

Fulvia Abbondante
Emergenza sanitaria, stato di diritto e *big data*

ABSTRACT: *The contribution analyzes the impact that the current pandemic from Covid -19 will have on the collection of sensitive data transformed, thanks to the use of algorithms, into Big data and on the potential impact, in the short and long term, that the use this data can produce the proper functioning of democracy, separation of powers, fundamental rights, equality principle. The existing regulatory solutions are completely inadequate because they move in a logic still linked to an elementary digital environment unable to face the challenges of rapid changes that technology imposes.*

SOMMARIO: 1. Emergenza pandemica ed altre emergenze – 2. *Big data* e pandemia – 3. Le sfide allo stato di diritto dei *Big data*: il Sesto Potere – 4. *Big data* e tutela dei diritti fondamentali – 5. *Big data* e principio di uguaglianza – 6. Brevi riflessioni conclusive.

1. Emergenza pandemica ed altre emergenze

È possibile affermare, anche rasentando la banalità, che il nostro tempo è nonostante l'apparente, illusorio e per certi versi ipocrita senso di tranquillità che vuole trasmettere - il tempo delle emergenze. Dalla metà del ventesimo secolo si è assistito a un susseguirsi di avvenimenti eccezionali - crisi ambientali, economiche e sanitarie nonché a un'inedita forma di emergenza determinata una forma sconosciuta di violenza quale è il terrorismo - che con intensità diverse hanno interessato singoli ambiti territoriali o interi continenti. Eppure, nell'alveo del termine emergenza ricomprendiamo fenomeni molto diversi fra loro quanto alla genesi, allo sviluppo e alle possibili soluzioni. Quella epidemiologica, pur condividendo alcuni tratti comuni con le altre tipologie di eventi straordinari precedentemente citati, presenta alcune caratteristiche che non consentono di assimilarla alle altre forme di situazioni eccezionali. Non ha una dimensione territoriale delimitata o delimitabile, non è prevedibile né rispetto alla sua durata né alla sua evoluzione e l'assenza di certezze sulla modalità di contagio produce indecisione rispetto ad ogni progettualità presente e futura. L'etimologia e l'origine stessa della parola "pandemia" ci riconduce alla sua natura totalizzante sia in termini quantitativi, poiché è la globalità del genere umano interessata dal contagio, sia qualitativi, in quanto assorbe e sovverte ogni aspetto della vita individuale e collettiva.

Non si tratta di un fenomeno nuovo. Ogni epoca è stata attraversata dalla diffusione di agenti patogeni che hanno generato significative trasformazioni sugli assetti economici, sociali e giuridici in corso¹. Rimosse generalmente dal racconto storico tradizionale - ma non dalla letteratura che ci ha regalato capolavori le cui narrazioni hanno sullo sfondo appunto il contagio - le pandemie hanno sempre rappresentato un fattore di svelamento di tendenze già presenti e latenti nel tessuto sociale e un potente motore di innovazione scientifica.

¹ Sul punto di v. il recente lavoro di G. BRECCIA-A. FREDIANI, *Epidemie e guerre che hanno cambiato il corso della storia*, Newton Compton Editore, 2020.

L'attuale emergenza epidemiologica si differenzia anche da quelle più recenti², per la presenza della tecnologia digitale che ha consentito di svolgere "in sicurezza" molte delle attività fondamentali che caratterizzano la nostra quotidianità.

Durante le fasi di confinamento è emerso con maggiore evidenza quello che la dottrina più attenta aveva già da tempo sottolineato e cioè che Internet non è solo lo strumento privilegiato per l'esercizio della libertà di manifestazione del pensiero o per un'inedita forma di comunicazione interpersonale, ma un mezzo per realizzare molteplici diritti fondamentali ricompresi sia nelle Carte Costituzionali sia in documenti internazionali del dopoguerra: istruzione, lavoro, ricerca.

La Rete è dunque soprattutto un mezzo di inclusione sociale, a condizione però che gli utenti possano godere di una connessione a banda larga stabile e sicura, l'unica in grado di assicurare l'accesso ai servizi ad alto contenuto tecnologico³.

La prima questione che si è posta, dunque, nel momento acuto della crisi sanitaria è quella del definitivo superamento del *digital divide* e la necessità di intervenire, oramai senza indugio, per la creazione di infrastrutture in grado di assicurare supporti informatici e connessione gratuita alle famiglie in condizioni economiche disagiate e la *broad band*⁴.

Decisioni in tal senso non sono più rinviabili se non altro perché, come sottolineano gli esperti, le pandemie si ripresenteranno ciclicamente costringendo le popolazioni mondiali a lunghi periodi di confinamento e alla necessità di utilizzo continuo del Web.

Una seconda questione emersa, in questa tragica esperienza è la necessità di un'adeguata alfabetizzazione digitale presupposto necessario per un uso anche solo basilare delle potenzialità della Rete. Un problema peraltro preso in considerazione in modo parziale dai governi che hanno concentrato la loro attenzione e le loro politiche di istruzione tecnologica guardando quasi esclusivamente alle giovani generazioni e trascurando una parte significativa e ancora lavorativamente e socialmente attiva quali gli anziani⁵. L'emersione di tali criticità, connesse alle utilità positive della Rete, è stata l'occasione per discutere su altre più inquietanti problemi che sono direttamente legati al lato meno nobile ed oscuro di Internet.

² Anche nel 2009 l'Organizzazione Mondiale della Sanità dichiarò la pandemia da influenza suina che si rivelò molto più circoscritta e meno contagiosa rispetto alle previsioni iniziali.

³ Tra le prime G. DE MINICO, *Tecnica e diritti sociali nella regulation della banda larga*, in (a cura della stessa), *Dalla tecnologia ai diritti Banda larga e servizi a rete*, Napoli, Jovene, 2010, 9 ss.; ID., *Antiche libertà e nuova frontiera digitale*, Torino, 2016, 44 ss.

⁴ Più specificamente sul nesso fra emergenza epidemiologica e superamento del divario digitale v. P. ZUDDAS, *Covid-19 e digitale divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria* in *Osservatorio costituzionale*, 2/ 2020, 285 ss.

⁵ Su tale aspetto particolare v. R. FATTIBENE, *Sviluppo tecnologico e dimensione sociale nell'Unione Europea*, in *Rass. Dir. Pubbl. Eur.*, 1-2/ 2002, 191. Sulle misure di alfabetizzazione digitale adottate in altri paesi europei e specificamente nel Regno Unito ci si permette di rinviare a F. ABBONDANTE, *E-learning: la nuova dimensione dell'apprendimento*, in (a cura di) G. DE MINICO, *Dalla tecnologia ai diritti. Banda larga e servizi a rete* in G. DE MINICO (cur.), *Dalla tecnologia ai diritti*, cit., 228, nota 10.

2. Big data e pandemia

Smart working, didattica a distanza⁶, *e-business* sono divenute, dunque, parole di uso comune ed individuano modalità di esercizio di diritti fondamentali già presenti, con gradazioni diverse, nelle società contemporanee. Volenti o nolenti – anche i più recalcitranti – tutti siamo stati costretti a fruire di servizi ed applicazioni forniti dalla tecnologia digitale per svolgere tali attività essenziali.

All'utilizzo massiccio di Internet è corrisposto un aumento esponenziale del caricamento di nostri dati personali sulla Rete. È oramai chiaro a tutti che Internet è libero ma non gratuito, nel senso che la merce di scambio che noi regaliamo con disinvoltura e per necessità ai fornitori di servizi e contenuti nel ciberspazio, sono appunto le nostre informazioni personali⁷. L'accumulo di tali notizie costituisce quello che, con un'immagine icastica, vengono definiti "il petrolio del Terzo Millennio"⁸, i cd. *Big data*. Questi ultimi rappresentano l'aggregazione di tutte le informazioni che vengono veicolate sul Web che, attraverso processi costanti di analisi realizzati attraverso potenti algoritmi, si trasformano in un'entità diversa che assume un autonomo valore economico – rispetto alla parte elementare che li compone - in ragione della capacità predittiva sui probabili comportamenti di intere categorie di soggetti⁹.

Volendo seguire una suggestione proveniente dalla dottrina sociologica i metadati rappresentano il Sesto potere¹⁰ che succede, sovrapponendosi, al quarto rappresentato dalla stampa e al quinto dalla radio televisione ma molto più pericoloso ed insidioso.

La manipolazione che stampa e televisione realizzano – attraverso l'alterazione delle notizie o lo strumento propagandistico – viene conseguita in maniera visibile poiché tali strumenti agiscono sulla captazione del consenso dall'esterno e su una massa indistinta di soggetti. Si tratta di mezzi in grado di persuadere e non certo di prevedere¹¹. Tant'è che, nel tempo, alla maggiore consapevolezza del ruolo e dell'importanza che i *mass media* assumevano per orientare l'opinione pubblica è corrisposto, da parte di molti ordinamenti, la predisposizione di apposite normative anticoncorrenziali di settore al fine di garantire il pluralismo dell'informazione l'unico antidoto alle possibili derive antidemocratiche del sistema. La molteplicità delle fonti ha rappresentato e rappresenta un indice significativo della salute e della maturità di una democrazia¹².

⁶ Sull'esperienza complessiva di tale modalità di insegnamento nel contesto universitario v. il recente lavoro di S. PRISCO, *La didattica universitaria a distanza: "filosofia", opportunità, limiti e rischi*, in Dirittifondamentali.it, 2/2020.

⁷ Così L. EDWARDS-M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, 18/2017, 33.

⁸ L'icastica espressione è di M. BOGNI-A. DEFANT, *Big data: diritti IP e problemi di privacy*, in *Diritto industriale*, 2/2015, 117.

⁹ B. RABAI, *I big data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, 3/2017, 407.

¹⁰ La suggestione è tratta Z. BAUMAN-D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma – Bari, 2012 che utilizzano tale espressione con un'accezione differente da quella utilizzata nel presente saggio.

¹¹ Tale impostazione è condivisa con G. ARBIA, *Statistica, nuovo empirismo e società nell'era dei Big Data*, Edizioni Nuova Cultura, Roma, 2018, 81.

¹² In tal senso le note pronunce della nostra [Corte costituzionale n. 826 del 1988](#) e ancora più chiaramente [n. 112 del 1993](#).

Il condizionamento che si realizza con lo sfruttamento dei *Big data* si contraddistingue, invece, per la invisibilità e per la capacità invasiva.

L'osmosi tra dimensione pubblica e privata, resa possibile dall'avvento delle piattaforme *social*, ha consentito, proprio grazie ai processi di aggregazione delle informazioni veicolate in rete e dalla "lettura" veloce realizzata dalle *machine learning*, di conoscere in modo incisivo orientamenti, vulnerabilità, insicurezze, paure, di ogni singolo soggetto aspetti insomma che rientrano nell'alveo dell'intimità personale e che consentono di tracciare l'identità più profonda del cibernauta¹³. Una conoscenza tanto accurata che permette attraverso un uso sapiente del *marketing* di orientare in maniera nascosta, qualsiasi scelta dell'utente in Rete.

Per comprendere le ragioni della voracità degli *Over the Top* è fondamentale capire che esiste un meccanismo di autoriproduzione costante. Quando vengono generati dati, questi, a loro volta, possono essere confrontati con nuovi *dataset*, che generano nuovi aggregati di informazioni che vengono comparati con ulteriori nuovi dati raccolti. Un processo infinito che serve ad acquisire conoscenze specifiche su individui o collettività¹⁴.

Ecco le ragioni per cui l'epidemia è un'occasione inaspettata, ma ghiotta per i signori della rete. In questa fase l'attenzione degli studiosi è appuntata sull'uso delle *app* di tracciamento, di cui si farà un breve accenno successivamente, eppure l'impiego quotidiano e ininterrotto di Internet, a causa della crisi epidemiologica ha fatto sì che altri milioni di dati sono stati caricati sul Web (andando a nutrire la massa già imponente di informazioni esistenti) che opportunamente trattati saranno in grado di stabilire le reazioni, le opinioni, le convinzioni rispetto all'epidemia in corso.

Senza trascurare il fatto che, attraverso l'uso degli *smartphone* e degli strumenti di geolocalizzazione già presenti su tali *devices*, le *big companies* possono acquisire notizie in grado di individuare gli spostamenti dell'utente e ricavare informazioni sull'esposizione al contagio o sulla eventuale positività rispetto al Covid-19 e dunque risalire a tutti quei dati cd. detti sensibili, oggetto di una particolare attenzione da parte dei regolatori nazionale ed europeo.

La combinazione fra l'attuale emergenza pandemica e l'uso (o l'abuso?) dei *Big data* pongono nuove e complesse sfide allo Stato di diritto nei suoi tre pilastri fondamentali: separazione dei poteri, diritti fondamentali e il principio di uguaglianza.

3. Le sfide allo stato di diritto dei Big data: il Sesto potere

Senza voler scomodare la letteratura distopica o catastrofista la raccolta di dati avvenuta nel periodo di isolamento dovuto alla crisi sanitaria diverrà l'oggetto dei desideri di governi - anche loro possessori di ingenti quantità di informazioni - e partiti politici che sfrutteranno le predizioni fornite dagli algoritmi per orientare, a bocce ferme, il consenso elettorale.

¹³ Sull'intreccio fra dimensione pubblica e privata si vedano le considerazioni di M. CALISE-F. MUSELLA, *Il principe digitale*, Laterza, Roma-Bari, 2019, 13-14.

¹⁴ Tale fenomeno viene definito con un termine pittoresco ma efficace di "bastard data" da J. McNAMEE, *Is "privacy" still relevant in a world of batard data?*, in [EDRI](#).

L'impiego delle informazioni ricavate dall'analisi dei *Big data* per controllare il gradimento dei votanti è un fenomeno di cui si è avuto contezza solo con l'esplosione del caso *Cambridge Analytica* e sull'influenza che, una propaganda mirata in alcune aree del Regno Unito, ha avuto sul referendum Brexit.

Ora anche l'emergenza sanitaria produce meccanismi di insicurezza a vari livelli e la risposta all'evento pandemico, nella sua fase iniziale, è stato pesantemente condizionato, non solo dall'andamento della curva del contagio, ma anche dagli umori dei cittadini e dalle ricadute sull'economia globale che hanno condotto a scelte, in molti casi, irresponsabili e ad improvvisi cambi di rotta. Le vere criticità si presenteranno, tuttavia, nel post Coronavirus, dove un utilizzo accorto dei dati potrebbe portare a condizionare, in maniera incisiva, i futuri momenti elettorali – sospesi o rinviati proprio in ragione della diffusione dell'agente patogeno – ad un momento più favorevole per questo o quel partito politico o candidato.

Riprendendo la suggestione del precedente paragrafo ha ancora senso parlare di separazione dei poteri secondo l'accezione di Montesquieu – che pur essendo imprescindibile ancor oggi per aversi uno Stato di diritto – era pensata in un mondo non con una complessità di gran lunga inferiore a quella presente. Non può ignorarsi che questo nuovo “potere” controlla profondamente, non solo le scelte dei singoli, ma influenza ed orienta le decisioni di governi e parlamenti, incapaci di decidere nel nome dell'interesse generale inseguendo momentanei interessi parziali.

L'indipendenza dell'un potere dalle altre serve a poco se poi esecutivo e legislativo singolarmente considerati subiscono forti pressioni esterne.

Ha ancora senso parlare di sovranità popolare in un contesto di informazione polarizzata e dove il rapporto fra chi governa e chi è governato si è trasformato in una relazione di “identificazione” più che di rappresentanza.

Del tutto illusoria appare la fiducia che il decisore sovranazionale anche nel recente Regolamento Europeo (*General Data Protection Regulation*) 2016/679¹⁵ all'art. 6, ripone nella prestazione del consenso preventivo come cardine della tutela della *privacy*.

Un siffatto strumento se da un lato rappresenta il presupposto legittimazione al trattamento dei propri dati personali non è in alcun modo in grado di garantire la conoscibilità piena dell'impiego che di essi ne verrà fatta. L'autorizzazione fornita dal cibernauta poteva funzionare solo in un ambiente digitale elementare.

Il consenso viene, infatti, prestato al “buio” dall'utente¹⁶ – moltissima occasione non è né libero né tantomeno consapevole visto che molti *providers* accordano l'accesso al servizio solo previa autorizzazione al trattamento dei dati – e anche colui che userà i dati non sa in anticipo quale impiego ne verrà fatto e, anche conoscendo l'eventuale uso futuro, nulla impedisce che la finalità del trattamento muti nel corso del tempo ovvero cambi in ragione dei successivi processi di combinazione realizzati dagli algoritmi.

¹⁵ Su tale aspetto ha indagato soprattutto la dottrina straniera *ex multis* L. EDWARDS, *Privacy, Law, Code and Social Networking Sites*, in (cur.) I. BROWN, *Research Handbook on governance of the Internet*, Edward Elgar, London, 2013, 324-327; R.F. JOERGENSEN, *The Unbearable Lightness of User Consent*, in *Internet Policy Review*, 4/2014, 1 ss., B. VAN ALSENOY-E. KOSTA-J. DUMORTIER, *Privacy notices versus informational self-determination: Minding the gap*, in *International Review of Law, Computers & Technology*, 2 /2014, 185 - 203.

¹⁶ La felice espressione è di G. DE MINICO, *Big data e la debole esistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto Pubblico*, 1/2019, 92.

Lo strumento pure spesso invocato delle grandi *companies* dell'anonimizzazione o pseudonimizzazione dei dati appare del tutto inadeguato se la possibilità di re-identificare le informazioni aggregate è resa agevole dall'uso combinato dell'Intelligenza Artificiale e la tecnologia delle *Internet of things*¹⁷.

Tutti questi elementi compongono una quando non certo confortante se si aggiunge che, all'interno delle notizie caricate attraverso l'uso delle piattaforme, una cospicua quantità rientra nella categoria dati sensibili il cui trattamento è autorizzato solo attraverso un esplicito consenso.

Spesso accade che la legittima autorizzazione fornita per i dati personali – quali quelli relativi alla profilazione – conducono nel processo di trattamento con *machine learning* ad *outputs* in grado di ricomprendere anche informazioni rientranti in quelle considerate protette per le quali l'utente non ha prestato in alcun modo un consenso espresso.

L'introduzione della *privacy by design* o della portabilità dei dati che rappresentano un apprezzabile passo avanti da parte del decisore politico europeo sono misure timide e che si muovono ancora nella logica di un rapporto quasi paritario e binario fra utente e soggetti che fruiscono dei dati, mentre la presenza dell'intelligenza Artificiale ha di fatto modificato in maniera profonda il cyberspazio¹⁸.

Questi strumenti deboli di tutela del cittadino, pertanto, non sono in grado di contrastare gli altri profili problematici connessi allo sfruttamento dei *Big data* che incidono su diritti fondamentali tanto sul principio di uguaglianza gli altri due pilastri dello Stato di diritto.

4. Big data e tutela dei diritti fondamentali

Quanto alla sfida sui diritti fondamentali un buon punto di partenza sono le *app* di tracciamento per il contenimento del contagio.

Il nostro paese dopo numerosi ripensamenti circa la tipologia di applicazione da adottare – obbligatoria o facoltativa; la modalità di raccolta dati centralizzata o decentralizzata¹⁹ – ha messo a disposizione dei cittadini un modello di *contact tracing* che nonostante tutte le correzioni fatte in corso d'opera, desta moltissime perplessità. I dati caricati sono infatti dati relativi alla nostra salute e tutte le garanzie, da un punto di vista pratico, si rivelano insufficienti.

L'anonimizzazione o pseudonimizzazione, come detto, sono facilmente aggirabili vanificando le cautele che la disciplina europea richiede per il trattamento di dati sensibili come quelli che riguardano la salute.

¹⁷ Cfr. P. OHM, *Broken promises of privacy: responding to the surprising failure of anonymization*, in 57 *Ucla Law Review*, 2010, 1701 ss. In ambito sovranazionale si è espresso anche ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, in [PDP Journals](#)

¹⁸ Sul punto ancora G. DE MINICO, *Big data e la debole esistenza delle categorie giuridiche. Privacy e lex mercatoria*, cit., 97.

¹⁹ Sul complesso percorso legislativo per la predisposizione dell'applicazione di tracciamento in Italia e sulle questioni irrisolte si veda C. PERLINGIERI, *Coronavirus e trattamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità*, in [Actualidad Juridica Iberoamericana](#) n. 12, 12 mayo 2020.

L'impegno che i due giganti statunitensi hanno preso sulla distruzione dei dati conservati sui propri *server*, una volta cessata l'esigenza di tracciamento, seppure violato non sarebbe conoscibile ed eventualmente sanzionabile.

A prescindere dalle questioni più strettamente tecniche appare evidente che per come è stata configurata, nel nostro paese, l'applicazione appare inutile per l'esiguità della copertura raggiunta e dalla sua sostanziale inefficacia poiché la sola rintracciabilità del contagiato e dei suoi contatti senza essere seguita dall'esecuzione di tamponi rende superfluo il *tracing*.

Ma l'*app* di tracciamento è solo la punta dell'*iceberg*.

Un'attenta lettura dei documenti pubblicati sul sito del *Board* della protezione dei dati personali europeo, nel momento di maggiore confusione, concitazione e paura svela che è giunta una lettera della Missione degli Stati Uniti presso l'Unione Europea per ottenere il trasferimento, da parte di enti pubblici e privati, di dati sanitari dal nostro continente per finalità di ricerca a soggetti terzi.

In risposta alla domanda di autorizzazione all'invio delle informazioni²⁰ l'Autorità sovranazionale, richiamando l'art. 7 delle sue linee guida del 3/2020, ha concesso la trasmissione di *sensitive data* in materia sanitaria per agevolare la predisposizione di un vaccino anti Covid-19, previo consenso esplicito dell'interessato ai sensi dell'articolo 49 del Regolamento Europeo purché evidentemente si tratti di misure eccezionali²¹.

5. Big data e principio di uguaglianza

L'utilizzo come detto degli algoritmi e della possibilità di riconoscere singolarmente il soggetto titolare dell'informazioni sensibili pone una serie di questioni in ordine alla possibilità di discriminazione.

In questa ipotesi il *focus* si sposta sull'uso di *machine learning*.

La presunta, asetticità e neutralità della tecnica si scontra con un dato di fatto incontrovertibile: le innovazioni tecnologiche sono prodotte da umani e come tali condizionati dal *background* del soggetto che li programma e dunque anche da pregiudizi, imprecisioni, limiti.

D'altro canto, appare oramai sempre più chiaro che l'infallibilità delle macchine è un mito. Nessuna attività predittiva, per quanto sofisticata, può trasformarsi in preveggenza e dunque margini di errore anche infinitesimali sono sempre possibili. La probabilità di sbaglio è spiegabile anche dal modello di apprendimento per le macchine intelligenti basato su informazioni anche passate piene di preconcetti e approssimazioni.

Un uso massiccio di informazioni sensibili processate dall'Intelligenza Artificiale favorisce la cosiddetta medicina predittiva i cui effetti benefici per la salute umana sono conosciuti ma espone al pericolo di diventare un moltiplicatore di disuguaglianze già esistenti, attraverso il fenomeno della *cd. black box* espressione che sta ad indicare la

²⁰ EDPB, Response to the US Mission to the EU - 24/04/2020.

²¹ EDPR, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, al sito web [edpb](https://edpb.europa.eu), 12-13.

difficoltà anche per i programmatori di riconoscere i percorsi seguiti dagli algoritmi per produrre quel determinato risultato²².

Immaginiamo se le informazioni raccolte in questi mesi, sia attraverso i normali canali di collazionamento, sia le *app* di tracciamento sia i dati sanitari spostati negli Stati Uniti venissero rivenduti a società di assicurazioni – in Italia problema è sentito solo per il momento sentito marginalmente – le quali in virtù delle predizioni effettuate accorderanno la copertura contrattuale solo a quelle persone che per ragioni genetiche, ambientali, di condizioni sociali sono in grado di sviluppare un numero di patologie invalidanti molto basse²³.

Nessuno ci assicura che, in un non lontano futuro, le scelte tragiche – quali quelle di selezionare pazienti anziani o giovani vulnerabili per evitare il sovraffollamento delle terapie intensive già peraltro normalmente praticate ma che hanno suscitato un legittimo clamore durante la fase di picco pandemico – verranno decise da *machine learning*. Certo l'art. 22 della disciplina europea garantisce che la decisione pubblica automatizzata sia accompagnata dal supporto umano ma l'operatore sanitario potrà sempre affidarsi, soprattutto in momenti di grande fatica e disagio psicologico, alla scelta meno umanamente problematica e ritenuta più rassicurante dell'algoritmo.

6. Brevi riflessioni conclusive

La tecnica non è buona e né cattiva e non esiste una soluzione unica rispetto a temi così articolati e variegati.

Infatti, è possibile distinguere due piani di azione su cui dovrebbe orientarsi il decisore politico. Il primo è agire sui *Big data* nella loro dimensione collettiva²⁴ concentrando l'attenzione non solo sulla tutela della *privacy* affidata al debole utente che non può controllare, se non in minima, parte il destino delle proprie informazioni.

La prospettiva da assumere è quella che tenga conto del valore economico dei metadati nel loro insieme e dell'incidenza che essi producono sul corretto funzionamento del mercato.

Come per stampa e televisione, l'accentramento monopolistico determinava non solo una distorsione fra *competitors* ma altresì la violazione di un valore costituzionalmente garantito quale la libertà di informazione nella sua accezione più ampia.

Mutatis mutandis il ragionamento può valere anche per la realtà immateriale della Rete. Nel mondo di Internet vi è un movimento circolare e, peraltro vizioso, in cui

²² In generale il classico F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, Massachusetts, Harvard University Press, 2015; più specificamente, sui rischi soprattutto nel campo della medicina, dell'uso dell'Intelligenza Artificiale C. CASONATO, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *Biodiritto-BioLaw Journal*, Special Issue 2/2019, 718.

²³ Tale preoccupazione era già stata segnalata da A. HOWARD-J. BORENSTEIN, *The ugly truth about ourselves and our robot creations: The problem of bias and social inequity*, in *Science Engineering Ethics*, 24/2018, 1521.

²⁴ Sul punto, sebbene in una prospettiva diversa, v. M.F. DE TULLIO, *La privacy e i big data verso una dimensione costituzionale collettiva*, in *Politica del diritto*, 4/2016, 663-664.

l'utente che fornisce i dati se li vede restituiti o utilizzati per fini non sempre corrispondenti alle ragioni per cui li aveva gratuitamente forniti. In questo rapporto apparentemente binario si colloca un terzo soggetto – i giganti del Web - che da questo processo ne ricavano guadagni alterando non solo la corretta competizione tra imprese ma incidendo significativamente sul gioco democratico, sull'equilibrio dei poteri mettendo in crisi anche i meccanismi di garanzia presenti nelle democrazie più consolidate.

Rompere questa catena è possibile attraverso gli strumenti del diritto *antitrust* – pur presenti nel diritto europeo – ma a patto di innovare logica applicativa attraverso l'utilizzo combinato diritto anticoncorrenziale e *privacy* in modo da tutelare entrambe i valori, in questo caso, non antitetici ma complementari²⁵.

Il secondo *focus* deve concentrarsi sull'Intelligenza Artificiale.

Da tempo ci si interroga sulla creazione di un'etica dell'*Artificial Intelligence*. Un argomento di certo suggestivo che pone però problemi molto complessi.

È difficile definire in maniera univoca e definitiva il termine “etica”. Concetto che, in un mondo globalizzato, risente dei differenti approcci culturali che ogni comunità umana gli attribuisce e di cui non può non tenersene conto²⁶.

Si tratta di un filone di analisi che è solo agli albori ma ha il merito di aver avviato un dibattito grazie al quale si è presa coscienza che le scienze pratiche e dure non possono esaurire il complicato mondo dell'innovazione tecnologica²⁷. I documenti elaborati, da entità pubbliche sovranazionali e nazionali negli ultimi anni il sintomo di questa nuova attenzione ad un tema tanto affascinante quanto di difficile soluzione²⁸.

Una secondo possibile approccio è quella di rendere conoscibile il codice fonte dell'algoritmo.

Si insite oggi sulla necessità di una maggiore trasparenza da parte degli *Over the Top* sui meccanismi che sono alla base della scelta effettuate dalle macchine intelligenti.

Una soluzione quest'ultima parziale, non sempre praticabile che potrà essere bilanciata dal superamento o meglio integrazione di categorie giuridiche quali la responsabilità oggettiva per rischio di impresa - qualora l'effetto discriminante derivi dal cattivo utilizzo dei dati da parte dell'Intelligenza Artificiale - in nome del principio di uguaglianza che si antepone (o dovrebbe) sempre ai diritti economici.

Tale estensione consentirebbe l'intervento del giudice che potrà verificare se la scelta operata attraverso l'uso di *Artificial Intelligence* sia effettivamente discriminatoria superando anche il baluardo della tutela del diritto di proprietà intellettuale e la difficoltà di una decodificazione del linguaggio altamente tecnico, quale quello

²⁵ Tale soluzione viene individuata con ampie e profonde argomentazioni da G. DE MINICO, *Big data e la debole esistenza delle categorie giuridiche. Privacy e lex mercatoria*, cit., 97-98.

²⁶ Su questo specifico aspetto M. TADDEI-L. FLORIDI, *How AI can be a force for good*, in *Science*, 361/2018, Issue 6404, 751-752. Più di recente G. DE MINICO, *L'algoritmo giuridico è intelligente ma deve tener conto delle differenze*, [Il Sole 24 ore](#) del 22 giugno 2020, che sostiene appunto la necessità di una “biodiversità algoritmica”.

²⁷ In tal senso P. ZELLINI, *La dittatura del calcolo*, Piccola Biblioteca Adelphi, Milano, 2018.

²⁸ Un resoconto dei numerosi lavori intervenuti sul tema è contenuto in S. QUINTARELLI-F. COREA-F. FOSSA-A. LOREGGIA-S. SAPIENZA, *AI: profili etici Una prospettiva etica sull'Intelligenza Artificiale: principi, diritti e raccomandazioni*, in [Biodiritto-BioLaw Journal](#), 2019.

informatico, risolvibile grazie all'ausilio di specialisti, gli unici in grado di valutare se la macchina intelligente ha operato con logiche diseguali²⁹.

L'impiego dei modelli predittivi si rivelano, peraltro utilissimi in ben altri campi in cui il ruolo svolto dai *Big data* e dagli algoritmi sarebbero funzionali alla realizzazione dei valori di solidarietà ed eguaglianza.

Da tempo virologi ed epidemiologi hanno sottolineato la prevedibilità dei contagi. Sarebbe auspicabile utilizzare le potenzialità degli *machine learning* per ottenere, in tempi brevissimi, i dati sulla concentrazione di popolazione per alcune aree del territorio al fine di individuare possibili zone ad alto rischio di diffusione dell'agente patogeno. Insomma, una mappatura delle condizioni demografiche e sanitarie che, in futuro, potrebbero evitare la drammaticità della situazione in cui ci siamo trovati, oppure incentivare l'innovazione tecnologica nel settore dell'*healthcare management* in modo da realizzare, in campo sanitario, risultati virtuosi: una tutela effettiva del diritto alla salute grazie ad una migliore organizzazione complessiva ed una più razionale ed efficiente allocazione delle risorse. *Big data* e algoritmi possono essere un potente alleato per le future pandemie. Speriamo che la lezione di oggi serva anche per domani.

²⁹ Ancora G. DE MINICO, *op. cit.*, 99.