GIUSEPPE TROPEA
Professore ordinario presso il Dipartimento di Giurisprudenza, Economia e Scienze Umane dell'Università degli Studi di Reggio Calabria
giuseppe.tropea@unirc.it

RECENSIONE A S. ZUBOFF, *IL CAPITALISMO DELLA SORVEGLIANZA. IL FUTURO DELL'UMANITÀ NELL'ERA DEI NUOVI POTERI*, ROMA, LUISS UNIVERSITY PRESS, 2019 (CON UNA POSTILLA SU PRIVACY E COVID-19)

1. *Chi sa? Chi decide? Chi decide chi decide?*

Mai come in questa drammatica fase d'emergenza e paura è importante leggere il libro della Zuboff, che prova a rispondere a queste capitali domande. Il *Panopticon* di Bentham fa capolino, evidentemente. Come anche i dispositivi di controllo del potere secondo Michel Foucault.

Ma siamo ben al di là, si potrebbe dire nella post-biopolitica, più e meglio che nella psicopolitica[1].

È un lucido manifesto dei nostri tempi. È un ausilio importante per il giurista, pur essendo scritto da una economista versata nella filosofia e nello studio delle scienze sociali[2]. Ha una straordinaria attualità e ricchezza di spunti, specie nella misura in cui tratta anche degli intrecci pubblico-privato di quell'inedito fenomeno che l'autrice definisce la «renderizzazione del profondo».

In questo senso, il pensiero va al dibattito di questi mesi sulla profilazione come metodo, definito "alla coreana", per limitare e/o prevenire il diffondersi del Covid-19. Un altro versante, fra i tanti, in cui si è oggi chiamati dall'epidemia, ciascuno per le proprie competenze e responsabilità[3], alla "scelta tragica" del bilanciamento. Qui, evidentemente, fra privacy e tutela della salute, declinata nel senso di interesse pubblico dall'art. 32 Cost.; allo stesso modo l'art. 2 Cost. non parla solo di diritti inviolabili, tra i quali proprio quello all'essere "lasciati soli", ma anche di inderogabili doveri di solidarietà[4].

2. *Il Capitalismo della Sorveglianza* è composto di quattro parti, ciascuna delle quali a sua volta strutturata in quattro o cinque capitoli.

Nella prima parte si affrontano "le origini" del capitalismo della sorveglianza, in particolare la "scoperta" del cd. "surplus comportamentale". Un ruolo fondamentale è svolto da Google, che avrebbe codificato una serie di

[1] BYUNG-CHUL HAN, *Psicopolitica*, Milano, 2016.

[2] Dichiarata l'influenza di autori come DURKHEIM, ARENDT, ADORNO, POLANYI.

[3] Politico, giurista pratico o teorico, intellettuale, cittadino.

[4] F. FRACCHIA, *Coronavirus, senso del limite, deglobalizzazione e diritto amministrativo: nulla sarà più come prima?,* in *www.dirittodelleconomia.it,* n. 3/2019, 575 ss.

strategie per istituzionalizzare il capitalismo della sorveglianza, con totale disprezzo per la privacy degli individui e in assenza di adeguate leggi in grado di fermarla, nella comunione di interessi con le agenzie di servizi segreti e con alcuni governi, specie dopo l'11/9. Tali strategie vengono descritte con la suggestiva formula "ciclo dell'esproprio", suddiviso in quattro fasi: *incursione, assuefazione, adattamento e reindirizzamento.*

Con la prima Google "entra" in uno spazio indifeso (il nostro telefono, una pagina web, la strada dove viviamo, etc.); con la seconda sopravanza la cause e le inchieste che avanzano col passo lento delle società democratiche; con la terza si mettono in atto adattamenti superficiali che soddisfano le richieste più urgenti di autorità governative o indipendenti; con l'ultima l'azienda mette in atto nuovi metodi, ed espedienti retorici, che ridirigono le operazioni contestate così da farle apparire adeguate agli obblighi legali e sociali.

La seconda parte ci descrive il "business della realtà": il fondamentale passaggio dal mondo online a quello reale, con l'uso di tutti gli aspetti dell'esperienza umana come strumenti (prodotti predittivi) per ottenere dati comportamentali. Molto interessante è, sul punto, la teoria del "non-contratto" che prende ad emblematico esempio il mondo delle assicurazioni automobilistiche. Gli automobilisti vengono persuasi ed incentivati, se non addirittura costretti, a un *do ut des* che collega i prezzi all'espansione di un'architettura dell'estrazione nel mondo reale, finalizzata ad ottenere "surplus comportamentale". Si tratta di transazioni integralmente mediate dai computer, non osservabili e non scrivibili nei contratti. In tal senso il "non-contratto" viene definito come esecuzione unilaterale che rende superflue le relazioni contrattuali, facendo svaporare una nozione millenaria istituzionalizzante come appunto il contratto.

I nuovi protocolli automatizzati finiscono ormai per influenzare e modificare il comportamento umano, per renderlo mezzo di produzione subordinato a mezzi di modifica del comportamento sempre più sofisticati e intrusivi. Si pensi agli esperimenti di contagio di Facebook o al "gioco" di realtà aumentata Pokémon Go, incubato da Google. L'autrice a questo punto si chiede: «Se il capitalismo industriale ha distrutto l'ambiente in modo tanto pericoloso, che danni può fare il capitalismo della sorveglianza alla natura umana?».

Nella terza parte si esamina l'ascesa del potere strumentalizzante, che implica un'epocale sostituzione: mentre nei totalitarismi novecenteschi lo Stato veniva trasformato in un progetto di possesso totale, l'ideologia strumentalizzante pone al centro il mercato digitale. Si badi, questo non significa che non vi siano persistenti intrecci e "staffette" con la sfera pubblica, come in modo formidabile ha evidenziato la macchina della sorveglianza messa in piedi dopo l'11/9, o, più di recente, la vicenda di Cambridge Analytica e il condizionamento del voto americano nel 2016 o anglosassone nel voto su Brexit nel 2018. E come oggi mostra plasticamente la richiesta di molti governi, compreso quello italiano, di utilizzo delle tecnologie di renderizzazione, profilazione e di "ragionamento" algoritmico in possesso di operatori e banche dati privati, per la lotta al Covid-19.

Peraltro, le origini colte del potere strumentalizzante vengono riscontrate nella prima fisica teoretica di Planck e nei lavori del comportamentista radicale Burrhus F. Skinner, usati – ancora dagli Stati – nella lotta alla minaccia comunista negli anni '50-'60. Un articolo del 1966 della *Harvard Law Review* parlava appunto di tracciamento elettronico, sorveglianza e controllo del comportamento, sostenendo di dover concentrarsi sui tentativi del governo di cambiare atteggiamento, visto che sembrano più probabili di eventuali tentativi privati. Skinner immaginava una "tecnologia del comportamento" che un giorno avrebbe consentito l'applicazione di metodi di modifica del comportamento all'intera popolazione umana.

Si segnala a questo punto un nuovo scarto: la migrazione ulteriore dal mondo virtuale al mondo sociale. La società "strumentalizzata" viene immaginata come la simulazione umana di un sistema di macchine in grado di apprendere: una "mente alveare" nella quale ogni elemento impara ed opera in concorso con gli altri.

Questo è punto fondamentale per ciò che si andrà a rilevare in seguito. Nel paragrafo intitolato «La sindrome cinese» si osserva come il governo di questo Paese stia appunto sviluppando un sistema di "credito sociale" destinato ad essere il "nucleo" del suo approccio ad internet. L'idea è di fare leva sull'esplosione dei dati personali per "migliorare" il comportamento dei cittadini. Il sistema traccia comportamenti "buoni" e "cattivi" in una serie di attività, sociali e finanziarie, assegnando in automatico premi e punizioni al fine di formare un comportamento volto alla costruzione della "sincerità economica, sociale, politica". L'obiettivo è fare in modo che ogni cittadino cinese lasci una scia di dati ricavabili da fonti pubbliche e private rintracciabili partendo dalle impronte digitali e da altre caratteristiche biometriche. Si tratta dell'apoteosi del potere strumentalizzante foraggiato dai dati pubblici e privati, e controllato da uno Stato autoritario: lo scopo è automatizzare la società, di cui si teme una crescita "pandemica" di sfiducia, per dar vita a comportamenti predefiniti, ritenuti desiderabili dallo Stato, e così prevenire l'instabilità.

Non si può non pensare al sistema capillare di tracciamento dei dati messo in capo dal governo cinese, e poi sud-coreano, nella vicenda Covid-19. Le applicazioni basate sui Big Data in Cina hanno utilizzato principalmente i dati forniti dal sofisticato e criticato sistema di sorveglianza, composto da circa 200 milioni di telecamere di sicurezza. Un *cluster* di software di analisi di immagini è stato e continua ad essere lo strumento utilizzato per far rispettare la quarantena ai pazienti infetti e per mappare i movimenti del virus. Il governo cinese ha utilizzato anche software di riconoscimento facciale nei luoghi di grande affluenza per il monitoraggio e il riconoscimento dei cittadini.

Tali software inoltre sono capaci di sottoporre a uno screening "invisibile" i cittadini per stabilirne la temperatura corporea. Questa immensa quantità di dati generati costituisce l'ingresso del sistema Health Code, in grado di assegnare a ogni cittadino un grado di pericolosità epidemica e ricavare previsioni su possibili nuovi focolai.

Mi pare che tale vicenda rischi di rappresentare, nella immane tragedia "unificante" che la sottende, un fattore di avvicinamento fra cultura occidentale ed orientale ancora sul punto fino a pochi mesi fa piuttosto distanti. Le nuove frontiere dell'automazione e dell'intelligenza artificiale sembrano compatibili con uno dei possibili scenari di consumo che questo virus sta attualizzando in modo devastante.

La stessa Zuboff ne evidenzia(va) le persistenti differenze: mentre nel capitalismo della sorveglianza occidentale lo Stato ha cominciato nel ruolo di incubatore e rifugio, per fare poi un passo indietro rispetto a grandi gruppi privati, dei quali oggi si deve necessariamente servire per avere accesso a un determinato tipo di potere, nel contesto orientale lo Stato continua a "guidare le danze", proprietario di un progetto politico, e non di mercato: una soluzione informatizzata in grado di dare forma a una nuova società di comportamenti automatizzati capace di garantire esiti politico-sociali predeterminati. La libertà cede il posto alla conoscenza, che appartiene integralmente allo Stato, che la usa per perpetuarsi.

Mi pare di poter dire che fra gli effetti dirompenti su tutte la categorie di pensiero sinora consolidate innescati dall'epidemia che stiamo convulsamente attraversando vi sia proprio questo meccanismo di avvicinamento fra modelli in origine diversi di "società strumentalizzata", sotto alcune unificanti "teste di capitolo": *i)* decidere i propri comportamenti in nome di un bene superiore (es. salute pubblica); *ii)* la pianificazione sostituisce la politica; *iii)* l'uso della pressione sociale per ottenere l' "armonia"; *iv)* l'utopia applicata prodotta dal controllo totale dei mezzi di modifica del comportamento; *v)* la fine dell'individualità, vista come minaccia a "collaborazione", "armonia", "integrazione".

Nella parte conclusiva dell'opera viene rimesso al centro il "diritto al santuario". Si evoca l'*asylon* greco, ciò "che non può essere derubato", lo spazio inviolabile. Si arriva così alla parte forse più scontata del saggio, almeno per il giurista, nella misura in cui si criticano le leggi statunitensi sulla privacy, che non avrebbero tenuto il passo dell'ideologia strumentalizzante, e da un lato si sostiene la necessità di estendere le tutele del quarto emendamento all'internet delle cose, dall'altro si guarda al modello europeo del regolamento GDPR (*General Data Protection Regulation)* come possibile barriera al "Grande Altro", potenzialmente idonea a ripristinare una divisione delle conoscenze in linea con valori e aspirazioni di una società democratica, anche se sul punto sarebbe necessaria, più che un'implementazione in sede legislativa e giudiziaria, una robusta presa di coscienza dei movimenti popolari. Ciò in quanto: «La democrazia è vulnerabile a quel che non ha precedenti, ma la forza delle istituzioni democratiche è l'orologio che determina quanto tali ferite siano gravi e durature. In una società democratica il dibattito e il contesto garantito dalle istituzioni ancora solide può orientare l'opinione pubblica contro forme inattese di oppressione e ingiustizia, per mostrare la strada a leggi e giurisprudenza».

3. Cosa può dire al gius-pubblicista italiano questo intrigante pamphlet? Tanto, evidentemente. E il fattore detonante è, in questo come di fatto in tutti i campi della cultura giuridica, l'epidemia.

Di recente si è colta, soprattutto in questo settore, l'importanza della contaminazione tra saperi[5], e se ne è rimarcata la necessità, in una prospettiva metodologica comparata e attenta al tema della globalizzazione dell'amministrazione e dei suoi giudici, anche con riguardo alle tematiche approfondite nel libro della Zuboff. In particolare, si fa l'esempio della giurisprudenza nazionale che riguarda l'applicabilità degli algoritmi nell'azione amministrativa e le conseguenze che l'impiego di formule matematiche ha sul versante del sindacato giurisdizionale.

Più in generale, ci si chiede: «quali sono i rapporti tra la rivoluzione tecnologica e lo Stato? In che modo le nuove tecnologie dell'informazioni e comunicazione influenzano la sovranità che protegge la democrazia? Potrebbe davvero l'unificazione tecnologica del mondo portare alla «scomparsa degli stati?»[6]. Non è questa la sede per aprire la discussione sui rapporti fra l'impatto devastante del Covid-19, sovranità statale e diritto amministrativo globale. Ci limitiamo a constare come il libro della Zuboff possa consentire nell'attuale contesto post-biopolitico, una rinnovata indagine sul tema degli algoritmi e dei *Big Data,* che inizia a penetrare nel dibattito giuridico, ma solo lambendo le tematiche sopra descritte.

Gli studi si sono sinora concentrati sui settori in cui decisioni amministrative si basano sugli algoritmi[7], talora spingendosi a valutare l'impatto delle nuove tecnologie sulla tutela di diritti fondamentali, come appunto il diritto alla riservatezza o alla protezione dei dati personali, bollandosi sovente come inadeguata la soluzione del consenso informato.

In alcuni casi, peraltro, il libro della Zuboff viene espressamente citato, ma sempre all'interno delle categorie tradizionali, seppure rivedute. Ad esempio, si osserva come il nucleo duro della contrasto giurisprudenziale in tema di decisioni algoritmiche sia il ruolo e la nozione di potere discrezionale[8] al tempo del capitalismo "immateriale" o, appunto, "di sorveglianza", e si plaude a quella giurisprudenza amministrativa secondo cui l'utilizzo di procedure robotizzate non può portare all'elusione di principi che conformano l'ordinamento e regolano lo svolgersi dell'attività amministrativa (trasparenza, comprensibilità, motivazione, proporzionalità).

Un passo avanti nella direzione approfondita dalle presenti note è fatto da chi osserva, sempre sulla base del testo della Zuboff, che se i dati in questione sono personali e le predizioni vengono utilizzate per classificare, valutare

[5] S. VALAGUZZA, *La contaminazione come metodo di conoscenza per la scienza giuridica. Una sperimentazione a partire dal diritto processuale,* in *Dir. Proc. Amm.*, 2019, 1285 ss.

[6] L. CASINI, *Lo Stato nell'era di* Google, in *Riv. Trim. dir. Pubbl.,* 2019, 1111 ss.

[7] G. AVANZINI, *Decisioni amministrative e algoritmi informatici. Predeterminazione, analisi predittiva e nuove forme di intellegibilità*, Napoli, Editoriale Scientifica, 2019.

[8] R. FERRARA, *Il giudice amministrativo e gli algoritmi. Note estemporanee a margine di un recente dibattito,* in *Dir. Amm.*, 2019, 780.

e prevedere il comportamento di uomini, donne e bambini — è quello che oggi va sotto il nome di "profilazione" — allora lo scenario cambia drammaticamente e occorrerà che il diritto, ed in primis quello costituzionale, cominci ad occuparsi con attenzione di questi temi. In particolare poi, se ad utilizzare questi algoritmi predittivi sono soggetti pubblici, quali i giudici o le pubbliche amministrazioni, allora l'allerta deve essere massima, anche perché si ritiene che il GDPR, pur affrontando il tema delle decisioni automatizzate che riguardano le persone, presenta un margine di applicazione abbastanza ristretto e non appare sufficientemente incisivo[9].

Anche lo studio dei *Big Data,* specialmente con funzione predittiva, consente di accostare l'uso che ne hanno fatto, in via pionieristica, aziende come *Google, Facebook* e *Amazon*, con l'impiego che iniziano a farne le amministrazioni, ad esempio nella riconfigurazione dei servizi in modo da intervenire efficacemente in via preventiva, nella analisi della concentrazione criminale e misurazione del livello di sicurezza del territorio, nel settore sanitario.

Anche qui il passaggio dal privato al pubblico è indicativo[10]. Da un lato il progetto *Flu Trends* con cui Google ha previsto dove si sarebbe diffusa un'epidemia influenzale sulla base delle ricerche fatte dagli utenti sui sintomi influenzali; dall'altro l'uso dei dati nel settore sanitario utile nel determinare le interazioni farmacologiche, per individuare effetti collaterali negativi e specifici farmaci.

Queste ricerche, oltre a mettere in evidenza le potenzialità positive, hanno evidenziato i lati oscuri dei dati. Sempre in ambito sanitario, qualche tempo fa il *Journal of the American Medical Association* suggeriva di integrare i database di cartelle cliniche, formazione scolastica e abitudini alimentari per attuare politiche di prevenzione nei confronti dei pazienti a rischio. La tentazione di usare in maniera più ampia e pervasiva i big data è forte. Sorge una questione di contrasto con la disciplina della riservatezza, in quanto vengono trattate grandi masse di dati di diversa natura, tra i quali dati sensibili. I big data, per spiegare la propria potenza, sembrano destinati a scontrarsi fisiologicamente con la privacy. Ciò comporta che debbano essere ridisegnati i contorni della riservatezza e i confini con gli interessi pubblici: appare necessario un maggiore ricorso alla ponderazione degli stessi, da effettuare a seconda degli interessi di volta in volta coinvolti, e una riconsiderazione della attuale disciplina della riservatezza. E così, se il godimento dei diritti fondamentali e l'importanza di alcuni interessi generali potrebbero giustificare una riduzione della tutela della riservatezza, in ogni caso sotto uno stretto scrutinio del principio di proporzionalità, dall'altro l'ipotesi di forme di controllo per ragioni di sicurezza e ordine pubblico sembrerebbero imporre un incremento della tutela.

Del resto, il duplice volto del diritto costituzionale alla salute, fondamentale diritto dell'individuo e interesse della collettività, già da tempo induce a ri-

[9] A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Riv. trim. dir. pubbl.*, 2019, 1149 ss.

[10] F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra open e big data*, in *Dir. Amm.,* 2017, 799 ss.

flettere sull'uso dei *big data* in ambito sanitario. Si pensi al loro impiego per studiare il decorso di una malattia su vasta scala oppure all'uso degli stesi in sistemi algoritmici per generare farmaci in grado di offrire una valida risposta a una determinata malattia[11].

È l'attuale dilemma che oggi viviamo nella vicenda che vede di fronte la lotta al Covid-19 da una parte e la tutela della privacy dall'altra.

4. I quotidiani di queste settimane, quando il "picco" dell'epidemia pare ormai superato, e ci si avvia alla cd. "fase 2", pubblicano editoriali, interviste e dichiarazioni di politici, e non solo, in cui si prospetta, anche come modalità di uscita *soft* (cd. *mitigation*) dalle durissime regole imposte dall'emergenza epidemiologica, il tracciamento informatico dei "positivi" (ancorché asintomatici), utilizzando una o più delle centinaia di sistemi e di app proposti da società private al governo.

Peraltro, secondo alcuni rapporti dei media, una startup di intelligenza artificiale dal Canada aveva dato il primo allarme di un focolaio localizzato di una malattia respiratoria pochi giorni prima dell'annuncio ufficiale dell'epidemia in Cina e ciò sarebbe stato possibile proprio utilizzando tecniche di apprendimento automatico per raccogliere dati da chat, social e media nel colloquio con i medici, di persone che riportavano i sintomi di quello che è poi stato conosciuto come Covid-19, la cui diffusione è stata successivamente rappresentata attraverso una varietà di visualizzazioni. Per non parlare della notizia secondo cui i ricercatori dell'*Oak Ridge National Laboratory* del Dipartimento di Energia degli Stati Uniti stanno che stanno usando un "supercomputer" (Summit di IBM) che, con una potenza computazionale pari a duecento milioni di miliardi di calcoli al secondo, ha consentito di simulare ben ottomila composti farmacologici nel giro di pochi giorni per modellare ciò che potrebbe influire sul processo di infezione e identificarne settantasette con il potenziale di compromettere la capacità del Covid-19 di attaccare e infettare le cellule ospiti.

Deve far riflettere che anche il Garante della privacy, Antonello Soro, in marito proprio al cd. *contact tracing* digitale, cioè l'uso dei dispositivi mobili dei cittadini per la mappatura e il tracciamento dei soggetti entrati in contatto con persone infette (il cd. modello coreano), abbia affermato la teorica possibilità di misure in tal senso, essendo ammissibili limitazioni della privacy a tutela di un altro fondamentale diritto individuale e interesse collettivo, quello alla salute, sia pure attraverso una previsione normativa e con garanzie di temporaneità e proporzionalità negli interventi. Nello stesso tempo sempre il Garante, con una nota del 2 marzo 2020, ha stigmatizzato ogni iniziativa "fai da te" nella raccolta dei dati, svolta da soggetti che non esercitano istituzionalmente queste funzioni in modo qualificato.

A livello di normativa interna, in origine l'unica fonte di rango primario sul punto risultava essere l'art. 14 del d.l. 9 marzo 2020, n. 14 (Disposizioni sul

[11] M. SINISI, *Uso dei* big data *e principio di proporzionalità,* in *www.federalismi.it,* n. 8/2020, 359.

trattamento dei dati personali nel contesto emergenziale) che prevede che «fino al termine dello stato di emergenza […] le strutture deputate pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati monitorare e a garantire l'esecuzione delle misure disposte ai sensi del decreto legge 23 febbraio 2020 n. 6 anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli art. 9 e 10 del regolamento UE 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19».

Tale disciplina derogatoria è apparsa a taluni[12] rispettosa del dato costituzionale e della disciplina nazionale ed europea in materia di privacy. Infatti, il nostro Codice della privacy (art. 2 *sexies*) e il diritto dell'Unione europea, in particolare agli artt. 9, comma 2, e 23 del GDPR, consentono limitazioni alla privacy per motivi di sanità pubblica.

D'altra parte le iniziative "unilaterali" delle Regioni, al di fuori della copertura normativa, iniziano a manifestarsi. Il vice presidente della regione Lombardia, ha dichiarato, ad esempio, che la Regione ha chiesto e ottenuto da gestori telefonici un numero imprecisato ma rilevante di dati di traffico telefonico di cittadini lombardi o persone viventi nel territorio della Regione e li ha incrociati con dati di altri interessati, prevalentemente risultati positivi a test sul coronavirus, al fine dichiarato di verificare se e in che misura le ordinanze del Governo e della Regione impattavano sui comportamenti dei cittadini. Altre regioni, come l'Umbria, hanno sperimentato "la via del consenso", tramite la promozione di applicazioni volontariamente utilizzate dai cittadini. Molto delicata, inoltre, è apparsa la posizione delle istituzioni votate alla ricerca scientifica, su tutte le Università. Si osservi che, anche in questo caso al di fuori da una copertura normativa primaria, con nota del 23 marzo 2020 inviata dal Ministro dell'Università ai Rettori, si richiede la comunicazione e condivisione di progetti e ricerche sul Covid-19, stante «l'importanza di avere con estrema urgenza un quadro completo dello stato dell'arte, che ci consenta di capire quali sono gli elementi già noti e pronti ad essere trasformati in "prodotti" ed "azioni" e soprattutto quelli che ancora non sono noti, ma sono necessari per sviluppare nuovi strumenti di *controllo* e di contrasto dell'epidemia» (corsivo di chi scrive). Questo nell'ambito di una "call for action" voluta dalla ministra dell'Innovazione per aziende, università, enti e centri di ricerca pubblici e privati, associazioni, cooperative, consorzi, fondazioni e istituti chiamate, attraverso le proprie tecnologie, a fornire un contributo nell'ambito dei dispositivi per la prevenzione, la diagnostica e il monitoraggio per il contenimento e il contrasto del diffondersi del Coronavirus (SARS-CoV-2) sull'intero territorio nazionale.

Bisogna quindi verificare se, al di là di un dato normativo ancora eccessivamente vago, si possano trovare appigli nella normativa europea in materia.

[12] D. DE FALCO, M.L. MADDALENA, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, paper in *www.federalismi.it,* Osservatorio Emergenza Covid-19.

Il richiamato regolamento UE 2016/679 (cd. GDPR) interpreta il trattamento delle informazioni personali (in rapporto al diritto alla riservatezza) anche alla luce della sua funzione sociale, affermando, al considerando n. 4 che: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (...)».

Inoltre, al considerando 46, prevede in effetti che «alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana».

Peraltro, ai sensi dell'art. 9 comma 2, lettera j), del GDPR, il divieto di trattare dati relativi alla salute senza il consenso dell'interessato non si applica quando il trattamento «è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale».

Si comprende, in questo senso, come la posizione del nostro garante della *privacy* sia tendenzialmente conforme a quella registrata in sede europea, dove il Comitato europeo per la protezione dei dati personali (EDPB) sostiene, con statement del 16 marzo 2020, che «l'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza». Preso atto che in alcuni Stati membri i Governi prevedono l'utilizzo di dati di localizzazione da dispositivi mobili per monitorare, contenere o attenuare la diffusione del COVID-19, l'EDPB sottolinea che «le autorità pubbliche dovrebbero innanzitutto cercare di trattare i dati relativi all'ubicazione in modo anonimo (ossia, trattare dati in forma aggregata e tale da non consentire la successiva re-identificazione delle persone), il che potrebbe permettere di generare analisi sulla concentrazione di dispositivi mobili in un determinato luogo ("cartografia")». Quando non è possibile elaborare solamente dati anonimi, la direttiva europea sulla privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica.

Questo passaggio è molto rilevante.

Bisogna infatti chiarire che tuttora sussiste in materia un margine di operatività della direttiva "e-Privacy", la quale avrebbe dovuto essere trasformata in un Regolamento ed essere approvata in modo da entrare in vigore contemporaneamente al GDPR. Peraltro, anche per questo, il GDPR fa esplicitamente salva la direttiva "e-Privacy" (direttiva 58/2002 CE), come specifica l'art. 95 del GDPR.

Tuttavia, poiché appunto non c'è stato il Regolamento, come sottolinea

nella sua *opinion* la presidente dello EDPB Jelinek, l'eventuale trattamento di dati di traffico telefonico anche a fini di geolocalizzazione ricade ancora sotto quanto previsto dalla direttiva 2002/58/CE, che prevede che gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli art.5 e 6, all'articolo 8 paragrafi da 1 a 4, e dell'articolo 9 della presente direttiva qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo1, della direttiva 95/46, «una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato di sistemi di comunicazione elettronica».

Quindi è certamente possibile un intervento sul *contact tracing* digitale, ma esso, per evitare la "sindrome cinese" evocata dalla Zuboff, deve rispettare rigorosamente i seguenti presupposti: deve trattarsi di disciplina di carattere primario e rigorosamente proporzionata[13].

Il dubbio che si è subito posto, tuttavia, è che, stanti i presupposti emergenziali inediti nei quali ci si è trovati ad operare, questi requisiti non potessero essere rispettati[14].

Quanto alla fonte, il rischio non mi pare che possa tanto configurarsi nell'alternativa fra una legislazione organica che preveda il procedimento da adottare e l'autorità giudiziaria cui eventualmente il cittadino possa rivolgersi, ovvero di un intervento governativo con decreto-legge, posto che nel nostro caso proporzionalità implica il carattere assolutamente temporaneo del trattamento. È vero, infatti, che il fine non può che essere quello dell'uscita dall'emergenza: occorre dunque che gli strumenti messi in campo abbiano solo ed esclusivamente questa finalità ed abbiano una durata limitata nel tempo, tale da garantire che, una volta terminata l'emergenza, i dati vengano distrutti e non siano più utilizzabili se non, eventualmente, in forma aggregata ed anonima, al solo fine di ricerca.

D'altra parte queste due prospettive appaiono conciliabili, nella misura in cui la decretazione d'urgenza possa poi essere eventualmente corretta, migliorata e "messa a regime" attraverso l'ineludibile passaggio parlamentare, che deve evidentemente costituire la sede per realizzare la *accountability* politico-governativa fondamentale in questo settore. Responsabilità che è anche, peraltro, garanzia di pieno controllo giurisdizionale, ma, ancor prima, appunto, regole procedurali chiare di profilazione dei dati. Tutto ciò è fondamentale anche per un altro convitato di pietra, spesso ignorato, rappresentato dalle piattaforme private digitali che potrebbero non dare il proprio consenso, temendo dalla diffusione indiscriminata dei dati un grande danno – quanto meno – reputazionale. Che ciò ben possa accadere è piuttosto scontato, peraltro anche con

[13] E. CARLONI, *"Fisime per la privacy" Protezione dei dati personali e interesse pubblico nella pandemia*, paper pubblicato nel blog *www.ridiam.it*; F. PIZZETTI, *A rischio le libertà dei cittadini, urgente un intervento giuridico*, in *www.agendadigitale.it*.

[14] Si rinvia a G. TROPEA, *Il contact tracing digitale e l'epidemia: sindrome cinese?,* in *www.lacostituzione.info,* 9 aprile 2020.

riguardo ad Enti pubblici: si pensi alla vicenda che ha interessato l'INPS in seguito alla richiesta di massa del bonus di 600 € previsto dal decreto "Cura Italia", con dati sensibili di molti contribuenti esposti online.

Il vero problema è piuttosto un altro. Come si è detto, le iniziative *de facto* o di livello normativo comunque non primario (ancora ci piace parlare di *soft* law, sic!) tendono a moltiplicarsi, evidentemente ponendosi fuori dal sistema tracciato dal combinarsi fra fonte europea e fonte nazionale. Si pensi, ad esempio, alla recente nota ENAC del 23 marzo 2020, prot. 32363, relativa all'uso dei droni per il monitoraggio dello spostamento dei cittadini sul territorio comunale, con la quale si autorizzano tutti gli «Enti di Stato di cui all'art. 744 del Codice della Navigazione e delle Polizie Locali dei Comuni italiani» ad operare in deroga a svariati requisiti di registrazione e di identificazione nonché anche su aree urbane, senza la necessità di alcuna autorizzazione da parte di ENAC. Questa vicenda dovrebbe allarmare tutti, come cittadini. Non si dimentichi, peraltro, che dopo un primo intervento il 16 luglio 2015, l'ENAC ha pensato bene di emendare il proprio regolamento cinque mesi dopo, vale a dire il 21 dicembre di quello stesso anno. Alla luce di queste e altre analoghe esperienze nazionali degli stati membri, la Commissione

europea ha dovuto correre ai ripari, presentando una proposta di revisione del regolamento UE 216/2008, al fine di riappropriarsi dei poteri normativi in materia di droni fin qui delegati, tra gli altri, appunto all'ENAC[15].

Del resto ricerche informate[16] hanno dimostrato come negli scorsi anni l'uso dei droni in pace e in guerra (cd. "targeted killing", cioè l'uccisione mirata di persone ritenute pericolose per lo Stato cui appartiene il drone) sia spesso stato sottratto alle regole della trasparenza, anche in Paesi come gli USA, dove notoriamente è presente il FOIA (*Freedom of Information Act).*

Quanto alla proporzionalità bisogna intendersi. Mi pare che in questa materia la proporzionalità implichi soluzioni pseudo-anonimizzate che evitino trattamenti che esulino da compiti e responsabilità di tipo epidemiologico, carattere assolutamente temporaneo del trattamento, suo legame con strategie di "vigilanza attiva" (tamponi sui soggetti potenziali positivi non sintomatici).

Dal combinato disposto degli articoli 5 e 6 del Regolamento, che determinano le condizioni di liceità e le finalità della raccolta dati, si ricavano i principi generali che il titolare del trattamento deve seguire nella raccolta dei dati personali degli utenti. In particolare, il regolamento europeo sancisce la necessità che i dati personali vengano raccolti per finalità determinate, esplicite e lecite nei limiti di quanto necessario per il raggiungimento dello scopo peri quali sono stati raccolti. L'unione di questi due principi determina la nascita del c.d. principio di minimizzazione del trattamento.

Tale principio è cardine della normativa europea, per cui non può subire ingiustificate limitazioni.

[15] U. PAGALLO, *Intelligenza artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi intelligenti*, n. 3/2017, 615 ss.

[16] M.G. LOSANO, *Trasparenza e segreto: una convivenza difficile nello Stato democratico*, in *Dir. pubbl.*, 2017, 657.

I principi di pertinenza, adeguatezza e non eccedenza nell'uso dei dati rappresentano gli unici indicatori capaci di guidare verso un uso dei dati corretto e coerente con le esigenze sanitarie, senza valicare gli opposti interessi alla riservatezza del dato: il dato circola in quanto e nella misura in cui esso si renda necessario per i fini posti a tutela della salute (individuale e collettiva).

Più discutibile mi pare invece l'approccio di chi ritiene che in questi casi la proporzionalità deve attuarsi tramite l'immediata adozione di misure di massimo rigore che, se fondate invece su approccio improntato a gradualità potrebbero poi implicare, data la presumibile inefficacia, successivi provvedimenti beni più invasivi dei diritti individuali e della collettività. Una cosa è la valutazione giurisdizione che in sede cautelare viene effettuata in questi convulsi e tristi giorni, rispetto alla quale può essere comprensibile una particolare attenzione del giudice per l'interesse pubblico alla salute, altra è la proporzionalità e adeguatezza delle misure legislative che determineranno presumibilmente il trattamento digitale dei dati, che deve essere adottata nel rispetto dei principi d'una società democratica, ai sensi dell'art. 15 della direttiva 58/2002 CE. Peraltro può essere utile notare che quando il giudice amministrativo ha affrontato sinora *ex professo* la questione della compatibilità del potere di ordinanza con la privacy (nel caso dell'ordinanza del sindaco di Messina che, fra l'altro, imponeva la registrazione on-line dei dati personali di coloro che intendessero attraversare lo stretto) ha perentoriamente data un parere nel senso dell'illegittimità – anche su questo fronte – del provvedimento, per violazione della potestà legislativa statale[17].

Un altro aspetto problematico ha a che fare con il tema delle decisioni amministrative automatizzate tramite algoritmi, come si è detto sopra molto dibattuto nella giurisprudenza amministrativa[18]. È corretto ritenere che, seppure vi siano spiragli in tal senso nel GDPR, il decisore politico non possa far coincidere l'esito dell'algoritmo con una misura limitativa ad applicazione automatica; l'uomo deve poter correggere eventuali errori commessi dall'algoritmo[19].

Infine, i nostri dati debbono confluire in un server di proprietà rigorosamente pubblica, per evitare che la tracciatura venga utilizzata come merce di scambio in una trattativa con i Google di turno, ampiamente esaminati nell'indagine critica della Zuboff, dalla quale hanno preso avvio le presenti note.

[17] Cons. St., sez. I, 7 aprile 2020, n. 735.

[18] Si veda il caso della distribuzione dei posti dei docenti delle scuole secondarie nell'ambito della cd. "buona scuola". Sul punto il giudice amministrativo sembra avere un approccio ancora non univoco: da una parte si registrano sentenze che contestano radicalmente un processo decisionale gestito unicamente da un algoritmo preimpostato e predefinito onde tener conto in automatico di posizioni personali (v. Tar Lazio, sez. III-*bis*, 27 maggio 2019, n. 6606), dall'altra vi sono decisioni più possibiliste, che pretendono però il rispetto dell'obbligo di motivazione, di trasparenza e di correttezza, oltre all'ampiezza del sindacato giurisdizionale (v. Cons. St., sez. VI, 8 aprile 2019, n. 2270).

[19] G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *www.lacostituzione.info*, 1 aprile 2020.

Il recente art. 6 del d.l. 30 aprile 2020, n. 28, è apprezzabile perché ha tenuto conto di molti dei suddetti rilievi, a cominciare proprio dalla fonte del diritto impiegata. Il decreto ha chiarito, inoltre, che i dati personali raccolti dall'applicazione saranno «esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19». Così come i dati raccolti non potranno essere utilizzati per finalità diverse, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini statistici o di ricerca scientifica. Ai sensi del co. 3, lett. c), poi, il trattamento effettuato per allertare i contatti deve essere «basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; è esclusa in ogni caso la geolocalizzazione dei singoli utenti». Non solo anonimato, ma anche facoltatività dell'installazione, e previsione che la mancata installazione dell'app non comporti alcuna conseguenza pregiudizievole. È quindi imposta la cancellazione dei dati alla data di cessazione dello stato di emergenza, e comunque non oltre il 31 dicembre 2020. Infine si prevede la titolarità pubblica della piattaforma e il coinvolgimento del Garante della privacy da parte del Ministero della salute, ai sensi dell'art. 36, par. 5, Regolamento (UE) 2016/679, nell'adozione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi per i diritti e le libertà degli interessati.

L'accesso dibattito di queste settimane, insomma, sembra aver prodotto i suoi frutti.

Non è possibile, ad ogni modo, abbassare la guardia. Bisogna far attenzione a che la "sindrome cinese" non prevalga, viceversa il "giuridico" non conterrà più l'amara prospettiva della più radicale post-biopolitica[20]. La quale ci avverte: «Quello che preoccupa è non tanto o non solo il presente, ma il dopo. Così come le guerre hanno lasciato in eredità alla pace una serie di tecnologie nefaste, dai fili spinati alle centrali nucleari, così è molto probabile che si cercherà di continuare anche dopo l'emergenza sanitaria gli esperimenti che i governi non erano riusciti prima a realizzare: che si chiudano le università e le scuole e si facciano lezioni solo on line, che si smetta una buona volta di riunirsi e di parlare per ragioni politiche o culturali e ci si scambino soltanto messaggi digitali, che ovunque è possibile le macchine sostituiscano ogni contatto - ogni contagio - fra gli esseri umani»[21]. L'appuntamento, forse, è solo rinviato.

[20] Per una esemplare immagine del giuridico che trova antidoti ai moniti della biopolitica, v. L.R. PERFETTI, *L'imperium colpisce ancora. Riflessione di diritto pubblico sul colpo di Stato durante la XVII legislatura repubblicana*, Soveria Mannelli, Rubbettino Editore, 2020.

[21] G. AGAMBEN, *L'invenzione di un'epidemia;* ID., *Contagio,* in *www.quodlibet.it*