"PROVA A PRENDERMI". ECOSISTEMA DIGITALE E CONSAPEVOLEZZA DEGLI UTENTI: UNO SPAZIO PER LA REGOLAZIONE NAZIONALE?[*]

CHIARA BERGONZINI[**]

Sommario

Abstract

In the Digital Era, there is already space for national laws about technology? The essay starts with three questions about the actual potential of regulation, its scope and authority. The second part focuses on the role of human persons – not only as digital consumers but also as "walking data generators" – which implies considerable legal consequences, from Data Protection to Antitrust. In conclusion, the essay suggests public education as a specific perspective and field in which national regulation could be effective.

Suggerimento di citazione

C. BERGONZINI, "Prova a prendermi". *Ecosistema digitale e consapevolezza degli utenti: uno spazio per la regolazione nazionale?*, in *Osservatorio sulle fonti*, n. 2/2022. Disponibile in: http://www.osservatoriosullefonti.it

[*] In corso di pubblicazione nel volume *Processi di regolazione e tecnologie digitali. Il ruolo dei privati*, Giappichelli, Torino 2022, che raccoglie gli esiti della ricerca Prin 2017 *Self- and Co-regulation for Emerging Technology: Towards a Technological Rule of Law* (SE.CO.R.E.TECH).

[**] Ricercatrice a t.d. di Diritto costituzionale nell'Università degli Studi di Macerata.
Contatto: chiara.bergonzini@unimc.it

Registrazione presso il Tribunale di Firenze n. 5626 del 24 dicembre 2007
Rivista inclusa nella classe A delle Riviste scientifiche di Area 12 – Direttore Prof. Paolo Caretti
ISSN 2038-5633

1. Introduzione

In una fase storica – la cd. Era digitale[1] – in cui i giuristi e i pubblicisti in particolare si trovano ad affrontare questioni (in larga parte[2]) inedite, ma senza dubbio ormai improcrastinabili, le riflessioni che seguono si focalizzano su un profilo specifico del fenomeno dei Big Data, cioè sugli spazi di regolamentazione rimasti al legislatore nazionale in un contesto caratterizzato, com'è ampiamente noto, dalla deterritorializzazione[3] dei rapporti giuridici. La chiave di lettura scelta è il ruolo giocato dagli utenti dei servizi digitali, perché consente di tenere al centro del discorso l'essere umano titolare di diritti, alla ricerca di un punto di equilibrio tra la cultura costituzionale del principio personalista e l'inesorabile avanzata degli algoritmi.

Il percorso, che inizia con una sommaria ricostruzione del fenomeno in esame, si snoda quindi attraverso tre domande. La prima: è *possibile* regolare l'ecosistema digitale? Nel «mondo della fattualità tecnologica»[4] bisogna infatti prendere atto che «lo spazio di fatto lasciato libero dal giurista lo conquista chi è capace di controllare la tecnologia, chi ha gli strumenti per comprenderla e per forgiarla»[5]. La seconda: ammesso che sia possibile, a quale *livello* di normazione è necessario, o opportuno, affidare tale compito? La terza: in un mondo privo di confini, esiste ancora uno spazio per il legislatore *nazionale*? E se sì, qual è?

È bene chiarire sin d'ora che si tratta di domande alle quali chi scrive non ambisce a trovare risposte diverse da quelle già accreditate in dottrina, ma che consentono di interrogarsi su un profilo – le competenze del legislatore interno – considerato per lo più residuale; il che, peraltro, è ormai oggettivamente un dato di fatto. Ciò nonostante, lo spunto per queste riflessioni è duplice: da un lato, che lo Stato non possa abdicare del tutto al proprio ruolo, e devolvere interamente la soluzione dei problemi ai livelli sovranazionali; dall'altro lato, che la Costituzione repubblicana, guardata attraverso le lenti dell'innovazione tecnologica (*infra*, par. 5), offra spunti per continuare a garantire effettività alla tutela dei diritti.

[1] La cd. Era digitale si considera iniziata nel 2002, anno in cui la quantità di dati archiviati in formato digitale ha superato quella dei dati archiviati in formato analogico.

[2] Non è del tutto nuovo il problema concettuale, come sottolinea G. D'ACQUISTO, *Decisioni algoritmiche. Equità, causalità, trasparenza*, Torino, Giappichelli 2022, p. 4, rilevando che «da sempre l'uomo impiega la tecnologia anche per discriminare».

[3] Cfr. G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, il Mulino, Bologna, 2016, p. 324 ss.

[4] L. MERLA, *Big Data e diritto: una sfida all'effettività*, in *Media Laws* (www.medialaws.eu), 1/2021, p. 221.

[5] Ivi, p. 227.

2. L'ecosistema digitale e i *Big Data* (cenni)

Quando si parla di Big Data, in ambito giuridico[6], il primo elemento che viene sempre sottolineato è che non ne esiste una definizione normativamente vincolante; essi vengono quindi descritti facendo riferimento «alla raccolta, all'analisi e all'accumulo di ingenti quantità di dati, tra i quali possono essere ricompresi dati di natura personale […] in ipotesi anche provenienti da fonti diverse»[7]. Il secondo elemento, consequenziale, è che «la natura massiva delle operazioni di trattamento reca la necessità che tali insiemi di informazioni (sia memorizzate, sia in streaming) siano oggetto di trattamento automatizzato, mediante algoritmi e altre tecniche avanzate, al fine di individuare correlazioni di natura (per lo più) probabilistica, tendenze e modelli»[8]. Per dare concretezza alle espressioni appena citate, "ingenti quantità" significa che i dati vengono misurati in Zettabyte (un trilione di gigabyte): nel 2020 ne sono stati creati o replicati 64,2, con una previsione in aumento a 79 Zb nel 2021 e di 180 Zb nel 2025[9]. Per questo è "consequenziale" che il loro trattamento sia affidato alle macchine: perché si tratta di dimensioni che il cervello umano non può – né potrà mai – gestire.

Uno dei modi più consueti per *descrivere* il fenomeno dei Big Data è di ripercorrerne la cd. filiera, formata di tre fasi: la raccolta dei dati (a sua volta composta di generazione, acquisizione, memorizzazione); la loro elaborazione (estrazione - integrazione - analisi); infine l'interpretazione (cui segue la decisione)[10]. Un'altra interessante prospettiva è quella di chi preferisce ragionare di *datificazione*, a sua volta scomponibile in «tre fattori essenziali: l'aumento esponenziale della quantità di dati prodotti nel mondo; la capacità di analisi dei dati e di estrazione di informazioni dai dati, svolta da parte di macchine a ciò addestrate; la possibilità e la capacità di prendere decisioni attraverso queste informazioni, anche grazie alla cd. *alghoritmic decision making*»[11].

[6] Diverso è ovviamente l'approccio dei tecnici, basato sulla logica matematica e sulla statistica, e rispetto al quale un inestimabile ausilio alla comprensione – per quanto possibile – è offerto da GIUSEPPE D'ACQUISTO, nel già citato *Decisioni Algoritmiche* e nel precedente *Intelligenza artificiale*, Torino, Giappichelli, 2021. Per la prospettiva filosofica, chi scrive si affida a L. FLORIDI, *Etica dell'intelligenza artificiale. Sviluppi, opportunità e sfide*, Raffaello Cortina Editore, Milano, 2022.

[7] AGCM – AGCOM – GARANTE PER LA PRIVACY, *Indagine conoscitiva sui Big Data*, 10 febbraio 2020 (reperibile nei siti delle tre Autorità), p. 7.

[8] *Ibidem*, citando la Risoluzione del Parlamento europeo del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali.

[9] Cfr. *Quanti dati sono generati ogni minuto nel 2021?*, *Infodata* de *Il Sole 24 Ore*, 27 dicembre 2021, in https://www.infodata.ilsole24ore.com/2021/12/27/quanti-dati-generati-minuto-nel-2021/.

[10] Cfr. AGCM – AGCOM – GARANTE PER LA PRIVACY, *Indagine conoscitiva sui Big Data*, cit., p. 8 ss.

[11] S. CALZOLAIO, *Introduzione.* Ubi data, ibi imperium*: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di Informatica e Diritto*, n. 1/2021, 5; Ead., *(Voce) Protezione dei dati personali*, in *Digesto delle Discipline pubblicistiche*, *Aggiornamento*, Utet Giuridica, Milano, 2016, p. 594 ss.; v. anche S. TORREGIANI, *La circolazione dei dati secondo l'ordinamento giuridico europeo.*

Entrambe le impostazioni, differenti solo quanto a punto di osservazione[12], consentono di focalizzare i due passaggi che dalla prospettiva di questa analisi assumono maggiore rilevanza, e che si collocano nella fase di raccolta, cioè la *generazione* e *l'acquisizione* dei dati[13].

La generazione dei dati può avvenire da parte sia degli utenti, sia delle macchine. Nella prima ipotesi, le persone producono dati innanzitutto interagendo con i propri *device* (principalmente, anche se non solo, computer o smartphone, quindi utilizzando ad esempio posta elettronica, navigazione satellitare, *social networks*, ecc.): ciascuna di queste attività quotidiane viene scomposta in singoli eventi e tracciata, e i relativi dati vengono poi acquisiti e memorizzati. Non solo: alla produzione "attiva" di dati si sommano quelli raccolti dalle funzionalità dei dispositivi (o dalle app) e quelli generati pur *in assenza di interazione diretta* con i dispositivi digitali: gli esempi classici sono la geolocalizzazione dello *smartphone*, se attivata, e le videocamere di sorveglianza. La seconda ipotesi è quella dell'*Internet of Things* (IoT), in cui sono le macchine a comunicare tra loro, scambiandosi e producendo dati[14]: nato per l'industria – l'esempio tipico è la manutenzione predittiva – l'IoT è rapidamente passato a oggetti di uso comune, come gli elettrodomestici o gli orologi/bracciali *smart*; una delle prospettive più interessanti dell'IoT è rappresentata dalle *Smart City*[15].

L'acquisizione dei dati – il secondo passaggio poco sopra menzionato – avviene immediatamente dopo la loro generazione: i dati vengono acquisiti tramite gli stessi dispositivi coinvolti nella fase genetica, entrando nella disponibilità di chi sviluppa e rende operativo il sistema (il fornitore); dal punto di vista giuridico, almeno per ora, la parola chiave è il "consenso" dell'interessato.

Il rischio dell'ipertrofia normativa, in *Rivista italiana di Informatica e Diritto*, n. 1/2021, p. 47 ss.

[12] La prima prospettiva mira infatti a descrivere il processo tecnico, mentre la seconda lo contestualizza come fenomeno socio-economico; ma le fasi sono, ovviamente, le stesse.

[13] Per non appesantire il testo, si segnala che per la parte di descrizione delle due fasi della filiera dei Big Data analizzate, in assenza di specifici richiami, il riferimento è la già citata *Indagine conoscitiva sui Big Data* delle tre Autorità, spec. 10-13. Si dà per sottinteso, ma è bene precisarlo, che tutte le fasi della filiera acquisiscono rilevanza (e problematicità) giuridica perché finalizzate alla decisione algoritmica, che resta quindi tecnicamente il perno di tutte le questioni teoriche.

[14] «L'idea di base dell'IoT è connettere diversi oggetti del mondo reale – come sensori, attuatori, RFID (Radio-Frequency Identification), lettori di codici a barre, telefoni cellulari, ecc. – e farli cooperare l'uno con l'altro al fine di completare un compito comune, attraverso l'uso di microprocessori presenti negli oggetti»: *Indagine conoscitiva sui Big Data*, p. 11.

[15] Nella specifica prospettiva della costruzione di *policy* e delle *Smart City* v. A. SOLA, *Utilizzo di Big Data nelle decisioni pubbliche tra innovazione e tutela della privacy*, in *Media Laws* (www.medialaws.eu), 3/2020, p. 196 ss.; più in generale, cfr. A. PERRUCCI, *Dai Big data all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche*, in *Analisi Giuridica dell'Economia*, 1/2019, p. 61 ss. Di *Smart City* si occupa specificamente il contributo di Y. GUERRA, *Il fenomeno delle* smart city *come esempio di co-regolazione delle nuove tecnologie. La democrazia locale di fronte alle sfide globali* in *Processi di regolazione e tecnologie digitali*, cit.

È a questo punto che, ragionando di Big Data, viene in rilievo la distinzione tra dati personali e non. Com'è noto, la disciplina europea del GDPR[16] – considerata modello globale di *Data Protection* – definisce dato personale (cioè il proprio ambito oggettivo di applicazione) «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale» (art. 4.1)[17]. Per acquisire la disponibilità di questo tipo di dati, i fornitori dei sistemi operativi o delle app devono chiedere il permesso all'utente che li ha generati: ai sensi dell'art. 6 del GDPR, infatti, il trattamento di dati personali è lecito solo se ricorre una delle condizioni elencate, la prima delle quali è il consenso dell'interessato[18]. Tutto ciò che non rientra nella definizione di dato personale prevista al punto 1 dell'art. 4 è considerato dato non personale (o dato anonimo) e, quindi, non è soggetto alla disciplina regolamentare[19].

Bisogna a questo punto precisare che i Big Data sono tendenzialmente anonimi, il che parrebbe sufficiente a porre gli utenti al riparo da un trattamento

[16] Regolamento (Ue) del Parlamento europeo e del Consiglio del 27 aprile 2016 n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - GDPR).

[17] Per una descrizione estesa della nozione e delle tipologie, v. S. CALZOLAIO, *(voce) Protezione dei dati personali*, cit., p. 605-607.

[18] GDPR, art. 6 - *Liceità del trattamento*

«1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti».

[19] L'Unione europea ha disciplinato la materia per il profilo della *libera circolazione* dei dati non personali, con l'omonimo Regolamento (Ue) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018.

non consensuale di informazioni che li riguardano, in alcuni casi anche molto intimamente: basti pensare al fatto che i dispositivi indossabili come gli *smartwatch* rilevano, tra gli altri, dati sanitari. È invece osservazione comune in dottrina come, in realtà, uno dei punti più critici di questo nuovo ecosistema sia l'evidenza per cui la distinzione tra dati personali e non tende a scomparire, e anche piuttosto velocemente. In linea teorica, è evidente che nel momento in cui un utente inserisce il proprio nome, indirizzo e numero di telefono per un acquisto online, si tratta di dati personali; è altrettanto evidente che in linea di massima i sistemi di geolocalizzazione non sono interessati all'identità di chi percorre un determinato tragitto, ma a raccogliere il maggior numero possibile di posizioni per offrire i percorsi in tempo reale.

La classificazione, sulla carta semplice e netta, diventa però in concreto evanescente[20], per due ordini di ragioni. Primo, perché se è vero che la regola europea impone che i dati personali vengano resi anonimi[21] di default[22], è altrettanto vero che è tecnicamente possibile fare il percorso inverso. Secondo, e soprattutto, perché come si anticipava la filiera dei Big Data è gestita da macchine, e in particolare da algoritmi di Intelligenza Artificiale (IA); e quando si ragiona di IA bisogna tenere presente che una delle caratteristiche tanto

[20] Parte della dottrina è infatti già alla ricerca di nuove soluzioni, adottando prospettive a prima vista sorprendenti per la nostra tradizione giuridica: v. S. CALZOLAIO, *From Privacy by design to Data by design (PIPL, DSL and European data protection)*, in corso di pubblicazione in *HangZhou Law Review* 2022, spec. parr. 3 e 4. L'Autore si concentra in particolare sulla maggiore efficacia dell'approccio cinese alle definizioni, basato sulla distinzione tra *informazioni* sulle persone (rilevanti quando vengono in causa diritti e interessi delle medesime) e dati veri e propri (rilevanti quando emerge la prospettiva della sovranità digitale dello stato), a prescindere dalle informazioni in essi contenuti, perché il dato è considerato entità fisica e deve essere sotto il controllo dello Stato.

[21] È la cd. pseudonimizzazione, definita (GDPR, art. 4.5) come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

[22] GDPR, art. 25 (Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita): «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica».

affascinanti quanto potenzialmente devastanti degli algoritmi è che *non è prevedibile a priori quali tipi di connessione siano in grado di individuare*[23]. Il che significa, in sostanza, che una re-identificazione del soggetto potrebbe anche essere involontaria[24]. Svanisce così il confine tra dati personali e non, tanto da indurre parte della dottrina[25] a ritenere che la distinzione stessa sia ormai superata e comunque poco efficace ai fini della tutela dei diritti, anche quando si tratta di dati *indubbiamente* personali: nonostante una disciplina europea apparentemente granitica nella tutela dell'interessato, è proprio il requisito-cardine del consenso ad essersi rivelato progressivamente meno utile, suscitando numerose riflessioni critiche. Pur nell'impossibilità, in questa sede, di approfondire la crescente produzione scientifica sul tema, il suo rilievo è tale da richiedere almeno due precisazioni.

Innanzitutto, secondo il GDPR il consenso deve essere preventivo rispetto a *ogni* trattamento di dati personali e, considerando il numero di interazioni quotidiane di ciascuno con dispositivi digitali, è realisticamente impossibile che la condizione sia effettivamente rispettata. Basti pensare alle preferenze sui *cookie*, cioè quelle finestre che si aprono durante la navigazione online, in cui sono elencate diverse opzioni relative alla cd. *Cookie policy*: dietro la grafica, peraltro spesso fuorviante, si nascondono proprio i consensi al trattamento dei dati – di *tutti* i dati – non solo da parte del sito che in quel momento si sta visualizzando, ma delle cd. terze parti[26], il cui elenco è spesso celato dietro un ulteriore pulsante e che comunque non consente, alla lettura, di capire di quali soggetti si tratti.

[23] Non è un caso che CATHY O'NEIL abbia intitolato il proprio libro-denuncia più noto *Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia* (Bompiani, Milano, 2017). Sul tema v. anche M. PALMIRANI, *Big Data e conoscenza*, in *Rivista di Filosofia del diritto*, 1/2020, p. 73 ss., la quale sottolinea la necessità di «introdurre accanto al diritto alla *spiegabilità* dell'algoritmo e della decisione automatica finale (ossia dell'esito) anche il principio della *conoscibilità* dei dati non tanto e non solo quelli che sono stati contribuiti o osservati dall'utente, ma anche quelli che hanno contribuito al processo quindi quelli inferiti, derivati, collettivi, statistici, anche se anonimi» (p. 87, corsivi testuali). Il suggerimento è concettualmente ineccepibile, ma desta più di qualche perplessità sul piano della concreta realizzabilità.

[24] Tra i numerosi slittamenti semantici che caratterizzano la materia in esame rientra anche la nozione di "volontarietà": nel testo ci si riferisce allo sviluppatore dell'algoritmo, che spesso non ha previsto – né, quindi, voluto – un obiettivo poi raggiunto dall'algoritmo medesimo; ma individuare connessioni imprevedibili è *esattamente* il compito della macchina. Ci si trova, insomma, in un ecosistema in cui la "involontarietà" umana diviene un output sistematico. Ragiona su «un mondo senza volontà e con una sola rappresentazione» G. D'ACQUISTO, *Intelligenza artificiale*, cit., p. 15 ss.

[25] S. CALZOLAIO, *Introduzione,* cit.; Ead., *(voce) Protezione dei dati personali*, cit., p. 594 ss.; v. anche S. TORREGIANI, *La circolazione dei dati secondo l'ordinamento giuridico europeo,* cit.

[26] Il GDPR definisce «terzo» (art. 4.10) «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».

In secondo luogo, a suscitare consistenti dubbi è la validità del consenso prestato quando esso viene dato, ad esempio, ad una app (i cd. *permessi* che le app chiedono al momento dell'installazione, o del primo utilizzo se preinstallate dal fornitore). L'esempio classico è la geolocalizzazione, necessaria per l'utilizzo dei navigatori satellitari, nonché solitamente prevista di default dai *social network* e dai motori di ricerca. Il consenso prestato all'attivazione della funzione nel momento dell'installazione o del primo utilizzo di un dispositivo può giuridicamente considerarsi valido dopo, ad esempio, un anno, o anche un solo mese? Certo, si può ragionevolmente pensare che si tratti di dati anonimi e che quindi la loro "cessione"[27] sia tutto sommato irrilevante per la persona. Al netto del persistere del problema giuridico in merito a qualificazione e validità di un simile consenso, la ragionevolezza dell'ipotesi viene meno, in ogni caso, se ci si sofferma sulla capacità degli algoritmi poco sopra illustrata di creare connessioni tra miriadi di dati anonimi che possono finire per re-identificare il soggetto, anche involontariamente; per non menzionare gli usi impropri – vietati ma non per questo meno diffusi – che di simili dati viene quotidianamente fatto[28]; o le loro potenzialità a fini di sorveglianza, anche da parte di autorità pubbliche[29].

Un'ultima notazione in merito all'ecosistema digitale – a mo' di ponte tra la descrizione del fenomeno e la sua regolazione – consiste nel rilevare che i dati sono, quindi, contemporaneamente *origine* e *materiale* degli algoritmi. E se si guarda il fenomeno non più dalla prospettiva degli utenti, ma da quella dei proprietari degli algoritmi, è facile notare che chi ha la capacità tecnica di implementarli e svilupparli si trova in posizione di vantaggio competitivo sul mercato. Si parla, infatti, di oligopoli digitali: sono le cd. Smart Tech, o Big Tech, o OTT (*Over The Top*), precisamente individuabili in pochi colossi che si contendono, escludendo tutti gli altri, il dominio digitale sul pianeta. Ed è qui il costituzionalismo viene chiamato in causa.

3. Tre domande per il diritto costituzionale: un fenomeno regolabile?

Venendo così alle domande anticipate in apertura, la prima è se sia *possibile* regolamentare il fenomeno[30]: il dubbio sorge non solo perché come si diceva la ricerca e lo sviluppo sono monopolizzati dai privati – le Big Tech – in vantaggio competitivo sul mercato, ma soprattutto perché il regolatore pubblico ha

[27] Sul valore dei dati come prezzo del servizio digitale v. *infra*, par. 5.

[28] L. FLORIDI, Etica dell'intelligenza artificiale, cit., p. 182, individua cinque aree criminali potenzialmente interessate da crimini di IA: commercio, mercati finanziari e insolvenza; droghe nocive o pericolose; reati contro la persona; reati sessuali; furto e frode, contraffazione e sostituzione di persona.

[29] La constatazione è comune, tanto da giustificare paralleli con vicende storiche apparentemente lontane come la Stasi: v. L. MERLA, *Big Data e diritto*, cit., p. 224.

[30] Cfr. S. CALZOLAIO, *(Voce) Protezione dei dati personali*, cit., p. 608 ss.

sinora tentato di *inseguire*, prendendo consapevolezza delle ricadute problematiche quando erano ormai molto oltre la soglia di regolamentazione[31].

La risposta deriva da una scelta di fondo: la dottrina che si è occupata di tale profilo[32], pur prendendo atto delle oggettive difficoltà dell'operazione, converge infatti sull'idea che ci si trovi di fronte a un nuovo potere, privato, che ha la forza degli Stati anche in termini di PIL e che con gli Stati si rapporta *alla pari*[33]. Il punto è che, se resta fermo lo statuto epistemologico della disciplina, il fatto che in questa fase storica e in questo settore (onnipervasivo, peraltro) il potere abbia assunto tali vesti non esime i costituzionalisti, il diritto costituzionale e le autorità pubbliche dal tentare, almeno, di disciplinare un fenomeno che può incidere molto pesantemente sulla democrazia[34] e su *tutti* i pilastri dello Stato di diritto. In sostanza, se il fine ultimo dello Stato rimane la tutela delle persone contro il potere, il fatto che quest'ultimo sia in mano, almeno nel cd. mondo occidentale, a cinque multinazionali digitali non è una ragione sufficiente per arrendersi davanti al compito della sua limitazione.

[31] Un esempio significativo è quello del settore dell'*home sharing*, su cui v. G. MENEGUS, *Processi di regolazione della* Sharing Economy*: oltre la* self-regulation, in *Osservatorio sulle fonti*, n. 3/2021 (www.osservatoriosullefonti.it). Per usare le parole di L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 86: «[a]lcuni hanno insistito sul fatto che leggi e regolamenti giungerebbero sempre troppo tardi senza mai tenere il passo dell'IA, quando in realtà le norme non riguardano il *ritmo* ma la *direzione* dell'innovazione, poiché dovrebbero guidare il corretto sviluppo di una società. Se ci piace dove stiamo andando, possiamo andarci alla velocità che vogliamo» (corsivi aggiunti). Il problema evidenziato nel testo si colloca esattamente in tale prospettiva di assenza di direzione (e con il consistente dubbio che almeno in Italia anche la meta sia, in realtà, ignota).

[32] La bibliografia sul tema si sta ampliando velocemente, ma v. almeno: M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, *Relazione al Convegno annuale del Gruppo di Pisa*, Genova, 18 giugno 2021, in *Rivista del Gruppo di Pisa* n. 2/2021 (https://gruppodipisa.it/rivista/la-rivista-gruppo-di-pisa), ove anche ampie indicazioni bibliografiche; M. MANETTI, *Regolare Internet*, in *Media Laws* (www.medialaws.eu), n. 2/2020; A. SIMONCINI - S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di Filosofia del diritto*, 1/2019, p. 87 ss.; F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

[33] È famoso il cd. caso San Bernardino, cioè il conflitto, durato un anno, tra Apple e FBI in cui la prima, alla richiesta di fornire alla polizia federale statunitense il software per la decrittazione dell'Iphone di un terrorista che nel 2015 aveva ucciso 15 persone e ferite oltre 20, ha pervicacemente *rifiutato* di farlo: v. N. ZAMPERINI, *Manuale di disobbedienza digitale*, Roma, Castelvecchi, 2019, p. 100-102.

[34] «Se gli algoritmi vivono in un mondo in cui l'informazione è una produzione sociale, i loro sogni sono politici, e si nascondono dietro schermi ideologici e propagandistici»: D. CARDON, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, Mondadori, Milano, 2018, p. IX. Sul tema v. P. COSTANZO, *La «democrazia digitale» (precauzioni per l'uso)*, in *Diritto pubblico*, 1/2019, p. 71 ss.; M. BETZU - G. DEMURO, *I big data e i rischi per la democrazia rappresentativa*, in *Media Laws* (www.medialaws.eu), 1/2020, p. 218 ss.

4. Quale livello di normazione?

Una volta effettuata la scelta di fondo, riconoscendo la *necessità* di una disciplina dei Big Data, il secondo, conseguente, quesito è: quale *tipo* di regole? La domanda va declinata in due accezioni, di nuovo logicamente successive: in primo luogo, si tratta di scegliere tra auto ed etero regolazione; in secondo luogo, se si opta per un intervento pubblico, a quale livello di governo tale regolazione deve essere affidata.

Quanto al primo profilo, seguendo il filo rosso della *ratio* del costituzionalismo è inevitabile concludere che almeno per alcuni settori non sia affatto auspicabile lasciare che i privati si auto-limitino, dato che da tale eventuale – e realisticamente remota – facoltà dipende la tutela di numerosi diritti fondamentali. Nessuno crede più alla retorica dello spazio digitale come luogo della libertà[35], mentre è ormai sin troppo nutrita la serie di vicende a dir poco allarmanti: basti pensare ai casi *Cambridge Analytica*, o *Compas*[36], o *PredPol*[37].

Abbandonando l'illusione della auto-regolazione del settore, la natura stessa del fenomeno in esame indica poi la risposta al secondo quesito, per cui il livello di normazione necessario, nel nostro caso, è senza dubbio europeo. È banale affermare che a seguito alla scomparsa dei confini la sfida vada affrontata sul più vasto ambito territoriale possibile; così come è banale rilevare il fallimento del primo tentativo europeo di *Data Protection* tramite direttiva, che ha imposto l'adozione del GDPR[38]. Quindi normativa europea, e dotata di diretta applicabilità, per non lasciare agli Stati la tentazione di assecondare interessi economici particolari, in un settore peraltro tradizionalmente cruciale come la tutela della concorrenza.

[35] Un interessante affresco della «infrastruttura culturale delle techno-corporation» è offerto di nuovo da N. ZAMPERINI, *Manuale di disobbedienza digitale*, cit., p. 66 ss.

[36] V. A. SIMONCINI - S. SUWEIS, *Il cambio di paradigma*, cit., p. 94 ss.

[37] Un software di previsione dei reati su base territoriale adottato in diverse città degli Stati uniti, la cui applicazione produce conseguenze gravemente discriminatorie perché nelle città americane «in cui, per la maggior parte, vige una sorta di segregazione razziale, la geografia è un dato che sostituisce perfettamente la razza»: C. O'NEIL, *Armi di distruzione matematica*, cit., p. 129.

[38] GDPR, considerando n. 9: «Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE».

4.1 La proposta di regolamento europeo sull'Intelligenza Artificiale : i settori di intervento

Esempio paradigmatico è la proposta di regolamento europeo sull'Intelligenza Artificiale presentata il 21 aprile 2021[39], che costituisce anche un ottimo modello rispetto all'obiettivo di queste riflessioni. Ai nostri fini non è necessario scendere nei dettagli di un testo giuridicamente articolato e tecnicamente piuttosto faticoso; limitandosi pertanto al piano definitorio, la proposta di regolamento (titolo II) distingue innanzitutto, seguendo un approccio basato sul rischio, tre tipi di pratiche, «differenziando tra gli usi dell'AI che creano: i) un rischio inaccettabile; ii) un rischio alto; iii) un rischio basso o minimo»[40].

Il rischio viene considerato «inaccettabile» quando è «contrario ai valori dell'Unione, ad esempio perché viola i diritti fondamentali» e le relative pratiche sono vietate. La casistica elencata è sufficiente a rendere l'enormità del problema: il primo gruppo è costituto dalle pratiche che presentano «un elevato potenziale in termini di *manipolazione delle persone* attraverso *tecniche subliminali*, senza che tali persone ne siano consapevoli, oppure di *sfruttamento delle vulnerabilità* di specifici gruppi vulnerabili, quali i minori o le persone con disabilità, *al fine di distorcerne materialmente il comportamento* in maniera tale da provocare loro o a un'altra persona un *danno psicologico o fisico*». Tra le pratiche manipolative che interessano gli adulti e che potrebbero essere facilitate da sistemi di AI sono espressamente richiamate quelle «soggette alla normativa vigente in materia di protezione dei dati, tutela dei consumatori e servizi digitali, che garantisce che le persone fisiche siano adeguatamente informate e dispongano della libera scelta di *non essere soggette a profilazione* o ad *altre pratiche che potrebbero influire sul loro comportamento*». Un ulteriore gruppo di pratiche vietate riguarda quelle finalizzate alla «*attribuzione di un punteggio sociale basato sull'IA* per finalità generali da parte di autorità pubbliche». È infine vietato anche «il ricorso a *sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico* a fini di attività di contrasto, fatta salva l'applicazione di talune eccezioni limitate».

I sistemi di IA ad alto rischio sono l'oggetto specifico della disciplina regolamentare, che subordina la loro immissione sul mercato o la loro messa in servizio – a seconda che si tratti di componenti o di sistemi indipendenti – a una serie di requisiti obbligatori (titolo III). Va sottolineato come il considerando n. 27 premetta che «è opportuno limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute,

[39] Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'Intelligenza Artificiale (Legge sull'Intelligenza Artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final.

[40] COM(2021) 206 final, *Relazione*, 14, da cui anche le citazioni che seguono immediatamente nel testo (corsivi aggiunti).

la sicurezza e i diritti fondamentali delle persone nell'Unione», al fine di ridurre al minimo eventuali potenziali restrizioni al commercio internazionale. Nonostante questa delimitazione, la categoria annovera: i sistemi di identificazione biometrica remota "in tempo reale" e "a posteriori" (cons. n. 33); i sistemi di IA destinati a essere utilizzati come componenti di sicurezza ai fini della gestione del traffico stradale nonché della fornitura di acqua, gas, riscaldamento ed elettricità (cons. n. 34); i sistemi utilizzati nell'istruzione o nella formazione professionale «in particolare per determinare l'accesso o l'assegnazione delle persone [ai relativi istituti] o per valutare le persone che svolgono prove come parte o presupposto della loro istruzione» (cons. n. 35); i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per la gestione del personale (assunzione, selezione, promozioni, valutazioni, ecc.); l'accesso ad alcune prestazioni e servizi pubblici essenziali, come ad esempio il merito creditizio (cons. n. 37); le azioni delle autorità di contrasto (cons. n. 38); i sistemi di IA utilizzati nella gestione della migrazione, dell'asilo e del controllo delle frontiere (cons. n. 39); infine, i sistemi destinati all'amministrazione della giustizia e ai processi democratici (cons. n. 40).

Tralasciando, come si diceva, la disciplina vera e propria, il dato macroscopico è che in tutti i settori sopra elencati sono *già operativi* sistemi di Intelligenza Artificiale: dal che deriva, com'è ovvio, che *tutti* i diritti coinvolti nelle diverse categorie, nonché il principio di eguaglianza, sono *già* altamente a rischio. L'intervento europeo è quindi senza dubbio necessario[41]; il dubbio, invece, resta consistente sul piano dell'effettività[42].

5. Quale ruolo per il legislatore nazionale? Dati come prezzi dei servizi digitali …

Nel quadro sinora descritto, lo spazio per il legislatore nazionale appare decisamente ristretto. Vero è che la proposta di regolamento lascia espressamente agli Stati membri alcune scelte: ad esempio, in deroga al divieto previsto in materia di pratiche a «rischio inaccettabile», l'art. 7, par. 4 consente ad uno Stato di «autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico», entro i limiti e alle condizioni previste dal regolamento stesso. Ma si tratta di ipotesi specifiche, nelle quali «l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi» (cons. n. 18), cioè nei

[41] Sul ritardo nell'adozione del regolamento v. M. R. CARBONE, *Regolamento europeo sull'intelligenza artificiale in ritardo*, ecco perché, in *Agenda Digitale* (https://www.agendadigitale.eu/), 22 febbraio 2022.

[42] V. S. TORREGIANI, *La circolazione dei dati secondo l'ordinamento giuridico europeo*, cit.

casi di ricerca di potenziali vittime di reato, di determinate minacce per la vita o l'incolumità fisica delle persone o di attacco terroristico, o del rilevamento, localizzazione e identificazione degli autori o dei sospettati di reato rientranti nella disciplina del Mandato d'arresto europeo.

Restano inoltre esclusi dalla proposta di regolamento i sistemi non ad alto rischio, per cui è auspicata la creazione di codici di condotta volti a promuovere l'applicazione volontaria dei requisiti applicabili ai sistemi ad alto rischio e l'incoraggiamento ai produttori ad applicare requisiti supplementari relativi, ad esempio, alla sostenibilità ambientale (cons. n. 81).

Se si considera che tra le attività non ad alto rischio rientra sicuramente l'uso privato di *smartphone*, *tablet* e in generale apparecchi digitali, si torna ai punti da cui queste riflessioni hanno preso le mosse, cioè al ruolo degli utenti come generatori di dati, alla problematica configurazione del consenso quale base per il trattamento dei dati medesimi e, più in generale, a tutte le conseguenze derivanti dalla analisi ed elaborazione dei Big Data da parte di algoritmi di proprietà di privati monopolisti, che godono di vantaggio competitivo sul mercato e per i quali i dati sono "*the new oil*"[43].

Tale ultima notazione schiude peraltro un'ulteriore, cruciale angolazione giuridica: la dottrina conviene infatti che il settore chiave in cui operare sia quello dell'antitrust, con l'obiettivo di «spezzare gli oligopoli digitali»[44]. Il nodo centrale, da questa prospettiva, è che l'efficacia delle (necessarie) modifiche di alcuni dei fondamentali dell'antitrust dovrebbe basarsi sulla valorizzazione dei dati come *prezzo* per l'uso delle piattaforme[45]. In altre parole, e

[43] «I dati, i metadati e le informazioni di maggior valore […] sono quelli che si riferiscono alla singola persona, poiché costituiscono la base per generare un profilo dell'individuo, della famiglia (in senso economico) cui appartiene, del gruppo di suoi simili (più dal punto di vista della correlazione tra dati, che non di quanto una analisi sociologica può rilevare e descrivere), di un territorio, di un comparto economico, degli appartenenti a una fede religiosa o ad una associazione riservata e così via»: S. CALZOLAIO, *(voce) Protezione dei dati personali*, cit., p. 602. Se sul piano del valore economico non si può che concordare, avverte però della forzatura contenuta nell'analogia L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 67.

[44] L'espressione è presa a prestito da M. BETZU, *Poteri pubblici e poteri privati*, cit., p. 28. V., sul tema, G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche.* Privacy *e* lex mercatoria, in *Diritto pubblico*, 1/2019, p. 89 ss., spec. p. 99-106. Per un quadro generale v. G. COLANGELO, *Big Data, piattaforme digitali e antitrust*, in *Mercato Concorrenza Regole*, 3/2016, p. 425 ss.; A. GIANNACCARI, *La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi*, ivi, 2/2017, p. 307 ss.

[45] G. DE MINICO (ivi, p. 104) riassume in tre le «operazioni concettuali necessarie e preliminari» per affrontare adeguatamente il problema: «*a)* Concepire il mercato come luogo dove anche i diritti fondamentali possono essere violati, con vulnera non meno gravi di quelli arrecati ai diritti economici dei consumatori. *b)* Concepire il diritto, non più come una realtà divisibile in rigidi compartimenti stagni, incomunicabili tra loro, ma come composizione scomposta di sfere giuridiche che si possono mescolare – è accaduto per privacy e *competition* – e che si parlano […]. *c)* Passare da una valutazione dell'illecito antitrust ancorata al solo indice quantitativo dell'aumento del prezzo, in quanto entità di facile rilevazione, a una più sofisticata basata sulla qualità del servizio, come tale inclusiva degli standard di privacy, di più ardua quantificazione».

semplificando: il principale ostacolo che l'antitrust incontra, nell'affrontare l'ecosistema digitale, deriva dal suo essere basata sull'indice del pagamento di una somma di denaro in cambio di un servizio; mentre le principali piattaforme, i motori di ricerca, i servizi di posta elettronica – insomma: i più importanti "luoghi globali" di generazione e raccolta dati – sono dichiaratamente gratuiti. La consapevolezza è diffusa da tempo nel settore, anche per le Big Tech: non è un caso che Facebook (Meta), nel novembre del 2019, abbia cambiato il proprio *claim* da "*è gratis e lo sarà sempre*" a "*è veloce e semplice*". Passata in sordina[46], la modifica è probabilmente addebitabile[47] all'approvazione, qualche mese prima, della direttiva Ue n. 770/2019[48], il cui considerando n. 24 apre con la constatazione per cui «[l]a fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico». Nel testo della direttiva, la definizione di prezzo viene estesa (art. 2.7), oltre alla somma di denaro, alla «rappresentazione di valore digitale dovuto come corrispettivo per la fornitura di contenuto

[46] Le (poche) testate online che hanno menzionato la notizia sottolineavano l'assenza di comunicazioni ufficiali da parte dell'azienda: cfr. ad es. K. MCCARTHY, *What we know about the small change to Facebook's slogan*, in https://abcnews.go.com/, 28 agosto 2019.

[47] Si intende, con ciò, la modifica strutturale della piattaforma, che era stata nel frattempo (il 29 novembre 2018) sanzionata dall'AGCM per pratica commerciale scorretta, consistente nella pratica ingannevole di informare gli utenti esclusivamente della gratuità del servizio, «senza evidenziare le finalità commerciali di utilizzo dei dati»: S. GOBBATO, *Big Data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *Media Laws* (www.medialaws.eu), 3/2019, p. 157.

[48] Dir. (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, considerando n. 24: «La fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico. Tali modelli commerciali sono utilizzati in diverse forme in una parte considerevole del mercato. Oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali. La presente direttiva dovrebbe pertanto applicarsi ai contratti in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o servizi digitali al consumatore e in cui il consumatore fornisce, o si impegna a fornire, dati personali. I dati personali potrebbero essere forniti all'operatore economico al momento della conclusione del contratto o successivamente, ad esempio nel caso in cui il consumatore acconsente a che l'operatore economico utilizzi gli eventuali dati personali caricati o creati dal consumatore utilizzando il contenuto digitale o il servizio digitale. Il diritto dell'Unione in materia di protezione dei dati personali prevede un elenco esaustivo di fondamenti giuridici per il trattamento lecito dei dati personali. La presente direttiva dovrebbe applicarsi ai contratti in cui il consumatore fornisce, o si impegna a fornire, dati personali all'operatore economico. Ad esempio, la presente direttiva dovrebbe applicarsi nel caso in cui il nome e l'indirizzo email forniti da un consumatore al momento della creazione di un account sui social media siano utilizzati per scopi diversi dalla mera fornitura di contenuti digitali o servizi digitali o non conformi agli obblighi di legge. La presente direttiva dovrebbe altresì applicarsi nel caso in cui il consumatore acconsenta a che il materiale che caricherà e che contiene dati personali, come fotografie o post, sia trattato a fini commerciali dall'operatore economico. Gli Stati membri dovrebbero tuttavia mantenere la facoltà di decidere in merito al soddisfacimento dei requisiti in materia di formazione, esistenza e validità di un contratto a norma del diritto nazionale».

digitale o di servizio digitale». La dichiarazione del principio è di rilievo, ma il riferimento al corrispettivo lo rende a dir poco vago (ci si dovrebbe aspettare che sia il fornitore del servizio ad esplicitare che l'uso è pagato in dati? E quali dati? E di quale parte del servizio?); così come il suo recepimento nel diritto interno è ad oggi pressoché irrilevante, non essendone state tratte conseguenze giuridicamente vincolanti[49]. Che ciò sia effetto dell'azione delle lobby, o della difficoltà tecnica nella regolazione, o di una sorta di *bias* cognitivo dei decisori politici[50] – o, più probabilmente, della combinazione dei tre elementi – è tutto da chiarire; quel che è certo è che ancora più a monte si colloca un problema di percezione da parte degli utenti, oggi pressoché del tutto *inconsapevoli* di "stare pagando" in dati.

5.1 (segue) …e persone come generatori di *Big Data*: un problema di consapevolezza degli utenti

Ebbene, è proprio su tale ultima lacuna che, a parere di chi scrive, si apre per il legislatore nazionale uno spazio, la cui ampiezza dipende in ultima analisi da quale ruolo si attribuisce alle *persone* coinvolte nella filiera dei Big Data. Se si osserva la normativa sinora approvata o in approvazione è facile infatti rilevare come essa guardi agli utenti in veste di consumatori, preoccupandosi della tutela della parte debole in rapporto con un colosso globale, e quindi di fornire una disciplina (teoricamente) molto restrittiva in particolare sulle attività di AI ad alto rischio, così come fa il GDPR per la *Data Protection*. Il che, alla luce dell'incommensurabile differenza di posizione tra i due soggetti, è peraltro ben comprensibile; ma si rivela non più sufficiente nell'era dei Big Data.

Pare infatti che questo sia solo *uno* dei modi in cui si possono vedere gli utenti nell'ecosistema digitale: dalla descrizione della filiera esposta all'inizio di queste riflessioni emerge chiaramente, infatti, che in tale incredibilmente complesso sistema gli utenti non sono solo consumatori, ma anche – e per certi aspetti soprattutto – *produttori* di dati[51]. Il problema è che non lo sanno. E finché le persone non saranno consapevoli sia del funzionamento (almeno a grandi linee) della filiera in discorso, sia del ruolo cruciale da loro stesse giocato al suo interno, sarà realisticamente impossibile che percepiscano i dati da loro generati come un valore (forse "il" valore) non solo sufficiente a compensare

[49] Il recepimento della direttiva è infatti affidato al d.lgs. n. 173 del 4 novembre 2021, che modifica il Codice del consumo accogliendo l'estensione della definizione di prezzo citata nel testo (d.lgs. 206/2005, art. 135-*octies*, lett. *g)*) e senza ulteriori chiarimenti, salvo richiami generici al GDPR.

[50] Cfr. G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche*, cit., spec. p. 104-105, ma *passim*.

[51] L'espressione *walking data generators* è stata coniata nel 2012: v. S. CALZOLAIO, *(voce) Protezione dei dati personali*, cit., p. 598.

l'utilizzo delle piattaforme ecc., ma addirittura in certi casi eccessivo rispetto al servizio offerto (ad esempio, l'accesso a un *social network*).

Adottando questa prospettiva, il problema diventa insomma l'*analfabetismo digitale*, rispetto al quale lo spazio per il regolatore nazionale – in attuazione non solo e non tanto della normativa europea, ma soprattutto della Costituzione – potrebbe essere recuperato attraverso una delle più classiche funzioni dello Stato, cioè l'istruzione.

Anche questo tema è all'attenzione dottrina, sebbene declinato principalmente nei confronti degli operatori dei Big Data. Partendo dal presupposto che sia necessario «interiorizzare i valori tutelati dal diritto costituzionale nelle macchine», ad esempio, Simonicini e Suweis ritengono che occorra intervenire «quando scienziati e tecnologi sono ancora in formazione per spiegare il valore di principii quali la "*privacy by design*" oppure il principio della "comprensibilità" degli algoritmi predittivi»[52]. Nonostante l'apparente distanza, peraltro, i punti di contatto sono sorprendenti: la decisione algoritmica coinvolge temi tradizionali della riflessione giuridica e ancor prima filosofica, quali *equità*, *causalità*, *trasparenza*, che in questo settore assumono il ruolo cruciale di principi necessari ad attenuare i numerosi pericoli derivanti dall'assoluta razionalità – e quindi sostanziale stupidità[53] – degli algoritmi. «[L]a macchina è un decisore pienamente razionale, che non ha interessi da difendere e il cui risultato sarà sempre lo stesso se non cambiano i dati impiegati per assumere la decisione. Le decisioni automatizzate sono dunque certamente caratterizzate dall'assenza di contraddizioni»[54]; tuttavia, «questa maggiore obiettività rispetto alle decisioni umane non è priva di rischi. C'è ad esempio un problema legato alla finalità della decisione, alla scelta dei dati in ingresso e della loro qualità, che è rilevantissimo»; così come è cruciale la fase di interpretazione dei risultati, che possono rivelare ad esempio l'esistenza di un *bias* algoritmico discriminatorio[55].

Un'adeguata formazione degli operatori – nonché dei decisori politici, inevitabilmente tentati dall'apparente oggettività delle decisioni algoritmiche[56] –

[52] A. SIMONCINI - S. SUWEIS, *Il cambio di paradigma*, cit., p. 103, che proseguono: «[d]al momento che la tecnologia è sempre più integrata con la vita delle persone, occorre che valori come la dignità e la libertà della persona stessa divengano parte integrante della formazione di coloro che poi lavoreranno a quelle tecnologie. Di qui il ruolo delle agenzie formative ovvero delle associazioni professionali o accademiche».

[53] «Sono stupide come un vecchio frigorifero, eppure le nostre tecnologie smart giocano a scacchi, parcheggiano un'automobile o interpretano le scansioni mediche meglio di noi»: L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 59.

[54] G. D'ACQUISTO, *Decisioni algoritmiche*, cit., p. 3, da cui anche la citazione che segue immediatamente nel testo.

[55] Ivi, p. 44 ss.

[56] Cfr. A. CARDONE, *"Decisione algoritmica" vs decisione politica? A.I. Legge Democrazia*, Editoriale Scientifica, Napoli, 2021. Ragionando (p. 26) della possibilità di ricorrere a una «burocrazia parlamentare specificamente destinata a mettere a servizio dei parlamentari le risorse dell'intelligenza

è quindi certamente necessità primaria, ma, ancora una volta[57], non sufficiente. Pare infatti cruciale – anche per spezzare gli oligopoli digitali valorizzando innanzitutto la percezione di indicatori diversi dal prezzo (come la qualità del servizio, che include il livello di protezione delle informazioni) – una vera e propria alfabetizzazione digitale rivolta alla collettività. Che analizzi l'ecosistema digitale dalla prospettiva dell'eguaglianza sostanziale[58], o da quello della libertà di espressione[59], la dottrina concorda sulla necessità di rafforzare la *cognizione* delle persone; e come si anticipava poco sopra, si tratta di un obiettivo – forse l'unico, oggi – raggiungibile dal legislatore nazionale, attraverso il sistema di istruzione pubblica. I dati, se da un lato sono tutt'altro che incoraggianti, dall'altro lato evidenziano la bontà della conclusione: dal *Digital Economic and Society Index* (DESI) 2021 emerge che «[p]er l'edizione 2021 dell'indice di digitalizzazione dell'economia e della società (DESI) l'Italia si colloca al 20º posto fra i 27 Stati membri dell'UE»; e che, a parte qualche progresso a livello infrastrutturale, «è significativamente in ritardo rispetto ad altri paesi dell'UE in termini di capitale umano. Rispetto alla media UE, registra infatti livelli di competenze digitali di base e avanzate molto bassi»[60].

Con un'ultima precisazione: se la funzione è classica, quello che deve essere aggiornato sono le modalità. Per avere un minimo di possibilità di successo,

artificiale per la ricostruzione dei dati fattuali e dello stato dell'arte della materia da normare», l'Autore nota che ciò potrebbe senza dubbio offrire «significative leve per riequilibrare il rapporto tra Parlamento e Governo nel procedimento legislativo, soprattutto nelle materie ad elevata complessità tecnica e scientifica»; sottolinea anche, però, che «questo tipo di organi pongono delicati problemi di indipendenza dei soggetti che operano al loro interno e di trasparenza e conoscibilità non solo dei codici degli algoritmi utilizzati, ma anche dei dati processati attraverso detti algoritmi», in assenza dei quali le decisioni «risultano opache proprio in relazione alle premesse valutative costruite grazie agli strumenti dell'intelligenza artificiale» (p. 27).

[57] V. *supra*, par. 5, a proposito del ruolo degli utenti nella filiera dei Big Data.

[58] G. DE MINICO, *I Big Data e la debole resistenza delle categorie giuridiche*, cit., p. 99, critica il GDPR, tra l'altro, perché il suo approccio «nega che la conoscenza dell'algoritmo sia un diritto soggettivo» e ritiene il Regolamento «inadempiente perché decide di tenere i cittadini al buio digitale: nulla della valutazione, neanche il mero esito, è reso disponibile, neppur nelle forme selettive di pubblicità destinate alle sole categorie sociali coinvolte. […] Noi invece riteniamo che la valutazione rappresenti il punto di avvio di quel processo cognitivo circolare che, partito dal basso dai dati dei cittadini del web, ritorni come flusso di bit ai medesimi, le cui condotte sono state oggetto delle previsioni algoritmiche».

[59] «In realtà […] gli unici rimedi che sembrano opponibili alla deriva antidemocratica della Rete sono due: a monte, il rafforzamento della pubblica istruzione, che deve comprendere la consapevolezza nell'uso dei media; a valle, la creazione di siti, pubblici o garantiti dai poteri pubblici, cui il cittadino posso rivolgersi per valutare la qualità e la credibilità delle notizie che riceve»: M. MANETTI, *Regolare Internet*, cit., p. 51.

[60] *Relazione annuale sul DESI 2021*, in https://digital-strategy.ec.europa.eu/, 24 febbraio 2022, 3. Il DESI è l'indicatore sintetico rappresentativo del monitoraggio che la Commissione europea svolge, dal 2014, appunto sui progressi degli Stati nel settore digitale. Per i precedenti v. V. PAGANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di Informatica e Diritto*, 1/2021, p. 11 ss., p. 16.

l'alfabetizzazione digitale non dovrebbe essere ridotta a due righe nei programmi di Educazione civica nelle scuole, ma consistere in un'operazione capillare (che coinvolga tutti i livelli di governo), sostenuta da fondi adeguati e non esclusivamente rivolti alle tradizionali agenzie formative, come ad esempio premialità su iniziative del Terzo Settore. Gli strumenti non mancano, il quadro sovranazionale è propizio[61], le risorse disponibili (su tutte, e per limitarsi alle più citate, il PNRR[62]), la direzione è indicata dagli studi di tutte le discipline che si occupano del tema.

Qualcosa si muove: nell'ambito del PNRR è stato attivato il programma *Italia digitale 2026*, che contiene l'azione *Competenze digitali* con l'obiettivo di «colmare il gap di competenze digitali, con almeno il 70% della popolazione che sia digitalmente abile entro il 2026»[63]. Una delle iniziative strategiche è *Repubblica digitale*, descritta in *home page* del sito dedicato[64] come «l'iniziativa strategica nazionale, promossa dal Ministro per l'innovazione tecnologica e la transizione digitale e coordinata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio, che ha l'obiettivo di ridurre il divario digitale e promuovere l'educazione sulle tecnologie del futuro, supportando il processo di sviluppo del Paese». Dei quattro assi di intervento, il primo è «*Istruzione e Formazione Superiore* - per lo sviluppo delle competenze digitali all'interno dei cicli d'istruzione»; il quarto è «*Cittadini* - per sviluppare le competenze digitali necessarie a esercitare i diritti di cittadinanza e la partecipazione consapevole alla vita democratica»[65].

Nel momento in cui si concludono queste riflessioni[66] il Piano è ancora agli esordi, quindi non è possibile valutarne gli effetti; nelle intenzioni gli obiettivi sono chiari e condivisibili e le azioni ben progettate, ma non si teme di eccedere nel pessimismo se si osserva che, finora, piani di *policy* altrettanto promettenti si sono schiantati sugli scogli della realizzazione, zavorrati da un ottuso approccio iperburocratico e, probabilmente, minati sin dall'origine da una scarsa comprensione sia politica sia amministrativa della loro assoluta necessità. Perciò – e auspicando una smentita – non resta che attendere gli esiti di tale

[61] V. *Governance of Artificial Intelligence in the Council of Europe*, in *Algorythm Watch* (https://algorithmwatch.org/), 22 maggio 2022.

[62] V. A. NAPPO, *La sfida digitale del PNRR: il digital divide*, in *Osservatorio Istituzionale del Centro Studi d'Europa* (https://europacentrostudi.org/), 3 maggio 2022.

[63] Le informazioni sono disponibili nell'apposita sezione del sito del Dipartimento per l'Innovazione tecnologica e la transizione digitale (https://innovazione.gov.it/).

[64] https://repubblicadigitale.innovazione.gov.it/it/

[65] Gli altri due sono «il potenziamento e lo sviluppo delle competenze digitali della forza lavoro, sia nel settore privato che nel settore pubblico» e «lo sviluppo di competenze specialistiche ICT per nuovi mercati e nuovi posti di lavoro». Per i dettagli del Piano Operativo, v. https://repubblicadigitale.innovazione.gov.it/ - *Programma*.

[66] Maggio 2022.

promessa e massiccia opera di alfabetizzazione digitale, confidando di riuscire almeno ad attenuare l'asimmetria informativa tra tecnici e persone comuni: «è particolarmente importante che l'IA sia spiegabile, poiché la spiegabilità è uno strumento fondamentale per costruire la fiducia nel pubblico e la sua comprensione. La creazione di una società della buona IA richiede un approccio che tenga conto di tutte le parti interessate (*multistakeholder*), che è il modo più efficace per assicurare che l'IA soddisfi le esigenze della società, consentendo a sviluppatori, utenti e legislatori di essere tutti coinvolti e di collaborare sin dal principio»[67].

[67] L. FLORIDI, *Etica dell'intelligenza artificiale*, cit., p. 288.