PER UNA TEORIA GENERALE DEI DIRITTI DIGITALI*

Abstract

Il presente saggio propone, nel quadro teorico-giuridico di un costituzionalismo digitale democratico, una "genesi logica" dei diritti digitali. L'approccio individuato consente di sviluppare una ricostruzione sistematica delle diverse famiglie di diritti digitali, ciascuna delle quali risponde a specifiche "funzioni costituenti" richieste da un governo democratico degli ambienti digitali. Rispetto al dibattito in corso, il saggio intende pervenire a una visione sistematica dei diritti digitali, capace di rispondere sia alle esigenze di tutela maturate nell'ambito della rete, sia a quelle emerse in relazione ai sistemi di intelligenza artificiale di ultima generazione. Si tratta di una ricostruzione teorica, portatrice di un'istanza critica rispetto al diritto digitale esistente, e programmatica rispetto al diritto digitale futuro. In conclusione, si richiama il necessario nesso tra questa ricostruzione e le rivendicazioni dei soggetti interessati, affinché le istanze teorico-critiche trovino la strada della loro realizzazione pratica.

This essay proposes, within the theoretical-legal framework of a democratic digital constitutionalism, a 'logical genesis' of digital rights. The approach identified makes it possible to develop a systematic reconstruction of the different families of digital rights, each of which responds to specific 'constituent functions' required by a democratic governance of digital environments. With respect to the current debate, the essay intends to arrive at a systematic vision of digital rights, capable of responding both to the protection needs that have matured in the network environment and to those that have emerged in relation to the latest generation of artificial intelligence systems. This is a theoretical reconstruction, which is critical with respect to the digital law that actually exists, and programmatic with respect to future digital law. In conclusion, we recall the necessary link between this reconstruction and the claims of the stakeholders, so that the theoretical-critical instances find their way to practical realisation.

Keywords: Digital Rights, Internet, Artificial Intelligence, Digital Constitutionalism, Digital Regulation.

* Questo lavoro, parte di una ricerca più ampia sulla regolazione democratica dei poteri digitali, deve molto ai confronti condotti all'interno dell'Officina Informatica su "Diritto, Etica, Tecnologie" istituita e coordinata dal Prof. Thomas Casadei presso il CRID – Centro di Ricerca Interdipartimentale su Discriminazioni dell'Università di Modena e Reggio Emilia, nonché al continuo dialogo con gli studenti e le studentesse che hanno frequentato l'insegnamento di "Informatica giuridica" da me tenuto presso l'Università di Camerino, nel corso di laurea in "Scienze Giuridiche per l'Innovazione organizzativa e la Coesione sociale".

1. Meriti e limiti del costituzionalismo digitale

Il dibattito sul "costituzionalismo digitale", in corso ormai da più di due decenni[1], ha avuto il merito di richiamare l'attenzione sulla centralità dei diritti nella regolazione dei poteri privati, oltre che pubblici, che guidano gli sviluppi delle nuove tecnologie e che costituiscono, di fatto, un'oligarchia globale.

La proliferazione di "manifesti", "carte" e "dichiarazioni" sui "diritti in Internet" o su "principi e diritti nell'era digitale" mostra come non si tratti di una discussione puramente accademica, ma di un "movimento costituente" con cui studiosi/e e attivisti/e, dentro e fuori le istituzioni, hanno inteso rispondere ai bisogni, alle criticità e ai conflitti che accompagnano la digitalizzazione dell'esistenza umana[2].

Tuttavia, gli approcci teorico-giuridici adottati finora su questo terreno scontano, a mio avviso, alcuni limiti che mettono a rischio il progetto di "costituzionalizzare" gli ambienti digitali, in particolare attraverso il riconoscimento e la garanzia di "nuovi diritti", o lo sviluppo di nuove interpretazioni dei diritti tradizionali.

In primo luogo, il "costituzionalismo digitale" si è a lungo focalizzato sui "diritti in *Internet*". Questa prospettiva, comprensibile fino alla metà degli anni 2010, non è più adeguata alle trasformazioni in corso stimolate dalla diffusione del cosiddetto "Internet delle cose"[3] e, soprattutto, dalla nuova stagione dell'intelligenza artificiale basata sugli algoritmi di *machine learning* e sui *big data*[4].

Inoltre, la trasformazione del web nell'epoca della sua "piattaformizzazione"[5] e del «capitalismo della sorveglianza»[6] non sempre è stata messa a fuoco dai costituzionalisti digitali come fonte di nuove e radicali criticità democratico-costituzionali e, dunque, come contesto in cui rivendica-

[1] Per un quadro d'insieme dei principali argomenti in discussione entro questa prospettiva si può vedere, da ultimo, O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 3, 2023, pp. 569-594.

[2] E. CELESTE, *Digital Constitutionalism. The Role of Internet Bills of Rights*, Adington-New York, 2023.

[3] Per un inquadramento generale di queste tecnologie dal punto di vista delle loro implicazioni giuridiche, si veda R.H. WEBER, R. WEBER, *Internet of Things. Legal Perspectives*, Berlin-Heidelberg, 2010.

[4] Per una ricostruzione accessibile dell'evoluzione storica dell'IA e per una puntuale riflessione sugli obiettivi e sulle modalità più efficaci di regolazione di tali sistemi, rimando per tutti a G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, 2022.

[5] Per una storia critica di Internet, che mette a fuoco cause e conseguenze della sua privatizzazione e commercializzazione prima, e dell'avvento delle grandi piattaforme poi, si veda B. TARNOFF, *Internet for the People. The Fight for Our Digital Future*, London-New York, 2022.

[6] S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (2019), Roma, 2023.

re specifici diritti soprattutto di tipo politico, relativi alla partecipazione della cittadinanza alla regolazione delle piattaforme.

In secondo luogo, il "costituzionalismo digitale" ha spesso sottovalutato la natura specificamente *democratica* della "crisi costituzionale" in corso, determinata dal fatto che le regole di funzionamento degli ambienti digitali in cui si svolge una parte crescente della nostra esistenza sono decise, in prima istanza, dalle società informatiche. Dal momento che tali regole sono funzionali al modello di business affermato dalle *big tech* – Google, Amazon, Facebook, Apple, Microsoft (GAFAM) – il deficit democratico che affligge la digitalizzazione planetaria ha molte caratteristiche in comune con quello prodotto dalla globalizzazione neoliberale[7].

Ne sono risultate diverse ambiguità teorico-pratiche, riconducibili in ultima analisi a una mancata critica dell'economia politica digitale e del ruolo svolto dal diritto, dai giuristi e dalle autorità pubbliche nell'affermazione del regime oligopolistico di GAFAM. Così, ad esempio, alcuni studiosi hanno ritenuto legittimo assegnare parte del "potere costituente digitale", ossia del potere di plasmare le regole fondamentali degli ambienti cibernetici, direttamente alle grandi società informatiche, che della regolazione in senso costituzionale dovrebbero invece essere l'oggetto[8].

Altri studiosi, invece, hanno ristretto in modo eccessivo gli spazi di trasformabilità dell'attuale ecosistema digitale attraverso una regolazione costituzionalmente orientata, promuovendo una "negoziazione di interessi" all'interno di un ordine economico-politico già stabilito, e assunto come sostanzialmente immodificabile, piuttosto che un conflitto profondo sul tipo di "mondo digitale" in cui si vuole vivere.

Forse anche a causa di queste ambiguità, finora non sono emerse nel dibattito né una definizione precisa di che cosa siano e di quali siano i "diritti digitali", né una loro giustificazione rigorosa, né una loro ricostruzione sistematica. Nel tentativo di colmare queste lacune teoriche, intendo proporre una «genesi logica»[9] dei diritti digitali, accompagnata da alcune indicazioni necessariamente sommarie sul "sistema di garanzie" che dovrebbe accompagnare la loro piena realizzazione.

---

[7] R.W. MCCHESNEY, *Digital Disconnect. How Capitalism Is Turning the Internet Against Democracy*, New York, 2013.

[8] Per questa e altre critiche al costituzionalismo digitale, si raccomanda P. TERZIS, *Against digital constitutionalism*, in *European Law Open*, 2024, pp. 1-17.

[9] Traggo da Jürgen Habermas questo approccio teorico-metodologico, ritenendolo preferibile ad altri per almeno tre ragioni: la sua vocazione alla completezza e alla sistematicità nella ricostruzione dei diritti; la sua capacità di mettere in luce le diverse "funzioni costituenti" che i diritti assolvono nell'attuare il principio democratico; il suo riconoscimento dei diritti politici come centro di gravità del sistema, pur nella natura interdipendente e indivisibile

Come i diritti tradizionali, ritengo che anche quelli digitali possano essere utilmente classificati in quattro grandi famiglie – civili, politici, sociali e culturali, giudiziari – corrispondenti ad altrettante "funzioni costituenti" necessarie per fare un uso legittimo del diritto all'interno di un regime costituzionale democratico. Le diverse famiglie di diritti codificano, in questa prospettiva, le condizioni necessarie a sviluppare e mantenere forme di vita emancipate, su cui sono gli stessi interessati a doversi mettere d'accordo.

Nell'avviare operazioni ricostruttive di questa natura, occorre sempre tener desta la consapevolezza che si tratta di un'istanza teorico-giuridica, finalizzata a fare emergere un "dover essere" interno al diritto e alla sua logica normativa. Tale istanza consente «la critica del diritto invalido e la progettazione del diritto dovuto, l'uno indebitamente prodotto dalla politica e l'altro da questa indebitamente non prodotto»[10].

Il rischio di sfociare, lungo questo percorso, nell'utopia giuridica è un rischio calcolato e forse inevitabile. Se è vero che stiamo attraversando una crisi costituzionale, causata in parte dalla "rivoluzione digitale", abbiamo bisogno di una teoria critica del diritto e dell'informatica giuridica e di una teoria generale dei diritti digitali che ci indichino come traghettare le conquiste del costituzionalismo democratico del Novecento nel nuovo secolo, individuando e costruendo strada facendo le soggettività sociali e politiche che possono farsene carico.

2. Diritti (civili) a un uso pieno, libero e sicuro degli ambienti digitali

La prima funzione costituente è quella che *istituisce* i soggetti stessi del diritto e dei diritti, ossia la loro capacità di (inter)agire in quanto persone giuridiche, garantendo loro «la maggior misura possibile di pari libertà soggettive»[11]. Su questa base è possibile identificare una prima famiglia di diritti digitali, di natura personale, analoghi ai tradizionali diritti civili, chiamati a garantire a tutti e a ciascuno l'*uso pieno, libero e sicuro degli ambienti digitali e dei sistemi di intelligenza artificiale.*

Questa definizione si basa sull'ipotesi che, oggi, coloro che sono interessati a democratizzare la "rivoluzione digitale", potrebbe ragionevolmente rivendicare tre usi delle nuove tecnologie: un uso *libero* da forme ingiustificate o eccessive di condizionamento o controllo; un uso *pieno* rispet-

dei diritti. Si veda J. HABERMAS, *Fatti e norme. Contributi a una teoria discorsiva del diritto e della democrazia* (1992), Roma-Bari, 2013.

[10] L. FERRAJOLI, *La costruzione della democrazia. Teoria del garantismo costituzionale*, Roma-Bari, 2021.

[11] J. HABERMAS, *Fatti e norme*, cit., p. 446.

to alle risorse e alle opportunità che tali tecnologie offrono allo sviluppo individuale e collettivo; un uso *sicuro* rispetto al rischio di subire danni materiali, biologici, esistenziali o morali, o di vedere alterati i presupposti etici, giuridici e istituzionali di una società democratica.

In questa prima famiglia possono essere distinti specifici gruppi di diritti digitali, individuabili a partire dalle funzioni necessarie per consentire a tutti e a ciascuno di fare *concretamente* un uso libero, pieno e sicuro delle tecnologie digitali. In questo senso, ritengo che negli ambienti digitali debbano essere garantiti i diritti a: 1) essere e "sentirsi" persone a tutti gli effetti; 2) accedere alle informazioni e alle conoscenze disponibili online; 3) agire individualmente e collettivamente, secondo finalità di tipo comunicativo, sociale, culturale, economico, politico, istituzionale. Nell'esercizio di questi diritti/libertà digitali fondamentali deve essere garantita, a tutti e a ciascuno, integrità e sicurezza rispetto a tutti e tre i livelli degli ambienti digitali: quello fisico, quello logico e quello sociale.

Alcune rapide considerazioni sulla ragion d'essere e sui contenuti di questi diversi gruppi di diritti personali. In un regime costituzionale democratico, il diritto deve tutelare innanzitutto la capacità di tutti gli esseri umani di concepirsi e riconoscersi reciprocamente come soggetti imputabili di azioni e omissioni: senza questa condizione non si potrebbe regolare efficacemente una "società di individui liberi e uguali". Il concetto di "personalità giuridica" formalizza e configura la capacità degli esseri umani di sentirsi gli autori responsabili di atti aventi rilevanza anche giuridica, ossia di essere *soggetti di diritto*[12].

Se questo è vero, una tecnologia digitale che avesse come conseguenza diretta o indiretta la compromissione della capacità d'agire e di sentirsi persone degli esseri umani, limitando, condizionando o distruggendo le condizioni che consentono di prendere decisioni libere e consapevoli, dovrebbe essere vietata o, quanto meno, dovrebbe sottostare a rigide regole d'uso commisurate ai rischi sollevati e ai vantaggi attesi. Minando le condizioni di possibilità della personalità giuridica, infatti, una simile tecnologia disumanizzerebbe la società e metterebbe a repentaglio la sensatezza stessa del diritto, oltre che la sua legittimità.

[12] Non tutte le persone giuridiche sono esseri umani. Accanto alle persone umane, che chiamiamo "fisiche" o "naturali", esistono le "persone giuridiche" o "artificiali", come gli Stati o le società commerciali: entità dotate di personalità giuridica dal diritto e da questo istituite come centri di imputazione di atti o di situazioni. Sulla possibilità di estendere la personalità giuridica a entità naturali o macchiniche, si veda S. PIETROPAOLI, *Persone non umane? Una riflessione sulla frontiera digitale del diritto*, in R.M. AGOSTINO, G. DALIA, M. IMBRENDA, S. PIETROPAOLI (a cura di), *Frontiere digitali del diritto. Esperienze giuridiche a confronto su libertà e solidarietà*, Torino, 2022, pp. 1-21.

Da questo punto di vista i processi di datificazione e automatizzazione dell'esistenza umana, che oggi accompagnano e orientano la digitalizzazione sempre più spinta, costituiscono un rischio sistemico per le società fondate sul diritto almeno per due ragioni. La prima è che tali processi tendono a ridurre la persona umana ai dati che essa rilascia, consapevolmente o meno, negli ambienti digitali o che vengono "estratti" dai suoi comportamenti allo scopo di produrre «valore»[13]. La seconda è che alcuni tipi di trattamento dei dati personali influiscono fortemente sull'architettura delle nostre scelte, sia dentro che fuori gli ambienti digitali, secondo modalità poco o per nulla trasparenti, prestandosi ad abusi e producendo effetti discriminatori[14].

Non si tratta solo di problemi contingenti, causati da errori, ma di processi connaturati alla "colonizzazione" capitalistica e burocratica degli ambienti digitali, fondata sul tracciamento costante degli esseri umani e sulla registrazione sistematica dei loro comportamenti. Tali processi possono essere fermati, o almeno mitigati, attraverso norme giuridiche e pratiche sociali fondate sull'«autodeterminazione informativa»[15]. In base a tale principio, *sono ammissibili solo quei processi di digitalizzazione, datificazione e automatizzazione che assegnano alle persone umane un pieno e persistente controllo sui propri dati e sull'uso che ne viene fatto, in particolare su loro stesse*. Questo principio è il fondamento dei numerosi diritti digitali connessi alla "protezione dei dati personali"[16].

Per quanto riguarda la libertà d'agire digitale, ritengo se ne possano distinguere tre categorie fondamentali in base agli ambiti esistenziali interessati: le libertà d'azione sociale (necessarie per esprimersi, comunicare, cooperare, organizzarsi per finalità comuni); le libertà d'iniziativa econo-

---

[13] A.A. CASILLI, *Schiavi del clic. Perché lavoriamo tutti per il nuovo capitalismo?* (2019), Milano, 2020.

[14] F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge (MA), 2015.

[15] La nozione di "autodeterminazione informativa" è stata introdotta da Stefano Rodotà. Vista la sua portata fondamentale, ritengo debba meritare il rango di "principio", più che di diritto. L'autore ha messo in luce, tra i primi in Italia, il rischio connesso alla datificazione dell'esistenza: «Quando la relazione tra i poteri pubblici e privati e le persone viene basata su di un ininterrotto *data mining*, sulla raccolta senza limiti di qualsiasi informazione che le riguardi, e affidata poi all'algoritmo, le persone sono trasformate in astrazioni, la costruzione della loro identità viene sottratta alla loro consapevolezza, il loro futuro affidato al determinismo tecnologico. Tutto questo incide sui diritti fondamentali, mette in discussione la libera costruzione della personalità e l'autodeterminazione, imponendo così di chiedersi se e come la società dell'algoritmo possa essere democratica». Si vedano S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995; ID., *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[16] In un regime democratico costituzionale, ogni persona fisica deve poter esercitare almeno: il diritto a essere informato in modo sintetico e comprensibile sugli aspetti qualificanti della raccolta dati cui è sottoposto online; il diritto di accedere a tutti i propri dati in possesso di un determinato soggetto pubblico o privato operante in rete; il diritto a rettificare, integrare o aggiornare i propri dati; il diritto di interrompere in qualsiasi momento un trattamento dei propri dati che violi dei diritti fondamentali e di chiedere l'annullamento delle decisioni adottate su tale base; il diritto di revocare il consenso al trattamento, laddove questo sia ammesso come base legale sufficiente; il diritto a che i propri dati vengano cancellati in caso di abuso o di esaurimento delle finalità del trattamento; il diritto alla deindicizzazione di contenuti di natura personale dai motori di ricerca laddove non si riscontri un prevalente interesse pubblico alla loro persistente accessibilità online.

mica (necessarie per produrre, vendere, scambiare, acquistare beni e servizi sui mercati digitali); le libertà d'azione civica (necessarie per accedere a beni e servizi gestiti dalle pubbliche amministrazioni digitali).

I membri di una comunità democratica devono riconoscersi reciprocamente il medesimo grado di libertà digitali, estendendone la portata e l'esercizio quanto più possibile ma comunque in modo compatibile con le libertà degli altri, l'integrità individuale, la sicurezza collettiva e la tutela di altri interessi pubblici. Gli specifici beni richiesti per poter esercitare concretamente queste libertà devono essere tutelati da altrettanti diritti che, in caso di conflitti, richiedono procedure per un loro bilanciamento equo ed efficace.

In particolare, le libertà d'agire sociale richiedono di riconoscere come minimo il diritto alla libertà di espressione, di comunicazione e di associazione negli ambienti digitali. Tali libertà, fondamentali per una democrazia costituzionale, trovano il loro limite nella tutela della pari dignità sociale e dell'integrità di tutti i membri della società, con particolare riguardo ai membri di gruppi storicamente e attualmente segnati da vulnerabilità[17]. Ciò comporta, ad esempio, il divieto dei discorsi e dei reati d'odio online, con la conseguente censura delle pagine web che li contengono o li incoraggiano, dei profili e dei gruppi social che li producono e diffondono; ma anche l'introduzione di "aggravanti digitali" per quei reati come la pornografia minorile, gli atti persecutori e la diffusione non consensuale di materiale sessualmente esplicito che, consumati per via informatica o telematica, accrescono il loro potenziale di offensività.

La libertà d'iniziativa economica, in un sistema capitalistico di mercato soggetto ai principi di un costituzionalismo democratico, richiede di riconoscere negli ambienti digitali come in quelli non digitali i seguenti tipi di diritti: il diritto all'autonomia negoziale; il diritto a svolgere un'attività lavorativa di propria scelta, confacente alle proprie aspirazioni, in condizioni libere da sfruttamento e discriminazioni; il diritto di possedere, utilizzare, disporre e trasmettere beni e servizi, sia fisici che digitali; il diritto ad accedere e operare su mercati digitali aperti e concorrenziali, non oligopolistici o monopolistici; i diritti dei consumatori in materia di informazioni contrattuali e sicurezza dei prodotti.

[17] Per una definizione concettuale dei discorsi d'odio online e per le relative sfide di natura giuridica, mi permetto di rinviare a F. OLIVERI, *Diritti degli internauti, obblighi degli Stati, responsabilità delle piattaforme digitali: problemi regolativi in materia di odio online*, in *Teoria e Critica della Regolazione Sociale*, 2, 23 (*Teoria e prassi dell'informatica giuridica: una riflessione filosofica*), 2021, pp. 105-125.

Vale per le attività economiche che si svolgono in ambienti digitali la medesima condizione di fondo valida per quelle che si svolgono in ambienti non digitali: esse non possono svolgersi in contrasto con l'utilità sociale generale o in modo da recare danno alla salute, alla sicurezza, alla libertà, alla dignità umana, all'ambiente.

La libertà d'azione civica riguarda tutte le forme d'interazione, regolate dalla legge, tra i membri di una comunità giuridica e le istituzioni specializzate a cui, nelle società complesse, sono affidate le funzioni amministrative. Il suo esercizio, in un'epoca di digitalizzazione delle pubbliche amministrazioni, richiede siano riconosciuti almeno i seguenti diritti: il diritto di accedere a tutti i servizi pubblici erogati dall'amministrazione anche attraverso siti web, portali o altri canali digitali, con modalità semplici e gratuite; il diritto a utilizzare un'identità digitale unica per accedere a tali servizi; il diritto di richiedere e ottenere anche per via telematica l'accesso a dati, documenti e informazioni detenuti dalle pubbliche amministrazioni e da altri enti, senza bisogno di dimostrare un interesse specifico; il diritto di partecipazione ai procedimenti amministrativi telematici; il diritto alla legalità, alla pubblicità e alla motivazione dei provvedimenti adottati con modalità (semi)automatiche; il diritto a non essere sottoposti a decisioni amministrative interamente automatizzate; il diritto a non essere discriminati nelle relazioni con la pubblica amministrazione anche nel caso in cui, per scelta o impedimento, non ci si avvalga di strumenti digitali; il diritto a eseguire pagamenti spettanti a qualsiasi titolo alla pubblica amministrazione mediante servizi elettronici[18].

L'esercizio delle libertà digitali comporta rischi per i singoli e per la società. L'integrità personale e collettiva può essere minacciata e compromessa in molti modi negli ambienti digitali e nelle interazioni con sistemi di intelligenza artificiale: garantirla in modo equilibrato costituisce una necessità, nel quadro di un costituzionalismo democratico, per consentire un uso pieno e sicuro delle nuove tecnologie. Il diritto penale dell'informatica svolge un ruolo centrale nel tutelare i numerosi beni giuridici e i corrispettivi diritti che entrano in gioco in questo ambito: la sua definizione e implementazione devono, comunque, essere coerenti con i principi del garantismo[19].

[18] La garanzia di tali diritti deve ispirare il perseguimento, da parte delle pubbliche amministrazioni, degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nel rispetto dei principi di uguaglianza e di non discriminazione. Ancorché fondamentali, le libertà d'azione civica nei rapporti con la pubblica amministrazione digitalizzata non esauriscono il campo della "cittadinanza digitale", che va identificata nella titolarità e nell'esercizio paritetico di *tutti* i diritti necessari all'implementazione del principio democratico negli ambienti informatici.

[19] L. FERRAJOLI, *Diritto e ragione. Teoria del garantismo penale*, Roma-Bari, 1989; ID., *Giustizia e politica. Crisi e rifondazione del garantismo penale*, Roma-Bari, 2024.

3. Diritti (politici) di partecipazione e controllo sugli ambienti digitali

La seconda funzione costituente è quella che istituisce i soggetti di diritto come co-autori delle norme giuridiche cui sono sottoposti, consentendo loro di riconoscerle come il risultato di un processo pubblico e regolato di auto-legislazione. A questo scopo, occorre garantire a tutti gli interessati, quelle «pari opportunità di partecipazione ai processi formativi dell'opinione e della volontà»[20] da cui soltanto si origina diritto legittimo in un regime costituzionale democratico.

Rispetto agli ambienti digitali, si tratta della famiglia di diritti *politici* finalizzati a garantire l'autonomia pubblica dei soggetti di diritto, ossia ad assicurare a tutti e a ciascuno un *controllo democratico condiviso rispetto ai processi di digitalizzazione, datificazione e automatizzazione dell'esistenza*. In virtù di questi diritti, occorre sia garantita la partecipazione popolare più ampia possibile alla discussione, alla definizione e all'implementazione delle regole vigenti gli ambienti digitali, con particolare attenzione alle "tecno-regole" ossia alle stringenti norme di comportamento incorporate dai programmatori, per conto delle società informatiche, nel codice e negli algoritmi che governano quegli ambienti.

In effetti, le tecno-regole hanno la peculiarità di venire applicate in maniera automatica nell'interazione con gli esseri umani, senza la loro collaborazione attiva o consapevole, e senza l'intervento di soggetti terzi incaricati di sorvegliarne l'*enforcement* e verificarne la validità. Come ha chiarito il costituzionalista Lawrence Lessig, online a ciascuno è «lecito fare quanto egli è, di fatto, in grado di fare […], ma egli è in grado di fare solo ciò che è stato abilitato a fare […]. Non si può scegliere se cedere o meno alla richiesta di una password: si deve obbedire, se si vuole entrare nel sistema»[21].

Gli attuali sviluppi dell'intelligenza artificiale richiedono, inoltre, di distinguere tra tecno-regole deterministiche e probabilistiche. Le prime operano in modo interamente predeterminato su base logico-matematica: salvo errori, la loro implementazione è l'esito prevedibile di una programmazione esplicita e completa. Le seconde, invece, operano in modo solo parzialmente prestabilito: la loro implementazione è l'esito di algoritmi di apprendimento automatico che, dopo

[20] J. HABERMAS, *Fatti e norme*, cit., p. 142.

[21] L. LESSIG, *Code And Other Laws Of Cyberspace*, New York, 1999. Le tecno-regole interagiscono con altre quattro tipologie regolative: le norme giuridiche, le norme sociali, le regole economiche, le regole d'uso private sottoscritte dagli utenti nel momento in cui accedono a piattaforme e altri ambienti digitali complessi. Le norme giuridiche, per ottenere effetti vincolanti, possono agire sulle tecno-regole modificando l'architettura degli ambienti digitali.

essere stati "addestrati" su grandi quantità di dati, vengono fatti interagire con gli utenti e con l'ambiente, producendo esiti non sempre spiegabili[22].

La diversa natura degli ambienti digitali, ossia le diverse tipologie di attori presenti e di regole vigenti in ciascuno di questi, richiede una appropriata differenziazione dei diritti politici esercitabili dagli interessati. Occorre garantire a tutti e a ciascuno la più ampia facoltà possibile di partecipare a: 1) procedure di co-legislazione, in cui dibattere e adottare le regole giuridiche ritenute necessarie per garantire l'esercizio di tutti gli altri diritti digitali, indicando per ciascuno di essi contenuti minimi, limiti, criteri di bilanciamento e correlativi obblighi in capo ai soggetti dotati del potere di assicurarli o negarli; 2) procedure di co-regolazione, in cui dibattere e adottare le regole d'uso o gli "standard di comunità" vigenti negli ambienti digitali "privati", come le piattaforme digitali; 3) procedure di co-gestione e personalizzazione, libera e consapevole, della propria esperienza online e delle proprie interazioni con sistemi di intelligenza artificiale.

Co-legislazione, co-regolazione e co-gestione rappresentano tre livelli, progressivamente più specifici e ristretti, in cui gli interessati *devono* poter partecipare alla definizione delle regole digitali cui sono sottoposti. In virtù del principio democratico, infatti, «le norme giuridiche sono pienamente valide se sono approvabili da tutti i consociati in un processo discorsivo di statuizione, a sua volta giuridicamente costituito»[23].

La differenziazione di questi tre livelli, così come il loro rapporto, è ispirato a principi di *sussidiarietà gerarchica delle fonti*. Da una parte, i livelli superiori stabiliscono gli obiettivi generali da perseguire, ossia i diritti fondamentali da garantire e i corrispettivi obblighi da assegnare, le strategie da adottare per raggiungere tali obiettivi e le condizioni per delegare parte dell'attività regolativa ai livelli inferiori, ove questi siano riconosciuti come meglio attrezzati allo scopo (sussidiarietà). Dall'altra parte, ciò che viene deciso nei livelli inferiori non può andare sostanzialmente in contrasto con quanto stabilito dai livelli superiori: i termini d'uso delle piattaforme digitali non possono derogare alla garanzia dei principi generali dell'ordinamento e dei diritti fondamentali, così come le opzioni di personalizzazione dell'esperienza online devono essere coerenti sia con i principi generali dell'ordinamento che con le regole d'uso applicabili (gerarchia delle fonti).

In breve: negli ambienti digitali gli spazi di autoregolamentazione dei soggetti privati, che siano società o singoli individui, vanno incoraggiati quanto più possibile ma, al tempo stesso, de-

[22] M. HILDEBRANDT, *Algorithmic regulation and the rule of law*, in *Philosophical Transactions A*, 376, 2128, 2018.

[23] J. HABERMAS, *Fatti e norme*, cit., p. 128.

vono essere circoscritti alla scelta dei *mezzi tecnici* ritenuti più efficaci per perseguire, in concreto, gli *obiettivi giuridico-politici* fissati dalla legislazione, implementati dall'amministrazione, difesi ed eventualmente precisati dalle corti.

In sede di co-legislazione gli interessati discutono e deliberano, innanzitutto, sui diritti digitali di cui ritengono necessario godere per vivere una vita libera e dignitosa, e su quali soggetti abbiano il potere e l'obbligo di garantirli efficacemente. La discussione verte anche sulle strategie regolative ritenute di volta in volta più efficaci, rispetto all'ambito di regolazione e ai soggetti coinvolti. In questo senso, la co-legislazione può: 1) intervenire sulle regole dei mercati digitali, attraverso disposizioni in materia di concorrenza, di commercio e pagamenti elettronici, di sicurezza dei prodotti e dei servizi, di tassazione delle società tecnologiche; 2) prescrivere determinati obiettivi e contenuti irrinunciabili per le regole d'uso di piattaforme, servizi digitali e sistemi di IA; 3) incoraggiare, attraverso determinate campagne pubbliche, lo sviluppo e la diffusione di determinate norme sociali per l'uso degli ambienti digitali; 4) prescrivere ai soggetti competenti determinate modifiche alle regole architettoniche degli ambienti digitali, dando luogo a *tecno-diritto* in senso stretto[24].

Promuovere tali forme di partecipazione è un *obbligo* delle autorità pubbliche, per quanto riguarda le procedure di co-legislazione, e dei soggetti pubblici e/o privati coinvolti, per quanto riguarda le procedure di co-regolazione. Ciò significa, in concreto, che i legislatori dovrebbero adottare norme di "diritto digitale" dopo aver svolto adeguate procedure partecipative e deliberative (come, per altro, sarebbe auspicabile in ogni ambito della legislazione). Ma significa anche che le grandi piattaforme o altri fornitori di servizi online non dovrebbero adottare termini d'uso o standard di comunità senza che si siano svolte adeguate procedure di co-regolazione con gli utenti o con i possibili interessati (ben diversamente da quanto avviene oggi, quando le regole d'uso vengono passivamente accettate dagli utenti, desiderosi di accedere il più rapidamente possibile a un servizio online).

In concreto, si possono immaginare e codificare varie forme di partecipazione alla definizione delle regole degli ambienti digitali da parte degli interessati, sia in presenza che per via tele-

[24] Come è normale in un settore disciplinare ancora giovane, come quello dell'informatica giuridica, si assiste di frequente a oscillazioni terminologiche. Alla luce di quanto fin qui affermato, propongo di distinguere tra "tecno-regole" e "tecno-diritto": le prime sono le regole incorporate nel codice e negli algoritmi dai loro programmatori secondo le indicazioni dei proprietari e dei gestori degli ambienti digitali; il secondo è l'insieme delle norme giuridiche che operano negli ambienti digitali servendosi delle tecno-regole, ingiungendo ai proprietari e ai gestori di tali ambienti di modificarle.

matica: si tratta di elaborare attivamente e collettivamente le regole che meglio rispondono al tipo di "società digitale" in cui si vuole vivere.

Se, come prevedibile, la partecipazione diretta di tutte le persone interessate si rivelasse impraticabile, occorrerà predisporre adeguati meccanismi di rappresentanza, dal livello locale a quello globale, delegando allo scopo associazioni, movimenti e collettivi accreditati come "difensori dei diritti digitali".

Rispetto all'esigenza di partecipare alla definizione delle regole delle nuove tecnologie e di controllarne l'implementazione, il principale ostacolo non mi pare tuttavia di natura tecnica, ma etico-politica: il fatto di vivere in ambienti le cui regole sono stabilite da altri, ma in cui sono in gioco la nostra libertà e i nostri diritti, sembra non essere avvertito dalla grande maggioranza delle persone come un problema.

4. Diritti (sociali e culturali) abilitanti a un esercizio paritario degli altri diritti digitali

La terza funzione costituente è quella che assicura a tutti gli interessati le risorse – sociali, economiche, tecnologiche, culturali, informative – che li abilitano a esercitare tutti i diritti digitali, in concreto e in condizione di massima parità possibile. Rispetto alle nuove tecnologie, si tratta di diritti analoghi ai tradizionali diritti sociali e culturali, chiamati a garantire a tutti e a ciascuno l'*accesso effettivo e consapevole alla rete, agli ambienti digitali, ai sistemi di intelligenza artificiale* e alle loro molteplici funzionalità. Tali diritti sono cruciali per contrastare le molteplici forme che assumono le diseguaglianze digitali[25].

In questa famiglia figurano, essenzialmente, tre categorie di diritti: 1) diritti di accesso agli ambienti digitali e alle loro risorse; 2) diritto all'informazione rispetto al funzionamento degli ambienti digitali, compreso l'esercizio dei propri diritti; 3) diritto a una formazione di qualità in termini di conoscenze, abilità e competenze richieste per (inter)agire in modo consapevole e critico negli ambienti digitali, comprendendo adeguatamente le relative informazioni ricevute.

La natura abilitante di questi diritti è evidente e difficile da sottovalutare nella sua importanza. Nessuno dei diritti digitali enunciati e discussi fin qui, ma anche nessuno dei diritti tradizionali oggi sempre più spesso esercitati attraverso procedure digitali, potrebbe essere effettiva-

[25] E.J. HELSPER, *The digital disconnect. The social causes and consequences of digital inequalities*, London, 2021. Per una ricostruzione delle molteplici dimensioni del fenomeno, si veda S. VANTIN, *I divari digitali nell'epoca della rete globale*, in TH. CASADEI, S. PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, seconda edizione ampliata e aggiornata, Milano, 2024, pp. 297-311.

mente goduto, se non fosse tecnicamente possibile connettersi alla rete in modo stabile, sicuro, veloce, economico, se l'accesso paritario ai contenuti della rete venisse impedito o alterato, se il mero accesso tecnico non fosse supportato da adeguate informazioni e accompagnato da conoscenze, abilità e competenze critiche, tali da rendere tutte e tutti in grado di comprendere il funzionamento delle nuove tecnologie e prevenirne i rischi.

Tra i diritti di accesso, occorre garantire nell'ordine: 1) il diritto a una "connettività significativa", ossia a una connessione di livello adeguato rispetto a quanto tecnicamente possibile e a quanto richiesto per fare un uso pieno della rete; 2) il diritto a un'accessibilità piena e paritaria dei contenuti e delle funzionalità della rete, senza censure, senza discriminazioni rispetto alla provenienza, alla destinazione e alla tipologia dei dati, ma anche rispetto al tipo di dispositivo usato per la connessione; 3) il diritto alla protezione da distacchi arbitrari e punitivi della rete.

Asserire il diritto a una connettività significativa significa porre precisi obblighi in capo alle autorità pubbliche e, per quanto di loro competenza, anche ai soggetti privati di garantire un livello di connettività tale da consentire agli utenti un'esperienza online sicura, soddisfacente, arricchente e produttiva a un costo accessibile[26]. La significatività della connessione si misura in termini di qualità dei servizi di rete – disponibilità, sicurezza, velocità, tempi di latenza, affidabilità, stabilità – ma anche di dispositivi utilizzati[27] e di costi sostenibili per l'acquisto dei mezzi di connessione.

Asserire il diritto a un'accessibilità piena e paritaria degli ambienti digitali significa, invece, mettere in luce la necessità di politiche pubbliche e condotte private che rispettino il principio di *neutralità della rete e dei dispositivi*. Il primo principio obbliga tutti i fornitori di servizi digitali a garantire un accesso equo e non discriminatorio ai contenuti e alle applicazioni online da loro gestiti[28]. Il secondo principio obbliga gli stessi a non discriminare o limitare l'accesso a contenuti,

[26] D. THAKUR, T. WOODHOUSE, *Meaningful Connectivity. A New Target to Raise the Bar for Internet Access*, 2020.

[27] Nella maggior parte dei paesi a basso reddito la connessione avviene tramite dispositivi di telefonia mobile. Ciò si verifica anche nelle fasce vulnerabili della popolazione dei paesi ad alto reddito. Il problema, sottovalutato dalle statistiche mondiali sul *digital divide*, è che l'esperienza di rete può variare significativamente tra connessioni desktop e mobili a causa di diversi fattori. A titolo d'esempio, schermi più grandi, tastiere e mouse facilitano la navigazione, la visualizzazione di contenuti multimediali e l'utilizzo di applicazioni complesse, specialmente per motivi di studio o lavoro. Sul punto si veda, tra i tanti, T. CORREA, I. PAVEZ, J. CONTRERAS, *Digital inclusion through mobile phones? A comparison between mobile-only and computer users in Internet access, skills and use*, in *Information, Communication & Society*, 23, 7, 2020, pp. 1074-1091.

[28] Un caso esemplare di violazione del principio di neutralità della rete è costituito da Internet.org, l'applicazione di "accesso gratuito a Internet" promossa da Facebook nei paesi a basso reddito negli anni '10 del nuovo secolo. L'accesso gratuito fornito da Internet.org era limitato a un numero ristretto di siti web e app, tra cui ovviamente Facebook, il che non permetteva agli utenti di accedere all'intera gamma di contenuti e servizi disponibili su Internet. In India il programma è stato contestato da un gruppo di attivisti che, grazie alla campagna *Save the Inter-*

servizi o applicazioni in base al tipo di dispositivo utilizzato per la connessione. Il blocco di determinati contenuti e servizi online deve sempre essere fondato su violazioni di norme giuridiche, la cui applicazione al caso specifico deve essere validata dalle competenti autorità di garanzia (si veda dopo).

Infine, il diritto a non essere disconnessi in modo arbitrario e punitivo dalla rete, implica un divieto delle pratiche di *Internet shutdown*[29] operate dai propri governi per "motivi di sicurezza", o da potenze straniere durante un conflitto armato[30].

Il diritto all'informazione è chiamato a garantire a tutti coloro che operano e interagiscono in ambienti digitali la possibilità di sapere e comprendere come funziona la rete, i programmi, le applicazioni, le piattaforme, i servizi online, i sistemi di IA che utilizzano. Affinché tali informazioni possano raggiungere il numero più ampio possibile di persone, esse devono essere formulate in modo semplice, chiaro, conciso, completo, devono essere facilmente accessibili e devono essere periodicamente verificate e aggiornate.

A tale diritto corrispondono precisi obblighi di *trasparenza* da parte dei proprietari e degli operatori di ambienti digitali, rispetto al livello fisico, logico e sociale di tali ambienti. Le informazioni dovute possono includere, tra le altre cose: le modalità e le finalità del trattamento dei dati personali, le politiche di moderazione dei contenuti, le finalità e il funzionamento degli algoritmi utilizzati per personalizzare i contenuti e le raccomandazioni, tutte le informazioni necessarie a poter utilizzare e difendere pienamente i propri diritti digitali, quali dati sono stati usati per addestramento dei sistemi di IA, la loro fonte, le modalità di raccolta, i rischi che potrebbe presentarne l'uso, l'identità dei creatori, dei proprietari e degli utilizzatori dei sistemi di IA, l'indicazione chiara se si sta interagendo con contenuti o con agenti artificiali, l'indicazione chiara

---

net, hanno aperto un ampio dibattito sulla neutralità della rete. In seguito alle critiche l'applicazione Internet.org è stata ribattezzata *Free Basics*, ma la maggior parte delle criticità precedentemente rilevate non sono state rimosse. Si veda, tra molti, R. PRASAD, *Ascendant India, digital India: how net neutrality advocates defeated Facebook's Free Basics*, in *Media, Culture & Society*, 40, 3, 2018, pp. 415-431.

[29] La nozione di "*Internet shutdown*" (letteralmente "interruzione di Internet") comprende un'ampia gamma di interferenze e limitazioni all'uso della rete, realizzate attraverso il danneggiamento o la disattivazione di infrastrutture fondamentali, l'interferenza con le informazioni di routing, la manipolazione del sistema dei nomi dominio, l'implementazione di meccanismi di filtraggio, la drastica limitazione della velocità di connessione. I governi usano generalmente tali pratiche per eludere le proprie responsabilità in gravi violazioni dei diritti umani, nel quadro di azioni repressive contro proteste popolari o di azioni militari contro formazioni paramilitari e altri soggetti classificati come pericolosi per l'ordine pubblico e la sicurezza dello Stato.

[30] Nel 2023, l'organizzazione *Access Now* e la coalizione *#KeepItOn* hanno documentato 283 Internet shutdown in 39 paesi del mondo. Sul diritto a non essere disconnessi, si vedano almeno J. RYDZAK, *Disconnected. A Human Rights-Based Approach to Network Disruptions*, in *Global Network Initiative*, 9, 2018; A.R. GOHDES, *Repression technology. Internet accessibility and state violence*, in *American Journal of Political Science*, 64, 3, 2020, pp. 488-503.

se si è sottoposti a decisioni interamente o parzialmente automatizzate, il diritto a ricevere spiegazioni esaurienti rispetto agli esiti di questo genere di decisioni[31].

Il diritto a una formazione di qualità in materia di tecnologie digitali comporta obblighi, in capo alle autorità pubbliche, di promuovere attraverso il sistema pubblico dell'istruzione lo sviluppo di competenze digitali che vadano oltre le mere abilità informatiche. Spesso ci si riferisce a questo campo col termine "alfabetizzazione digitale": non si tratta solo di saper usare computer e smartphone, ma di possedere le conoscenze e le abilità necessarie per sfruttare al meglio le tecnologie digitali al fine di apprendere, comunicare, lavorare, accedere a servizi, esercitare diritti e partecipare attivamente alla società, nella piena consapevolezza del funzionamento e dei rischi connessi agli ambienti digitali.

Si tratta, dunque, di sviluppare una comprensione complessiva dell'impatto sociale, economico, politico ed etico delle tecnologie digitali, inclusi i sistemi di intelligenza artificiale di ultima generazione, così da promuoverne un uso critico, responsabile e consapevole, ma anche trasformativo, in modo da rendere gli ambienti digitali più democratici ed equi, oltre che più sicuri.

In assenza di politiche educative di questo livello, rischia di verificarsi quanto denunciato precocemente da Carlo Formenti, in termine di stratificazione digitale-sociale: «l'élite degli utenti colti accede in misura enormemente superiore alle opportunità (economiche, culturali, formative, informative, comunicative, di partecipazione politica, ecc.) offerte dai nuovi media, rispetto alla massa degli utenti di fascia medio-bassa, i quali usano la rete quasi esclusivamente a fini di *entertainment* e consumo privato»[32].

5. Diritti (giudiziari) di difesa dei diritti digitali in caso di violazione

La quarta e ultima funzione costituente di una comunità democratica è quella che assicura, in modo paritario, vie di ricorso efficaci nel caso in cui i diritti digitali in senso stretto o i diritti tradizionali esercitati in ambienti digitali non vengano riconosciuti o siano stati violati, in tutto o in parte. Si tratta di una famiglia di diritti tradizionalmente inclusi tra i diritti civili ma che, per la loro centralità nel sistema delle garanzie costituzionali, meritano di essere trattati come una cate-

[31] Su molti di questi temi, si veda F. PASQUALE, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale* (2020), Roma, 2021.

[32] C. FORMENTI, *Cybersoviet. Utopie postdemocratiche e nuovi media*, Milano, 2007.

goria a sé stante, di «diritti giudiziari»[33]. Tali diritti comportano, in particolare, per le autorità pubbliche l'obbligo di garantire a tutti e a ciascuno un'effettiva tutela giurisdizionale dei propri diritti, affidandone la cura a soggetti terzi tra le parti. Tali soggetti devono, a loro volta, essere istituiti e regolati per legge in modo da essere facilmente accessibili, da operare in modo indipendente e imparziale, da disporre di adeguati poteri di indagine e sanzione e di efficaci strumenti di rimedio.

Da una parte, la digitalizzazione, la datificazione e l'automatizzazione sempre più profonde dell'esistenza moltiplicano le aspettative di tutela e le occasioni di vulnerabilità per singoli e gruppi: cresce, dunque, una nuova e specifica *domanda di giustizia*. Dall'altra parte, la trasposizione dei diritti giudiziari negli ambienti digitali richiede, per essere efficace, che si tenga conto adeguatamente delle peculiarità di questi ambienti: la loro ubiquità, il numero enorme e l'estrema rapidità delle interazioni che vi si svolgono quotidianamente e che potrebbero dar luogo a violazioni di diritti, il potere esercitato dai soggetti privati che ne decidono le tecno-regole e le regole d'uso.

Nonostante l'importanza crescente del tema, finora l'attenzione nel dibattito teorico-giuridico è stata monopolizzata soprattutto dai problemi sollevati dalla "giustizia robotica" o "algoritmica", ossia dall'uso estensivo di procedure automatizzate nelle diverse attività connesse alla funzione giurisdizionale: dall'inquadramento dei fatti rispetto alle norme applicabili all'interpretazione delle norme rispetto ai singoli casi, dal calcolo delle pene a quello dei rischi di recidiva, dall'uso di strumenti di riconoscimento facciale ed emozionale nel corso delle indagini fino alla redazione di sentenze. Salvo poche eccezioni manca, invece, una riflessione sistematica su come debbano e possano essere garantiti i diritti digitali, in linea con gli standard del garantismo costituzionale[34].

Visto il pluralismo normativo degli ambienti digitali, occorre predisporre un sistema di tutele altrettanto plurale, capace di garantire a tutti e a ciascuno la facoltà di "agire in giudizio" a partire dal livello normativo rispetto al quale si è consumata la violazione contestata: su questa base possono venire legittimati i meccanismi di reclamo, segnalazione, moderazione e "ricorso paragiurisdizionale" gestiti dalle piattaforme digitali e dai fornitori di servizi online, per assicurare il rispetto delle proprie "regole d'uso", ma anche delle norme giuridiche applicabili[35]. Al tempo stesso, la delicatezza delle questioni sollevate in tema di diritti e di loro bilanciamenti, e la possibilità che la

[33] J. HABERMAS, *Fatti e norme*, cit., p. 144.

[34] O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2021.

[35] T. GILLESPIE, *Custodians of the Internet. Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, New Haven, 2018.

violazione chiami in causa gli stessi soggetti che possiedono o gestiscono gli ambienti digitali, impedisce di delegare a questi ultimi la risoluzione in via definitiva delle controversie più importanti[36].

Ne risulta un sistema di tutele organizzato secondo su un principio di *sussidiarietà gerarchica*. Reclami ed esposti per violazioni di diritti digitali devono poter essere indirizzati: 1) ai proprietari o ai responsabili degli ambienti digitali nel cui contesto è avvenuta la violazione lamentata; 2) a figure di garanzia istituite nei luoghi di lavoro ad alto tasso di digitalizzazione; 3) ad autorità pubbliche di vigilanza e garanzia, possibilmente uniche, specializzate nella tutela dei diritti digitali; 4) a sezioni, eventualmente specializzate, del sistema giudiziario.

La numerazione allude al rilievo costituzionale crescente delle questioni sollevate, dal punto di vista dei diritti coinvolti, della gravità della violazione e dell'ampiezza del suo impatto, non a un ordine di procedibilità che richieda l'esaurimento dei mezzi di ricorso del livello inferiore per poter adire le istanze di livello superiore. Analogamente, la scelta di avviare un determinato percorso di tutela non deve pregiudicare la possibilità di avviarne altri in seguito.

L'elemento qualificante di questa proposta consiste nel tentativo di trovare un punto d'equilibrio tra obiettivi di efficacia (misurati, ad esempio, in termini di "casi" trattati quotidianamente a costo zero dai livelli inferiori) e obiettivi di equità (misurati, ad esempio, dal rispetto dei principi del garantismo costituzionale). Vista l'impossibilità di rinunciare a questi ultimi obiettivi, occorre riflettere su come implementarli anche nelle pratiche di tutela para-giurisdizionale messe in campo dalle piattaforme e dalle altre società private di servizi digitali: ciò rientra tra le materie oggetto di co-regolazione di cui sopra.

Per poter essere legittimi, ritengo che i meccanismi para-giurisdizionali di tutela dovrebbero prevedere almeno: informative dettagliate sui meccanismi interni di segnalazione e ricorso; regole d'uso chiare e dettagliate su quali azioni e quali contenuti siano ammessi e quali siano suscettibili di censura, in linea con i principi costituzionali in materia di libertà di espressione e di tutela della dignità e dell'integrità personale; modalità possibilmente rapide di intervento, soggette a precisi termini temporali.

Rispetto ai titolari dell'azione, deve essere possibile promuovere ricorsi collettivi anche da parte di soggetti organizzati della società civile, eventualmente accreditati come "difensori dei diritti digitali". Possono essere introdotte figure di "segnalatori attendibili", che devono dimostrare

[36] Per i motori di ricerca, la questione è emersa in relazione al cosiddetto "diritto all'oblio", oggetto del famoso caso "Google Spain": la Corte di Giustizia dell'Unione Europea ha attribuito di fatto alla stessa Google il potere di decidere, in prima istanza, quale diritto far prevalere, se quello all'oblio o quello all'informazione.

particolare competenza nell'identificazione e nel trattamento di contenuti illegali online, operando con diligenza, accuratezza e obiettività, in modo indipendente dagli stessi proprietari o gestori della piattaforma.

Le "sanzioni" previste, dalla rimozione o dall'oscuramento parziale dei contenuti fino alla sospensione temporanea o definitiva dell'account, passando per semplici avvertimenti fino alla demonetizzazione e alla limitazione di funzionalità connesse alla promozione a pagamento di contenuti, devono essere chiaramente illustrate nelle regole d'uso, devono essere dissuasive e devono rispondere a stretti criteri di proporzionalità, in base alla gravità, alla frequenza, all'impatto e ad altre considerazioni. Anche le ripetute segnalazioni infondate e abusive, finalizzate a far sanzionare contenuti o profili sgraditi, devono essere sanzionabili.

Deve essere sempre previsto e illustrato nelle regole d'uso un meccanismo di ricorso contro sanzioni che si ritengono infondate o eccessive, soprattutto nel caso in cui la "decisione" sanzionatoria sia stata assunta da un agente macchinico: il ricorso deve essere trattato da revisori umani, adeguatamente formati allo scopo. Ai fini di un possibile ricorso, le "sanzioni" devono essere sempre motivate in maniera chiara, rispetto alle regole d'uso o ad altre norme che si ritengono violate, sia nel caso in cui la richiesta venga accolta sia che venga respinta.

Nel caso di sanzioni che incidano in modo duraturo sui diritti delle persone o dei soggetti collettivi colpiti (ad esempio, nel caso della cancellazione prolungata o definitiva di un profilo, specie se riferito a un personaggio pubblico o a un'organizzazione sociale, politica o sindacale), la decisione del soggetto privato deve essere validata da un'autorità garante indipendente o deve essere da questa demandato a una corte, con procedura urgente.

Nel caso della autorità di garanzia, fermi restando i principi del garantismo già richiamati, si richiedono ulteriori requisiti per farne la pietra angolare dei diritti giudiziari digitali.

Tali autorità devono avere competenza su tutti i diritti digitali, così da non frammentare le giurisdizioni amministrative rispetto alla tutela dei dati personali, alle garanzie in materia di sistemi IA, di servizi digitali, ma anche per poter affrontare casi che incrociano più aree tematiche e più diritti contemporaneamente. Queste devono poter essere accessibili a tutti coloro che ritengono di aver subito violazioni dei loro diritti, essendosi collegati a un ambiente digitale da terminali situati sul territorio coperti dalla sua giurisdizione.

Le modalità secondo cui inoltrare un reclamo o una segnalazione devono essere comprensibili e di facile utilizzo. Occorre prevedere un termine massimo di poche settimane per una prima

pronuncia di ammissibilità, e un successivo termine analogo per la decisione di merito. Contro il rigetto di un reclamo deve essere possibile fare ricorso al giudice ordinario entro trenta giorni dalla data di comunicazione dello stesso.

Per garantire la terzietà e l'indipendenza di queste autorità di garanzia, la loro nomina deve essere basata su requisiti di competenza posti al vaglio da specifici comitati misti, con rappresentanti eletti e rappresentanti delle associazioni di difesa dei diritti digitali. Per quanto riguarda il cruciale requisito dell'indipendenza, occorre intendere il termine sia come distacco formale e funzionale dal governo, sia come disponibilità di poteri adeguati e risorse sufficienti far fronte ai propri compiti in maniera efficace.

I costi per la gestione delle autorità di garanzia uniche in materia di diritti digitali devono essere sostenuti dalla fiscalità generale, con un particolare contributo proveniente da apposite tasse sulle grandi società informatiche, sottoposte all'obbligo di fatturare integralmente quanto "prodotto" sul territorio nazionale.

Le autorità di garanzia devono poter disporre di rimedi efficaci, in termini di condanna al risarcimento dei danni verso persone fisiche e giuridiche, appellabile presso l'autorità giudiziaria. Devono poter disporre di una funzione di deterrenza verso coloro che esercitano "poteri digitali", dalle società che forniscono servizi digitali ai titolari del trattamento dei dati, attraverso sanzioni amministrative adeguatamente dissuasive, di livello proporzionato al fatturato e alla gravità delle condotte. Le loro decisioni devono essere vincolanti, ma anche appellabili presso corti ordinarie.

6. Conclusioni

Se preso sul serio, il principio democratico prescrive di considerare come titolari di diritti tutti coloro che sono destinatari di determinate norme. In questa prospettiva, la comunità giuridico-politica non si fonda su preesistenti (ma, in realtà, storicamente costruite) identità etniche, linguistiche o culturali, ma semplicemente sul fatto di vivere in modo continuativo gli effetti normativi di un dato ordinamento.

Per la loro natura transnazionale, de-territorializzata e ubiqua, gli ambienti digitali possono essere regolati in modo democratico solo se attribuiscono un "diritto ad avere eguali diritti digitali" a chiunque viva in una società digitalizzata, operi in un ecosistema informatico o interagisca con sistemi di intelligenza artificiale. In altre parole, la titolarità dei diritti digitali si dà a prescin-

dere dal luogo dove si trovano le persone interessate e da dove hanno sede i soggetti dotati di "poteri digitali", cui tali persone rivolgono le proprie legittime aspettative di non lesione e di prestazione.

Emerge qui, in conclusione, il profilo di un "soggetto costituente digitale" che mette in crisi la tradizione giuridico-politica moderna, nella misura in cui allude a una soggettività che non può in nessun modo essere ricondotta a una comunità stabile, ben definita dal punto di vista territoriale, storico o culturale. La digitalizzazione globale dell'esistenza mette a nudo la natura aperta, contingente e conflittuale di qualsiasi "potere costituente", segnalando quanto sia aporetico ogni tentativo di fissarne i confini e i titolari una volta per tutte[37].

In questa prospettiva, l'espressione "popolo digitale" va usata in senso lato per designare tutti/e coloro che non hanno la proprietà degli ambienti digitali, ma su cui si esercita un qualche tipo di potere/diritto digitale: se i membri di tale "popolo disperso" saranno in grado di organizzarsi in contropotere e riconoscersi come fonte di ogni potere/diritto digitale legittimo, è una questione empirica che non può essere prevista per via teorica.

Ciò che, per realismo, non si può negare è che oggi "il popolo della rete" assomiglia più a uno «sciame»[38], aggregato secondo dinamiche populiste e consumistiche, che a una soggettività socialmente e politicamente consapevole, capace di convergere intorno a rivendicazioni comuni. Tuttavia, la posta in gioco della democratizzazione costituzionale della rivoluzione digitale è tanto elevata da poter costituire un potente fattore di aggregazione e organizzazione per una cittadinanza attiva digitale.

In continuità con la grande storia del costituzionalismo democratico, anche i diritti digitali potranno essere definiti con chiarezza nelle norme e resi effettivi da un adeguato sistema di garanzie solo se i soggetti direttamente interessati ne faranno un tema di rivendicazione e di lotta sociale.

FEDERICO OLIVERI
Università di Camerino

[37] A. NEGRI, *Il potere costituente. Saggio sulle alternative del moderno*, Roma, 1992.
[38] B.-C. HAN, *Nello sciame. Visioni del digitale*, Milano, 2015.