubbliche amministrazioni ad accelerare la transizione digitale delle interazioni con i cittadini e le imprese.

---

[*] Licia Califano è Professore ordinario di Diritto costituzionale presso il Dipartimento di Giurisprudenza di Urbino.
Indirizzo mail: licia.califano@uniurb.it

[1] F. BERNABE', *Libertà vigilata,* Editori Laterza, Roma - Bari. 2012.

L'applicazione di nuove modalità di calcolo e di analisi, le sempre maggiori capacità sia di raccolta che di conservazione (si pensi alle grandi banche dati ma più in generale ai big data) e analisi di dati personali hanno completamente modificato il concetto stesso di tutela della privacy, rendendo di fatto obsolete, o comunque non più efficienti, le norme che fino a qualche anno fa tutelavano la riservatezza degli individui intesa semplicemente come diritto ad essere lasciati soli[2].

Nel mondo digitale "essere lasciati soli" non basta, dal momento che è l'individuo stesso che, più o meno consapevolmente, produce contenuti e con essi genera dati personali che viaggiano liberamente in rete.

Così, se pensiamo a Facebook dobbiamo chiederci se siamo in presenza di una piazza virtuale, un luogo neutro dove si formano e agiscono liberamente quelle formazioni sociali dove si svolge la personalità individuale, in conformità ai principi costituzionali, o abbiamo di fronte un orizzonte più complesso e, certamente, a tratti più oscuro.

Dalla osservazione che siamo di fronte ad una grande agenzia pubblicitaria, che vende spazi pubblicitari e li mostra costantemente ai propri iscritti, possiamo giungere a chiederci quanto l'uso della rete per le interazioni sia funzionale a creare dialogo, tolleranza e attenzione per le ragioni degli altri o invece, all'opposto, quanto sia reale il rischio di irrigidire contrapposizioni e ostilità.

A ben guardare tutto il mondo digitale tende a sottrarre il cittadino alla regola base degli ordinamenti democratici, costruita sul confronto e la scelta fra opinioni diverse. E' un mondo che, al contrario, tende alla creazione di enclave che si chiudono, ciascuna in se stessa, in una dinamica mirata a far arrivare a ciascuno opinioni confermative di ciò che si presume rappresenti già una posizione, comunque un orientamento già assunto da ciascuno sulla base di un giudizio o di un pregiudizio poco importa.

Se davvero quelle che si formano in rete sono le formazioni sociali dei tempi nuovi, allora, si è osservato, la funzione cui assolvono è esattamente opposta a quella educazione agli affari collettivi per cui le aveva valorizzate il costituente[3].

E' il tema della democrazia digitale che ha proposto all'attenzione di tutti noi costi e benefici che le nuove tecnologie pongono ai sistemi democratici contemporanei.

Come conciliare i due aspetti è domanda che deve condurci, forse, non tanto al problema astratto di quanto, in che misura l'innovazione tecnologica metta in crisi i sistemi democratici, ma forse, piuttosto, ribaltando la prospettiva, a chiederci quali siano le sfide che l'avanzamento tecnologico pone alla democrazia e, lungo questa strada, come individuare e scegliere l'ordine delle priorità delle sfide cui far fronte. Un percorso di cauta ponderazione e analisi delle incognite poste dal processo tecnologico, che coinvolge anzitutto la comprensione dell'impatto prodotto dal cambiamento e, di conseguenza, la priorità delle scelte in grado di facilitare, ad esempio, la trasformazione dei modelli partecipativi.

E non può sfuggire, al giurista, che punto di partenza è la necessità di definire i contorni della sovranità digitale e gli strumenti del diritto per limitarla.

Perché se guardiamo meglio i tratti di questo nuovo sovrano tecnologico, scavando oltre l'immagine dell'innovazione come fattore di crescita, di sviluppo e di liberazione

---

[2] Sull'uso delle nuove tecnologie in relazione ai rischi per i diritti degli individui e delle formazioni sociali T.E. FROSINI – O. POLLICINO – E. APA – M- BASSINI (a cura di), *Diritti e libertà in Internet*, Le Monnier, Firenze, 2017. Ma vedi anche G. DE MINICO, *Antiche libertà e nuove frontiera digitale*, Giappichelli, Torino, 2016.

[3] Così G. AMATO, *Prefazione*, in A. SORO (a cura di), *Democrazia e potere dei dati: libertà, algoritmi, umanesimo digitale,* Baldini+Castoldi, Milano, 2019.

della persona, ne scopriamo una dinamica interna di crescita esponenziale ed una sua diffusione che si mostra insofferente tanto all'idea di limitazioni, quanto alle forme conosciute di regolazione giuridica.

Superata in radice l'idea di una crescita lineare della tecnologia, di pari passo è la consapevolezza dell'enorme concentrazione economica che la potenza di automazione e di rielaborazione ha prodotto nelle mani dei privati.

Un nuovo potere che, esattamente come in passato si trasferisce da una sede ad un'altra: un potere che non ha più caratteri necessariamente pubblici o privati, personali o collettivi, ma ha essenzialmente caratteri tecnici. Un potere che fonda la sua legittimazione su competenze di carattere tecnico - scientifico e sulla capacità di implementazione tecnologica e di controllo delle informazioni che da tali sistemi derivano.

Il tema, peraltro, non è tanto il cambiamento di sede del potere, e con esso dei tratti della sovranità, e nemmeno che si tratti di mani ignote[4], il tema vero è la mancanza di regole capaci di fissare la misura del potere e proteggere i diritti fondamentali.

Nel paradigma digitale fatto di big data, di Internet delle cose, di intelligenza artificiale, di automazione di tutti i processi produttivi e comunicativi, l'incidenza sulla sfera individuale, sulla dignità e libertà dell'uomo da parte di chi detiene le conoscenze tecnologiche può manifestarsi in molti modi: dai sistemi che generano un controllo a distanza dell'individuo lavoratore all'informazione connessa al corredo genetico di ciascuno di noi, dalla profilazione piegata alle finalità elettorali e politiche alla massiva raccolta dei dati sanitari connessi a dispositivi medici che diventano un patrimonio economico inestimabile per le aziende farmaceutiche e le compagnie assicurative. E che dire, lungo questa strada, dell'uso dell'intelligenza artificiale nel settore militare e della sicurezza che può giungere a sostituire l'essere umano con un robot con risultati la cui imprevedibilità spaventa o, ancora, l'uso di algoritmi e robot che già ora cominciano a sostituire il giudice, ad esempio nella scelta di una famiglia cui affidare un bambino o, ancora nel valutare gli estremi e le ragioni che giustificano la carcerazione preventiva in relazione al rischio di fuga o reiterazione del reato.

Ecco allora la domanda, come si governa la tecnologia digitale?

Certamente non basta più la disciplina nazionale; è in regolazioni efficaci sovranazionali, che ci garantiscano una piattaforma comune, la miglior difesa della stessa sovranità nazionale.

In questo senso il nuovo Regolamento generale sulla protezione di dati (GDPR) può rappresentare uno strumento idoneo a fornire almeno qualche soluzione ai tanti interrogativi che ci stiamo ponendo[5].

In primo luogo l'impiego anzidetto di una fonte normativa sovranazionale, capace tanto di uniformare, quanto di lasciare spazio all'implementazione in ambito statuale. In secondo luogo, la positivizzazione e la conseguente giustiziabilità del principio di

---

[4] Sul punto R. BIN, *La sovranità nazionale e la sua erosione*, in A. PUGIOTTO (a cura di), *Per una consapevole cultura costituzionale. Lezioni magistrali*, Jovene Editore, Napoli, 2013, p. 369-381, ma vedi anche A. SIMONCINI, *Sovranità e potere nell'era digitale*, in T.E. FROSINI – O. POLLICINO – E. APA – M- BASSINI (a cura di), cit., p.19 ss.

[5] Sul GDPR sia consentito richiamare L. CALIFANO*, Il Regolamento Ue 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali*, in L. CALIFANO – C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona: il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Il Mulino, Bologna, 2017; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

responsabilizzazione e della valutazione di impatto preliminare; regole, queste, già testate in altri settori e che, chiamando in causa i soggetti privati, tenuti a definire e giustificare i limiti della propria azione, hanno dato buona prova di sé.

Vi è poi da considerare l'importanza di avere affermato la natura di diritto fondamentale della protezione dei dati personali.

In altre parole, per far fronte alle sfide che l'era digitale comporta le autorità pubbliche necessitavano di un nuovo e più moderno strumento normativo, in grado di superare i confini territoriali dei singoli Paesi e persino dei continenti (si pensi al principio del cd. *targeting*); uno strumento in grado di essere applicato in maniera omogena in tutta Europa, assicurando al contempo sia la massima circolazione delle informazioni che la massima tutela per gli individui.

Resta al fondo, in ogni caso, e prima di entrare nello specifico di singole questioni problematiche, una domanda che va oltre il diritto e che, al contempo, non possiamo esimerci dal porci preliminarmente. Se l'essenza dell'uomo risiede nella sua libertà, ovviamente intesa in senso alto, filosofico, quale espressione di consapevolezza, creatività e responsabilità, ne consegue che l'intelligenza artificiale di cui dotiamo le macchine che costruiamo potrà essere un fattore di crescita, una preziosa alleata, se sarà capace di conservare e magari stimolare la pienezza della condizione umana come vita libera. Ma, al contrario, di fronte alla trasformazione dell'uomo e del mondo alla obbedienza della logica dei numeri e della tecnologia in una condizione di democratica non libertà, bisognerà avere il coraggio di fermarsi e di stabilire la regola per cui un numero rilevante di Paesi dovrà porre un limite all'uso dell'intelligenza artificiale applicata a determinati ambiti.

2. La prima questione su cui condurre qualche riflessione più specifica, ci porta ai confini sempre meno protetti della nostra immagine, del nostro diritto a costruire liberamente noi stessi.

Più viviamo nella rete - sempre connessi - tanto più mostriamo la nostra vita quotidiana, le nostre abitudini e preferenze, rendendo così irrealizzabile e contraddittoria la pretesa di vedere rispettata e tutelata la nostra privacy come accadeva in passato.

La diffusione di IoT, delle tecnologie di *machine learning* e di intelligenza artificiale, stanno producendo una quantità di dati, personali e non, mai visti prima nella storia dell'uomo.

Questa quantità di dati e informazioni è ciò che oggi chiamiamo big data: banche dati in cui le informazioni contenute vengono automaticamente interconnesse e rielaborate sulla base di imperscrutabili algoritmi, per dare vita a informazioni di secondo grado (*data mining*), riutilizzabili per altri fini.

Se anche volessimo ipotizzare che tali risultati non consentono la re-identificazione degli interessati che avevano inizialmente ed inconsapevolmente fornito i dati grezzi (peraltro tutto da dimostrare!), nondimeno questo perfetto automatismo, basandosi su leggi probabilistiche, potrebbe condurre a categorizzazioni e classificazioni della società che, oltre ad essere discutibili sul piano dell'esattezza e della correttezza, portano con sé il rischio di generare pregiudizi e discriminazioni.

La normativa in materia di protezione dati rappresenta, dunque, un fondamentale presidio di garanzia, tanto in termini di diritti esercitabili dall'utente, quanto nella direzione di stimolo verso una logica di responsabilizzazione dei titolari coinvolti a vario titolo nella sempre più articolata filiera in cui si svolgono i trattamenti.

Una direzione, questa, che deve considerare prioritaria la necessità di escludere, o quantomeno minimizzare, il rischio di intendere la cessione dei propri dati quale tributo

necessario alla fruizione dei vantaggi offerti dalla rete[6]: una prospettiva preoccupante e inaccettabile sul piano culturale, prima ancora che giuridico.

Di qui l'importanza delle previsioni contenute nel già citato Regolamento generale europeo n. 679/2016 (GDPR), che delineano una cornice generale della protezione dei dati personali fondata su quattro pilastri: il rafforzamento dei diritti degli interessati; l'introduzione del principio di responsabilizzazione dei titolari del trattamento; il rafforzamento dell'apparato sanzionatorio per le violazioni della disciplina a danno degli interessati; una nuova visione della governance europea.

In particolare il testo regolamentare rafforza i diritti degli interessati, specificando meglio alcuni aspetti dei diritti già introdotti dalla precedente direttiva e introducendone di nuovi, già frutto di una elaborazione giurisprudenziale (diritto all'oblio) oppure di una riflessione sulle difficoltà che il "cittadino digitale" vive (diritto alla portabilità; opposizione al processo decisionale unicamente automatizzato).

Previsioni, queste, che si saldano con l'introduzione del principio di responsabilizzazione del titolare del trattamento; quest'ultimo, sia esso persona fisica o giuridica, deve essere il primo a garantire la privacy dei singoli, valutando preventivamente tutti i rischi del trattamento (valutazione di impatto preliminare), adottando tutte le adeguate misure di sicurezza e comunicando tempestivamente gli attacchi a tale sicurezza (obbligo di notifica del *data breach*), tenendo un registro accurato e aggiornato dei trattamenti, nominando il Responsabile per la protezione dei dati, per citare gli oneri principali.

D'altra parte, è una realtà indiscutibile che le piattaforme che utilizziamo per veicolare i nostri messaggi sono dei grandi "*hub*" dai quali chi li gestisce può captare dati su di noi e utilizzarli a nostra insaputa.

Così per tutte le ricerche effettuate in internet, ma si pensi alla installazione dei cookies, alla memorizzazione degli indirizzi IP o, più semplicemente, alla volontaria cessione di dati da parte nostra all'interno di form online, convinti così di ottenere in cambio un servizio solo apparentemente gratuito.

Una mappatura dei nostri dati da parte di soggetti privati e dei profili che di noi si possono estrarre; non a caso parliamo di profilazione quale trattamento automatizzato di dati personali che ormai avviene principalmente attraverso la tracciabilità e l'analisi della nostra presenza in rete (diffidiamo da chi scrive o pensa, magari anche con convinzione, che la profilazione consista in un trattamento di dati anonimi).

Un trattamento, effettuato principalmente a fini commerciali, che produce effetti da considerare attentamente per le conseguenze negative che comporta in termini anzitutto di massificazione delle opinioni, dei gusti e dei comportamenti, perché all'individuo viene riproposto sempre un contenuto affine a quello già oggetto di interesse o di ricerca. In altri termini, il "prodotto" che viene offerto all'individuo tramite la pubblicità mirata sarà sempre più vicino a quello che già conosce, pensa, apprezza ed ha acquistato, riducendosi così le possibilità che cambino o evolvano i gusti e le opinioni di ciascuno.

---

[6] In merito alla questione della cd. "*counterperformance*" ovvero dei dati come merce di scambio nella prestazione di servizi "apparentemente" gratuiti, si veda l'interazione tra il Regolamento generale sulla protezione dei dati 679/2016 e la Direttiva (UE) 2019/770 del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Si veda in generale sull'argomento, G. RESTA – V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, n. 2/2018.

Una massificazione inarrestabile che rischia di mettere in discussione conquiste essenziali, espressione della modernità quali la libertà e l'eguaglianza degli individui: la libera determinazione e la non discriminazione e omologazione.

Vi è poi da considerare il mancato rispetto del principio di trasparenza informativa, perché l'utente in nessun momento sa da parte di chi e come vengono gestiti i propri dati personali cui, peraltro, si ricollega un terzo problema: l'impossibilità per l'utente di esprimere un consenso informato a determinati trattamenti e, di conseguenza, il libero riutilizzo dei dati per finalità differenti da quelle per cui sono stati originariamente raccolti.

Un esempio banale per comprendere: cerco online informazioni su una malattia diagnosticata ad un mio familiare (magari su siti medici o comunque di settore) e ricevo in automatico notifiche pubblicitarie sulla mail personale da parte di aziende che vendono dispositivi medicali.

A ben vedere, il diritto all'oblio e al cd. "*delisting*" pur meritoriamente affermati in sede giurisprudenziale e oggi positivizzati in sede regolatoria, coprono solo una parte della complessità e gravità del fenomeno e ci riportano ai confini sempre meno protetti del diritto a costruire noi stessi e la nostra immagine.

Una volta di più, allora, la salvaguardia dell'autodeterminazione informativa, dell'autonomia e della responsabilità delle scelte deve diventare un terreno fertile che ci consenta di mantenere il governo delle nostre tracce digitali che oggi in misura crescente concorrono a definire la nostra identità e, con essa, la nostra stessa libertà.

3. Pensiamo ora ai rischi che corriamo se guardiamo al trasferimento in atto, del fenomeno ora descritto, all'ambito dell'esercizio dei diritti politici e al modo in cui si stanno affinando le tecniche di profilazione dell'elettore: campagne elettorali con monitoraggio di gusti e bisogni ne sono state fatte oramai diverse. Il caso "Cambridge Analytica" ha certamente rappresentato un terribile spartiacque in tal senso, dal momento che ha rivelato un sistema molto complesso e strutturato finalizzato alla profilazione elettorale.

Una gravità del fenomeno che ha spinto anche le istituzioni politiche europee a prendere posizione su tali temi; in occasione delle elezioni per il Parlamento europeo della primavera 2019, la Commissione ha varato un pacchetto di misure legislative al fine di "garantire elezioni europee libere e regolari"[7], volte ad assicurare il rispetto della privacy, il contrasto alle fake news e alla disinformazione, la trasparenza della propaganda politica online, per finire con norme più rigide per i finanziamenti dei partiti politici europei.

Un fenomeno, legato all'uso dei big data che, non vi è dubbio, rischia di cambiare il rapporto fra democrazia, rappresentanza politica e società.

L'utilità della profilazione elettorale consiste principalmente nella ottimizzazione dell'invio di messaggi elettorali, basati sulla previsione di comportamento ed opinione degli individui, di cui si sono studiate le abitudini attraverso operazioni di raccolta, analisi e rielaborazione delle informazioni presenti sul web, poi incrociate con ulteriori informazioni quali i dati relativi all'età, al reddito, allo stato civile etc., insomma, le "impronte digitali" lasciate sul web.

Trattandosi a tutti gli effetti di una profilazione (viene anche usato il termine tecnico di *micro-targeting*), questo tipo di trattamento genera molti problemi non solo dal punto di vista della privacy, a maggior ragione perché parliamo di dati idonei a rivelare potenzialmente opinioni e orientamenti politici e, dunque, dati che necessitano di una particolare tutela.

---

[7] M. RUBECHI, *Le modalità di elezione dei membri del Parlamento europeo*, in *federalismi.it*, n. 11/2019.

Le principali problematicità, analogamente a quanto visto per la profilazione commerciale, sono connesse all'opacità o assenza totale delle informazioni sul trattamento, al mancato rispetto del principio di legalità, all'assenza di una base legale, dal momento che nella maggior parte dei casi tali informazioni sono raccolte in origine per finalità del tutto diverse da quelle di marketing elettorale.

Per altro verso, se operazioni di questo genere servono a comprendere cosa i cittadini desiderano che i loro rappresentanti facciano e, dunque, cosa è bene che i candidati propongano per essere eletti, è evidente che le criticità non si fermano alla protezione dei dati.

Bisogna anzitutto chiedersi quale sia l'idea di democrazia che l'impiego di siffatti strumenti presuppone e, dunque, quali siano le nuove forme che la sovranità popolare e la rappresentanza politica assumono all'interno della società contemporanea al tempo dei big data[8].

In altre parole la domanda di fondo è in che modo evitare che il cittadino venga sempre più concepito (e si concepisca a sua volta) come utente o consumatore politico, piuttosto che come soggetto di partecipazione politica.

Perché, se per un verso i cittadini chiedono e pretendono più informazioni e dati per conoscere e controllare il potere politico - ma anche per partecipare, organizzarsi e mobilitarsi utilizzando la rete - dall'altro il rischio, già da tempo paventato[9], è che per questa strada si giunga ad un modello di "iperdemocrazia" basato sui limiti e sui controlli che i cittadini tramite la rete pretendono di esercitare sugli eletti.

Ora la Costituzione nella sua essenza stessa è limite al potere, e ognuno vede bene che con l'uso della rete e l'idea di una consultazione perenne dell'elettorato si registra tanto il prevalere del concetto di limite su quello di decisione e autorità, quanto l'effetto indotto di una crescente sfiducia del cittadino nei confronti degli eletti e delle istituzioni in generale.

Una dinamica che trasforma geneticamente il potere di controllo dei cittadini in automatico meccanismo di delegittimazione delle istituzioni, delineando così un esito paradossale proprio rispetto al concetto originario di sovranità popolare e rappresentanza.

Ma, è al contempo vero che se l'elettore è sempre più assimilato a un consumatore il primo effetto sarà, anche qui, quello della massificazione delle opinioni, della libera determinazione individuale, a tutto detrimento del pluralismo informativo e politico.

Non ultimo è il rischio che possa concretamente innestarsi un silenzioso meccanismo di svuotamento e, dunque, delegittimazione degli eletti e con essi dei partiti politici.

Questi ultimi originariamente svolgevano in via esclusiva il ruolo di intermediazione tra classe politica e società, tra eletti e cittadini. Una intermediazione ormai non più necessaria perché la "lettura" dei bisogni dei cittadini è affidata ad algoritmi e a tecniche di elaborazione e di calcolo.

Nell'era dei big data, dunque, i partiti politici hanno man mano perso il ruolo originario e sfruttano le informazioni nella convinzione di vincere le campagne elettorali, senza però rendersi conto che in questo modo in realtà non fanno altro che indebolire progressivamente loro stessi.

---

[8] Sia consentito il rinvio a L. CALIFANO*, Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in federalismi.it, n. 9/2017.

[9] S. RODOTA', *Iperdemocrazia. Come cambia la sovranità democratica con il web*, Editore Laterza, Roma-Bari, 2013.

È la democrazia "ibrida"[10], sempre più caratterizzata da un elevato grado di "disintermediazione".

Non vorrei essere fraintesa: l'utilizzo dei mezzi di comunicazione nell'era digitale non è un male in sé. Al contrario, essi possono rappresentare una risorsa per la democrazia rappresentativa, purché ci si limiti a concepire la rete e i social network in maniera strumentale e non finalistica, preservando il ruolo fondamentale di intermediazione democratica offerta dai partiti e dagli altri soggetti intermedi quali sindacati e associazioni.

4. C'è poi un ultimo profilo di riflessione che vorrei affrontare, in estrema sintesi pur consapevole dell'importanza crescente e delle complesse implicazioni etico -culturali prima ancora che giuridiche, e che ci conduce alle prospettive, in parte già realtà, di un uso predittivo dell'intelligenza artificiale, applicata al campo della medicina e della ricerca scientifica; in particolare nel settore della biologia molecolare dove la conoscenza sempre più profonda della struttura e delle funzioni del gene hanno condotto alla produzione di tecniche sempre più sofisticate di utilizzo del dato genetico[11].

Ragionamento che, in termini più generali, porta ad interrogarci sull'importanza che può assumere l'utilizzazione di banche dati in ambito medico-scientifico per ampliare le possibilità tanto di prevenzione e di cura di un numero crescente di malattie, quanto, ad esempio, di predisporre trattamenti farmacologici personalizzati o, ancora, le nuove tecnologie come supporto nella cura di malattie croniche e nell'assistenza domiciliare.

In proposito va anzitutto ricordato che i dati inerenti lo stato di salute (i dati « sensibili » del vecchio Codice privacy) sono sottoposti, nel nuovo regolamento europeo ad una tutela rafforzata. Per la prima volta in un testo normativo di questa rilevanza, si è inserita la definizione di dati genetici quali "dati personali relativi alle caratteristiche ereditarie o acquisite di una persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione".

A fronte di queste peculiarità e considerata l'inarrestabile crescita del progresso tecnologico e delle sempre più progredite tecniche di analisi genetica, il Legislatore europeo ha deciso di alzare il livello di tutela dei dati genetici, inserendoli nelle categorie particolari di dati (potemmo dire i "nuovi dati sensibili"), disciplinati all'art.9 GPDR.

Una categoria di dati, quelli genetici, che richiedono una particolare attenzione in ragione dei rischi per la dignità della persona che deriverebbero da un loro uso improprio. Perché la biomedicina è in grado di rivelare informazioni che riguardano non solo l'individuo singolo, ma anche ascendenti e discendenti - parliamo in tal senso di "portata narrativa" del dato genetico - e che, più di altre, possono essere usate per conoscere dati sul futuro di un individuo o di un intero gruppo biologico - parliamo in questo caso di "portata predittiva"del dato genetico.

Rischi che aumentano in maniera esponenziale in presenza di biobanche, pubbliche o private che siano, che concentrano e conservano una enorme quantità di informazioni sulle caratteristiche genetiche degli individui.

Una realtà, peraltro, che sempre più vede ampliarsi i settori in cui la genetica può trovare applicazione.

---

[10] Cfr. I. DIAMANTI, *Un salto nel vuoto. Ritratto politico dell'Italia di oggi*, I Robinson, Laterza, Napoli, 2013.

[11] L. SCAFFARDI, *Giustizia genetica e tutela della persona.* Uno studio comparato sull'uso (e abuso) delle Banche dati di DNA a fini giudiziari, Cedam, Padova, 2017. Ma sempre di L. SCAFFARDI (a cura di), *La Banca dati italiana del DNA. Limiti e prospettive della genetica forense*, Il Mulino, Bologna, 2019.

In primo luogo nell'ambito medico-scientifico, che dagli anni Cinquanta ad oggi ha vissuto grandi processi di trasformazione e di innovazione che hanno consentito importanti conquiste del vivere sociale e un miglioramento sostanziale delle condizioni di vita e delle possibilità di cura; ma le nuove scoperte nel campo delle biotecnologie e della scienza biomedica sempre più estendono le proprie potenzialità applicative all'ambito giudiziario (securitario - forense), dove le tracce genetiche e i database genetici rivestono ormai un'importanza primaria nel perseguimento delle finalità di prevenzione e accertamento dei reati e, conseguentemente, anche di garanzia di diritto di difesa degli individui. Vi è poi una progressiva crescente applicazione all'ambito dei contenziosi civilistici, ad esempio per l'accertamento della paternità, in ragione del grado di affidabilità di questa tipologia di dati, rivelando così un potenziale impatto ulteriore di carattere affettivo, relazionale e familiare che la conoscenza di queste informazioni può avere per i soggetti coinvolti.

Ancora una volta, l'eterna ansia dell'uomo di varcare ogni confine, di sapere, di conoscere, se ne rivela al contempo fragilità e debolezza, ci impone di confrontarci con il problema del limite. E la soluzione, ancora una volta, chiede il ricorso ad una eticità di comportamento, di un pensiero libero.

Cultura giuridica e diritto vivente

Cultura giuridica e diritto vivente - Rivista scientifica riconosciuta dall'ANVUR ai fini dell'ASN - è espressione del Dipartimento di Giurisprudenza (DiGiur) dell'Università di Urbino. Lo sviluppo e la manutenzione di questa installazione di OJS sono forniti da UniURB Open Journals, gestito dal Servizio Sistema Bibliotecario di Ateneo. **ISSN 2384-8901**