

Imbrigliare i giganti digitali nella rete del costituzionalismo ibrido. Spunti dall'approccio europeo alla governance dell'Intelligenza artificiale.

di Nicola Palladino

1. L'ascesa dei giganti: digitalizzazione e Big Tech

La teoria del *societal constitutionalism* di Gunther Teubner può fornire valide coordinate concettuali per comprendere ed affrontare le sfide poste dalla sempre più pervasiva digitalizzazione della società e dall'ascesa delle Big Tech, o giganti digitali¹.

Basandosi sulla teoria dei sistemi sociali di Luhmann (1975) e dei successivi sviluppi ad opera di Sciulli (1992) e Thornhill (2011), lo studioso tedesco muove le sue considerazioni a partire dalle dinamiche di differenziazione sociale. In quest'ottica, più un sottosistema sociale si rende autonomo più sviluppa una propria logica sistemica basata su uno specifico 'mezzo di comunicazione' che rende possibile e significativa l'interazione all'interno del sottosistema stesso (come ad esempio il denaro nel sottosistema economico, la legge per il sottosistema giuridico e così via). Più le attività di un sottosistema diventano rilevanti per il sistema sociale nel suo complesso, più si manifestano quelle che Teubner chiama tendenze "espansionistiche" e "totalizzanti" (Teubner 2011, 2012), intendendo con ciò che il sottosistema sfrutta il suo ambiente per alimentare la propria logica di funzionamento e la propria riproduzione, minacciando l'integrità e l'autonomia di individui, comunità ed altre sfere sociali.

Secondo questa prospettiva, la sempre più rilevante e pervasiva diffusione di Internet e delle tecnologie digitali nelle nostre società può essere concepita come un processo di autonomizzazione di un emergente sottosistema digitale. Sulla scia di Lessig (2006), possiamo identificare nel codice (*'code'*) il mezzo comunicativo proprio del sottosistema digitale, intendendo con questo non un qualche linguaggio di programmazione, quanto piuttosto l'architettura dei sistemi informatici che combinando componenti software e hardware rende possibile l'interazione fra diversi attori sociali nel mondo digitale, ne plasma l'esperienza e ne disciplina il comportamento. Se il codice ne costituisce il mezzo di comunicazione, la digitalizzazione o dataficazione (George 2019) può essere interpretata come la logica propria del sottosistema digitale. Quest'ultima viene dunque a consistere in un incessante processo di trasformazione della realtà sociale in informazione digitale in modo da essere processata ed elaborata da sistemi informatici al fine di estrarne nuova informazione con un valore aggiunto².

La logica della digitalizzazione ha ricevuto un grosso impulso dall'ascesa dei giganti digitali resa possibile dalle politiche di deregolamentazione e liberalizzazione nel settore delle telecomunicazioni promosse a livello internazionale dall'amministrazione Clinton a partire dagli anni novanta (Santaniello 2016). In particolare, il *Telecommunication Act* del 1996, da un lato liberalizzando il mercato telecomunicazioni, e dall'altro classificando gli *Internet Service Provider* (ISP) come *'information services'* -cioè come meri trasmettitori di informazioni prodotte da altri- ha consentito ai fornitori di servizi digitali di prosperare in un regime di pressoché completa deregolamentazione (Cowhet and Klimenko 2001, Mattelart 2001). Ciò ha permesso l'emergere di giganti del settore³, che, complice una carente legislazione sulla privacy, hanno avuto facoltà di raccogliere, conservare ed elaborare i dati trasmessi dai loro utenti in una condizione di sostanziale irresponsabilità. Negli stessi anni, sotto la spinta della World Intellectual Propriety Organisation (WIPO) anche i contenuti della rete, ed in particolare i codici sorgenti dei programmi sono stati privatizzati, favorendo la diffusione di codici

proprietari, chiusi e sottratti al pubblico scrutinio, quanto la concentrazione di capitali e quote di mercato in un ristretto numero di *software house*. I due fenomeni sono venuti a fondersi con l'avvento del Web 2.0, il quale aumentando l'interazione e lo scambio di informazioni fra utente e applicazione, ha incrementato esponenzialmente le possibilità di raccolta e riutilizzo di dati per lo sviluppo di modelli predittivi del comportamento umano, le cui implicazioni vanno ben oltre le originarie finalità di personalizzazione dei servizi e targetizzazione pubblicitaria (Zuboff 2019, van Dijck et al. 2018). Le Big Tech sono venute infatti a configurarsi come fondamentali centrali di estrazione, raccolta ed elaborazione di dati, capaci di far compiere un decisivo salto di qualità ai processi di digitalizzazione. Ciò ha permesso loro di acquisire un notevole potere non solo economico⁴, ma anche propriamente politico, inteso sia come capacità di condizionare il comportamento altrui, sia come capacità di influenzare le decisioni pubbliche (Sartori 1987), ponendo inquietanti interrogativi in termini di rispetto dei diritti umani e tenuta delle istituzioni democratiche.

Dalle rivelazioni di Snowden sappiamo come le tecnologie digitali possano essere impiegate per portare avanti programmi di sorveglianza di massa e come i giganti digitali siano pronti a prestarsi a tali operazioni (Greenwald 2014), in modo da essere legittimati agli occhi dei governi nelle loro attività di *data collection e processing*⁵. Lo scandalo Cambridge Analytica ha reso palese quali possono essere le potenzialità in termini di manipolazione del consenso dei modelli predittivi e delle pratiche di microtargetizzazione⁶.

Ma l'aspetto più problematico consiste forse nel fatto che l'accumulo di dati, know-how e infrastrutture da parte delle Big Tech determina un oligopolio nello sviluppo ed implementazione di tecnologie digitali avanzate, producendo due rilevanti conseguenze. Più le nostre interazioni sociali si spostano sulle architetture digitali, più le nostre possibilità d'azione (cosa non è possibile fare, cosa è possibile fare ed in che modo) vengono ad essere plasmate dalle specifiche tecniche definite dai proprietari di quei sistemi (Lessig 2006, Musiani et al. 2016, Brownsword

and Yeung 2008). In secondo luogo, gli apparati statali, per usufruire delle potenzialità offerte dalle nuove tecnologie (ma anche per contrastare le esternalità negative che esse stesse producono) sono sempre più portati a richiedere la collaborazione dei giganti digitali, se non a delegare loro l'esercizio di funzioni pubbliche, specie nel campo della sicurezza e dell'*enforcement*⁷. In entrambi i casi sussiste il rischio concreto che lasciando la regolazione di parti sempre più consistenti della nostra vita associata nelle mani di soggetti privati, libertà personali e garanzie procedurali di ordine costituzionale possano essere violate e messe in discussione.

2. Imbrigliare i giganti: la rete del costituzionalismo ibrido

Secondo la teoria di Teubner, la costituzionalizzazione di un sottosistema avviene quando le frizioni con altre sfere sociali fanno emergere "diritti fondamentali" intesi come "contro-istituzioni sociali e legali" (Teubner 2011:210), che consentono da un lato di liberare il "potenziale di dinamiche altamente specializzate" proprie del sottosistema, e dall'altro di istituzionalizzare meccanismi di auto-limitazione che preservino l'integrità e l'autonomia di individui ed altre sfere sociali (Teubner 2004:12). In quest'ottica infatti, i diritti fondamentali svolgono sia una funzione inclusiva, garantendo un accesso universale allo specifico 'mezzo di comunicazione' del sottosistema e quindi ai processi di rule-making, sia una funzione esclusiva, nel senso di definire i confini della sfera d'azione del sottosistema.

Un aspetto qualificante della teoria di Teubner consiste nell'idea che i diritti fondamentali possano essere costituiti all'interno di un sottosistema sociale solo attraverso un processo di generalizzazione e ri-specificazione; il che sta a significare che le loro funzioni, per essere effettive, devono darsi nel 'mezzo di comunicazione' proprio del sottosistema ed iscritte nella sua logica di funzionamento.

Il costituzionalismo societario di Teubner, inoltre, si configura come un processo di costituzionalizzazione ibrido, in cui l'autolimitazione di un sottosistema è la risultante delle pressioni,

resistenze e vincoli posti dalle altre sfere sociali, che si risolvono tipicamente in una compenetrazione tra i processi di normazione dei diversi sottosistemi coinvolti.

Rapportate ai processi di digitalizzazione ed al potere acquisito dalle Big Tech, queste considerazioni stanno ad indicare, in primo luogo, che i diritti fondamentali per essere realmente effettivi nel mondo digitale devono essere incorporati all'interno del design delle stesse architetture digitali, e, in secondo luogo che meccanismi di limitazione del sottosistema digitale non possono basarsi solo su forme di *self-regulation*, ma neanche solo sulla regolamentazione statale. Gli stati certo possono imporre vincoli alle Big Tech, sia tramite i mezzi della legislazione ordinaria (con i limiti sopra esposti) sia esercitando una "shadow of hierarchy" (Héritier and Lehmkuhl 2008). Tuttavia, affinché questi meccanismi siano effettivi e superino gli ostacoli posti dalla natura privatistica, transnazionale e infrastrutturale dei processi digitali, devono essere completati ed accompagnati dall'azione congiunta di una pluralità di attori.

In particolare, attori quali le comunità tecniche ed epistemiche possono svolgere un ruolo cruciale nel condizionare i comportamenti dei giganti tecnologici. Questi ultimi, infatti, rappresentano le sole comunità a possedere le conoscenze ed abilità necessarie a tanto a comprendere le implicazioni sociali e politiche di determinate scelte tecniche quanto a tradurre in termini di code e architetture, diritti fondamentali e garanzie di rango costituzionale (Palladino 2021, Liddicoat and Doria 2012). Specialmente quando operano all'interno di *standard setting organizations*, o all'interno di *expert groups* con una funzione consultiva di organismi internazionali o nazionali, le comunità tecniche ed epistemiche possono produrre una convergenza a livello transnazionale verso un insieme comune di norme, regole e specifiche tecniche (Cath and Floridi 2017, Cogburn 2017)⁸.

Un'altra rilevante categoria di attori, parzialmente sovrapposta alla precedente, è costituita dai lavoratori delle Big Tech, delle loro associazioni professionali e rappresentanze sindacali. Da un lato abbiamo una forza lavoro altamente qualificata e dif-

facilmente sostituibile impiegata nei dipartimenti di ricerca e sviluppo o a livello di management che -come hanno dimostrato numerosi casi riguardanti Facebook, Google, Amazon, Microsoft- si è rivelata capace di un notevole potere di influenza sulle scelte strategiche e di policies delle corporation digitali (Gasser and Schmitt 2020)⁹. Dall'altro lato abbiamo le masse di lavoratori non qualificati, si pensi agli impiegati nella logistica di Amazon, i rider dei servizi di delivery, agli autisti di Uber, che per primi subiscono forme di controllo e razionalizzazione algoritmica, le cui proteste stanno introducendo le prime forme di regolamentazione (con tanto di disclosure e review dei codici ed algoritmi utilizzati) di questi nuovi rapporti di produzione destinati ad avere una sempre più pervasiva diffusione¹⁰.

Anche i media e l'opinione pubblica possono avere un ruolo significativo. Nella misura in cui riescono a politicizzare le implicazioni di determinate scelte tecniche possono non solo sollecitare l'intervento pubblico, fare pressioni sull'azienda sfruttando la leva reputazionale, ma anche introdurre elementi di razionalità economica trasformando la tutela dei diritti fondamentali in determinanti del comportamento degli utenti/consumatori.

3. Costituzionalismo ibrido all'opera: la strategia europea sull'intelligenza artificiale

L'intelligenza artificiale (IA), più di altre tecnologie emergenti, enfatizza e rende manifesta la logica propria del sottosistema digitale e le sue conseguenze. Tralasciando i progetti di intelligenza artificiale generale¹¹, ancora fermi ad un embrionale stadio di sviluppo, parlando di intelligenza artificiale ci si riferisce a tecnologie quali algoritmi di *machine learning*, *natural language processing* o reti neurali, che permettono di svolgere compiti specifici (catalogare delle foto, fare una diagnosi clinica, dare un punteggio ad un CV) in base ad inferenze statistiche elaborate a partire da database di grandi proporzioni¹². Da questi l'IA estrae correlazioni, pattern e modelli predittivi che poi applica per risolvere i compiti per cui è stata progettata. Le IA quindi di per sé sono insensibili a fattori che esulino dal calcolo probabilistico,

e spesso ciò si traduce nella riproduzione di *bias* contenuti nei dati che hanno addestrato la macchina, o nell'amplificazione di disuguaglianze sociali esistenti o nella limitazione dell'autonomia dei soggetti (O'Neil 2016, Santaniello 2019)¹³.

Da diversi anni le istituzioni europee stanno dedicando una notevole attenzione al tema dell'intelligenza artificiale, producendo una serie di documenti che sembrerebbero dare luogo ad uno dei più interessanti ed articolati esempi di *societal constitutionalism* applicato alla sfera digitale, specie per quanto riguarda i due punti qualificanti di questo processo: l'iscrizione dei diritti fondamentali nel design dei sistemi di IA, e la natura ibrida del processo.

Per esempio, le *Ethic Guidelines for Trustworthy AI*¹⁴ rilasciate dall' High Level Expert Group on Artificial Intelligence della Commissione Europea si rifanno esplicitamente ad "un approccio all'etica dell'IA basato sui diritti fondamentali sanciti dai trattati UE, dalla Carta dei diritti fondamentali dell'Unione europea e dal diritto internazionale in materia di diritti umani" (EU COM 2019, p.9).

I diritti fondamentali vengono identificati come "la base più incoraggiante per individuare principi e valori etici astratti che possono essere resi operativi nei sistemi di IA" (Idem), e da questi se ne ricavano una serie di requisiti¹⁵ che i sistemi di IA devono soddisfare nel loro ciclo di vita comprensivo delle fasi di ricerca, progettazione, acquisizione dei dati, training, implementazione ed uso, e che in massima parte si traducono in vincoli all'attività delle Big Tech e delle compagnie che sviluppano e commercializzano applicazioni di IA.

Anche il più recente *Artificial Intelligence Act (AIA)*¹⁶ fa esplicito riferimento ai valori e diritti fondamentali della Ue, ed attraverso la definizione di requisiti ed obblighi proporzionati per tutti i partecipanti alla catena del valore, si propone di promuovere e proteggere i diritti tutelati dalla Carta europea, ed in particolare: il diritto alla dignità umana (articolo 1), il diritto alla privacy e protezione dei dati personali (articoli 7 e 8), il diritto alla non discriminazione (articolo 21) e alla parità tra donne e uomini

(articolo 23), la tutela della libertà di espressione (articolo 11) e di riunione (articolo 12), la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa (articoli 47 e 48); i diritti dei lavoratori a condizioni di lavoro giuste ed eque (articolo 31), i diritti dei consumatori (articolo 38), i diritti del minore (articolo 24) e dei disabili (articolo 26).

Oltre a vietare alcuni tipi di applicazioni ritenuti incompatibili con i valori dell'Unione ed i diritti umani (applicazioni con finalità manipolatorie o discriminatorie, sistemi di riconoscimento biometrico in tempo reale); l'AIA indica una serie di requisiti specifici che le applicazioni di IA considerate ad alto rischio¹⁷ sono tenute a soddisfare obbligatoriamente, mentre le applicazioni a basso rischio sono incoraggiate ad adeguarvisi su base volontaria. I requisiti richiesti incidono in maniera significativa sulla definizione delle architetture e nella governance di queste tecnologie, prevedendo, tra l'altro, l'implementazione di sistemi di gestione del rischio, controllo della qualità, data governance e meccanismi di supervisione umana. Vengono inoltre posti obblighi di trasparenza che oltre a prevedere una serie di informazioni da essere comunicate agli utenti finali, richiedono la predisposizione di sistemi di registrazione automatica delle operazioni del sistema (logs) ed altra documentazione tecnica consultabile atta a rendere 'esplicabili'¹⁸, le scelte compiute dalla macchina, e quindi scrutinabili i sistemi di IA prodotti dalle Big Tech.

Un altro aspetto rilevante della strategia europea sull'intelligenza artificiale consiste nel coinvolgimento -portato avanti sin dai suoi primi passi- di un'ampia platea di attori. Un ruolo di particolare rilievo è stato svolto dalle comunità tecniche ed epistemiche di cui si è detto in precedenza. A questo proposito va osservato come la comunicazione della Commissione "*Artificial Intelligence for Europe*"¹⁹ del 2018, dove vengono definiti gli indirizzi strategici in materia, sviluppa le indicazioni fornite dal *European Group on Ethics in Science and New Technologies*, un organo consultivo di estrazione accademica a supporto della Presidenza della Commissione. Anche le *Ethics Guidelines*, sono state redatte da un *experts group* composto da 52 membri, per la maggior parte stu-

diosi, ricercatori e sviluppatori insediati tanto nelle università e nelle pubbliche amministrazioni, quanto nel privato e nel terzo settore, alcuni dei quali già estensori di altri rilevanti documenti in materia quali l'*Ethically Aligned Design* dell'IEEE o gli *Asilomar AI principles* (Palladino 2021). In maniera ancora più significativa, l'AIA prevede che i requisiti previsti dalla regolamentazione vengano soddisfatti attraverso specifiche soluzioni tecniche sviluppate in accordo con *standard* internazionali e conoscenze scientifiche acquisite, piuttosto che prescritte via legge. Si tratta di un passaggio estremamente rilevante che di fatto affida alle *standard setting organizations* e la comunità tecnica, la traduzione in termini di code delle prescrizioni del legislatore e quindi l'effettiva costituzionalizzazione delle architetture digitali.

Non va sottovalutato il ruolo giocato anche da altri attori nella strategia europea, tanto nella elaborazione delle politiche, quanto nell'influenzare il concreto design dei sistemi di IA. L'*expert group* sull'IA della Commissione, le cui raccomandazioni sono state in gran parte recepite nei successivi documenti di policy europei, comprendeva NGO, sindacati ed associazioni di categoria compagnie private, e rappresentanti di entità pubbliche. L'attività di *policy-making* delle istituzioni europea ha potuto giovare anche del contributo dell'*AI Alliance* una piattaforma multistakeholder che ha raccolto l'adesione di oltre 4000 soggetti e che ha partecipato attivamente alla costruzione e validazione dell'*Assessment List for Trustworthy AI*, uno strumento pratico concepito per guidare gli sviluppatori nell'implementazione dei principi e requisiti proposti dalla UE. Va inoltre considerato che tanto le *Ethics Guidelines* che l'*Assessment List* raccomandano di coinvolgere gli *stakeholders* nelle varie fasi di sviluppo di una IA, garantendo così un accesso allargato al 'codice' e quindi la funzione inclusiva dei diritti fondamentali teorizzata da Teubner.

In termini più generali, l'intera iniziativa europea si basa sul principio di '*trustworthiness*', cioè sul creare una IA affidabile in quanto resa controllabile e inoffensiva dall'incorporazione dei diritti umani. Si tratta ovviamente di una scelta strategica basata sull'attribuzione di un valore geopolitico ed economico ai diritti fondamentali, attraverso cui la UE punta ad affermarsi come re-

golatore globale della IA ed a vincere eventuali resistenze all'utilizzo di questa tecnologia²⁰. Ma si tratta anche di una scommessa basata sull'esistenza di una opinione pubblica consapevole, non solo europea, sensibile all'impatto socio-politico di questa nuova tecnologia. Una scommessa che la UE cerca di vincere attraverso ingenti investimenti nell'alfabetizzazione digitale, nella ricerca sulla "explicable IA" e nello sviluppo di strumenti che diano alle persone maggior controllo sui propri dati.

4. Conclusioni

L'insieme dei documenti di policy prodotti dalle istituzioni dell'Unione Europea nel dispiegamento di una propria strategia sull'Intelligenza Artificiale forniscono un valido esempio di come, quelli che qui abbiamo identificato come elementi imprescindibili per una effettiva costituzionalizzazione del sottosistema digitale, possano essere concretamente formalizzati ed implementati.

In primo luogo, abbiamo la centralità dei diritti fondamentali intesi come contro-istituzioni in grado di contrastare la tendenza espansiva e totalizzante della logica della digitalizzazione della società. In secondo luogo, le politiche europee sull'IA prevedono la traduzione dei diritti fondamentali nei codici propri del sottosistema digitale, andando a definire requisiti, e sistemi di controllo che devono essere incorporati nelle architetture e nel design dei sistemi di IA. Allo stesso tempo però questo lavoro di operativizzazione dei diritti fondamentali non è concepito come una prerogativa esclusiva dell'autorità pubblica, ma anzi si realizza attraverso il coinvolgimento di una pluralità di soggetti tanto nello sviluppo della produzione legislativa, quanto nella progettazione delle soluzioni più appropriate per tradurre i requisiti previsti dalla legge in specifiche tecniche. Quest'ultimo aspetto rende conto della natura necessariamente ibrida dei processi di costituzionalizzazione nella sfera digitale, che sarebbe velleitario pretendere sia che possano essere emergere in maniera quasi spontanea dalle stesse Big Tech nella ricerca di un equilibrio con il proprio ambiente esterno, sia che possano essere imposte ed implementate dal solo potere Statale. La costituzio-

nalizzazione ibrida della governance dell'intelligenza artificiale potrebbe essere ulteriormente rafforzata attraverso l'istituzione di una autorità di regolamentazione ad hoc, multistakeholder e dotata della necessaria expertise, incaricata di vigilare sulla effettiva conformità delle soluzioni adottate dalle Big Tech con i requisiti per una IA affidabile e rispettosa dei diritti umani.

Va inoltre notato come l'AIA costituisca solo un tassello di un approccio più generale alla governance delle tecnologie digitali che si compone anche della General Data Protection Regulation, del Digital Services Acts, del Digital Markets Acts e del Digital Governance Act (Floridi 2021).

Tutte queste iniziative, pur non senza differenze ed aporie, condividono il comune richiamo ai diritti fondamentali, alla necessità che questi vengano incorporati nel design e nelle architetture delle tecnologie digitali ed il coinvolgimento di una pluralità di soggetti, e nel loro complesso sembrano delineare il tentativo dell'Unione Europea di realizzare un vero e proprio costituzionalismo digitale (Santaniello et al. 2018; Celeste 2019, De Gregorio 2021), capace di sfruttare le potenzialità delle nuove tecnologie digitali ma al contempo limitare l'azione ed il potere dei giganti digitali, salvaguardando l'autonomia ed integrità di individui e comunità. In questo modo l'Unione Europea ambisce a conquistare le leadership della governance globale della sfera digitale sfidando tanto il modello neoliberale statunitense quanto il modello puramente sovranista cinese.

L'autore ha ricevuto finanziamenti dal programma Horizon2020 Ricerca ed Innovazione dell'Unione Europea nell'ambito del progetto HUMAN+ COFUND Marie Skłodowska-Curie, grant agreement No.945457.

The author has received funding from the European Union's Horizon 2020 Research and Innovation Programme under the HUMAN+ COFUND Marie Skłodowska-Curie grant agreement No. 945457.

Note

- ¹ Con i termini *Big Tech*, *Tech Giant*, o *Big Five* ci si riferisce usualmente ad un gruppo ristretto di aziende dell'economia digitale, Google, Amazon, Facebook, Apple, Microsoft, indicate anche con l'acronimo GAFAM. Le considerazioni proposte in questo testo fanno riferimento ad una concezione meno restrittiva, considerando come giganti digitali le corporation transnazionali operanti nel settore delle tecnologie digitali (comprendendo anche aziende come IBM, Zoom, Netflix, etc.).
- ² Il valore aggiunto non va in questo caso concepito nella sua originaria accezione economica quanto piuttosto all'interno della stessa logica della datificazione, come valore numerico capace di sintetizzare una grande quantità di informazione di partenza e le relazioni fra diversi dati.
- ³ Va notato che con la stipula dell'Agreement on Basic Communication promosso dal World Trade Organisation nel 1998, i colossi statunitensi poterono consolidare ed estendere la propria posizione dominante su scala globale, divenendo delle realtà transnazionali.
- ⁴ Secondo dati del 2021, le GAFAM occupano 5 delle prime 6 posizioni nella classifica globale delle compagnie con più alta capitalizzazione. Nicola Petit ha coniato il neologismo "moligopolio" per definire la condizione di molte Big Tech, le quali sono singolarmente detengono una posizione dominante in relazione a qualche specifica attività digitale (Amazon per l'e-commerce, Google per i motori di ricerca, etc.), ma collettivamente costituiscono un oligopolio che controlla il mercato digitale e i cui membri competono fra loro per la supremazia (Petit, 2020).
- ⁵ Edward Snowden, ex contractor della National Security Agency degli Stati Uniti ha fornito prove documentali su come aziende quali Verizon, google, Facebook, Apple abbiano consentito un accesso incondizionato e illegale alle comunicazioni dei propri utenti da parte delle agenzie di intelligence statunitensi, inglesi, australiane e canadesi. Più recentemente, in Cina, aziende pubbliche e private stanno collaborando nell'implementazione del Social Credit System, un complesso sistema di valutazione dell'affidabilità di persone, imprese e istituzioni (Liang 2018).
- ⁶ Cambridge Analytica è una società di *data analytic* accusata di essersi impossessata illegalmente de dati di oltre 87 milioni di utenti Facebook e di averli utilizzati per sviluppare avanzate tecniche di psicomatria e profilazione influenzando significativamente diversi processi elettorali, tra cui il referendum sulla Brexit ed le presidenziali USA del 2016. Per maggiori dettagli cfr. <https://www.vice.com/en/article/mg9vvn/how-our-likes-helped-trump-win>.

7 Al di là dei casi di collaborazione in programmi di sorveglianza di massa menzionati nella nota 5, altri casi emblematici sono costituiti dalle richieste fatte dai governi nei confronti dei social media, ed in particolare Facebook, affinché assumano un atteggiamento proattivo nella individuazione e rimozione di contenuti illegali e pericolosi, delegando loro di fatto la definizione dei confini della libertà di espressione (Gillespie 2018); dal coinvolgimento di Google ed Apple nello sviluppo di applicazioni per il tracciamento della pandemia di Covid ; dai tentativi di utilizzare gli ISP per perseguire violazioni dei copyrights. Un altro aspetto che esula dal campo della sicurezza e dell'enforcement, ma desta comunque preoccupazione, è il trasferimento su sistemi cloud privati di documenti e applicazioni delle amministrazioni pubbliche.

8 A tale proposito, vanno ricordati: 1) la *Global Initiative on Ethics of Autonomous and Intelligent Systems* del *Institute of Electrical and Electronics Engineers (IEEE)*, da cui è scaturito l'*Ethically Aligned Design report*, un ambizioso documento di oltre 280 pagine di raccomandazioni su come implementare un approccio etico all'IA (<https://standards.ieee.org/industry-connections/ec/autonomous-systems.html>); 2) il *Code of Ethics and Professional Conduct* dell'*Association for Computing Machinery* (<https://www.acm.org/code-of-ethics>); 3) il *Joint Technical Committee* sull'Intelligenza Artificiale organizzato dall'*International Standard Organization (ISO)* e dall'*International Electrotechnical Commission (IEC)* (<https://www.iso.org/committees/6794475.html>).

9 Nel 2018, le proteste dei dipendenti di Google hanno portato al ritiro dell'azienda dal Progetto Marven del Pentagono per cui avrebbe dovuto sviluppare una intelligenza artificiale da utilizzare su droni militari, e successivamente all'adozione di un codice ed un comitato etico in materia di intelligenza artificiale (AI Now 2018). L'anno seguente la contrarietà dei lavoratori dell'azienda ha portato il colosso di Mountain View a ritirarsi da un altro progetto, denominato DrangonFly con cui l'azienda intendeva creare una versione del suo motore di ricerca conforme alle pratiche censorie del governo cinese (<https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-must-drop-dragonfly-4c8a30c5e5eb>). Negli stessi anni, le proteste degli impiegati hanno giocato un ruolo fondamentale anche nel far ritirare Amazon e Microsoft da collaborazioni col governo statunitense sul terreno delle tecnologie di riconoscimento facciale (<https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html>; <https://www.theverge.com/2018/6/22/17492106/amazon-ice-facial-recognition-internal-letter-protest>).

¹⁰ Le rivendicazioni sindacali dei rider hanno portato in Italia alla condanna di Deliveroo e Glovo da parte del Garante per la Privacy e tribunali ordinari per l'utilizzo di algoritmi discriminatori (<https://www.irpa.eu/il-caso-deliveroo-lalgoritmo-frank-e-la-discriminazione-by-design/>; <https://www.altalex.com/documents/news/2021/07/14/privacy-garante-sanziona-foodinho-milioni-euro>). In Spagna i sindacati hanno ottenuto che i rappresentanti dei lavoratori siano informati sui parametri, regole e istruzioni alla base degli algoritmi impiegati dalle piattaforme di food-delivery (<https://europa.today.it/lavoro/legge-rider-dipendenti-spagna.html>). Negli ultimi anni gli scioperi dei dipendenti di Amazon impiegati nella logistica si stanno facendo sempre più frequenti e diffusi nel mondo, portando ai primi interventi legislativi (<https://www.latimes.com/business/story/2021-08-31/la-fi-amazon-warehouse-injuries-ab701-bill-calosha>).

¹¹ Per intelligenza artificiale generale (AGI) si intendono sistemi in grado di replicare l'intelligenza umana intesa sia come capacità di passare da un compito ad un altro senza necessità di riprogrammazione, sia, in alcune accezioni, come consapevolezza delle proprie azioni.

¹² Per una più dettagliata esposizione delle tipologie e meccanismi di funzionamento delle IA, si consulti Russel e Norving 2009.

¹³ Un caso divenuto paradigmatico è costituito da Google Photo, una applicazione per la classificazione automatica delle foto addestrata che ha assorbito bias razzisti durante il training finendo per etichettare come 'gorilla' le immagini di afroamericani (<https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai>); una distorsione tra l'altro riemersa recentemente anche in alcune funzioni di Facebook (https://www.corriere.it/tecnologia/21_settembre_05/neri-come-primati-l-algoritmo-facebook-scambia-uomini-colore-scimmie-scuse-social-61a40384-0e30-11ec-90a7-94fb0e4dd84c.shtml). Un altro caso di scuola riguarda l'utilizzo dell'applicazione COMPAS da parte delle corti di giustizia per calcolare la probabilità di recidiva dei detenuti, che si è scoperto produrre sistematicamente falsi positivi e falsi negativi che penalizzano la popolazione afroamericana (<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>).

¹⁴ <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>

¹⁵ I requisiti individuati sono: supervisione umana, sicurezza e solidità tecnica, privacy e data governance, trasparenza, diversità, non discriminazione ed equità, benessere sociale ed ambientale, accountability.

¹⁶ <https://eur-lex.europa.eu/legal-content/ENTXT/?uri=CELEX%3A52021PC0206>

¹⁷ Vengono definite applicazioni ad alto rischio le applicazioni destinate ad essere impiegate come componente di sicurezza di un prodotto, le applicazioni impiegate in settori sensibili in attività sensibili, quali identificazione biometrica, gestione di infrastrutture critiche, selezione e valutazione dei lavoratori, valutazione della pericolosità o recidività di una persona sottoposta ad un procedimento giudiziario etc. (per un elenco complete si consulti l'Allegato III dell'AIA); e più in generale tutti i sistemi di IA che "presentano un rischio di danno per la salute e la sicurezza, o un rischio di impatto negativo sui diritti fondamentali" di gravità e probabilità paragonabili a quelli esplicitamente menzionati nell'Allegato III.

¹⁸ Sul concetto e le pratiche 'explainability' si consulti Meske et al. 2020.

¹⁹ <https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe>

²⁰ Entrambi gli obiettivi sono dichiarati esplicitamente nella già citata comunicazione della commissione *Artificial Intelligence for Europe*, e ribaditi nelle successive comunicazioni *Building Trust in Human-Centric Artificial Intelligence* del 2019, e *White Paper on Artificial Intelligence* del 2020.

Riferimenti delle opere citate nel testo e bibliografia d'interesse

- AI Now, 2018, *AI Now Report 2018*, <https://ainowinstitute.org/reports.html>.
- R. BROWNSWORD, K. YEUNG, 2008, *Regulating Technologies*, Hart Publishing, Oxford.
- C. CATH, L. FLORIDI, 2017, *The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights*, in "Sci Eng Ethics", n. 23, pp. 449-468.
- E. CELESTE, 2019, *Digital constitutionalism: A new systematic theorisation'*, in *International Review of Law, Computers & Technology*, 33, 76-99.
- D. COGBURN, 2017, *Transnational Advocacy Networks in the Information Society*, Palgrave MacMillan, New York.
- P. COWHEY, M. KLIMENKO, 2001, *The WTO agreement and telecommunications policy reform*, Policy Research Working Paper, no. WPS 2601.
- EU COM, 2019, *Orientamenti Etici per una Intelligenza Artificiale Affidabile*, <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>
- G. DE GREGORIO, 2021, *The rise of digital constitutionalism in the European Union*, in "International Journal of Constitutional Law". <https://doi.org/10.1093/icon/moab001>
- L. FLORIDI, 2021, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, in: "Philosophy & Technology", 34(3).
- E. GEORGE, 2019, *Digitalization of Society and Socio-political Issues*, Wiley, London.
- T. GILLESPIE, 2018, *Custodians of the Internet Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press.
- G. GREENWALD, 2014, *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*, Metropolitan Books, New York.
- A. HÉRITIER, D. LEHMKUHL, 2008, *The Shadow Of Hierarchy And New Modes Of Governance*, in "Journal Of Public Policy", n.28(1), pp. 1-17.
- L. LESSIG, 2006, *Code 2.0*, Basic Books, New York.
- F. LIANG, V. DAS, N. KOSTYUK, M.M. HUSSAIN, 2018, *Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure*, in "Policy & Internet", n.10, pp. 415-453.

J. LIDDICOAT, A. DORIA, 2012, *Human rights and Internet protocols: Comparing processes and principles*, https://www.unesco-ci.org/cmscore/sites/default/files/2013wsis10/human_rights_and_internet_protocols-_comparing_processes_and_principles28129.pdf. Accessed 1st September.

N. LUHMANN, 1975, *Potere e Complessità Sociale*, Il Saggiatore, Milano.

A. MATTELART, 2001, *Histoire de la société de l'information*, Editions La Découverte, Paris.

C. MESKE, E. BUNDE, J. SCHNEIDER, M. GERSCH, 2020, *Explainable Artificial Intelligence: Objectives, Stakeholders, and Future Research Opportunities*, in "Information Systems Management", DOI: 10.1080/10580530.2020.1849465.

F. MUSIANI, D.L. COGBURN, L. DENARDIS, N. S. LEVINSON, 2016, *The Turn to Infrastructure in Internet Governance*, Palgrave MacMillan, New York.

C. O'NEIL, 2016, *Weapons of math destruction: How big data increases inequality and threatens democracy*, Crown Publishers, New York.

N. PALLADINO, 2021, *The role of epistemic communities in the "constitutionalization" of internet governance: The example of the European Commission High-Level Expert Group on Artificial Intelligence*, in "Telecommunications Policy", vol. 45(6).

N. PETIT, 2020, *Big Tech and the Digital Economy: The Mologopoly Scenario*, Oxford University Press, Oxford.

S. RUSSEL, P. NORVIG, 2009, *Artificial intelligence: A modern approach*, Prentice Hall.

M. SANTANIELLO, 2019, *Il giudizio di Talos. Valutazione, algoritmi, Macchine*, in "Cartografie Sociali", n.8, pp. 85-102.

M. SANTANIELLO, 2016, *Net democracy: la sfida democratica all'Internet governance*, in: (a cura di) E. De Blasio M. Sorice, "Innovazione democratica. Un'introduzione", pp. 63-86, Luiss University Press, Roma.

G. SARTORI, 1987, *Elementi di Teoria Politica*, il Mulino, Bologna.

G. TEUBNER, 2011, *Transnational Fundamental Rights: Horizontal Effect?*, in "Netherlands Journal of Legal Philosophy", n.40(3), pp. 191-215.

G. TEUBNER, 2012, *Constitutional Fragments: Societal Constitutionalism and Globalization*, Oxford University Press, Oxford.

G. TEUBNER, 2004, *Societal Constitutionalism: Alternatives to State-Centred Constitutional Theory?*, in C. JOERGES, IY SAND, G. TEUBNER (EDS) "Transnational Governance and Constitutionalism", Hart Publishing, Oxford, pp.3-28.

C. THORNHILL, 2011, *A Sociology of Constitutions: Constitutions and State Legitimacy in Historical-Sociological Perspective*, Cambridge University Press, Cambridge.

J. VAN DIJCK, T. POELL, M. DE WAAL, 2018, *The Platform Society*, Oxford University Press, Oxford.

S. ZUBOFF, 2019, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York.