Luisa Torchia

Poteri pubblici e poteri privati nel mondo digitale

(doi: 10.1402/112711)

il Mulino (ISSN 0027-3120)
Fascicolo 1, gennaio-marzo 2024

Ente di afferenza:
Università Luiss (luiss)

POTERI PUBBLICI E POTERI PRIVATI NEL MONDO DIGITALE

LUISA TORCHIA

È UN DATO DI ESPERIENZA COMUNE CHE LA SOCIETÀ IN CUI VIVIAMO OGGI sia una società digitale: la vita di ogni giorno – trasporti, banche, sanità, istruzione, affari, commercio, politica, relazioni sociali – si svolge mediante il ricorso abituale, diffuso e pervasivo alle tecnologie digitali. In questo mondo digitale la linea di demarcazione fra la vita *online* e la vita *offline* è ormai sempre più evanescente, mentre è allo stesso tempo sempre più evidente che la tecnologia porta con sé grandi vantaggi e benefici, ai quali non vogliamo rinunciare, e grandi rischi e pericoli, dei quali non sempre siamo pienamente consapevoli.

Esplorare il modo in cui il potere, pubblico e privato, si atteggia e si sviluppa nella società digitale è quindi oggi utile, anzi necessario, sia per comprendere il mondo in cui viviamo, sia per meglio definire, e ancor più ridefinire, il mondo in cui vogliamo vivere. Tale esplorazione, che cercherò qui di illustrare, muove da alcune domande di fondo.

La prima è relativa alla natura del potere: quando il potere diventa tecno-potere, pubblico o privato che sia, si tratta di un potere diverso rispetto al potere tradizionale? La seconda domanda tocca, invece, la natura della società digitale: in questa società il ricorso alla tecnologia aumenta o riduce la libertà individuale e collettiva? La terza domanda è relativa agli effetti della tecnologia sullo Stato: il richiamo sempre più frequente da parte degli Stati nazionali e della stessa Unione europea alla sovranità digitale introduce un concetto nuovo e diverso rispetto alla sovranità tradizionale? La quarta domanda, infine, riguarda il rapporto fra tecnologia e regimi politici: la ricerca della sovranità digitale comporta l'evoluzione o la trasformazione della democrazia in tecno-democrazia e delle autocrazie in tecno-autocrazie o tecno-dittature e produce un tecno-nazionalismo o addirittura un tecno-protezionismo in base ai quali cambiano le dinamiche di relazione non solo fra poteri pubblici e poteri privati, ma anche fra Stati o addirittura blocchi sul piano geopolitico?

IL SOVRAFFOLLAMENTO DI POTERI E LO SVILUPPO DEI POTERI PRIVATI DIGITALI

L'ipotesi che guida questa esplorazione è che il mondo digitale sia sovraffollato di poteri, pubblici e privati, e che le relazioni fra questi poteri costitui-

scano un reticolo intricato, attraversato da dinamiche non necessariamente convergenti.

Innanzitutto, si può senz'altro rilevare la tradizionale dinamica per cui il potere pubblico cerca di mantenere un controllo tendenzialmente generalizzato, mentre i poteri privati cercano di sfuggire al controllo pubblico o almeno di eluderne i tratti più intrusivi. Emerge, però, anche la competizione fra i poteri pubblici per il dominio tecnologico, che, tradotto nei termini propri del linguaggio del potere pubblico, viene chiamato, appunto, sovranità digitale: questa lotta per il dominio tecnologico è oggi, ad esempio, un elemento fondamentale del confronto fra gli Stati Uniti e la Cina. E, a loro volta, i poteri privati competono fra loro per essere o restare dominanti sul mercato, per crescere sempre di più, per produrre sempre nuovi prodotti e nuovi servizi.

Quello digitale è un mondo sovraffollato di poteri, pubblici e privati, le cui relazioni costituiscono un reticolo intricato

Per meglio comprendere queste dinamiche e il modo in cui esse interagiscono e producono effetti sempre più rilevanti sul piano globale, conviene fare un passo indietro e guardare all'origine dei poteri digitali privati. Si tratta di poteri che nascono grazie all'incontro fra la capacità di innovazione del settore privato e la decisione del potere pubblico di garantire un ambiente favorevole allo sviluppo dell'innovazione. L'innovazione tecnologica si sviluppa fuori dalle grandi istituzioni di ricerca – viene sempre citato in proposito il famoso garage in cui Bill Gates, *dropout* dell'Università di Harvard, diede i natali a Microsoft – ma anche grazie a esse: basti ricordare che Internet nasce come Arpanet, alla fine degli anni Sessanta, grazie al centro militare Arpa e ad alcune università della California [01].

Il clima culturale in cui la nuova tecnologia si sviluppa è quello dei tecnolibertari californiani della Silicon Valley, animato da sfiducia nell'autorità, nelle gerarchie, nel governo e soprattutto nel «sistema», di modo che, almeno agli inizi, la tecnologia era vista anche come uno strumento per non essere dipendenti dal sistema. Quel sistema non era peraltro affatto animato da intenti di controllo, ma piuttosto dalla convinzione, caratteristica dell'ordinamento americano anche per altri settori dell'economia, che la regolazione impedisce e ostacola l'innovazione e deve essere quindi sempre tarata verso il minimo necessario, se e quando necessario. Questo approccio è stato seguito in modo pedissequo sotto la presidenza Clinton, quando nel 1996 fu inserita la Section 230 nel Communications Decency Act – non a caso definita come «le 26 parole che hanno creato Internet» –, garantendo ai fornitori di servi-

zi digitali un regime di esonero dalla responsabilità e quindi rendendoli immuni dalla principale rete di contenimento del potere privato che è appunto la responsabilità (e quindi l'obbligo di rispondere per le proprie condotte e per gli effetti di quelle condotte). La ragione principale di questa immunità stava nella volontà di consentire lo sviluppo dell'innovazione tecnologica da parte di imprese aventi natura di startup, delle quali non era neanche sicura e tantomeno garantita, al tempo, la sopravvivenza, come dimostra il fatto che Amazon ha a lungo operato in perdita nei primi anni di vita.

Il potere tecnologico si è sviluppato quindi in un ambiente favorevole, senza alcun vincolo o controllo *ex ante*, il che ha consentito alle grandi piattaforme di crescere ed espandersi su base globale, offrendo i propri servizi secondo modalità e regole che esse stesse, a lungo e in larga misura ancora oggi, hanno definito.

Questo risultato dimostra che l'approccio americano alla regolazione – se pure almeno in parte ideologico, perché fra mercato e regolazione sceglie sempre il mercato come strumento atto a influenzare in modo soddisfacente i comportamenti dei poteri privati – è realistico, specie quando l'oggetto della ipotetica regolazione è l'innovazione. Regolare l'innovazione è, infatti, non solo difficile, ma spesso impossibile come attività *ex ante*: non si può regolare la ruota prima che sia stata inventata e una volta che è stata inventata non la si può disinventare.

In ogni caso, grazie alla convergenza fra capacità di innovazione e ambiente regolatorio molto favorevole, quelle startup sono oggi imprese globali di dimensione ed estensione probabilmente mai raggiunte prima, rilevanti non solo sul piano economico, ma anche sul piano sociale e politico.

LE DIMENSIONI E I CARATTERI DEI POTERI PRIVATI DIGITALI

Per dare un'idea delle dimensioni basta qualche numero, relativo rispettivamente al peso in Borsa, al peso sul mercato e al peso sulla società.

Per la Borsa americana Apple è la prima società ad avere toccato il valore di tremila miliardi di dollari. Nel suo complesso Wall Street è dominata dalle cosiddette *big tech*, perché cinque società – Apple, Microsoft, Alphabet, Amazon e Nvidia – equivalgono al 25% dell'intero indice di Borsa. La Borsa americana ha quindi una «testa pesante» – in gergo, è *top-heavy* – e qualsiasi movimento di quelle cinque società ha effetti che si ripercuotono sull'indice, sia per quanto riguarda il Nasdaq, sia per quanto riguarda il Dow Jones.

La presenza sul mercato delle grandi piattaforme è pervasiva: negli ultimi vent'anni Amazon, Apple, Google, Meta e Microsoft hanno acquistato complessivamente 770 startup. Tim Cook, l'amministratore delegato di Apple, ha dichiarato che il ritmo di acquisizioni di Apple ha portato all'acquisto di una nuova società ogni tre/quattro settimane negli ultimi sei anni. Sono

stati così acquisiti tutti i possibili concorrenti, con l'effetto di rendere strutturalmente più difficile l'accesso al mercato, di rendere il mercato sempre meno contendibile e di accentuare enormemente l'integrazione verticale delle grandi piattaforme.

La presenza sul mercato delle grandi piattaforme è pervasiva, con l'effetto di rendere strutturalmente più difficile l'accesso al mercato

Altrettanto significativo è il peso delle piattaforme digitali sulla società. Qui è persino difficile scegliere fra i tanti dati che testimoniano l'estensione e la pervasività dei servizi digitali: basterà ricordare che nel 2022 sono state registrate oltre tre miliardi di visite mensili su Amazon, o che l'anno seguente ci sono stati oltre tre miliardi di utenti attivi mensili su Facebook, dei quali oltre due miliardi si collegano a Facebook ogni giorno; e che, tutti i giorni, nel giro di un solo minuto vengono inviati oltre quaranta milioni di messaggi su WhatsApp.

Non vi è dubbio, quindi, che i grandi fornitori di servizi digitali siano ormai poteri privati globali di grandi dimensioni, dotati di un enorme peso economico e di presenza e influenza molto pervasive sul piano sociale.

Si tratta, però, di poteri con alcune caratteristiche peculiari, per i quali si può richiamare la definizione di potere che dobbiamo a Foucault, nella sua analisi della microfisica del potere [02]. Foucault ci ha spiegato che bisogna andare oltre la definizione di potere come capacità di imposizione, di interdizione, di repressione, perché questa è una concezione puramente giuridica, criticabile e insufficiente in quanto, per usare le sue parole, «ristretta» e «scheletrica». Il potere va considerato, invece, come una rete produttiva che passa attraverso tutto il corpo sociale, produce cose, induce piacere, forma sapere, crea discorsi. Per comprendere il potere bisogna allora guardare al suo carattere reticolare, piuttosto che al suo carattere verticale, e alla sua capacità di influenza, piuttosto che alla sua dislocazione spaziale.

Seguendo questo insegnamento, occorre prima indagare la compresenza di caratteri tradizionali e di caratteri nuovi nei poteri privati digitali e verificare poi se e come, nel mondo digitale in cui viviamo, sia cambiato il potere pubblico.

I poteri privati digitali presentano numerosi caratteri tradizionali. Innanzitutto essi sono operatori economici e quindi imprese, la cui attività principale consiste nel vendere servizi o beni, o direttamente o come intermediari fra fornitori di servizi e di beni e acquirenti. Come tutti gli operatori economici tradizionali, inoltre, anche se a volte sembrano immateriali, essi

hanno importanti strutture fisiche. Senza infrastrutture fisiche e cavi sottomarini non esisterebbe il cyberspazio, così come fisici sono i server e i calcolatori, la cui potenza computazionale è in crescita geometrica, con il consumo altrettanto crescente dell'uso di terre rare, petrolio, carbone, energia. È stato anzi osservato che l'industria digitale è un'industria estrattiva, al pari di molte industrie tradizionali, tanto che la *carbon footprint* dell'infrastruttura computazionale mondiale equivale a quella dell'industria aereonautica al suo picco e sta crescendo a un passo ancora più veloce [03].

E naturalmente sono fisiche le risorse umane, che non sono solo i ben pagati ingegneri, tecnici e programmatori della Silicon Valley. I pacchi di Amazon vengono recapitati in tutto il mondo grazie anche a condizioni lavorative che ricordano, almeno in Europa, un passato che sembrava superato. Ogni lavoratore addetto alla linea dei pacchi lavora su un turno di dieci ore, con mezz'ora di pausa non pagata per il pranzo e la possibilità di fermarsi per non più di quindici minuti per ogni turno, in un ambiente lavorativo nel quale i tentativi di sindacalizzazione sono ostacolati con ogni mezzo.

Condizioni forse ancora peggiori vigono per le centinaia di migliaia di persone impiegate per moderare i contenuti, il cui numero va crescendo perché è ormai accertato che l'attività di moderazione dei contenuti non può essere interamente affidata ad algoritmi, ma richiede l'intelligenza umana. Gli algoritmi non sempre comprendono il contesto nel quale si inserisce una frase, o una fotografia, o un video, e non sono in grado di individuare in modo consistente, intelligente appunto, i contenuti da escludere e quelli che invece sono, ad esempio, espressione di ironia o di satira o, al contrario, sono offensivi nella sostanza e non nella forma. Le persone addette alla moderazione dei contenuti si trovano quasi sempre nei Paesi più poveri e non solo sono pagate pochissimo, ma sono esposte a tutta la violenza e l'odio che imperversano sulla Rete, con danni psicologici molto gravi, tanto che nel 2020 Meta ha raggiunto un accordo transattivo per chiudere un'azione giudiziaria promossa da diecimila moderatori di contenuti e ha pagato 552 milioni di dollari come compensazione per danni alla salute mentale di quelle persone.

Gli algoritmi non sempre comprendono il contesto di una frase o di una fotografia e non sono in grado di individuare i contenuti da escludere

Le grandi piattaforme presentano quindi tratti tradizionali, anzi a volte antichi, del potere. A questi si aggiungono, però, anche tratti nuovi e inediti. Fra questi, particolarmente importante è l'influenza sociale e politica che si aggiunge al peso sul mercato e sull'economia. Si tratta, inoltre, di una influen-

za sociale e politica che, a differenza di quanto avviene per altri operatori economici, non è un effetto solo del potere economico, ma è direttamente connessa alla natura dell'attività e dei servizi offerti. Le grandi piattaforme non solo vendono servizi, ma sono anche uno strumento per la costruzione di comunità (ad esempio con l'uso di *rating* e *reviews*, o di *tweets*) e per la comunicazione individuale e collettiva; sono ormai parte del discorso pubblico, incidono sull'opinione pubblica, consentono allo stesso tempo più libertà e partecipazione e più sorveglianza e repressione [04]. Emerge qui un carattere inedito dei poteri privati digitali, perché mentre nella storia passata vi sono numerosi esempi di soggetti titolari di un enorme potere economico o, alternativamente, titolari di una grande capacità di influenza sociale in determinati settori o Paesi, oggi si concentra in capo a pochi soggetti un potere sia multidimensionale quanto alla sua natura, sia universale quanto alla sua estensione.

Un grande potere che si sviluppa in assenza di regolazione diventa facilmente un potere senza limiti e il potere illimitato è per definizione pericoloso, perché può abusare o utilizzare arbitrariamente la sua potenza senza che nessuno sia in grado di opporsi, con rischi per la democrazia, apparsi del resto evidenti con gli episodi di manipolazione dell'opinione pubblica registrati, ad esempio, per le elezioni americane del 2016 o, venendo all'Europa, per il referendum sulla Brexit. La tecnologia può essere, inoltre, uno strumento molto efficace di controllo e di repressione, sia nelle autocrazie e nelle dittature, come dimostra l'ampio uso della tecnologia nella repressione delle opposizioni in Iran e in Cina, sia nelle democrazie, dove c'è il rischio che si sviluppi il «capitalismo di sorveglianza», secondo l'efficace formula di Shoshana Zuboff [05].

Le Costituzioni democratiche sono ricche di regole e strumenti volti a limitare il potere pubblico, proprio per garantire e difendere i diritti fondamentali da quello che viene considerato il potere più forte e quindi anche il potere più pericoloso, ma l'esperienza ha mostrato che quegli stessi diritti sono messi gravemente a rischio dai poteri digitali con effetti del tutto nuovi, che dipendono strettamente proprio dalla natura dell'attività delle piattaforme. Per essere redditizia, infatti, questa attività richiede la raccolta di enormi quantità di dati, non a caso definiti come il petrolio del mondo digitale, ed è un triste dato di fatto che i discorsi di odio, le notizie false, la violenza, la rivendicazione identitaria aggressiva e lo svilimento delle identità altrui producono molti più click e attirano molti più utenti della pacata riflessione e dei dibattiti aperti: e per vendere pubblicità, prodotti e servizi ciò che conta è attirare il maggior numero di contatti possibile.

Non si tratta di un fenomeno nascosto, non percepibile o non percepito. Negli ultimi anni si sono moltiplicate le denunce di casi in cui era evidente

che le piattaforme erano a conoscenza degli effetti nocivi dei contenuti pubblicati, ma invece di intervenire con strumenti di moderazione e di controllo hanno negato l'evidenza o cercato di occultarla. Il caso più famoso è forse quello dei cosiddetti *Facebook files*, denunciato sul «Wall Street Journal», in cui una *whistleblower* ha pubblicato documenti interni da cui risultava che Facebook sapeva che Instagram ha effetti «tossici» sugli adolescenti, ma non fa niente per attutire quegli effetti e non tiene conto delle segnalazioni relative ad attività di traffico di esseri umani e di droga, perché dovrebbe altrimenti chiudere molti account. Sempre Facebook, inoltre, utilizza sistemi diversi di controllo sui contenuti, più intrusivo per la generalità degli account e più leggero, invece, per alcune categorie di persone, fra le quali, paradossalmente, rientrano soggetti come Trump, noti per il frequente ricorso allo *hate speech* e alle *fake news*, con il risultato che proprio coloro che dovrebbero essere più soggetti all'attività di moderazione dei contenuti vengono invece lasciati più liberi.

Negli anni si sono moltiplicate le denunce di casi in cui le piattaforme erano a conoscenza degli effetti nocivi dei contenuti pubblicati

Proprio il caso dell'ex presidente Trump ha posto però un problema di carattere generale, relativo al rapporto tra la libertà di espressione e le regole sinora autodefinite da parte delle grandi piattaforme. Persino Facebook ha dovuto sospendere l'account di Trump dopo che, durante l'attacco dei suoi sostenitori a Capitol Hill il 6 gennaio 2021, sulla base dell'idea del tutto falsa che le elezioni presidenziali fossero state rubate, lo stesso Trump si è spinto con i suoi messaggi oltre ogni limite ragionevole. Si è aperto, infatti, un dibattito sulla titolarità del potere di incidere sulla libertà di espressione e ci si è chiesti se sia ragionevole e conforme ai valori costituzionali di fondo – nell'ordinamento americano, ma il problema si pone allo stesso modo in tutte le democrazie – affidare questo potere a un soggetto privato come Facebook e alle sue regole interne o se non occorra una regola pubblica, dell'ordinamento generale, che stabilisca definitivamente che ciò che è illecito offline deve esser illecito anche online, modificando così quel regime di immunità e salvaguardia che, come si è visto in precedenza, ha accompagnato gli esordi dello sviluppo dei poteri privati digitali.

In effetti, la crescita del peso e dell'influenza di questi poteri privati digitali senza limiti efficaci è arrivata al punto in cui è stata messa in dubbio la stessa capacità dei poteri pubblici di governare e mantenere il proprio ruolo nel mondo digitale. E questo dubbio ha innescato una reazione diffu-

sa, perché, come sempre quando il potere privato rischia di sovrastare il potere pubblico o di imporre le proprie regole, il potere pubblico reagisce e si pone quindi il problema di individuare gli strumenti di reazione, scegliendo fra quelli già esistenti o costruendone di nuovi, più adatti alla natura dei nuovi fenomeni da controllare e regolare.

STRUMENTI DI CONTROLLO, REGOLE E INTELLIGENZA ARTIFICIALE

Il principale fra gli strumenti tradizionali a disposizione del potere pubblico è, naturalmente, la disciplina antitrust. Non è un caso che la prima legge americana in materia di antitrust sia nata proprio con l'obiettivo di limitare il potere privato rispetto agli interessi pubblici, come espressamente dichiarò uno dei suoi padri nel corso del dibattito dinanzi al Congresso, affermando: «If we will not endure a king as a political power, we should not endure a king over the production, transportation, and sale of any of the necessities of life. If we would not submit to an emperor, we should not submit to an autocrat of trade, with power to prevent competition and to fix the price of any commodity» [06].

In Europa, ma ormai anche negli Stati Uniti e in Cina, oggi le grandi piattaforme digitali sono oggetto di indagini e interventi antitrust molto più aggressivi rispetto al passato, come dimostra il rinnovato attivismo della Federal Trade Commission nei confronti di Google e gli interventi del governo cinese nei confronti di Alibaba, che hanno portato alla separazione strutturale del gruppo in diverse compagnie.

Naturalmente gli effetti sono molto diversi nelle democrazie e nelle dittature. In America e nell'Unione europea i poteri privati digitali si difendono nei procedimenti antitrust e contestano davanti ai giudici le sanzioni irrogate, mentre in Cina la multa di due miliardi ad Alibaba è stata accettata con «sincerità e con la determinazione di obbedire» senza alcun tentativo di contrasto o di resistenza – scelta che probabilmente avrebbe attivato una funzione punitiva ben più incisiva.

Spesso si pensa che la disciplina antitrust non sia abbastanza efficace come strumento di controllo e contenimento delle grandi piattaforme

È diffusa però oggi la convinzione che la disciplina antitrust non sia abbastanza efficace come strumento di controllo e contenimento delle grandi piattaforme per almeno due ragioni, direttamente connesse alle dimensioni economiche e alla natura dell'attività [07]. Quanto al primo profilo, è evidente che le grandi piattaforme ormai detengono posizioni tendenzialmente monopolistiche e l'assenza di concorrenti rende inefficaci gli strumenti volti a garan-

tire la competizione sul mercato, quando il mercato finisce per coincidere con un unico operatore. L'irrogazione di sanzioni antitrust è, inoltre, difficilmente significativa per imprese che dispongono di enormi risorse. Per fare solo un esempio, quando la Federal Trade Commission ha imposto una multa di cinque miliardi di dollari, la multa è stata salutata con soddisfazione dai commentatori come una fra le più alte sanzioni mai irrogate, ma lo stesso giorno in cui la multa è stata irrogata il valore delle azioni di Meta in Borsa è cresciuto dell'1,8%, aggiungendo 10 miliardi al suo valore di mercato, proprio in ragione della conclusione del procedimento antitrust.

Quanto al secondo profilo, il problema che si pone non è relativo solo alle condotte dei poteri digitali sul mercato, ma anche allo *spillover* della loro attività e all'influenza sulla sfera sociale e politica, in tutti i Paesi, rispetto al quale la disciplina antitrust non è uno strumento idoneo e, per la verità, i tradizionali strumenti di regolazione del potere privato hanno efficacia molto limitata.

La disciplina legislativa e costituzionale, nell'ordinamento italiano come in altri ordinamenti democratici, assicura garanzie all'autonomia privata come libertà nei confronti del potere pubblico e, per altro verso, pone limiti a questa libertà per garantire altri privati: così per il lavoratore rispetto al datore di lavoro, o per l'utente rispetto al gestore dei servizi, o per il consumatore rispetto al produttore o al venditore di beni.

Le Costituzioni contengono il potere pubblico, per il quale introducono limiti e contrappesi, ma poco dicono sui poteri privati: la dimensione privata viene in luce come libertà da tutelare e quindi i diritti fondamentali hanno dimensione verticale, lungo l'asse dei rapporti tra autorità e libertà, ma non orizzontale, fra i diversi diritti garantiti ai soggetti privati.

Il problema che si pone di fronte ai poteri privati digitali è, invece, preservare la struttura politica e sociale, nei sistemi democratici come nei sistemi autocratici. Se vi fosse stato bisogno di una conferma dei termini di questo problema, essa è divenuta chiara a tutti con l'introduzione di ChatGPT. I modelli di linguaggio utilizzati per ChatGPT non sono motori di ricerca che cercano i fatti. Sono invece modelli che rilevano i *patterns* e una volta individuato il *pattern*, il modello «indovina» l'opzione migliore in una sequenza e «genera», quindi, una soluzione a un problema, un testo o un'immagine.

Come spesso accade con gli indovini, non è però possibile distinguere il falso dal vero e le informazioni generate possono essere, in effetti, risultati «fabbricati» o, per dirla con i termini utilizzati dai ricercatori del settore, sono effetto di «allucinazioni». Sono stati inventati numeri, nomi, date, citazioni, bibliografie, interi saggi, articoli inesistenti sul «Financial Times» e Bloomberg. Nel caso più famoso un avvocato a New York ha chiesto a ChatGPT di preparare la memoria di difesa in un processo e il testo prodotto era

pieno di precedenti inventati e di citazioni inesistenti, dei quali fortunatamente la corte si è avveduta.

Anche il processo di produzione ha dato luogo a controversie, perché i modelli vengono addestrati utilizzando gratuitamente miliardi di dati che in effetti appartengono ad altri. Il caso più noto è quello del «New York Times», che ha deciso di impedire a ChatGPT di utilizzare i suoi archivi per addestrare il modello e ha avviato un'azione legale contro OpenAI e Microsoft per violazione del diritto di autore per l'uso non autorizzato (e gratuito) di milioni di articoli del giornale.

I modelli di Intelligenza Artificiale vengono addestrati utilizzando gratuitamente miliardi di dati che in effetti appartengono ad altri

Il problema con l'Intelligenza Artificiale generativa non è più, quindi, soltanto se i contenuti sono offensivi, ma se sono autentici. Distinguere il falso dal vero è molto difficile, perché non è possibile risalire all'origine di ciò che viene prodotto tramite l'Intelligenza Artificiale. Si tratta inoltre di un problema aggravato dal fatto che, al contrario di quanto accade per altri professionisti, come ad esempio i medici e gli avvocati, nel campo dell'Intelligenza Artificiale non esiste un sistema professionale che produca prassi, protocolli, principi deontologici e valori condivisi.

E qui si è realizzata una virata del dibattito pubblico sul tema: si sono moltiplicati lettere e appelli, a volte firmati dagli stessi scienziati, ingegneri e imprenditori che hanno contribuito allo sviluppo dell'Intelligenza Artificiale e si è posto il problema del rapporto fra innovazione e profitto. La gravità del problema è resa evidente dalla cronaca recente, con il licenziamento e poi il ritorno di Sam Altman come amministratore delegato di OpenAI. Non è per la verità stato chiarito se le ragioni del licenziamento fossero collegate ai rischi connessi a un nuovo sistema di intelligenza generativa Q*, che sembra potrebbe essere immessa sul mercato prima ancora di sapere quali sono i suoi effetti. La vicenda ha mostrato, però, l'inevitabilità del conflitto fra i tentativi di gestire l'Intelligenza Artificiale, tranne che per una società *non profit*, come era OpenAI, e l'esigenza di enormi investimenti che l'Intelligenza Artificiale richiede. Era stato detto agli investitori in OpenAI che dovevano considerare il loro investimento come una donazione, perché OpenAI prometteva di operare nel miglior interesse dell'umanità e avrebbe potuto in ogni momento fermare lo sviluppo di nuovi prodotti se sorgevano problemi o rischi etici. Ma quando OpenAI è andata sul mercato per raccogliere fondi e Microsoft ha investito tredici miliardi di dollari, è diventato evidente che la logica *for profit* avrebbe prevalso sulla logica *non profit*.

A questo punto è cambiato anche il linguaggio del dibattito. Il tecno-ottimismo, che ha sinora enfatizzato i vantaggi e i benefici dell'Intelligenza Artificiale, che sicuramente esistono, ha cominciato a cedere il passo a un tecno-pessimismo e a volte a una tecno-apocalisse, che è giunta a paventare l'estinzione dell'esperienza umana. Al di là dei toni apocalittici, che molto raramente sono di una qualche utilità, c'è una convinzione che si sta ormai diffondendo: il fenomeno va regolato e va regolato almeno in parte *ex ante*, valutando i possibili impatti ed effetti delle soluzioni tecnologiche prima che esse sfuggano a ogni limite e controllo. La novità consiste nel fatto che i termini del dibattito non sono più sul se regolare, ma su come regolare e con quali strumenti [08].

TECNODEMOCRAZIE E TECNOAUTOCRAZIE: STATI UNITI, UNIONE EUROPEA E CINA

Enfatizzando un po' il ricorso a un linguaggio immaginifico, si potrebbe dire che l'approccio alla regolazione porta alla emersione di tecnodemocrazie e di tecnoautocrazie e, ancor più, a un diffuso tecno-nazionalismo.

Per semplificare si può ricorrere alla ripartizione in tre modelli o, *rectius*, approcci principali, molto ben illustrati in un libro recente non a caso intitolato *Digital Empires* [09]: l'approccio americano, l'approccio europeo e l'approccio cinese.

L'approccio americano è animato da una forte fiducia nel mercato e da un'altrettanto accentuata sfiducia nella regolazione, considerata come un ostacolo alla innovazione. Secondo questo approccio, i governi non capiscono la tecnologia e quindi non dovrebbero regolarla, perché il rischio di produrre danni è maggiore degli eventuali benefici. Questo approccio, che ha sicuramente come si è visto consentito alle imprese tecnologiche di crescere dallo stadio di startup a quello di oligopoli o monopoli, va oggi però mutando, con una enfasi sempre maggiore sui pericoli, piuttosto che sui vantaggi dello sviluppo tecnologico, come dimostrano tre eventi significativi recenti, verificatisi nel giro di pochi mesi.

L'approccio americano è animato da una forte fiducia nel mercato e da un'altrettanto accentuata sfiducia nella regolazione

A giugno 2023 il presidente Biden ha incontrato alla Casa Bianca i leader di Amazon, Anthropic, Google, Inflection, Meta, Microsoft e OpenAI e ha definito il gruppo delle *big tech* «essenziale per guidare l'innovazione con responsabilità e sicurezza», mentre le sette aziende si sono impegnate a rispettare alcuni principi fondamentali per lo sviluppo dell'Intelligenza Artificiale – in

particolare, i principi di protezione, sicurezza e fiducia – e hanno detto di essere disponibili sia a consentire a esperti di sicurezza indipendenti di sottoporre a test i loro sistemi di Intelligenza Artificiale prima dell'immissione sul mercato, sia a condividere dati sulla sicurezza con il governo e l'accademia. Sempre Biden ha emanato il 30 ottobre scorso un *executive order* sull'Intelligenza Artificiale, per definire nuovi standard di sicurezza a protezione della *privacy*, dell'uguaglianza e dei diritti civili e per tenere sotto controllo i rischi connessi alla continua diffusione di nuove applicazioni tecnologiche nella vita economica, sociale e politica americana.

La Federal Trade Commission, per parte sua, il 21 novembre ha autorizzato, per la prima volta, processi obbligatori di *compliance* per prodotti e servizi fondati su meccanismi di Intelligenza Artificiale.

Nell'ordinamento americano va emergendo, quindi, la tendenza del potere pubblico a cercare forme e strumenti di coregolazione con i poteri privati digitali e, allo stesso tempo, a porre – se non vere e proprie regole – almeno indirizzi e principi che fungano da rete di contenimento dei rischi e, sia pure in modo ancora sperimentale, operino come base per la costruzione di un nuovo regime regolatorio.

L'approccio europeo è molto diverso, anzi per certi versi opposto: se negli Stati Uniti si dubita della capacità del governo di comprendere la tecnologia, nell'Unione europea si dubita della capacità delle grandi imprese tecnologiche (nessuna delle quali è europea) di comprendere e rispettare i fondamenti della democrazia costituzionale e l'insieme di diritti e valori fondamentali che costituiscono parte integrante e irrinunciabile dell'ordinamento europeo. Per assicurare il rispetto di quei diritti e quei valori si ritiene necessario, quindi, imporre complessi sistemi di obblighi, di regole e di limiti contro qualsiasi ipotesi di abuso di potere, pubblico o privato che sia. La propensione regolatoria dell'Unione europea è, naturalmente, anche un effetto del limitato bilancio di cui dispone, di modo che la strategia europea è volta a spostare il campo di gioco dalla tecnologia alle regole – perché le regole costano meno delle politiche industriali, specie nel settore tecnologico che richiede investimenti sempre più ingenti – con il risultato, secondo i critici, di divenire un nano tecnologico e un gigante regolatorio.

L'Unione ha così adottato, dopo il regolamento sulla *privacy* del 2016, molti altri regolamenti sia in materia di gestione e organizzazione dei dati, sia in materia di mercati digitali, di servizi digitali, di cybersicurezza e di Intelligenza Artificiale. Si tratta di testi normativi molto complessi e articolati, che non è naturalmente possibile analizzare qui, ma che condividono un approccio regolatorio basato su un regime di gradazione del rischio che muove, appunto, dall'assunzione che la tecnologia sia rischiosa e comporti pericoli sia per i diritti individuali, sia per gli interessi pubblici e collettivi. Al fine

di controllare e mitigare questi rischi, si introducono significativi obblighi *ex ante*, preordinati ad assicurare almeno trasparenza, diffusione delle informazioni e conoscibilità delle tecniche utilizzate, perché per limitare il potere occorre che il potere sia visibile e non nascosto [10].

L'Unione europea ha adottato diversi regolamenti in materia di gestione e organizzazione dei dati, di mercati e di servizi digitali, di cybersicurezza

Naturalmente il controllo sul rispetto di queste regole non è facile, per una molteplicità di ragioni, dalla sproporzione fra le risorse in possesso dei regolati rispetto alle risorse a disposizione dei regolatori, alla carenza delle capacità professionali necessarie (concentrate nel settore privato), all'asimmetria fra la territorialità dei regolatori e la dimensione globale dei regolati.

Paradossalmente, però, proprio questo ultimo elemento gioca, in alcuni casi almeno, come fattore di effettività delle regole europee, perché è già emerso, relativamente alla disciplina della *privacy* dei dati, che per le piattaforme globali il costo di *compliance* può essere più basso del costo di abbandonare il mercato europeo e, di conseguenza, diventa vantaggioso dover applicare un'unica regola uniforme, anche se più vincolante come è quella europea, rispetto all'applicazione di tante regole locali, magari meno incisive, ma che richiedono un maggiore sforzo organizzativo. A conferma di questa tendenza si possono citare le sollecitazioni degli amministratori delegati di Apple e di Meta al governo americano perché adotti una legge sulla *privacy* in stile europeo, in modo da avere una cornice di riferimento comune.

L'approccio cinese, infine, è saldamente basato sul controllo statale e quindi del partito, con un modello di potere pubblico che pone l'accento sull'unità, sull'uniformità, sulla concentrazione. Il governo cinese non ha quindi esitato a imporre, nel nome della «prosperità collettiva», vincoli e obblighi molto incisivi sulle piattaforme digitali cinesi, per assicurarsi che il loro potere non superi o comunque non possa fronteggiare il potere dello Stato/partito. Per altro verso il governo cinese si serve delle compagnie tecnologiche – cinesi, ma non solo – per aumentare la sua capacità di controllo della popolazione e, soprattutto, della eventuale opposizione. È stato imposto, così, alle compagnie cinesi di realizzare un sistema di sorveglianza di Intelligenza Artificiale denominato Sharp Eyes, con l'obiettivo di creare «un sistema di sorveglianza nazionale onnipresente, pienamente integrato, sempre al lavoro e pienamente controllabile» ed è stato chiesto alle compagnie americane di fornire dati relativi ai loro utenti: e anche le piattaforme americane, così potenti in casa e in Europa, hanno ceduto alle richieste del governo cinese, tradendo le regole che asseriscono di rispettare in altri ordinamenti,

perché il mercato cinese è troppo importante per correre il rischio di esserne esclusi.

TECNO-NAZIONALISMO E SOVRANITÀ DIGITALE

Le differenze fra i tre approcci sinora illustrati sono profonde, ma essi hanno anche qualcosa in comune, perché ciascuno di essi è alla base della tendenza alla creazione di un nuovo tecno-nazionalismo, in nome del quale risuona lo slogan della sovranità digitale[11], che ciascun ordinamento rivendica. Per l'Unione europea, la presidente della Commissione Von der Leyen ha affermato già nel discorso sullo stato dell'Unione del 2020 che «è in gioco la sovranità digitale dell'Europa, sia su piccola che su larga scala».

La sovranità digitale, rispetto alla nozione tradizionale di sovranità, presenta un carattere nuovo, perché viene invocata sia per assicurare la difesa contro interferenze esterne e quindi il controllo sul territorio (naturale e digitale) nazionale, sia, innovativamente, per espandere le regole di ciascun ordinamento, che seguono, per così dire, i cittadini di quell'ordinamento: per le regole sulla privacy sinora, e potenzialmente per la nuova regolazione europea in materia di mercati e servizi digitale e di Intelligenza Artificiale, gli obblighi imposti hanno proiezione extraterritoriale.

L'emersione del tecno-nazionalismo porta naturalmente con sé una tendenza alla frammentazione della Rete e alla competizione, se non al conflitto, fra grandi poteri pubblici. Questa tendenza è evidente, ad esempio, nel settore della cybersicurezza, considerata oggi quinto dominio ed essenziale per le operazioni militari quanto lo sono terra, acqua, aria e spazio, e nel settore della produzione di *chips* avanzati e di semiconduttori.

Il tecno-nazionalismo porta con sé una tendenza alla frammentazione della Rete e alla competizione, se non al conflitto, fra grandi poteri pubblici

L'Unione europea, con il Cyber Solidarity Act, sta creando un sistema di polizia parallelo e un'infrastruttura paneuropea composta da centri operativi di sicurezza nazionali e transfrontalieri in tutta l'Ue che rilevano le minacce, con il fine di costruire un cyberscudo europeo, rafforzato da una clausola di mutua difesa e da una clausola di solidarietà. Sulla produzione di *chips* avanzati e di semiconduttori, e soprattutto sulla loro esportazione in Cina, è intervenuto il Chips Act europeo e sono state adottate misure fortemente restrittive negli Stati Uniti, considerate appunto aggressive e ostili dal governo cinese.

Il contrasto fra Stati Uniti e Cina non è, peraltro, solo diretto ma anche indiretto, e si concretizza mediante tentativi di ampliare la sfera di influenza in un mondo sempre più polarizzato. Il tasso di dipendenza dal sistema cinese di molti Paesi in Africa, Asia e Sud America va crescendo in ragione dell'acquisto di tecnologia cinese e della contestuale importazione delle regole che accompagnano quelle infrastrutture, mentre, di converso, Stati Uniti e Unione europea hanno istituito un Trade and Technology Council con l'obiettivo di mitigare i conflitti regolatori fra Stati Uniti e Unione europea e di collaborare nel contrasto alle politiche cinesi di distorsione del mercato e di uso della tecnologia per obiettivi antidemocratici.

Il mondo digitale è, però, complesso e conosce non solo conflitti, ma anche tentativi di convergenza.

LA TASSAZIONE GLOBALE E L'INTELLIGENZA ARTIFICIALE «COSTITUZIONALIZZATA»

Il primo sviluppo riguarda una funzione pubblica – e statale – fondamentale, e cioè il potere di imporre tasse. L'argomento è stato a lungo oggetto di conflitto fra gli Stati Uniti e il resto del mondo, perché i primi hanno a lungo sostenuto di essere l'unica giurisdizione dotata del potere di tassare le piattaforme, mentre il resto del mondo, e gli Stati europei in particolare, chiedevano che una parte almeno del valore prodotto per le piattaforme nei mercati nazionali potesse essere tassato localmente. A seguito di lunghe negoziazioni, nell'ottobre del 2021 l'Ocse ha annunciato che è stato raggiunto un accordo fra 136 Paesi su un sistema di tassazione globale che entrerà in vigore fra il 2023 e il 2024.

Il sistema prevede due diverse misure generali: in attuazione della prima, una quota dei profitti delle multinazionali, comprese le imprese digitali, sarà tassata localmente anche nel caso in cui quelle imprese non siano fisicamente presenti sui mercati locali, mentre la restante quota viene tassata Paese per Paese in ragione, appunto, della rilevanza della presenza delle imprese e dei loro clienti. In attuazione della seconda misura, si introduce una tassa uniforme minima del 15%, applicabile a imprese che raggiungano una determinata soglia – fra le quali rientrano sicuramente le imprese digitali – in modo da limitare la concorrenza al ribasso fra Stati nell'imposizione fiscale. L'effetto più importante di queste misure è che si comincia a tassare l'economia digitale come una parte dell'economia nel suo complesso, erodendo così il regime di favore separato del quale ha goduto sinora.

Il secondo sviluppo è relativo a una nuova fase del ciclo fra autoregolazione ed eteroregolazione che ha accompagnato sinora lo sviluppo del mondo digitale. La lunga fase iniziale di esenzione da qualsiasi regola si va ormai esaurendo e si va affermando la convinzione condivisa che vi sia necessità di

regole poste dal potere pubblico. Proprio il rafforzamento della eteroregolazione sta però facendo emergere una nuova tendenza all'autoregolazione, che si caratterizza per essere volta non all'elusione delle regole dell'ordinamento generale, ma piuttosto a una sorta di interiorizzazione almeno di alcuni principi.

Un esempio importante di questa tendenza è l'attività di Anthropic, una startup fondata nel 2021 da Dario e Daniela Amodei, due fratelli italo-americani di San Francisco, dopo aver lasciato OpenAI. Anthropic ha pubblicato un paper intitolato *Constitutional AI* nel quale si cerca di rispondere alla domanda: quali valori deve avere l'Intelligenza Artificiale? E come li si applica *ex ante*, in modo da evitare gli errori e gli abusi preventivamente, visto che il controllo *ex post* è insufficiente? Anthropic ha costruito appunto una Costituzione, nella quale si trovano un insieme di principi tratti da una varietà di fonti, fra le quali Costituzioni nazionali, la Dichiarazione dei diritti umani delle Nazioni Unite, le migliori pratiche in una serie di settori, principi tratti dall'esperienza dell'uso dell'Intelligenza Artificiale o elaborati da altri laboratori di ricerca che operano nel settore.

Ci troviamo di fronte a un passaggio da un mondo digitale libero e sregolato a un mondo che richiede sempre più regole, pubbliche e private

Gli obiettivi dichiarati di questo tentativo sono far funzionare l'Intelligenza Artificiale non sulla base dei dati forniti per addestrarla, e quindi sulla base delle inferenze statistiche, ma sulla base di principi stabiliti *ex ante*, come appunto si fa nelle Costituzioni, che stabiliscono i valori e i diritti fondamentali come un *a priori* e, in base a questa scelta consapevole, rendere noto a tutti quali sono i principi che regolano l'attività (e dunque eliminare l'opacità e l'inconoscibilità degli algoritmi così spesso lamentata dai giuristi e dagli attivisti dei diritti umani). Si tenta, inoltre, di controllare i risultati e i prodotti dell'Intelligenza Artificiale mediante la stessa Intelligenza Artificiale «costituzionalizzata», di modo che non vi sia necessità di ricorrere a esseri umani per la moderazione dei contenuti, perché gli elementi dannosi o malevoli vengono espulsi mediante un controllo automatizzato.

Lo sviluppo di Anthropic è abbastanza promettente da indurre Amazon a investirvi quattro miliardi di dollari, ma occorrerà naturalmente verificare se anche in questo caso, come per OpenAI, la logica *for profit* finirà per prevalere sul tentativo di costituzionalizzazione.

L'esplorazione condotta sinora consente di svolgere alcune considerazioni conclusive. Siamo di fronte a un passaggio da un mondo digitale libero e sregolato a un mondo che richiede sempre più regole, pubbliche e private. Gli strumenti in proposito non mancano e possono essere trasposti, con i necessari adattamenti, da altri settori regolati. Fra gli strumenti che possono più facilmente essere riconfigurati per l'applicazione ai poteri privati digitali si possono indicare un regime di responsabilità del produttore come dell'utilizzatore, nuove regole antitrust, ma anche sistemi di autorizzazione e licenze all'immissione sul mercato: nessuno si sognerebbe di mettere sul mercato un farmaco o un'automobile senza aver prima verificato mediante processi di *trial* e accurati controlli la sicurezza del prodotto da commercializzare. Si possono introdurre e sperimentare anche strumenti di gradazione, limitazione e mitigazione del rischio e di valutazione di impatto, o attribuire poteri di intervento ad autorità internazionali, secondo il modello della *governance by accident* oggi in funzione per l'industria aeronautica, in base al quale le autorità internazionali nell'aviazione hanno il potere di imporre cambiamenti sui processi di produzione e di funzionamento degli aerei una volta che sia emerso un difetto o un problema. E non dobbiamo dimenticare che persino il pericolo di un olocausto nucleare è stato scongiurato, in passato, grazie al diritto internazionale e alla istituzione dell'Agenzia internazionale per l'energia atomica.

Tutti questi e altri strumenti di regolazione potrebbero essere ridisegnati in modo da essere applicati al potere tecnologico, ma occorre non dimenticare che il potere tecnologico è una concentrazione di potere non solo economico, ma anche politico e sociale: secondo uno slogan spesso ripetuto, è un potere che influenza in modo decisivo chi siamo, che cosa vogliamo, che cosa pensiamo. Appare inoltre sempre più evidente che le dinamiche fra poteri pubblici e poteri privati nel mondo digitale sono multidimensionali e reticolari e tutti i poteri allo stesso tempo si confrontano e si utilizzano a vicenda per perseguire i propri scopi.

Questo reticolo di relazioni fra poteri ha assunto una dimensione strategica che, di nuovo, non è solo economica, ma anche politica e sociale e tocca direttamente i diritti fondamentali, la democrazia, la geopolitica, i rapporti fra le democrazie e fra le democrazie e gli altri regimi politici, assumendo così una dimensione costituzionale al cui centro non c'è tanto e soltanto una questione di limitazione del potere, pubblico o privato che sia, ma anche di una sua redistribuzione e condivisione, dando più forza a quella che Habermas ha chiamato la sfera pubblica [12].

La storia passata, come la cronaca recente, dimostra senza ombra di dubbio che, quando il potere non è distribuito e condiviso, ma è invece trop-

po concentrato e troppi ne sono esclusi, le società si polarizzano, diventano instabili e sono soggette a lacerazioni profonde. La sfera pubblica digitale non può, allora, essere lasciata solo alla dinamica fra poteri pubblici e poteri privati, ma richiede la partecipazione attiva e consapevole della società, degli individui, delle associazioni, delle comunità, in una sfida che interpella ciascuno di noi.

LUISA TORCHIA è professoressa ordinaria di Diritto amministrativo nell'Università di RomaTre, dove dirige anche il master su «Lo Stato digitale». È socia fondatrice dell'International Society of Public Law e dell'European Public Law Organization. Fa parte dell'Associazione di cultura e politica «il Mulino». Tra i suoi lavori, *Il principio di equivalenza nell'ordinamento europeo* (Il Mulino, 2006), *I nodi della pubblica amministrazione* (ES, 2016) e il recente *Lo Stato digitale. Una introduzione* (Il Mulino, 2023). Per il Mulino ha inoltre curato *Attraversare i confini del diritto* (2016) e *La dinamica del diritto amministrativo. Dieci lezioni* (2017).

Questo articolo rielabora il testo della XXXVIII Lettura del Mulino, tenutasi il 25 novembre 2023 nell'Aula Magna dell'Università di Bologna, preceduta dalle seguenti parole: «Grazie al Mulino per l'invito a tenere la Lettura del 2023, grazie a Giovanna Movia per la presentazione e al Rettore per l'introduzione, grazie all'Università di Bologna che ci ospita in questo bellissimo luogo dove è sempre un piacere tornare e grazie naturalmente a tutti voi per essere qui oggi». Data la sterminata letteratura nella materia oggetto della Lettura, in questo testo sono citati soltanto gli studi ai quali si fa riferimento diretto, senza alcuna pretesa di completezza.

01 Sul ruolo dello Stato nell'innovazione, anche tecnologica, cfr. M. Mazzucato, *The Entrepreneurial State. Debunking Public vs. Private Sector Myths*, London, Anthem Press, 2013; trad. it., *Lo Stato innovatore*, Roma-Bari, Laterza, 2014.

02 M. Foucault, *Microfisica del potere. Interventi politici*, ed. it. a cura di A. Fontana e P. Pasquino, Torino, Einaudi, 1977[4].

03 Per un'analisi molto critica e molto informata cfr. K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, New Haven, Conn., Yale University Press, 2021.

04 Cfr. C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Washington, D.C., Crown Books, 2016.

05 S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, trad. it. Roma, Luiss University Press, 2020.

06 Congressional Record - Senate, vol. 21, 1890, p. 2457 (Sen. Sherman).

07 M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, «Diritto pubblico», n. 3/2021, pp. 739 ss.

08 Cfr. G. Resta, *Poteri privati e regolazione*, in *Potere e Costituzione*, *Enciclopedia del diritto*, I Tematici, vol. 5, diretto da M. Cartabia e M. Ruotolo, Milano, Giuffrè, 2023, pp. 1008 ss. e O. Pollicino, *Potere digitale*, *ibidem*, pp. 410 ss.

09 A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, Mass., Oxford University Press, 2023.

10 S. Cassese, *Le strutture del potere*, intervista di A. Sardoni, Roma-Bari, Laterza, 2023, p. 189.

11 G. Finocchiaro, *La sovranità digitale*, «Diritto pubblico», n. 3/2002, pp. 809 ss.

12 Per una riflessione sul tema aggiornata per la società digitale cfr. J. Habermas, *Reflections and Hypotheses on a Further Structural Transformation of the Political Public Sphere*, «Theory, Culture & Society», n. 4/2022, vol. 39, pp. 145 ss.