

## Scienza, tecnocontrollo e public-policy nell'era COVID-19

*Andrea Monti*

*Università Gabriele d'Annunzio Chieti-Pescara*

### Riassunto

Questo articolo analizza i problemi emersi dall'impiego della tecnologia nella definizione ed attuazione delle misure di contrasto alla pandemia COVID-19. Evidenzia il ruolo della scienza nel supporto ai processi decisionali e la necessità di distinguere i diversi ambiti di attendibilità delle informazioni ai fini del *policy by number*. Segnala l'impatto dell'uso (pur involontariamente) sinergico dei dati nella comunicazione pubblica e in quella dei media come funzionale all'induzione di uno stato di *learned helplessness* favorito dall'opera "infantilizzante" delle tecnologie dell'informazione che si traduce in una minore reattività verso la limitazione dei diritti e delle prerogative democratiche del cittadino. Sostiene, a seguito di una analisi comparata, che la resistenza all'impiego esteso delle tecnologie dell'informazione per contrastare la pandemia – e in generale per la gestione della sicurezza – sia causata dal ritardo tecnologico italiano che ha impedito di fondare la riflessione giuridica su concrete scelte di *public policy* e sulle relative attuazioni normative.

*Parole chiave:* COVID-19, tecnocontrollo, privacy, pubblica sicurezza, sovranità digitale, Asian Values

**Abstract.** *Science, Techno-Control and Public Policy in the COVID-19 Era*

This paper analyses the problems arising from the use of technology in the definition and implementation of measures to combat the COVID-19 pandemic. It highlights the role of science in supporting decision-making processes and the need to distinguish between different areas of information reliability for policy by number purposes. It points out the impact of the (albeit unintentionally) synergistic use of data in public and media communication as functional to the induction of a state of learned helplessness fostered by the "infantilising" work of information technology, which translates into less reactivity towards the limitation of citizens' democratic rights and prerogatives. We sustain, following a comparative analysis, that the resistance to the extended use of the information technologies to counteract the pandemic – and in general, for the management of security – is caused by the Italian technological delay which has prevented the legal reflection on concrete choices of public policy and the relative normative implementations.

*Keywords:* COVID-19, mass control, privacy, public security, digital sovereignty, Asian Values

DOI: 10.32049/RTSA.2020.2.12

### 1. Introduzione

L'emergenza COVID-19 ha evidenziato in modo chiaro – ma non per questo preso nella dovuta considerazione – il ruolo centrale della scienza e della tecnologia nel condizionare le scelte politiche e di conseguenza le norme emanate in loro applicazione.

Non si tratta solo e soltanto delle pur fondamentali questioni legate alla ricerca medico-scientifica, ma anche del modo in cui, da un lato, le tecnologie dell'informazione sono diventate la spina dorsale e l'apparato neuromuscolare del Paese e, dall'altro, hanno posto seri interrogativi sui limiti del loro utilizzo non solo per il controllo diffuso del contagio, ma per l'estensione delle forme di sorveglianza e condizionamento della vita individuale nelle

mani della Presidenza del Consiglio dei Ministri,<sup>1</sup> e il funzionamento della pubblica amministrazione.

Il dibattito pubblico sugli aspetti tecnologici si è concentrato sulla pericolosità delle cosiddette “app” di *contact-tracing*<sup>2</sup> in nome di un vago e indefinito concetto di “privacy” che «è diventato troppo generico e impreciso per costituire uno strumento analitico di qualche utilità» (Wacks, 2016, p. 3)<sup>3</sup> o su generici “allarmi” sul rischio della creazione di uno Stato di polizia, ma in realtà sono rimasti sullo sfondo dei temi centrali come, innanzi tutto, il ruolo della scienza e del *data-analytics* nel supporto alle attività di *public policy* e il controllo sulla sovranità nazionale su dati e identità digitale che rivestono un ruolo

---

<sup>1</sup> Per esempio, ma esula dal perimetro di questo lavoro, andrebbe analizzato il modo in cui sta cambiando il ruolo istituzionale della Presidenza del Consiglio. Nel corso del tempo, infatti, sono diventate suo dominio la protezione civile prima afferente al Ministero degli interni con la legge 24 febbraio 1992, n. 225 (*Istituzione del Servizio nazionale della protezione civile*), poi lo status di “Autorità di sicurezza nazionale” e il comando sui servizi segreti con la legge 3 agosto 2007, n. 124 (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*), l’esercizio della *golden share* con la legge 11 maggio 2012, n. 56 (*Conversione in legge, con modificazioni, del decreto-legge 15 marzo 2012, n. 21, recante norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell’energia, dei trasporti e delle comunicazioni*), la possibilità di dichiarare lo stato di emergenza con una sola “deliberazione” ex articolo 2 comma III Legge 23 agosto 1988, n. 400 (*Disciplina dell’attività di Governo e ordinamento della presidenza del Consiglio dei ministri*) e 24 comma I decreto legislativo 2 gennaio 2018, n. 1 (*Codice della protezione civile*) senza alcun obbligo di “passaggio” parlamentare, la definizione della strategia nazionale di sicurezza cibernetica per la tutela della sicurezza delle reti e dei sistemi di interesse nazionale grazie al decreto legislativo 18 maggio 2018, n. 65 (*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*), l’estensione dei poteri speciali (*golden power*), la definizione dei soggetti che svolgono una funzione essenziale o la prestazione di servizi essenziali e il potere di “spegnere” sistemi e reti di telecomunicazioni con la legge 18 novembre 2019, n. 133 (*Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*).

<sup>2</sup> Si tratta di software in grado, una volta installati su uno *smartphone*, di rilevare la presenza di contagiati e segnalare ex post l’avvenuto potenziale incontro con un soggetto risultato infetto dal virus sfruttando varie tecnologie, dal GPS al Bluetooth, incorporate nei terminali e di comune utilizzo in altri ambiti come l’uso di mappe e l’erogazione di informazioni contestualizzate rispetto al luogo dove si trova l’utente.

<sup>3</sup> Il virgolettato della parola *privacy*, che accompagnerà tutte le occorrenze, è necessario per via della difficile sussumibilità del termine all’interno dell’ordinamento giuridico italiano. Benché spesso il concetto venga utilizzato come sinonimo di protezione dei dati personali, in realtà questo è discutibile. Gli articoli 7 e 8 della *Carta dei diritti fondamentali dell’Unione Europea* e il testo del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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) non utilizzano mai il termine, mentre la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) e le bozze del regolamento che la sostituirà riferiscono il concetto di *privacy* alla mera e sola segretezza delle comunicazioni.

fondamentale nella gestione della sicurezza e dell'incolumità dei cittadini in questa fase di emergenza (non solo) sanitaria.

Il rapporto fra scienza, tecnologia e *public policy*, dunque, non si esaurisce nel fornire indicazioni al Regolatore per assumere decisioni politiche, ma investe l'essenza stessa della dialettica democratica, dalla trasparenza dei rapporti verso il cittadino, al bilanciamento degli interessi pubblici con le libertà fondamentali per il tramite di un'accettazione (o del rifiuto) della dimensione tecnologica del governo di un Paese.

In altri termini, ed è questa la sintesi, è necessario confrontarsi con il fatto che la libertà (o la schiavitù) di un Paese dipende, volenti o nolenti, dalla (in)capacità non solo di governare, ma di essere promotori dell'integrazione di scienza e tecnologia nel tessuto della nazione.

## **2. Scienza, dati e *public policy***

Il rapporto fra esercizio del potere e *public policy* è stato efficacemente descritto in questi termini: «Ruling is an assertion of the will, an attempt to exercise control, to shape the world. Public policies are instruments of this assertive ambition» (Goodin, 2008, p. 3).

Ma un *public policing* che non voglia essere praticato con metodi *à la* Gorgia e Callicle – e dunque sulla base della suggestione manipolativa della massa – deve essere necessariamente basato su dati ed evidenze (Brownson, Chriqui e Stamatakis, 2009) possibilmente di valore scientifico intersoggettivo. Pertanto, quando la scienza viene usata per determinare scelte politiche – e in particolare in materia di sicurezza, cioè di compressione dei diritti fondamentali – è importante domandarsi innanzi tutto cosa sia “scienza” visto l'affollamento di discipline ed esperti che, qualificandosi come “portatori di sapere” si candidano ad essere parte del potere decisionale.

Diciamo subito, senza voler entrare in dibattito molto complesso, che in questo ambito gioca un ruolo fondamentale la possibilità di qualificare come “scientifico” il sapere prodotto da discipline diverse da quelle tradizionalmente associate al mondo delle *hard*

*science.*

Abbandonata da tempo la falsificabilità popperiana come unico criterio di scientificità, l'epistemologia si è concentrata piuttosto sul ruolo della verificabilità intersoggettiva dei predicati come misura del valore di una teoria.

Sembra vi sia poca consapevolezza del metodo che da parecchi secoli ha prodotto i risultati scientifici sotto gli occhi di tutti, ossia quel metodo che si basa sulla diffusione dei dati ottenuti e sulla trasparenza delle procedure osservativo-sperimentali che dovrebbero permettere risultati ripetibili (ritrovabili in tempi diversi ma dallo stesso ricercatore usando le stesse tecniche nello stesso laboratorio) e riproducibili (ritrovabili in tempi diversi da chiunque lo possa fare usando anche tecniche e laboratori diversi). Senza trasparenza dei dati e delle procedure empiriche e senza riproducibilità semplicemente non c'è più la scienza galileiana cui siamo abituati da parecchi secoli: un punto piuttosto ovvio, ma anche piuttosto trascurato, come molti avvertono (Boniolo, 2018).

Discende dal modo di applicare questi due criteri – trasparenza dei dati e riproducibilità dei risultati – lo spostare l'ago della bilancia a favore di una conoscenza rigorosa piuttosto che euristica di una determinata disciplina. «Se si abbandonano gli usuali criteri metodologici di scientificità, come poter avversare il montante irrazionalismo cui assistiamo? Quale differenza fra scienza e magia, fra, per esempio, trattamenti medici scientificamente validati e trattamenti esoterici proposti da ciarlatani e da imbrogliatori?» (Boniolo, 2018).

Rispetto, dunque, all'annosa questione della possibilità di qualificare tali le “scienze” sociali, il problema non è l'etichetta che le definisce quanto, appunto, il livello di verificabilità intersoggettiva dei loro predicati.

Euristicamente, sociologia, diritto, economia e psicologia possono produrre risultati di limitato valore o che consentono di raggiungere risultati di breve periodo, ma non per questo sono meno importanti e non hanno bisogno di ammantarsi di scientificità per contribuire alla crescita del sapere. Lo spiega bene Fredrick von Hayek nella *lectio* tenuta in occasione del conferimento del premio Nobel per l'economia nel 1974:

There is as much reason to be apprehensive about the long run dangers created in a much wider field by the

uncritical acceptance of assertions which have the appearance of being scientific as there is with regard to the problems I have just discussed. What I mainly wanted to bring out by the topical illustration is that certainly in my field, but I believe also generally in the sciences of man, what looks superficially like the most scientific procedure is often the most unscientific, and, beyond this, that in these fields there are definite limits to what we can expect science to achieve (von Hayek, 1974).

Ciò che conta dal punto di vista del *policy maker*, dunque, è la capacità di individuare il corretto ambito applicativo della disciplina che utilizza per decidere, evitando di dare valore generale e generalizzante a teorie e dati che non sono in grado di giustificare questa opzione.

Tuttavia, anche essendo in grado di distinguere la differente capacità esplicativa di una disciplina e dunque la validità delle sue conclusioni, bisogna tenere da conto che guardare alla scienza come elemento costitutivo di una scelta politica pone quattro ordini di problemi: non tutto ciò che è chiamato “scienza” lo è effettivamente, la scienza non offre certezze ma spiegazioni dalla validità limitata, essere un valido scienziato non implica possedere anche sensibilità politica, una decisione politica può divergere da una valutazione scientifica per ragioni di opportunità – o di ignoranza.

La storia anche recente è testimone di molti esempi clamorosi della difficoltà di coniugare il potere decisionale con la razionalità scientifica. Paradigmatica la vicenda dell'aumento *ex lege* del livello di non tossicità della concentrazione di atrazina nell'acqua potabile, dove la “scienza” – o meglio, gli “esperti” – furono il capro espiatorio della decisione politica (La Repubblica, 1988)<sup>4</sup>.

Specularmente, la necessità politica può richiedere l'attenuazione della neutralità scientifica ma questo attiene, o dovrebbe attenersi al momento della scelta e non a quello della determinazione e presentazione dei risultati di una ricerca:

If the content of science – not just its application – can and must involve values, then presenting scientific

---

<sup>4</sup> Il riferimento è alla vicenda della decuplicazione dei valori di concentrazione dell'atrazina nell'acqua potabile disposta nel 1986 e fino al 1988 dall'allora Ministro della sanità Carlo Donat-Cattin. A fronte delle polemiche provocate dal provvedimento che rese “potabile per legge” l'acqua corrente, il ministero si difese sostenendo di avere seguito le decisioni di una commissione di tecnici.

results as entirely neutral is deceptive. It means ignoring the value assumptions that go into science and the value implications of scientific results. Important value assumptions will be hidden behind a cloak of neutrality in public debates over policy and morality. (Kincaid, Dupré e Wiley 2007, Kindle Locations 63-64).

Senza voler evocare lo spettro di Trofim Lysenko, in questo senso è altrettanto paradigmatico il caso del National DNA Database inglese. L'inclusione selettiva di determinati reati (e dunque dei loro autori) nel database, la conservazione eccessivamente lunga di profili e campioni (Marper v UK - 2008CEDU1581), l'espansione dell'utilizzo giudiziario del *phenotyping* (McLean e Lamparello, 2014) contribuiscono alla definizione della politica criminale del Regno Unito potenzialmente giustificando una sorta di approccio deterministico (Sohrabi, 2015) o comunque basato su pregiudizi etnici (House of Commons Home Affairs Committee, 2010).

This is not the place to analyse the political implications of targeting specific crimes as a genetic profiling source. Suffice it to say that if, for instance, only the authors of violent crimes are to be included in the national DNA database, and such violent crimes are mainly committed by members of a certain race or social class, the statistics based on the database-supported convictions will inevitably yield information that, notwithstanding its limited value, is likely to influence lawmakers toward targeting that specific group. (Monti e Wacks, 2019).

Una lettura poco attenta al tema dell'uso politico della scienza – o una fiducia neopositivista nella traslazione *tout-court* delle scoperte scientifiche in un ambito politico-normativo – potrebbero condurre ad invocare applicazioni *tranchant* di questi metodi su un ingenuo presupposto determinista. Ma basta studiare la storia delle “DNA Wars” (Aronson, 2007; Bieber, 2008) e avere approfondito le implicazioni politiche sull'uso dei database genetici per finalità di polizia (Monti, 2010), o avere analizzato il tentativo di far entrare le “neuroscienze” nel processo penale (Gennari, 2018) per rendersi conto di quanto il rapporto fra scienza, politica e diritto sia molto più complesso di quanto consentano approcci meno meditati.

Rivolgersi alla scienza, infatti, non implica per il potere politico il doverne seguire per forza le indicazioni. A volte, come nel caso del cambiamento climatico, questo accade per una precisa scelta (Meyer, 2019), perché – come nel caso del referendum sul nucleare – la volontà popolare è stata ritenuta prevalente sull'interesse pubblico all'indipendenza energetica, o ancora per via della scelta *lato sensu* politica di acquietare l'opinione pubblica. Oggi infatti – assistendo a una replica dei casi Di Bella e Stamina – siamo spettatori del caso Avigan, il farmaco anti-influenzale prodotto in Giappone assunto agli onori della cronaca come “efficace” contro il COVID-19 grazie a un video amatoriale diffuso da un turista italiano in vacanza a Tokyo.

Quello che atterrisce, come nel caso di Stamina e delle varie terapie anticancro proposte nel passato, è che questo tsunami di incompetenza riesca a convincere i politici e a indurre stimate agenzie come l'AIFA o le Istituzioni del Paese ad approvare sperimentazioni non già richieste dai vari virologi e clinici che questi farmaci (Avigan incluso) li conoscono bene e che stanno combattendo per noi. Qui non stiamo contestando il farmaco specifico quanto la procedura che lo starebbe portando in una sperimentazione che, capiamo bene, priverebbe molti pazienti di altri farmaci attualmente molto più promettenti. Ed è su questa base che AIFA non dovrebbe cedere alle pressioni e approvare una sperimentazione fondata sulle attuali conoscenze (Bucci, Corbellini e De Luca, 2020).

Un approccio alla scienza che è complementare a quello appena descritto, caratteristico del regime emergenziale è, infine, quello fideistico. Dalla scienza, quasi fosse una dea pagana sul cui altare consumare sacrifici umani, ci si aspetta “la cura” per il male anzi, la si esige. E quando il miracolo non arriva, allora la reazione violenta e irrazionale è quella di punire la divinità, rinnegandola e mettendola sotto processo in nome di un preteso “obbligo di salvezza”.

La visione scientifica oggi predominante porta l'uomo contemporaneo a ritenere che ogni evento possa essere previsto nella sua singola causalità e quindi che possano individuarsi anche i fattori responsabili dei singoli eventi. Conseguenzialmente i soggetti o gli organismi deputati ad evitare la produzione dei predetti fattori, possono essere chiamati a rispondere di un mancato (o insufficiente) intervento volto ad evitare la produzione di tali dannosi eventi (Politi, 2014, p. 5).

È quello che accadde, all'indomani del terremoto del 6 aprile 2009 che colpì l'Abruzzo interno, quando i componenti della Commissione grandi rischi vennero processati per non avere previsto ciò che era imprevedibile: il verificarsi del terremoto.

È vero che, *excusatio non petita*, il giudice di primo grado ebbe a specificare di non avere celebrato un “processo alla scienza”, ma è anche vero che il capo di imputazione contestava agli imputati, testualmente e prima della violazione dei doveri nella comunicazione verso l'esterno, l'effettuazione di una «valutazione dei rischi connessi all'attività sismica in corso sul territorio aquilano dal dicembre 2008 approssimativa, generica ed inefficace in relazione alle attività ed ai doveri di previsione e prevenzione. »

Cheché se ne possa dire, dunque, l'accusa è chiara nella sua contraddittorietà, per cui delle due l'una: o i terremoti si possono prevedere, e allora è possibile la «valutazione dei rischi connessi», oppure non è possibile antivederli, e allora non solo non può esserci la predetta “valutazione” ma nemmeno si possono configurare doveri di previsione e prevenzione del singolo evento<sup>5</sup>.

Quando, però, da un'attività libera nel fine come la politica si passa alla rigidità della normazione, tutte le sfumature di quella dimensione collassano sul determinismo formale della singola fattispecie basata, almeno sulla carta, su un rigido meccanismo di causa-effetto: “se fai X, accade Y”. E allora, più che di teorie scientifiche il decisore ha bisogno – o ha anche bisogno – di numeri per sostenere il suo *decisum*.

### **3. Policy by data, orientamento del consenso e controllo sociale**

La gestione del versante pubblico dell'emergenza COVID-19, cioè del rapporto con i cittadini, è stata caratterizzata dal massiccio uso di dati e della statistica per tradurre in decisioni le proposte di medici, scienziati, economisti ed esperti. Da subito, tuttavia, si è manifestata una impropria “statisticizzazione” dei dati (Koerth, Bronner e Mithani, 2020).

---

<sup>5</sup> Non sfuggono all'autore la vastità e la complessità dei temi sollevati dalle tre sentenze che hanno caratterizzato la vicenda e l'impossibilità di racchiudere in un obiter dictum il dibattito dottrinale innescato dalle decisioni.

Senza voler entrare troppo nel dettaglio del modo in cui sono state comunicate le informazioni sui contagi, basta evidenziare due aspetti: l'assenza di indicazioni sulla significatività statistica dei dati sui contagi e l'intrinseca disomogeneità del campione utilizzato.

La significatività statistica è un valore che consente di capire quanto i risultati che vengono presentati siano reali oppure frutto di un esito casuale.

Se la fonte delle informazioni ci indica anche il grado di significatività, abbiamo una migliore possibilità di capire dove siamo. Questo grado di significatività è semplicemente espresso come probabilità, come quando l'istituto del censimento ci dice che ci sono diciannove probabilità su venti che i suoi numeri abbiano uno specifico livello di precisione. Nella maggior parte dei casi nulla al di sotto di quel cinque per cento di significatività può essere considerato sufficiente. In alcuni il livello richiesto è l'uno per cento, il che significa che ci sono novantanove probabilità su cento che una certa differenza, o qualcos'altro, sia reale. Un dato così altamente probabile è talvolta descritto come "praticamente certo" (Huff, 2005, p. 67).

Perché dei dati siano statisticamente significativi, inoltre, è fondamentale che il campione sulla quale si basano sia costruito secondo determinati criteri. Nel caso dei dati su contagi, guarigioni e decessi basta constatare che questi erano il frutto di rilevazioni eseguite in modo autonomo e non coordinato dalle singole strutture sanitarie, il che ha minato alla base la loro capacità esplicativa. Come è noto, infatti,

un campione può dirsi rappresentativo del proprio universo quando c'è l'identità delle proporzioni secondo le quali sono presenti, nell'uno e nell'altro, i vari caratteri della popolazione. [...] Se la proporzionalità tra campione e universo sussiste con riguardo a qualsivoglia carattere (o variabile), potremo aspettarci che anche con riguardo alle variabili ancora incognite, sulle quali ci proponiamo di indagare con il nostro sondaggio [...] vi sia quell'identità di proporzioni tra campione ed universo che costituisce il presupposto della rappresentatività statistica (Brusati, 2003).

Di conseguenza, già per ciò solo i dati resi disponibili dalla Protezione civile non potevano avere una capacità predittiva. Il che non ha impedito però che, progressivamente, la comunicazione dei valori assoluti venisse affiancata, sui mezzi di informazione, dalla loro

conversione in percentuali trasmettendo una percezione distorta del messaggio. Distorsione poi accentuata dal modo in cui sono stati utilizzati grafici e istogrammi per stabilire “trend di crescita” e “indici” di letalità e mortalità.

Sotto il primo profilo, è evidente che se l’andamento della curva dei contagiati dipende dalla definizione stessa di “contagiato” e dal modo in cui viene individuato, e non da una rilevazione statistica propriamente detta, il risultato è un grafico descrittivo di una situazione parziale e non una curva predittiva, in grado di consentire prognosi sul futuro.

Inoltre, la scelta di chi sottoporre a test condiziona anche l’indice di mortalità e quello di letalità del virus.

The UK has mainly tested people who are ill enough to be admitted to hospital. That can make the death rate appear much higher than in a country which had a wider testing programme. The more testing a country carries out, the more it will find people who have coronavirus with only mild symptoms, or perhaps no symptoms at all. So, the death rate in confirmed cases is not the same as the overall death rate (Morris e Reuben, 2020).

A loro volta, gli indici di letalità e mortalità sono – è il caso di dire – “influenzati” dalla definizione di “morte COVID-19”. In Inghilterra «the UK’s Office for National Statistics counts all deaths as Covid-19 where Covid-19 was mentioned on the death certificate, regardless of whether they were tested or if it was merely a suspected case of Covid-19» (Enriques, 2020). Germania e Hong Kong includono nell’elenco indifferentemente i pazienti morti “con” COVID-19 e “per” COVID-19. Negli USA i medici devono valutare la causa del decesso, distinguendo dunque – secondo la loro valutazione individuale – quello “per” da quello “da” Coronavirus (CDC, 2020).

Tutto questo è particolarmente rilevante rispetto alla significatività del qualificare come “esponenziale” l’andamento delle curve descrittive di contagi, morti e guarigioni. Queste, infatti, sono state costruite a ritroso, leggendo complessivamente e retrospettivamente i dati rilevati giorno per giorno. L’effetto finale (al netto di tutte le carenze e le limitazioni evidenziate *supra*) può anche essere “esponenziale”, ma questo varrebbe per il passato, e non certo per il futuro: basterebbe ridurre il numero dei tamponi, o eseguirli in zone meno

contagiate per appiattare la curva senza che il risultato abbia una qualche significatività.

Questa conclusione, proprio perché non immediatamente percepibile, si somma alla difficoltosa comprensione del significato dei numeri del coronavirus e ha delle conseguenze precise nella percezione delle persone: alterazione della capacità di giudizio (Peters, 2020) attribuzione di valore assoluto al numero dei contagiati (che invece è solo quello emerso dai test), adozione di comportamenti (anche sbagliati) in funzione della comparazione di dati provenienti da Paesi che seguono standard diversi (Kottasová, 2020).

Il tema della manipolazione dei dati per la costruzione del consenso non è certo di oggi.

A partire, infatti, dagli anni Trenta del XX secolo, la disponibilità di tecniche statistiche e campionarie per l'analisi degli atteggiamenti e delle dinamiche di opinione tramite survey e sondaggi, se contribuisce a far uscire definitivamente l'analisi dell'opinione pubblica dall'empirico del «mondo delle idee» (accentuando anche il primato dell'approccio psico-sociologico su quello prettamente filosofico), avvia però anche una svolta analitico-interpretativa nello studio dell'opinione pubblica che tende a marginalizzare la riflessione teorico-critica sul fenomeno, le sue articolazioni e le sue trasformazioni all'interno del modello di democrazia, e finisce per ridurre, anche involontariamente, l'analisi dell'opinione pubblica alla rilevazione delle opinioni collettive tramite survey e sondaggi (Grossi, 2016, Kindle Location 1025).

Oggi, tuttavia, assume una importanza centrale perché è evidente che i giudizi individuali sui comportamenti da tenere durante il picco dei contagi sono stati fortemente condizionati dalla qualità e dal tipo delle informazioni diffuse innanzi tutto dalle istituzioni. Formalmente, forse memore dell'accusa mossa dal pubblico ministero de L'Aquila e della sentenza di primo grado nel processo alla Commissione grandi rischi di cui si è detto *supra*, il Dipartimento della protezione civile è stato molto attento nel riportare i numeri assoluti del contagio e non a trasformarli percentuali. L'ufficio è stato, inoltre, scrupoloso nell'evidenziare in ogni dichiarazione pubblica che il numero dei contagiati derivava dai risultati dei tamponi eseguiti e dunque mettendo la cittadinanza nelle condizioni (formali) di capire che non venivano comunicate informazioni statisticamente valide.

In Inghilterra alcuni commentatori (Goodhart, 2020) hanno addirittura associato la scelta dell'emotivizzazione dell'emergenza compiuta da alcuni importanti media britannici,

all'accelerazione del processo di "infantilizzazione" (Gottschalk, 2019) del pubblico già innescata dall'ubiqua presenza di *smartphone* e dispositivi elettronici.

the infantile ethos becomes especially seductive in times of social crises and fear. And its favoring of simple, easy and fast betrays natural affinities for certain political solutions over others. And typically not intelligent ones. Democratic policymaking requires debate, demands compromise and involves critical thinking. It entails considering different viewpoints, anticipating the future, and composing thoughtful legislation. What's a fast, easy and simple alternative to this political process? It's not difficult to imagine an infantile society being attracted to authoritarian rule. Unfortunately, our social institutions and technological devices seem to erode hallmarks of maturity: patience, empathy, solidarity, humility and commitment to a project greater than oneself. All are qualities that have traditionally been considered essential for both healthy adulthood and for the proper functioning of democracy (Gottschalk, 2018).

È difficile capire se il complesso meccanismo di comunicazione istituzionale, privata e *fake* – che pure ha giocato un ruolo negativamente rilevante (Bechis, 2020) – abbia influito sulla condizione psicologica delle persone inducendo un senso di resa (Seligman, 1972, pp. 407-412) e facilitando l'accettazione dello stato di fatto (Seligman, 2011) cioè, nella specie, le limitazioni alle libertà civili, o se l'indebolimento delle facoltà critiche, abbia più facilmente condotto al compimento di scelte individuali meno ragionate. Fatto sta che solo in Italia, il 90% della popolazione ha accettato convintamente l'adozione delle misure di contenimento imposte dal governo (European Union Agency for Fundamental Rights, 2020, p. 14), e la paura del contagio giustifica stop alla democrazia e richiesta di un "uomo forte" per il 40% degli italiani (Diamanti, 2020).

La manifestazione più evidente del fenomeno di attenuazione del senso critico rispetto alle politiche pubbliche di sicurezza sanitaria è rappresentata dal modo in cui è maturata la scelta del governo italiano di utilizzare un software da installare sugli *smartphone* dei cittadini per gestire i contagi.

L'esperienza insegna che il distanziamento sociale e l'individuazione dei contagiati sono le misure fondamentali per arginare la diffusione di un virus.

Richiamando la dialettica fra scienza (nell'accezione più lata del termine) e decisione

politica, dal punto di vista della prima non ci sono difficoltà concettuali e operative insormontabili nel suggerire soluzioni che consentano di capire *ex post*, una volta contratto il virus, con chi sia entrata in contatto la vittima, oppure di avvertire in tempo reale se ci si trova vicino a un infetto, oppure ancora di fornire indicazioni per evitare luoghi a rischio contagio o assembramento o di informare le autorità sanitarie (o di pubblica sicurezza?) se qualcuno sta violando la quarantena obbligatoria o il perimetro assegnato, e infine facendo tutto o parte di quanto precede, consentire la condivisione dei dati (solo?) con la ricerca medico-scientifica.

Non è in discussione, dunque, il “se” ma il “come” queste misure devono concretamente essere attuate e se sia desiderabile raggiungere l’obiettivo tramite la tecnologia del controllo che, negli ultimi anni ha raggiunto capacità estremamente invasive e che consentirebbe un *enforcement* individualizzato delle misure di prevenzione e – soprattutto – di repressione.

È una questione estremamente concreta, come dimostra la scelta delle autorità del Minnesota che a seguito dei disordini provocati dalla morte di una persona di colore per mano della polizia dello Stato americano, hanno deciso di utilizzare i dati del sistema di *contact-tracing* per acquisire informazioni sugli autori delle violenze (Stobbe, 2020).

Astrattamente, non dovrebbe generare scandalo il fatto che uno Stato utilizzi, nei limiti del consentito dalle norme, qualsiasi strumento a sua disposizione per prevenire, contenere e sanzionare comportamenti illeciti. Di conseguenza, per contestualizzare il ragionamento nell’ambito del nostro sistema giuridico, se i dati raccolti per il tracciamento dei contagiati risultano utili per finalità di indagine penale, questi dovrebbero essere pacificamente utilizzabili dal pubblico ministero. D’altra parte, pur stabiliti per finalità diverse, gli obblighi di conservazione dei dati di traffico telematico, delle transazioni economiche e delle scritture contabili e delle cartelle cliniche già consentono al pubblico ministero di accedere ad una mole enorme di dati che ci riguardano. Includere anche quelli prodotti dall’applicazione di *contact-tracing*, quindi, non aggiungerebbe granché all’analisi teorica e alla questione pratica.

Ma, *hic Rhodus*, è kelsenianamente sufficiente che la presenza di una norma di copertura sia condizione per consentire allo Stato qualsiasi intrusione non solo e non tanto nella

“privacy”, ma nell’intero nucleo dei diritti e delle libertà fondamentali dell’individuo? O, in altri termini, il fatto che una forma di controllo sia tecnologicamente possibile implica necessariamente che deva essere praticabile – e in modo indiscriminato?

Il tema posto dall’urgenza della sorveglianza sanitaria diventa, dunque, decidere dove posizionarsi fra due estremi: la reclusione imposta con la forza e la possibilità di una “caccia all’uomo” tecnologicamente potenziata non solo per la prevenzione del contagio, e la fiducia cieca nella capacità umana di “fare la cosa giusta” sulla spinta di un dovere morale di solidarietà collettiva e di fiducia – rischiosamente trasformabile in “atto di fede”.

Si tratta, in altri termini, di trovare un bilanciamento fra estensione e profondità del controllo individuale, efficacia delle misure di contenimento, diritti individuali e collettivi, utilizzo delle tecnologie dell’informazione.

Trovare questo punto di equilibrio nella realtà del *policy making*, tuttavia, è estremamente difficile se si affronta il problema dando prevalenza alla componente tecnologica sacrificando quella normativa o – più ancora – i valori comuni che caratterizzano un determinato corpo sociale. Parliamo, in altri termini, del tema della gestione dei cambiamenti strutturali indotti dall’evoluzione tecnologica sulle politiche pubbliche:

tali trasformazioni vanno considerate come il risultato di un insieme più ampio di mutamenti istituzionali, sociali e culturali che coevolvono in maniera interdipendente. La transizione implica un cambiamento e una riconfigurazione delle tecnologie, degli attori e delle istituzioni, attraverso le interazioni, nel corso di lunghi periodi di tempo, fra tre livelli: quello micro delle nicchie, quello meso dei regimi socio-tecnici, e quello macro dei landscapes. I regimi socio-tecnici sono composti da tre dimensioni collegate: i) un insieme di attori (scienziati, users, policy makers, imprese) e gruppi sociali, che interagiscono e formano reti mutualmente dipendenti; ii) un insieme di prescrizioni formali, regole normative e cognitive che strutturano il comportamento degli attori; e iii) gli elementi materiali e tecnici (gli artefatti e le infrastrutture tecnologiche). L’allineamento fra questi elementi eterogenei produce quello che Hughes (1994) definisce *technological momentum* (Prontera, 2013, p. 296).

#### 4. Tecnologia e *public policy* in Cina, Corea del Sud e Taiwan

Esula dal perimetro di questo lavoro un'analisi dettagliata delle singole soluzioni tecnologiche adottate da ciascun Paese del continente asiatico, ma è interessante classificare gli approcci al *policy by data* adottati in funzione del sistema giuridico-politico di Cina, Corea del Sud e Taiwan perché ciascuno offre una risposta (parzialmente ma significativamente) diversa alla stessa domanda di sicurezza e prevenzione, le cui conseguenze verranno poi analizzate nelle conclusioni di questo lavoro.

##### 4.1 La Repubblica Popolare Cinese

In termini strettamente fattuali, le misure adottate in Cina non sono diverse da quelle di altri Paesi in Asia e nel resto del mondo: quarantena, individuazione dei contagiati, distanziamento sociale, triage al momento dell'accesso in un luogo pubblico, rilevazione della temperatura, sanificazione. Quello che fa la differenza è, invece, il modo in cui questi obiettivi sono stati raggiunti, e il dato peculiare rilevante diventa, dunque, la fortissima integrazione fra misure di controllo fisico, tecnologia della sorveglianza (The Economist, 2020) e controllo dell'opinione pubblica.

Da questo punto di vista è certamente possibile affermare che la struttura centralizzata della gestione della sicurezza nelle sue varie articolazioni (pubblica e nazionale) e la presenza di un sistema diffuso di controllo hanno favorito una reazione rapida ed efficiente che ha portato, per esempio, ad eseguire circa 7 milioni di test in dodici giorni per prevenire un ritorno del contagio nella città di Wuhan (Kumar, 2020).

L'analisi che segue è basata principalmente su quanto accaduto nella città di Nanjing (otto milioni e mezzo di abitanti), così come documentato nel *reportage* non di un occidentale, ma da un *videomaker* giapponese. La scelta è stata motivata proprio dalla nazionalità del regista, scevro dall'ossessione occidentale di «estendere a tutto il mondo, ma soprattutto ai cinesi, con le buone o con la forza, il proprio modello dei diritti

umani/fondamentali, e, insieme ad essi, le proprie scale di valori» (Di Plinio, 2011, p. 179). Una premessa, quest'ultima, necessaria per cercare di evitare una lettura metodologicamente non rigorosa delle scelte operate in tradizioni giuridiche alle quali mal si adattano i criteri della *Western Legal Tradition*.

Il dato che emerge con maggiore evidenza è la gestione unificata e coordinata della crisi, realizzata senza soluzione di continuità fra misure fisiche di contenimento e quarantena, controlli di polizia sanitaria estesi anche a soggetti privati, espansione della capacità di raccolta, elaborazione e riutilizzo di enormi quantità di dati, controllo dell'opinione pubblica sia tramite il continuo *memento* sugli obblighi da rispettare, sia in termini di prevenzione anche dura del dissenso, applicazione di pene molto dure, fino a quella capitale.

L'informazione sulle regole da seguire è martellante: a fianco di metodi più tradizionali come enormi e onnipresenti cartelloni per ricordare di rimanere in casa, non organizzare feste e non visitare parenti, gli stessi messaggi sono stati veicolati tramite droni, megaschermi e messaggi diffusi tramite gli altoparlanti nelle stazioni e nelle metropolitane. Ai controlli di polizia sul rispetto della quarantena, sono affiancati i comitati politici di quartiere che operano come vigilanza sanitaria, e i *compound manager* – una sorta di super amministratore di condominio – ai quali è attribuita la responsabilità di vigilare che gli occupanti ricevano ciò di cui hanno bisogno, ma anche di chiamare l'autorità in caso di violazioni. Analoga responsabilizzazione individuale sul rispetto degli obblighi di distanziamento sociale nei luoghi e mezzi pubblici, sanificazione e rilevazione della temperatura continua ad ogni accesso in luoghi chiusi ha riguardato i gestori degli esercizi e gli autisti. Il *contact tracing* è realizzato anche consentendo l'accesso a locali solo dopo avere scansionato un *QRCode* che rileva la presenza in uno specifico luogo, avere dichiarato le proprie generalità, il fatto di non essere stato, negli ultimi quattordici giorni, nella provincia di Hubei e annotato la propria temperatura corporea. Il sistema *Health Code*, parallelamente, assegna a ciascuna persona un codice colore autoesplicativo (verde, giallo, rosso) che varia in funzione dei luoghi attraversati: il passaggio (automatico) da verde a giallo implica la sottoposizione automatica della quarantena. In metropolitana, mentre gli altoparlanti ripetono ossessivamente le regole da rispettare, prima di entrare nel vagone

viene rilevata la temperatura corporea ed è obbligatorio fare il check-in tramite WeChat (il sistema di messaggistica usato in Cina) in modo da dichiarare la propria presenza associata al proprio numero di cellulare, linea di trasporto, carrozza e ora di ingresso. Un'altra applicazione indica (anonimamente) i luoghi nei quali sono stati rilevati contagi, dove sono stati installati dei muri artificiali per impedire che le persone potessero uscire di casa liberamente, ma fossero costrette a passare da specifici varchi (Takeuchi, 2020).

#### *4.2 Corea del Sud*

Anche la strategia adottata dalla Corea del Sud è stata basata su un approccio integrato e sinergico ma, a differenza di quanto avvenuto non solo in Cina ma anche nei Paesi occidentali, le autorità pubbliche hanno coinvolto i componenti della comunità accademica per *parlare* con le persone e *chiarire* i loro dubbi sugli aspetti scientifici della vicenda (Fendos, 2020). Un altro elemento fondamentale della risposta sudcoreana è stata la definizione di procedure operative standardizzate per la reazione rapida ai contagi. Imparando dagli errori commessi nella gestione della MERS (Kim, 2020) la Corea ha innalzato i livelli di allerta sanitaria sin dalle prime avvisaglie della presenza del coronavirus e, una volta rilevata la sua diffusione, ha attivato innanzi tutto un massiccio programma di *screening* per individuare il maggior numero di contagiati possibile. A questo proposito, è interessante rilevare che fra i fattori che hanno ritardato l'attivazione del sistema di emergenza sanitaria, agevolando l'iniziale notevole diffusione del Coronavirus sono state individuate le pratiche religiose di gruppo di una setta cristiana, la Chiesa di Shincheonji, e l'iniziale opposizione della setta a rendere pubblici i nomi degli adepti perché si sottoponevano ai test (Wong, 2020). In altri termini, l'effetto sinergico dell'esercizio di due diritti pienamente riconosciuti dall'ordinamento sudcoreano, quello alla libertà religiosa e quello alla riservatezza, ha impedito di intervenire tempestivamente su un grosso focolaio di infezione.

La scelta di eseguire da subito il maggior numero possibile di test, invece di aspettare che

i pazienti si presentassero in ospedale con sintomi oramai gravi, da un lato ha lasciato percepire un livello di gravità del contagio superiore a quello di Paesi che, invece, ne avevano eseguiti pochi o nessuno (con ciò evidenziando ancora una volta il problema dell'attendibilità dei dati di cui *supra*). In realtà, al contrario, si è dimostrata una soluzione efficiente per individuare con estrema precisione altri potenziali infettati grazie all'integrazione fra i dati disponibili nei vari sistemi informatici pubblici e privati, dalle transazioni delle carte di credito alla geolocalizzazione del telefono cellulare, dall'analisi delle registrazioni delle telecamere di videosorveglianza a quelli dei mezzi di trasporto pubblico (McCarry, 2020). In sostanza, ed è una questione centrale, il *contact-tracing* non è realizzato tramite accumulazione e centralizzazione nelle mani dello Stato dei dati relativi a una persona, ma tramite l'*integrazione* di questi dati che rimangono nella disponibilità dei singoli soggetti che li detengono. Le inevitabili preoccupazioni per la tutela della "privacy" e le difficoltà derivanti da una normativa estremamente rigorosa sono state superate per via dell'emergenza, ma questo non ha impedito una riflessione sul modo di gestire i dati dei contagiati e dei limiti alla diffusione pubblica di informazioni sui malati che possono consentire la loro deanonimizzazione:

On March 9, Korea's National Human Rights Commission issued a recommendation with a view to ameliorating privacy concerns, suggesting that the revelation of exceedingly detailed information was unwarranted. In response, on March 14, the KCDC issued a guideline to municipal and local governments, limiting the scope and detail of the information to be disclosed (Park, Choi e Ko, 2020).

A differenza di quanto accaduto in Cina, l'utilizzo di un sistema di controllo tanto pervasivo e impressionante quanto a capacità, di identificazione e l'applicazione delle altre misure di controllo anche tecnologiche, non sono state imposte dallo Stato con la forza né subite passivamente dalla cittadinanza: «South Korea is a democracy which respects and ensures the individual freedom of the people as much as possible, so we relied on people's voluntary cooperation based on their trust in public anti-epidemic authorities» (Campbell, 2020).

Come nota a margine per lo sviluppo delle conclusioni, è infine il caso di evidenziare la

enorme (e l'aggettivo non rende giustizia) potenza di calcolo e di risorse informatiche necessarie per ottenere in tempi rapidi le informazioni sugli spostamenti e i contatti di ogni singolo contagiato. Un risultato del genere è stato possibile solo ed esclusivamente per via di una precisa scelta politica sul ruolo della scienza e della tecnologia che ha reso possibile la creazione di infrastrutture avanzate e un loro utilizzo diffuso nella vita quotidiana. Da un lato, dunque, si è creata nella popolazione un'abitudine generalizzata alla loro presenza e, dall'altro, sono stati creati i presupposti per utilizzare queste tecnologie in emergenza senza necessità di investimenti o poteri speciali. E in questo contesto non va sottovalutato il ruolo della trasparenza dei poteri pubblici nella comunicazione al cittadino delle informazioni relative al coronavirus, alle iniziative per garantire la sicurezza e alle condizioni reali del Paese. Non solo la Corea del Sud si è prodotta in un enorme sforzo tecnologico di alto livello, ma si è relazionata alla pari con la comunità tecnologica privata rilasciando pubblicamente le API (Application Programming Interface) che hanno reso possibile la creazione di strumenti utili anche per questioni apparentemente meno urgenti come dei software per il reperimento di mascherine. Questo ha reso possibile l'accettazione consapevole di forme temporanee di tecnocollaborazione senza la paura che potessero trasformarsi in una condizione permanente.

#### *4.3 Taiwan*

Spicca inoltre, contraddicendo le letture che sostengono la monoliticità degli *Asian Values*, il modo in cui anche Taiwan – in modo non dissimile dalla Corea del Sud – ha bilanciato democrazia, tecnologia e sicurezza riuscendo addirittura a prevenire la diffusione del coronavirus invece di subirla.

Anche nel caso di Taiwan è l'esperienza drammatica del contatto con un altro virus – quello della SARS, nel 2003 – ad avere contribuito alla creazione di un sistema di procedure da attivare in caso di emergenza. Appena ricevuta la notizia dell'esistenza del virus da parte dell'Organizzazione Mondiale della Sanità, in meno di un mese il governo ha attivato

un'unità per la gestione delle emergenze e ha messo in condivisione i database del sistema sanitario nazionale e di quello dell'immigrazione mettendolo a disposizione di tutti i soggetti coinvolti nell'identificazione di persone contagiate.

Taiwan leveraged its national health insurance database and integrated it with its immigration and customs database to begin the creation of big data for analytics; it generated real-time alerts during a clinical visit based on travel history and clinical symptoms to aid case identification. It also used new technology, including QR code scanning and online reporting of travel history and health symptoms to classify travelers' infectious risks based on flight origin and travel history in the past 14 days. Persons with low risk (no travel to level 3 alert areas) were sent a health declaration border pass via SMS (short message service) messaging to their phones for faster immigration clearance; those with higher risk (recent travel to level 3 alert areas) were quarantined at home and tracked through their mobile phone to ensure that they remained at home during the incubation period (Wang, Ng e Brook, 2020).

Ad analizzare il modo in cui sono utilizzati data-base, l'uso di cellulari forniti dallo Stato per il monitoraggio della quarantena e le altre tecnologie descritte nell'articolo citato verrebbe da pensare che non ci sia alcuna sostanziale differenza con le misure adottate dalla Cina. In termini fattuali questo è probabilmente corretto, ma anche nel caso di Taiwan, come in quello sudcoreano, è il presupposto politico-giuridico ad essere profondamente diverso. La creazione di un sistema integrato di raccolta, analisi e condivisione di informazioni sulla cittadinanza e l'adozione di sistemi di tecnocontrollo sono regolate da norme stringenti e sono state ispirate a criteri di trasparenza e democrazia che fanno di Taiwan un caso di studio del rapporto fra tecnologia e *public policy* della sicurezza.

È certamente vero che il successo di Taiwan nel contrasto al coronavirus

can be explained by the unique historical contingencies that have shaped this young nation. Taiwan's self-confidence and collective solidarity trace back to its triumphal self-liberation from its own authoritarian past, its ability to thrive in the shadow of a massive, hostile neighbor that refuses to recognize its right to chart its own path, and its track record of learning from existential threats (Leonard, 2020).

È altrettanto vero tuttavia che, come la Corea del Sud, questo è stato possibile perché

Taiwan si è dimostrata capace di applicare efficacemente, e in un momento di crisi, una *agile governance* che è riuscita a gettare un ponte fra società civile e poteri dello Stato.

The catalyst in forming such trust among government actors, private sector, civil society organizations, and the general public was rooted in the equitable recognition in utilizing citizen data for the greater good. Although far from perfect, such a multistakeholder consensus was supported by legal and regulatory frameworks that ensure individual liberties are not compromised, under transparent and strict oversight (Manantan, 2020).

Anche nel caso di Taiwan, infine, va ricordato che le tecnologie dell'informazione hanno potuto rivestire un ruolo fondamentale nel contenimento del contagio essenzialmente perché sono un elemento strutturale delle scelte politiche, economiche e industriali dell'isola. Non a caso è lì che sono nati – e continuano a rimanere – giganti mondiali dell'elettronica, dell'informatica e della tecnologia di frontiera.

## **5. L'approccio italiano al tecnocontrollo della pandemia**

Se paragoniamo la risposta tecnologica italiana al problema coronavirus a quelle estremo-orientali di cui si è appena detto, non può non venire in mente il *Locomotive Act* emanato nel 1865 dal Parlamento del Regno Unito. Imponeva quella legge, voluta per proteggere cittadini e “rurali” dall'automobile a vapore – nuova diavoleria modernista – che qualsiasi veicolo semovente (e dunque, non trainato da forza animale) dovesse essere preceduto di sessanta yarde da una persona che «shall carry a red flag constantly displayed, and shall warn the riders and drivers of horses of the approach of such locomotives, and shall signal the driver thereof when it shall be necessary to stop». Oggi, se per strada vedessimo qualcuno agitare una bandiera ci aspetteremmo piuttosto di essere sul set di qualche film hollywoodiano che racconta “storie di velocità” e non certo di doverci mettere al sicuro per l'arrivo di un mostro meccanico.

Applicando la metafora del *Locomotive Act* alle condizioni attuali dell'uso delle

tecnologie dell'informazione e della sovranità digitale in Italia, dobbiamo constatare che siamo ancora al punto dell'obbligo dello sbandieratore che ci avvisa dell'arrivo del "mostro d'acciaio" mentre altrove sono già vecchie le automobili a guida autonoma di livello 5.

Fuor di metafora, possiamo dire che l'Italia non è stata in grado di trarre alcuna utilità dalla propria infrastruttura tecnologica, avendo piuttosto optato per soluzioni "muscolari" a qualsiasi livello e quando ha cercato di usare le tecnologie dell'informazione lo ha fatto realizzando tardi e male un'applicazione – "Immuni" – definita di *contact-tracing* ma che in realtà è poco più di uno strumento per comunicare *a posteriori*, a chi ha scelto di usarla, il probabile contatto con una persona contagiata e nulla più, nemmeno un minimo di geolocalizzazione.

Esemplare a questo proposito, il dibattito sulla possibilità di ricostruire *a posteriori* i movimenti di un contagiato. In Corea del Sud, come detto, l'obiettivo è stato raggiunto integrando dati provenienti da più fonti, compresi i gestori telefonici. In Italia il tema dell'integrazione dei database pubblici e privati non è stato nemmeno preso in considerazione, sprecando tempo nell'interrogarsi manicheisticamente se fosse meglio usare il bluetooth o i dati generati dalla rete di telefonia mobile per tracciare le persone.

Quali siano le motivazioni di questa scelta di *public policy* tecnologica non è dato saperlo perché non sono state rese pubbliche, il che già marca (negativamente) un punto importante nella gradazione del livello di oscurità del rapporto fra potere esecutivo e cittadino. Non perché – in nome di una malintesa interpretazione del concetto di democrazia diretta – tutti devano essere partecipi dei processi decisionali, ma perché ognuno deve poter esercitare il proprio diritto-dovere di controllore dei pubblici poteri.

Dalle dichiarazioni pubbliche rilasciate dal Ministero dell'innovazione si deduce che la tutela della "privacy" ha prevalso sia sulle necessità di gestire in modo razionale l'attività di individuazione dei potenziali contagiati, sia sul dovere, imposto dal Regolamento generale sulla protezione dei dati personali, di tutelare libertà e diritti fondamentali dell'individuo e dunque della vita prima e più di ogni altra.

È un pregiudizio antitecnologico che affonda le sue radici in quella linea di pensiero che considera la tecnologia intrinsecamente pericolosa e che, sulla base di un principio di

precauzione, previene e paralizza (GPDP, 2004) invece di consentire, ma verificando e punendo severamente gli abusi.

Oltre a impedire l'applicazione di soluzioni tecnologiche di provata utilità, questa paralisi culturale si è manifestata nell'incapacità di risolvere in modo alternativo il problema del controllo delle persone trovate al di fuori del proprio domicilio. È stato imposto di fatto – ma non di diritto, peraltro – l'uso della carta per “autocertificare” (*sic!*) invece di predisporre, per esempio, un sistema di registrazione preventiva su una piattaforma del Ministero degli interni o quantomeno la possibilità di inserire i dati del trasferimento sul proprio telefono, magari insieme al tracciamento del percorso da esibire a richiesta. Nulla che altrove non sia stato fatto, peraltro.

Inoltre, se escludiamo l'uso folkloristico dei droni da parte di qualche pattuglia di polizia locale, agli strumenti di controllo tecnologico sono stati preferiti metodi tanto “muscolari” quanto meno efficaci, basati sui tradizionali controlli di polizia e su altrettanto folkloristiche applicazioni dei poteri di sicurezza urbana ex art. 54 Testo unico degli enti locali in base ai quali dei sindaci hanno ritenuto di poter girare per la città intimando ai cittadini di tornare ai propri domicili.

Infine, anche dall'analisi del modo in cui le istituzioni hanno gestito la comunicazione verso i cittadini emergono molte perplessità.

A parte conferenze stampa, interviste e qualche spot pubblicitario, l'informazione sul coronavirus è stata essenzialmente monopolizzata (e spettacolarizzata) dai media i quali hanno rivendicato per loro stessi la qualifica di “informazione professionale” come baluardo contro le *fake news*. E il contrasto alla diffusione di informazioni false o comunque pericolose per la salute pubblica è stato affidato a un timido quanto pericolosissimo provvedimento dell'Autorità per le garanzie nelle comunicazioni.

Con la delibera 129-20 CONS del 18 marzo 2020, infatti, l'Autorità ha “invitato” le emittenti radiotelevisive a dare voce solo a medici e scienziati esperti per fornire informazioni attendibili e i fornitori di piattaforme di condivisione video ad adottare

ogni più idonea misura volta a contrastare la diffusione in rete, e in particolare sui social media, di

informazioni relative al coronavirus non corrette o comunque diffuse da fonti non scientificamente accreditate. Le predette misure devono prevedere anche sistemi efficaci di individuazione e segnalazione degli illeciti e dei loro responsabili (AGCOM, 2020).

Senza voler entrare nel complesso dibattito sul ruolo, sui poteri e sull'indipendenza delle autorità indipendenti, questo “invito” (atto palesemente *extra ordinem*) rappresenta una rilevante e grave lesione del diritto alla libertà di espressione. È grave e pericolosa la disapplicazione di fatto (perché di diritto l'Autorità non avrebbe il potere) del divieto generale di sorveglianza degli utenti stabilito dalla direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno e, in Italia, dal decreto legislativo 9 aprile 2003, n. 70 (*Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno*), come è grave e pericoloso avere creato il presupposto per superare (pur non avendo il potere di farlo) i divieti comunitari e nazionali di affidare a soggetti privati la gestione di sorveglianza e censura.

A questo approccio culturalmente ostile allo sviluppo tecnologico si è associata l'incapacità del legislatore di fatto e di quello di diritto, nel progettare correttamente il sistema delle sanzioni per la violazione delle misure di contenimento che ha provocato una silenziosa ma grave applicazione del diritto, o meglio, del potere, di prevenzione.

In prima battuta, infatti, sono stati emanati obblighi ma senza specifiche punizioni per i contravventori, se non una inutile (perché superflua) specificazione sull'applicabilità dell'articolo 650 del Codice penale e una fantasiosa applicabilità, per via interpretativa, dell'articolo 495 del Codice stesso. Tutto ciò trascurando la preesistenza di norme specifiche come l'articolo 260 del Testo unico delle leggi sanitarie. Poi la punibilità per la violazione di questi obblighi è stata ricondotta – con una operazione discutibile sotto il profilo della tecnica penalistica – all'interno di una sanzione amministrativa integrata con il richiamo ad altre norme penali. Ma prima e dopo, quale che fosse la sanzione prevista, nessun operatore di polizia aveva il potere di imporre alcunché ai contravventori: non l'arresto in flagranza,

non l'allontamento coattivo, e nemmeno qualsiasi altro obbligo di fare. Di conseguenza, a fronte di una violazione, l'unica azione possibile sarebbe stata quella di elevare il verbale di contestazione. Al contrario, complice ancora una volta la scarsa tecnicità dei legislatori, l'applicazione delle norme si è tradotta nel diritto del caso singolo, deciso sul momento dal singolo operatore di polizia come evidenzia il caso paradigmatico dell'elicottero dell'Arma dei Carabinieri che, a Mondello, in Sicilia, scaccia un bagnante dalla spiaggia usando la tempesta di sabbia provocata dalla rotazione delle pale (Ferro, 2020). In altre parole, per evitare il rischio di uno Stato di polizia, si è creato uno Stato di poliziotti.

È abbastanza paradossale che per paura di non meglio identificati “pericoli” per i diritti fondamentali rappresentati dalle tecnologie dell'informazione e sulla base dei quali è stata aprioristicamente rifiutata la possibilità di gestire più efficacemente il contagio abbiamo accettato senza battere ciglio una concreta, effettiva e subdola limitazione degli stessi diritti realizzata da norme confuse ed ellittiche e dall'elevazione a rango di fonte del diritto di “FAQ”, “inviti” e persino interviste televisive sul significato giuridico da attribuire alle parole.

Questa condizione di arretratezza è, evidentemente, frutto di un complesso intreccio di ritardi culturali e di assenza di visione per il Paese e costringe l'elaborazione giuridica pubblicistica su questi temi in un limbo, per la difficoltà di confrontarsi con casi concreti.

Mentre, dunque, ci si continua legittimamente ad interrogare sugli scenari futuri popolati da applicazioni distopiche della tecnologia, indagando il destino degli spazi di libertà individuale in un mondo in cui il potere (pubblico o privato, è da vedere) ha contemporaneamente capacità di controllo e di manipolazione del consenso, si dedica molto meno spazio al tecnocontrollo del quale lo Stato è vittima e che, grazie allo stato emergenziale, è diventato ancora più stringente.

Giustizia e università sono i due casi più eclatanti fatti emergere dall'emergenza coronavirus. La celebrazione delle udienze giudiziarie e lo svolgimento di lezioni ed esami dipendono dall'uso di piattaforme di comunicazione in mano ad aziende extracomunitarie che, grazie alla oramai proverbiale arretratezza tecnologica delle istituzioni, hanno di fatto preso il controllo di due settori critici per la sopravvivenza del Paese ed è realistico pensare

che, passata l'emergenza, non allenteranno la morsa.

Questo è l'ultimo esempio di “schiavitù elettronica” – la dipendenza dello Stato da tecnologie straniere – un tema esploso in tutta la sua gravità con la “questione 5G”<sup>6</sup> ma in realtà è in discussione (trascurato) da almeno vent'anni.

Già nel 1999, al Forum per la società dell'informazione organizzato dalla Presidenza del Consiglio dei Ministri, venne posto il tema dell'indispensabilità dell'uso di sistemi aperti, compatibili e trasparenti in tutti i servizi pubblici (ALCEI, 1999). Benché, tuttavia, nel corso del tempo alcune di queste istanze si siano fatte strada,<sup>7</sup> ancora oggi la pubblica amministrazione e componenti importanti delle infrastrutture critiche del Paese rimangono saldamente nelle mani di tecnologie e aziende straniere, per di più extra-comunitarie.

Non è questa la sede per analizzare le implicazioni geopolitiche della dipendenza tecnologica da un altro Stato – questione peraltro nota da sempre agli esperti di relazioni internazionali – ma non si può nemmeno evitare di accorgersi che le necessità emergenziali, acuite dai ritardi storici di cui si è detto, hanno accelerato il processo di perdita di sovranità dello Stato sui dati e sulle tecnologie dell'informazione (Monti, 2020).

Dal punto di vista del *policing* della sicurezza questa perdita di sovranità si è manifestata innanzi tutto a livello formale, con il riconoscimento del ruolo del settore privato nella cogestione della sicurezza nazionale e dell'attività giudiziaria. Non si tratta solo del “mero” dovere di collaborazione degli operatori di telecomunicazioni sancito con l'autorità giudiziaria e i servizi per la sicurezza della Repubblica, ma anche presa d'atto della inevitabile ingerenza straniera nella gestione delle infrastrutture rilevanti per la sicurezza nazionale che la legge 133/09 sul perimetro cibernetico nazionale ha cercato (malamente) di contrastare. Prima ancora, nel 2008, la ratifica<sup>8</sup> della Convenzione di Budapest sul crimine

---

<sup>6</sup> Sul finire del 2019, a fronte del rischio che tecnologie cinesi potessero monopolizzare la nascente rete italiana di quinta generazione mettendo a rischio la sicurezza nazionale, il governo fece ricorso alla decretazione d'urgenza (poi ratificata dal Parlamento con la legge 18 novembre 2019, n. 133) per creare un complesso sistema di verifica preventiva degli apparati da utilizzare nelle infrastrutture critiche e nei servizi essenziali del Paese.

<sup>7</sup> Vedi, per esempio, la tematica del riuso del software nella pubblica amministrazione l'uso di formati di file standard come XML su cui si basa, per esempio, il processo telematico o, più di recente, l'interpretazione evolutiva dell'articolo 20 del decreto legislativo 7 marzo 2005, n.82 (*Codice dell'amministrazione digitale*) che consente la sottoscrizione a distanza dei contratti utilizzando non più la sola firma digitale qualificata ma anche il Sistema pubblico per l'identità digitale.

<sup>8</sup> Legge 18 marzo 2008, n. 48 (*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*).

informatico<sup>9</sup> aveva già affidato a soggetti privati il compito di preservare gli originali informatici di quanto oggetto di sequestro (Lupària, 2009)<sup>10</sup>. E ancora prima, il recepimento della direttiva 24/2006<sup>11</sup> – annullata nel 2014 dalla Corte di giustizia UE<sup>12</sup> ma i cui recepimenti nazionali sono ancora in vigore – istituisce l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare obbligatoriamente i dati di traffico telematico degli utenti.

A questa condizione di forte dipendenza tecnologica, della quale questi esempi sono solo la punta dell'iceberg, corrisponde evidentemente una ridotta autonomia decisionale sia in termini di scelte politiche, sia in termini di concreta gestione dell'ordine e della sicurezza pubblica e dell'emergenza sanitaria, nel caso specifico.

Dall'altro lato questa debolezza strutturale dei processi decisionali insieme all'incremento improvviso e inarrestabile dell'uso delle tecnologie dell'informazione rendono la sicurezza interna più vulnerabile non solo ad azioni criminali, ma anche ad azioni di disobbedienza organizzata che si avvantaggiano della asimmetria del conflitto sociale mediato tramite la tecnologia.

## 6. Conclusioni

Fino allo scatenarsi della pandemia, il dibattito fra potere-dovere dello Stato di garantire ordine e sicurezza pubblica tramite il ricorso alla tecnologia è stato essenzialmente basato su

<sup>9</sup> Consiglio d'Europa, *Convenzione sul crimine informatico firmata a Budapest il 23 novembre 2001*.

<sup>10</sup> L'articolo 254-bis del Codice di procedura penale, inserito appunto dall'articolo 8 della legge 48/2008 prevede che i fornitori di servizi di comunicazione elettronica e postale conservino e proteggano gli originali dei dati informatici sequestrati dall'autorità giudiziaria, decidendo in autonomia quali misure possano garantire, in concreto, la disponibilità e l'integrità dei dati in questione. La ricaduta processuale, in termini di garanzie per l'imputato, della necessità o meno di rispettare *best practice* nella modalità di acquisizione dei dati informatici nel processo penale è un tema lungamente dibattuto in dottrina e solo parzialmente in giurisprudenza con la sentenza del caso Kercher, che si pronunciò sul valore probatorio delle analisi genetiche basate su campioni raccolti in modo non rigoroso (Cass. pen., sez. V, sent. 25 marzo 2015, n. 1105) esprimendo un principio di diritto applicabile analogicamente anche alla prova informatica.

<sup>11</sup> Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

<sup>12</sup> Sentenza della Corte (Grande Sezione) dell'8 aprile 2014 Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a. <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:62012CJ0293> (26/04/2020).

ipotesi virtuali e contrapposizioni “binarie” fra poteri e diritti senza che ci fossero banchi di prova in grado di fornire riscontri sperimentali. L’astrattezza di questo dibattito, radicalizzato fra posizioni distopiche e adesioni entusiastiche (oltre che ingenuie) all’idea delle “magnifiche sorti e tecnologicamente progressive” ha generato una forte inerzia nella definizione di una idea di *public policy* tecnologica coordinata.

Lungi dall’essere le nuove frontiere della democrazia – e di quella tecnologica, in particolare – la Corea del Sud e Taiwan hanno avuto però il merito di creare uno spazio di riflessione più ampio e da approfondire sul ruolo di scienza e tecnologia, rispetto all’asfittico dibattito europeo, sclerotizzato sul dualismo “libertà-sicurezza” o su quello che contrappone “privacy” a “controllo globale” e che vede nella Cina l’unico interlocutore, oltre il quale ci sono i proverbiali leoni.

Da un lato, infatti, nel modello cinese di gestione del contagio, la scienza ha avuto un ruolo marginale dal punto di vista del dibattito pubblico. Una volta definita la strategia, si è trattato “semplicemente” di azionare l’apparato organizzativo e tecnologico di controllo sociale già ampiamente rodato. Le (proporzionalmente poche) controversie hanno dunque riguardato piuttosto quello che da alcuni è stato percepito come un uso strumentale dell’emergenza sanitaria per espandere portata, estensione e durata delle misure di controllo per ragioni di prevenzione (Kuo, 2020; Ko, 2020) sicuramente agevolate dalla proprietà pubblica dei dati, o comunque della possibilità per lo Stato di disporre *uti dominus*. La differenza sostanziale nell’utilizzo dei sistemi di tecnocollaborazione fra i Paesi appartenenti alla *Western Legal Tradition* (nei quali pure situazioni analoghe sono frequentissime) e la Repubblica Popolare Cinese, dunque, è che quest’ultima ha la proprietà – o comunque la disponibilità centralizzata – non solo delle infrastrutture, ma anche delle piattaforme e dei dati.

Dall’altro, e a riprova della scarsa monoliticità – e forse dell’inesistenza o della scomparsa – del concetto di *Asian Values*, due Paesi condividono un approccio profondamente diverso, certamente ispirato ai *Western Values* ma integrato con costumi e tradizioni culturali che non sono state obliterate dal contatto con il principio del *rule of law*. Dunque, le scelte del governo sono state oggetto di un dibattito pubblico, sono state

comunicate in modo efficace e sono state attuate certamente con delle scorciatoie ma senza generare allarmi per la tenuta del sistema democratico (aggettivo utilizzato con la piena consapevolezza della non automatica e immediata traslabilità intercontinentale del termine). In particolare, il contrasto alla diffusione di notizie prive di fondamento o palesemente falso è stato gestito con una contro-comunicazione istituzionale e basata, ancora una volta sull'autorevolezza, invece che sull'applicazione "muscolare" delle prerogative statali.

In estrema sintesi, dunque, le esperienze citate dimostrano che certamente il tecnocollaboro è uno strumento estremamente funzionale alla gestione centralizzata della sicurezza (intesa innanzi tutto come sicurezza dello Stato dai cittadini). Ma dimostrano pure che non necessariamente un controllo tecnologico pubblico esteso ed invasivo si traduce automaticamente in limitazioni irreversibili dei diritti individuali. Tuttavia, fra le tante contraddizioni fatte esplodere ad ogni livello dalla pandemia COVID-19 c'è l'improvvisa consapevolezza che, pur volendo, in Italia non sarebbe stata possibile una soluzione tecnologica di tipo taiwanese o sudcoreano. E non, come accennato *supra*, per differenze culturali, politiche o giuridiche ma – banalmente – per il diverso approccio all'integrazione della tecnologia nei processi (in senso aziendalistico) dell'amministrazione che troppo spesso ci costringe ancora ad usare i muscoli invece del cervello.

Sotto un altro e non meno rilevante profilo, queste esperienze consentono una riflessione (certamente da approfondire) sul tema della sovranità nazionale sull'identità digitale e sui dati in Italia.

Centralizzare l'identità digitale ha certamente il merito di impedire alle grandi piattaforme extracomunitarie di accumulare informazioni di qualsiasi tipo sui cittadini tramite, per esempio, la diffusissima tendenza ad utilizzare gli account social come credenziali di accesso anche a servizi di altro tipo. Dall'altro lato, come dimostra l'esperienza cinese, la migrazione verso la scelta di usare le piattaforme come punto di accesso per fruire di servizi altrimenti non utilizzabili diventa uno strumento di censura e sanzione. Sono stati infatti documentati casi di arresto di dissidenti che riportavano fatti non graditi e con minacce di cancellazione degli account sui social network senza i quali – vista il grado elevato di digitalizzazione dei servizi di qualsiasi tipo – è impossibile fare qualsiasi

cosa (Le Belzic, 2020).

Parallelamente, l'emergenza coronavirus ha evidenziato la fondamentale importanza del controllo pubblico sui dati o, meglio, dell'esistenza o meno di un limite a questo controllo.

Sarebbe necessario riflettere sull'accettabilità di una condizione per la quale l'accesso a dati fondamentali come quelli necessari al *contact-tracing* (ma anche a indagini giudiziarie) sia rimesso alla benevolenza di multinazionali extracomunitarie che decidono autonomamente se, a chi, come e soprattutto (fino a) quando questi dati devono essere messi a disposizione. Così come ci si dovrebbe chiedere se sia un modello sostenibile, quantomeno dal punto di vista della sovranità statale, utilizzare formati di *file*, applicazioni software e hardware sottratti al controllo pubblico per far funzionare la pubblica amministrazione. E si dovrebbe considerare, visto che sempre di più i dati condizionano l'informazione, quale approccio regolamentare si dovrebbe avere sui dati perché chi controlla i dati controlla l'informazione.

Da qui, dunque, le domande decisive: possiamo permetterci, o dovremmo quantomeno auspicare, un controllo pubblico sull'identità digitale e sui dati? E rispondere positivamente non potrebbe essere una soluzione peggiore del male?

Ancora una volta, se le risposte devono arrivare dal contrasto astratto di posizioni ideologiche e di slogan, ben difficilmente potranno avere un qualche senso concreto. Viceversa, se una lezione si può trarre dalle esperienze sudcoreana e taiwanese è che invece di paralizzare l'attività del decisore con affermazioni apodittiche e aprioristiche, la dicotomia sorveglianza-libertà possa essere superata con uno sforzo di trasparenza che consenta un effettivo controllo diffuso sull'utilizzo delle tecnologie dell'informazione da parte dei poteri pubblici. Il punto, dunque, non è argomentare analogicamente dall'articolo 42 della Costituzione per affermare la natura pubblica o privata dell'informazione, ma stabilire il principio che dati e informazioni dovrebbero essere gestiti in modo che, ove la necessità si manifestasse, potrebbero essere immediatamente messi a sistema. Con ciò bilanciando la necessità di fare "ciò che serve" per gestire un'emergenza, rispettando nel contempo un principio di gradualità nella (pur inevitabile, a certe condizioni) limitazione delle libertà fondamentali.

Ci sono tre limiti ad una scelta del genere.

Il primo è puramente politico: è necessario uscire dal guado dell'indecisione e imprimere un'accelerazione forte alla modernizzazione tecnologica del Paese sulla base di scelte chiare (digitalizzazione, interoperabilità, interconnessione).

Il secondo è culturale prima ancora che politico o giuridico: fino a quando non verrà (ri)costruito e onorato un patto di trasparenza fra Stato e cittadino, la atavica e reciproca diffidenza del e verso il potere difficilmente consentirà di fare passi avanti.

Infine, senza l'abitudine sociale alla presenza di sistemi del genere, introdotti progressivamente e gestiti con democrazia e trasparenza (*supra*), sarebbe estremamente difficile ottenere un adeguato grado di accettabilità sociale di un sistema tecnologico tanto imponente.

## **Bibliografia**

- ALCEI - Associazione per la Libertà nella Comunicazione Elettronica Interattiva (1999). *È compito delle istituzioni liberarci dalla schiavitù elettronica*. Testo disponibile all'indirizzo web: <http://www.interlex.it/pa/alcei12.htm> (26/04/2020).
- Aronson J. (2007). *Genetic Witness: Science, Law, and Controversy in the Making of DNA Profiling*. New Brunswick: Rutgers University Press.
- AGCOM - Autorità per le garanzie nelle comunicazioni (2020). *Delibera 129-20-CONS Atto di richiamo sul rispetto dei principi vigenti a tutela della correttezza dell'informazione con riferimento al tema "coronavirus covid-19"*. Roma: AGCOM. Testo disponibile all'indirizzo web: <https://www.agcom.it/documents/10179/17914778/Delibera+129-20-CONS/2d750507-644c-44f4-8abf-1a93322daef4> (02/06/2020).
- Bechis F. (2020). *Così Russia e Cina fanno propaganda in Italia. Il rapporto del Copasir*. Testo disponibile all'indirizzo web: <https://formiche.net/2020/05/russia-cina-propaganda-italia-rapporto-copasir> (30/05/2020).

- Bieber F. (2008). The DNA Wars: Part I. *American Journal of Human Genetics*, 83, 3: 304. DOI: 10.1016/j.ajhg.2008.08.008.
- Boniolo G. (2018). Più etica, metodologia e filosofia per lo scienziato. *Scienzainrete.it*, 12 dicembre. Testo disponibile all'indirizzo web: <https://www.scienzainrete.it/articolo/pi%C3%B9-etica-metodologia-e-filosofia-lo-scienziato/giovanni-boniolo/2018-12-12> (24/04/2020).
- Brownson R., Chriqui J., Stamatakis K. (2009). Understanding evidence-based public health policy. *American Journal of Public Health*, 99, 9: 1576. DOI: 10.2105/AJPH.2008.156224.
- Brusati E. (2003). Come si fanno i sondaggi. *Induzioni*, 26: 5.
- Bucci E., Corbellini G., De Luca M. (2020). *AVIGAN e le terapie a furor di popolo*. *Scienzainrete.it*, 28 marzo. Testo disponibile all'indirizzo web: <https://www.scienzainrete.it/articolo/avigan-e-le-terapie-furor-di-popolo/enrico-bucci-gilberto-corbellini-michele-de-luca/2020> (20/04/2020).
- Campbell C. (2020). South Korea's Health Minister on How His Country Is Beating Coronavirus Without a Lockdown. *Time*, 30 aprile. Testo disponibile all'indirizzo web: <https://time.com/5830594/south-korea-covid19-coronavirus> (02/06/2020).
- CDC - Centers for Disease Control and Prevention (2020). *Instructions for Completing the Human Infection with 2019 Novel Coronavirus(COVID-19) Person Under Investigation (PUI) and Case Report Form*. Testo disponibile all'indirizzo web: <https://www.cdc.gov/coronavirus/2019-ncov/downloads/COVID-19-Persons-Under-Investigation-and-Case-Report-Form-Instructions.pdf> (24/04/2020).
- Diamanti I. (2020). L'emergenza giustifica uno stop alla democrazia per 4 italiani su 10. *Rep.*, 31 maggio. Testo disponibile all'indirizzo web: [https://rep.repubblica.it/pwa/generale/2020/05/31/news/l\\_emergenza\\_giustifica\\_uno\\_stop\\_alla\\_democrazia\\_per\\_4\\_italiani\\_su\\_10-258128992](https://rep.repubblica.it/pwa/generale/2020/05/31/news/l_emergenza_giustifica_uno_stop_alla_democrazia_per_4_italiani_su_10-258128992) (31/05/2020).
- Di Plinio G. (2011). *Fazhi (法治)*. L'espansione della *Western Legal Tradition* nella Cina del Terzo Millennio. *Iura Orientalia*, VII: 176. Testo disponibile all'indirizzo web: [http://www.iuraorientalia.net/IO/IO\\_07\\_2011/V\\_01\\_7\\_DiPlinio.pdf](http://www.iuraorientalia.net/IO/IO_07_2011/V_01_7_DiPlinio.pdf) (02/06/2020).

- Enriques M. (2020). Coronavirus: Why death and mortality rates differ? *BBC*, 2 aprile. Testo disponibile all'indirizzo web: <https://www.bbc.com/future/article/20200401-coronavirus-why-death-and-mortality-rates-differ> (25/04/2020).
- European Union Agency for Fundamental Rights (2020). *Coronavirus pandemic in the EU. Fundamental Rights implications*. Luxembourg: Publications Office of the European Union. Testo disponibile all'indirizzo web: [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-1\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin-1_en.pdf) (30/05/2020).
- Fendos J. (2020). Lessons From South Korea's COVID-19 Outbreak: The Good, Bad, and Ugly. *The Diplomat*, 10 marzo. Testo disponibile all'indirizzo web: <https://thediplomat.com/2020/03/lessons-from-south-koreas-covid-19-outbreak-the-good-bad-and-ugly> (01/06/2020).
- Ferro A. (2020). *Il bagnante di Mondello che ha preso 5 multe: "Pagherò ma vado in spiaggia, sono un uomo libero"*. *Il Giornale.it Palermo*, 16 aprile. Testo disponibile all'indirizzo web: <https://www.ilgiornale.it/news/palermo/bagnante-mondello-che-ha-preso-5-multe-pagher-vado-spiaggia-1854567.html> (02/06/2020).
- Garante per la protezione dei dati personali (2004). *Relazione 2004. Discorso del Presidente Stefano Rodotà*. Roma: GPDP. Testo disponibile all'indirizzo web: <https://www.garanteprivacy.it/documents/10160/10704/1093804> (02/06/2020).
- Gennari G. (2018). La macchina della verità si è fermata a Salerno... Fortunatamente. *Diritto Penale Contemporaneo*, 12: 5. Testo disponibile all'indirizzo web: <https://archiviodpc.dirittopenaleuomo.org/upload/7945-gennari2018a.pdf> (31/05/2020).
- Goodhart D. (2020). Pass the remote, there's too much emotion on the news. *The Sunday Times*, 26 Aprile.
- Goodin R., a cura di (2008). *The Oxford Handbook of Public Policy*. Oxford (UK): Oxford University Press.
- Gottschalk S. (2018). The infantilization of Western culture. *The Conversation*, 1 agosto. Testo disponibile all'indirizzo web: <https://theconversation.com/the-infantilization-of-western-culture-99556> (26/04/2020).
- Gottschalk S. (2019). *The Terminal Self*. Abingdon (UK): Routledge.

- Grossi G. (2016). *L'opinione pubblica. Teoria del campo demoscopico*. Roma-Bari: Laterza.
- Huff D. (2005). *Mentire con le statistiche*. Pescara: Monti & Ambrosini editori.
- Kim H. (2020). South Korea learned its successful Covid-19 strategy from a previous coronavirus outbreak: MERS. *Bulletin of the Atomic Scientists*, 20 marzo. Testo disponibile all'indirizzo web: <https://thebulletin.org/2020/03/south-korea-learned-its-successful-covid-19-strategy-from-a-previous-coronavirus-outbreak-mers> (01/06/2020).
- Kincaid H., Duprè J., Wiley A. (2007). *Value-Free Science?: Ideals and Illusion*. New York: Oxford University Press USA. DOI: 10.1093/acprof:oso/9780195308969.001.0001.
- Koerth M., Bronner L., Mithani J. (2020). Why It's So Freaking Hard To Make A Good COVID-19 Model. *FiveThirtyEight*, 31 marzo. Testo disponibile all'indirizzo web: <https://fivethirtyeight.com/features/why-its-so-freaking-hard-to-make-a-good-covid-19-model> (30/05/2020).
- Ko J. (2020). How China used technology to combat COVID-19 – and tighten its grip on citizens. *Amnesty International*, 17 aprile. Testo disponibile all'indirizzo web: <https://www.amnesty.org/en/latest/news/2020/04/how-china-used-technology-to-combat-covid-19-and-tighten-its-grip-on-citizens> (01/06/2020).
- Kottasová I. (2020). Why comparing coronavirus outbreaks in different countries can be misleading -- and even dangerous. *CNN Health*, 26 marzo. Testo disponibile all'indirizzo web: <https://edition.cnn.com/2020/03/26/health/number-of-cases-testing-data-intl/index.html> (30/05/2020).
- Kumar S. (2020). Wuhan tests millions in 12 days as China fears second virus wave. *Hindustan Times*, 26 maggio. Testo disponibile all'indirizzo web: <https://www.hindustantimes.com/world-news/wuhan-tests-millions-in-12-days-as-china-fears-second-virus-wave/story-efwADhcyzbuKU1wppIH11I.html> (27/05/2020).
- Kuo L. (2020). 'The new normal': China's excessive coronavirus public monitoring could be here to stay. *The Guardian*, 9 marzo. Testo disponibile all'indirizzo web: <https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay> (02/06/2020).
- Le Belzic J. (2020). Coronavirus in China. *DW Documentary*, 17 marzo. Video visibile

all'indirizzo web: <https://youtu.be/3K3fy5eKeuM> (1 giugno 2020).

- Leonard A. (2020). Taiwan Is Beating the Coronavirus. Can the US Do the Same? *Wired*, 19 marzo. Testo disponibile all'indirizzo web: <https://www.wired.com/story/taiwan-is-beating-the-coronavirus-can-the-us-do-the-same> (25/04/2020).
- Lupària L. (2009) *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest*. Milano: Giuffrè.
- MacLean C., Lamparello A. (2014). Forensic DNA phenotyping in criminal investigations and criminal courts: assessing and mitigating the dilemmas inherent in the science. *Recent Advances in DNA & Gene Sequences*. 8, 2: 104. DOI: 10.2174/2352092209666150212001256.
- Manantan M. (2020). Agile Governance Crushing COVID-19: Taiwan and South Korea. *The Diplomat*, 22 maggio. Testo disponibile all'indirizzo web: <https://thediplomat.com/2020/05/agile-governance-crushing-covid-19-taiwan-and-south-korea> (02/06/2020).
- McCarry J. (2020). Test, trace, contain: how South Korea flattened its coronavirus curve. *The Guardian*, 23 aprile. Testo disponibile all'indirizzo web: <https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve> (25/04/2020).
- Meyer R. (2019). Trump Isn't a Climate Denier. He's Worse. *The Atlantic*, 5 novembre. Testo disponibile all'indirizzo web: <https://www.theatlantic.com/science/archive/2019/11/ideology-behind-donald-trumps-paris-withdrawal/601462> (31/05/2020).
- Monti A. (2010). Conservazione dei campioni biologici e tutela dei diritti fondamentali della persona, Ambiguità semantiche, finalità dei trattamenti e limiti della genetic evidence e Catena di custodia e “doppio binario” per campioni e reperti. In Marafioti L. e Lupària L., a cura di, *Banca dati del DNA e accertamento penale*. Milano: Giuffrè.
- Monti A. (2020). Internet e ordine pubblico. In Cassano G. e Previti S., a cura di, *Il diritto di internet nell'era digitale*. Milano: Giuffrè Francis Lefebvre.
- Monti A., Wacks R. (2019). *Protecting Personal Information*. Oxford (UK): Hart Publishing.
- Morris C., Reuben A. (2020). Coronavirus: Why are international comparisons difficult?

*BBC News*, 18 maggio. Testo disponibile all'indirizzo web: <https://www.bbc.com/news/52311014> (24/04/2020).

Peters E. (2020). Is Obsessing Over Daily Coronavirus Statistics Counterproductive? *The New York Times*, 12 marzo. Testo disponibile all'indirizzo web: <https://www.nytimes.com/2020/03/12/opinion/sunday/coronavirus-statistics.html> (30/05/2020).

Politi F. (2014). *La sentenza del Tribunale dell'Aquila sulla responsabilità dei membri della Commissione "Grandi Rischi". Posizione del tema*. XII Convegno Nazionale di Diritto Sanitario, *Eternit - Stamina - L'Aquila: tre casi difficili tra scienza e diritto*, Alessandria, 14 novembre. Testo disponibile all'indirizzo web: [https://www.academia.edu/17283992/La\\_Sentenza\\_sulla\\_Commissione\\_Grandi\\_Rischi\\_a\\_LAquila](https://www.academia.edu/17283992/La_Sentenza_sulla_Commissione_Grandi_Rischi_a_LAquila) (26/04/2020).

Park S., Choi G., Ko H. (2020). Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies. *The Journal of the American Medical Association*, 323, 21: 2129. DOI: 10.1001/jama.2020.6602.

Prontera A. (2013). La dimensione tecnologica nelle politiche pubbliche. *Rivista Italiana di Politiche Pubbliche*, 2: 281. DOI: 10.1483/74202.

Repubblica, la (1988). Donat-Cattin ha prorogato i limiti per l'atrazina. *La Repubblica*, 1 aprile. Testo disponibile all'indirizzo web: <https://ricerca.repubblica.it/repubblica/archivio/repubblica/1988/04/01/donat-cattin-ha-prorogato-limiti-per.html> (24/04/2020).

Seligman M. (1972). Learned Helplessness. *Annual Review of Medicine*, 23, 1: 407. DOI: 10.1146/annurev.me.23.020172.002203.

Seligman M. (2011). Risk for fundamental rights is learned helplessness. *Harvard Business Review*, aprile. Testo disponibile all'indirizzo web: <https://hbr.org/2011/04/building-resilience> (26/04/2020).

Sohrabi S. (2015). The criminal gene: the link between MAOA and aggression. *BMC Proceedings*, 9, A49. DOI: 10.1186/1753-6561-9-S1-A49.

Stobbe M. (2020). *Mass gatherings, erosion of trust upend coronavirus control*. abcNEWS, 1 giugno. Testo disponibile all'indirizzo web: <https://abcnews.go.com/Health/wireStory/mass-gatherings-erosion-trust-upend-coronavirus-control-70989886> (01/06/2020).

Takeuchi R. (2020). *Nanjing, la città con zero contagi. La descrizione più realistica della*

*prevenzione dell'epidemia a Nanjing vista attraverso l'obiettivo di un regista giapponese* (titolo tradotto dall'originale cinese). Video visibile all'indirizzo web: <https://youtu.be/YfsdJGj3-jM> (01/06/2020).

The Economist (2020). *To curb covid-19, China is using its high-tech surveillance tools*, 29 febbraio. Testo disponibile all'indirizzo web: <https://www.economist.com/china/2020/02/29/to-curb-covid-19-china-is-using-its-high-tech-surveillance-tools> (08/06/2020).

UK House of Commons – Home Affairs Committee (2010). *The National DNA Database – Eighth Report of Session 2009-10 Volume II Ev 11*. Testo disponibile all'indirizzo web: <https://publications.parliament.uk/pa/cm200910/cmselect/cmhaff/222/22202.htm> (31/05/2020).

von Hayek F. (1974). *The Pretence of Knowledge*. Testo disponibile all'indirizzo web: <https://www.nobelprize.org/prizes/economic-sciences/1974/hayek/lecture> (31/05/2020).

Wacks R. (2016). *Privacy. Una sintetica introduzione*. Pescara: Monti & Ambrosini editori.

Wang J., Ng C. Y., Brook R. (2020). Response to COVID-19 in Taiwan. Big Data Analytics, New Technology, and Proactive Testing. *Journal of American Medical Association*, 323, 14: 1341. DOI: 10.1001/jama.2020.3151.

Wong T. (2020). Shincheonji and coronavirus: The mysterious 'cult' church blamed for S Korea's outbreak. *BBC News*, 14 marzo. Video visibile all'indirizzo web: <https://www.bbc.com/news/av/world-asia-51851250/shincheonji-and-coronavirus-the-mysterious-cult-church-blamed-for-s-korea-s-outbreak> (01/06/2020).