Covid-19: tra emergenza sanitaria e sistemi di digital contact tracing

Andrea Antonilli*

Alcune premesse

La diffusione del virus Covid-19, trasformatosi presto in pandemia, ha posto interrogativi circa le modalità utili a contrastare la sua espansione e, quindi, a preservare lo stato di salute di milioni di individui. Se inizialmente i paesi colpiti dal virus hanno adottato misure di distanziamento sociale, incoraggiato l'utilizzo di dispositivi di protezione individuale, nonché impiegato le Forze dell'Ordine per garantire l'applicazione ed il rispetto delle prescrizioni governative, a quasi sei mesi dalla sua comparsa sulla scena italiana ed internazionale sono state ideate ed introdotte misure di natura tecnologica, finalizzate al monitoraggio dei contagi e degli spostamenti degli individui. Oltre a ricorrere ai già consolidati sistemi di videosorveglianza ed alla biometria passiva (riconoscimento del volto in primis), numerosi sono stati i tentativi di sviluppare ed implementare applicazioni di *digital contact tracing*, ovvero a quei sistemi attivi di monitoraggio volti all'identificazione delle persone venute potenzialmente a contatto con una persona infetta ed alla successiva raccolta di informazioni aggiuntive su tali contatti. In altri termini, un controllo esteso sui network dei (presunti) contagiati.

Non si è ancora attenuato l'acceso dibattito tra coloro che ritengono come le misure tecnologiche di controllo e di sorveglianza – seppur invasive – siano necessarie per contrastare ulteriori conseguenze negative per la salute e persino utili nel fornire una corretta informazione ai cittadini, responsabilizzando le loro condotte e favorendo la loro collaborazione e chi ritiene che i governi nazionali stiano usando la scienza medica come strumento di raccolta digitale indiscriminata di dati ed informazioni, al presunto fine di esercitare potere e controllo sulle masse.

* Andrea Antonilli, Professore aggregato, insegna Criminologia e vittimologia presso l'Università degli Studi "G. d'Annunzio" di Chieti-Pescara.

1. Il digital contact tracing nel mondo: tra controllo indiscriminato e tutela dei diritti

I sistemi di digital contact tracing oscillano tra una polarità fortemente invasiva e un tentativo di controllo rispettoso della privacy[1].

Il primo polo è rappresentato dalla Cina, paese in cui il virus ha avuto modo di diffondersi con anticipo, dove le parole d'ordine sono state ricerca attiva dei casi e rapido tracciamento ed isolamento dei contatti (cfr. Li, Chen, Feng *et al.*, 2020). Il tutto si è tradotto in un monitoraggio indiscriminato ed altamente intrusivo che non ha riguardato solo i contagiati, ma ampie fasce della popolazione in generale. Prendendo a prestito una definizione dei uno dei maggiori esperti di sorveglianza – David Lyon (2018) – la Cina ha in quest'ottica realizzato un vero e proprio *surveillance state* (stato di sorveglianza) di sapore orwelliano, in cui la popolazione è stata sottoposta ad ampie pratiche di controllo da parte delle agenzie di intelligence con la piena collaborazione e mediazione di enti commerciali Internet e compagnie telefoniche – che forniscono i dati desiderati alle istituzioni pubbliche (Lombi e Moretti, 2020). Il tutto realizzato tramite lo sviluppo di un raffinato sistema di sorveglianza di massa, caratterizzato da tecnologia Gps, big data, traffico telefonico, riconoscimento biometrico e intelligenza artificiale (cfr. Zunino, 2020).

Il primo passo è stato quello di sviluppare un'app – denominata Alipay Health Code e diffusa a Hangzhou e nella provincia dello Zhejiang –in grado di calcolare il rischio di contagio, utilizzando sistemi attivi di tracciamento e di sorveglianza. L'applicazione – integrata nel sistema di pagamenti del colosso cinese Alibaba e nella app di istant-messaging cinese, Wechat – traccia gli spostamenti degli utenti e calcola il tempo trascorso nelle zone ad alto contagio. Grazie al convogliamento di molte altre informazioni – provenienti in misura maggiore da diffusi sistemi di riconoscimento del volto (efficaci anche in presenza della mascherina sul volto) in grado di identificare i passanti e di stimare la loro temperatura corporea –, l'app assegna automaticamente alle persone – in base allo stato di salute e ai recenti viaggi compiuti – un Qrcode assimilabile a uno dei tre codici (verde, giallo, rosso)[2] per stabilire chi è autorizzato a circolare nello spazio pubblico e chi

[1] Si veda lo studio di Altshuler e Hershkovitz, intitolato "Tracking Citizens: What is Going On in the World?". Materiale disponibile al sito: https://www.idi.org.il/%20parliaments/30997/31088.

[2] Il codice verde presuppone assenza di contagio; il codice giallo indica isolamento domestico; quello rosso indica che l'utente è positivo al virus e posto in isolamento forzato.

è tenuto a restare in isolamento. Il sistema Alypay Health Code, inoltre, condivide le informazioni con la polizia, stabilendo "un modello per nuove forme di controllo sociale automatizzato che potrebbero persistere molto tempo dopo la fine dell'epidemia" (Mozure, Zhong e Krolik, 2020) e che potrebbe riguardare – anzi già riguarda – anche alcune minoranze etniche e religiose in Cina (es. i musulmani uiguri). Inoltre, fra le tante controindicazioni che tale sistema presenta, vi è la possibilità che persone non infette ricevano un codice rosso, solo perché residenti in aree ad alto rischio. Può, inoltre, capitare che nessuno sappia per quanto tempo questo codice rosso rimanga attribuito, impedendo qualsiasi tipo di spostamento, o che nessuno sappia di preciso come poter cambiare lo status espresso da questo codice (cfr. Marucci, 2020) di un sistema di tracciamento che rischia di «individuare nuove forme di controllo sociale automatizzato che potranno resistere anche a lungo alla fine dell'epidemia» e che coincide con un «esperimento di massa per regolamentare le vite dei cittadini» (Mozure, Zhong e Krolik, 2020).

La Corea del Sud può considerarsi un caso intermedio, dal momento che pur potendo individuare dei punti di sovrapposizione – quali ad esempio l'utilizzo massivo di big data e di videocamere di sorveglianza – le modalità di controllo e di tracciamento dei cittadini sono sicuramente meno drastiche della Cina, anche se non applicabili all'Europa, secondo quanto previsto dal GDPR. Il governo sudcoreano ha deciso di utilizzare due app, ovvero Corona-100m[3] e Corona Map. Entrambe, interagendo col GPS degli smartphone, permettono di tracciare – grazie ai dati ricevuti dalle compagnie telefoniche, dalle società di carte di credito, dalle telecamere di sorveglianza nelle aree pubbliche e dai satelliti – gli spostamenti dei contagiati e della popolazione in generale. In aggiunta, le due applicazioni consentono di segnalare agli utenti quando tenersi lontano dalle aree a rischio contagio e comunicare ai frequentatori di quei luoghi la volontaria possibilità di sottoporsi alle opportune verifiche sanitarie[4]. Parimenti, sempre tramite la geolocalizzazione, il sistema consente «di verificare il rispetto della quarantena da parte di un utente sottoposto a restrizioni, oppure permette addirittura all'utente stesso di segnalare soggetti a rischio» (Pititto, 2020, p. 17). Bisogna tuttavia precisare come i dati raccolti vengano trasformati in stringhe di codice, quindi non riconducibili alla specifica identità degli individui. Difatti, le autorità sudcoreane – elemento questo che la fa differire

[3] L'app avvisa quando l'utente si trova a 100mt da una zona in cui è stato individuato un contagiato; mentre Corona Map consente di tracciare in tempo reale, una mappa degli spostamenti dei positivi al Covid-19.

[4] Tuttavia, quando il rifiuto di sottoporsi ai controlli sanitari non viene giustificato, scattano delle sanzioni.

dal modello cinese – propendono per una rigorosa riservatezza relativamente alle informazioni raccolte, prevedendo anche sanzioni pecuniarie e detentive per coloro che la violano.

In Europa, non vi è stata una convergenza verso un'unica soluzione di tracciamento digitale: ciascun paese-membro infatti ha deciso di agire in autonomia. Tuttavia, è possibile riscontrare come essi siano accomunati dalla presenza di una medesima legislazione in materia di protezione dei dati personali (GDPR) e dall'aver tratto ispirazione, nella scelta e nel funzionamento delle applicazioni digitali, dalle indicazioni emerse dal Pan-European Privacy-Preserving Proximity Tracing, ovvero: l'impiego del bluetooth, della crittografia e dell'anonimizzazione dei dati personali (cfr. Melissari, 2020). Quindi, il vecchio continente ha necessariamente optato, allontanando ogni possibile rischio di ingiustificato controllo di massa e di violazione della privacy, per un tracciamento digitale dei soli "positivi" e per una raccolta ed un trattamento di dati anonimi.

I modelli implementati sono principalmente di due tipi: centralizzato e decentralizzato. Entrambi prevedono una unità centrale che coordina e gestisce il flusso di dati, tuttavia nel primo modello questa ha accesso a molti più dati rispetto al secondo. Solitamente, quello decentralizzato propende per applicazioni con codice sorgente messo a disposizione da Google e Apple, che utilizza la tecnologia bluethooth a bassa energia. Peculiarità del modello è quella di far si che i dati raccolti tramite le app, per motivi di riservatezza, non vengono fatti convogliare costantemente in un server esterno, ma vengono immagazzinati direttamente e univocamente sulla memoria dello smartphone. Ne costituiscono un esempio quelle in uso in Germania (Corona-Warn-App), Italia (Immuni), Svizzera (SwissCovid) e Austria (Stop Corona).

Il modello centralizzato prevede, invece, che il controllo dei codici avvenga al di fuori dei dispositivi personali, raccogliendo metadati come il tempo di esposizione ed eventualmente la localizzazione dei telefoni cellulari. Prendendo ad esempio la Francia, l'app StopCovid condivide con il primo modello l'architettura ed il tipo di tecnologia, ma se ne distanzia per aver scelto di far confluire i dati relativi ai contatti degli individui in un server esterno, prestando il fianco ad alcune problematiche di trattamento dei dati e di privacy. Menzione a parte riguarda il Regno Unito dove, a seguito di una sperimentazione fallimentare di un'app sviluppata dal sistema sanitario nazionale, il governo ha affermato di voler prendere in considerazione la possibilità di appoggiarsi al sistema tecnologico di Apple e Google.

2. Il tracciamento digitale dei contatti in Italia: l'app Immuni

In Italia, tra le oltre 300 proposte presentate, il *Gruppo di lavoro data-driven per l'emergenza di Covid-19*, nominato dal Ministero per l'Innovazione tecnologica e la digitalizzazione, ha selezionato la mobile App denominata "Immuni", ideata dalla Bending Spoons S.p.A.[5] .

Probabilmente, l'aver optato per una applicazione – piuttosto che di altre soluzioni tecnologiche – trova spiegazione nella ampia diffusione di dispositivi mobili (smartphone e tablet in primis) e nella conseguente familiarità di utilizzo delle mobile app in genere. Gli smartphone hanno difatti riconfigurato gran parte delle nostre attività. Come sostenuto da Greenfield (2017, p. 11) nella sua pungente opera *Tecnologie radicali* «ci affidiamo a loro per documentare i luoghi in cui andiamo, le cose che facciamo, le nostre frequentazioni; contiamo su di loro per riempire gli spazi vuoti, i momenti di pausa e i silenzi che occupavano abitualmente gran parte della nostra vita».

L'operatività nazionale di Immuni ha avuto inizio, grazie alla implementazione di Apple e Google, il 15 giugno 2020. Compatibile con i due principali sistemi operativi per device mobili (Android e Ios), l'app – una volta scaricata volontariamente dagli store digitali o dal sito www.immuni.italia.it. – consente di sapere, sfruttando la tecnologia del bluethooth a bassa energia (BLE)[6], se l'utente è entrato in contatto con un soggetto contagiato. L'app raccoglie in modo anonimo i dati che, a loro volta, vengono crittografati, ma non raccoglie dati GPS o di posizione ed esegue tutte le elaborazioni sul dispositivo medesimo.

Ad ogni dispositivo, Immuni associa un identificatore (ID) di prossimità in nessun modo riconducibile all'utente, che viene continuamente trasmesso e catturato dagli altri smarphone prossimi e muniti della stessa app. Quando due o più soggetti restano a contatto per un periodo di tempo prolungato (stimato in circa 15 minuti), i loro smartphone memorizzano – solo ed esclusivamente nella loro memoria interna - gli ID degli altri, tenendo traccia del contatto. In altre parole, ha la peculiarità di conservare dati e meta-dati (durata del contatto e potenza del segnale ricevuto), assegnandogli un

[5] Immuni è stata selezionata poiché: scaricabile su base volontaria; gestibile da uno o più soggetti pubblici; consente l'anonimizzazione e la cancellazione dei dati raccolti; risponde ai requisiti di cyber-sicurezza volti alla protezione dei dati; utilizza il bluetooth a bassa energia,; il suo codice sorgente è open source.

[6] Il BLE consente lo scambio ravvicinato di piccole stringhe di codice, senza gravare sull'utilizzo e sul consumo della batteria, poiché si attiva nel momento in cui tra due device vi è una distanza inferiore al metro.

identificativo transitorio, costituito da codici muniti di chiave crittografica, che cambiano numerose volte ogni ora.

A chi si è trovato a stretto contatto con un utente risultato positivo al virus del COVID-19, l'app invia una notifica che lo avverte del potenziale rischio di essere stato contagiato ("notifica di esposizione")[7].

A secondo del livello di rischio[8], il potenziale contagiato può essere invitato: all'auto-isolamento (rischio basso), della durata di 14 giorni a partire dalla ricezione della notifica; a contattare il medico di famiglia (rischio medio), il quale valuterà i sintomi, li monitorerà e, in caso di persistenza degli stessi, contatterà le agenzie territoriali della salute competenti che inviteranno l'assistito ad eseguire il tampone; a raggiungere l'ospedale più vicino (rischio elevato).

Quando un soggetto risulta positivo al coronavirus, ha la possibilità di caricare - seguendo il protocollo DP-3T (Decentralized-Privacy-Preserving Proximity Tracking) - su un server ministeriale le sequenze alfanumeriche inviate agli altri smartphone[9].

Ritenuta dal commissario all'emergenza Domenico Arcuri «[…] la più idonea per la sua capacità di contribuire tempestivamente all'azione di contrasto del virus, per la conformità al modello europeo delineato dal Consorzio PEPP-PT e per le garanzie che offre per il rispetto della privacy» (Arcuri, 2020), Immuni sarà, all'interno del sistema Gateway, tra le prime applicazioni ad operare nell'Eurozona, grazie alla interconnessione con sistemi speculari di altri paesi membri (inizialmente il sistema integrerà Italia, Irlanda e Germania)[10].

[7] Immuni, a partire dallo scorso agosto, invia– settimanalmente - una notifica che informa gli utenti del fatto che non è avvenuto nessun contatto con contagiati.

[8] Questa operazione viene resa possibile calcolando la distanza tra i device ed il tempo in cui essi sono rimasti a contato nello spazio di prossimità. E' rischioso quel contatto avvenuto ad una distanza inferiore ai due metri e che si è protratto per più di 15 minuti.

[9] In caso di corrispondenza, l'app calcola il rischio di esposizione all'infezione di ogni identificativo e crea una lista dei contatti maggiormente a rischio. A questo punto, è possibile inviare loro una notifica, mantenendo una condizione di anonimato.

[10] Tale integrazione consentirà a coloro che si recheranno all'estero di inviare o ricevere segnalazioni in caso di contagio o di contatti di prossimità con soggetti positivi.

3. Immuni: fra luci ed ombre

Nonostante gli indubbi pregi dell'architettura tecnologica e della logica di funzionamento delle soluzioni di tracciamento digitale[11], Immuni non è stata esente da critiche, provenienti da vari ambiti.

Avanzati soprattutto nella fase iniziale relativa alla scelta del modello tecnologico da utilizzare per il tracciamento, i principali dubbi sono stati in parte superati prima dell'implementazione ufficiale del digital contact tracing, con la scelta della tecnologia bluethooth a breve intensità e con l'adozione di un nuovo sistema di cyber-sicurezza, volto a contrastare potenziali forme di attacco (violazione dei dati personali o data breach[12]).

Tuttavia, alcuni osservatori riscontrano la persistenza di alcune problematiche, relative a: una pericolosa dipendenza tecnologica – se non vera e propria sudditanza – dai due colossi digitali Apple e Google, tale da rendere le «app statali a semplici cornici applicative di un processo di tracciamento sanitario internazionale da loro direttamente effettuato attraverso infrastrutture proprietarie sulle quali non abbiamo alcun effettivo controllo» (Lisi, 2020); una soluzione tecnologica di tracciamento, il bluetooth, non particolarmente efficiente ed efficace e non in grado di svolgere tutte le funzioni previste dalle norme (tracciamento ad una prossimità di 1-2 metri per un tempo di 15 minuti), a causa della presenza di falsi alert, sia positivi che negativi[13]. In questo caso, un incremento eccessivo o totalmente assente del tasso di allarme potrebbe creare una serie di comprensibili problemi gestionali ed operativi.

I limiti di natura culturale riguarderebbero, in primis, il cd. *digital divide* e la carente alfabetizzazione tecnologico-informatica dell'utente medio e, in secondo luogo, una insufficiente – e per questo infruttuosa - comunicazione

[11]Ovvero, individuare un numero maggiore di soggetti asintomatici; ovviare alle dimenticanze del soggetto interessato; far emergere tutti quei contatti avvenuti superando la soglia critica spaziale e temporale ritenute sicura; abbattere i tempi di comunicazione con i contatti a rischio; facilitare il follow up dei soggetti coinvolti da parte delle autorità sanitarie; assicurare un minore investimento di risorse organizzative, finanziarie ed umane, rispetto alle tecniche paper-based (cfr. Resta, 2020).

[12] Il protocollo è in realtà vulnerabile ad alcuni attacchi (Nerd attack, Location tracking attack, Replay attack), anche se sono tuttavia piuttosto complicati da attuare. Per questo, la maggior parte dei cittadini può usare Immuni senza doversi preoccupare troppo della sicurezza dei propri dati (cfr. Gadotti A.,2020).

[13] Si tenga conto, ad esempio, che tale tecnologia non consente di discriminare se gli individui indossano o meno la mascherina o se tra due o più soggetti che si trovano in prossimità vi sia la presenza di una parete o di una barriera che renderebbe impossibile il contatto ed il contagio.

istituzionale, costituita da campagne informative quantitativamente e qualitativamente inidonee al raggiungimento di un numero sufficiente di download (pari a circa il 60% della popolazione).

Ciò potrebbe tradursi in una sostanziale impreparazione nell'utilizzo dei nuovi terminali tecnologici e nella scarsa propensione a cogliere l'importanza delle loro potenzialità intrinseche. Se a questo aggiungiamo che esistono alcune fasce della popolazione con condizioni svantaggiate di natura economica, sociale e politica (senza fissa dimora, migranti irregolari o sottoposti a protezione internazionale) impossibilitate a possedere uno smartphone e privi delle competenze minime necessarie, è facilmente comprensibile come il tracciamento digitale possa essere potenzialmente inefficace. Se, poi, al *digital divide* si unisce una non chiara campagna informativa istituzionale circa il funzionamento dei sistemi di digital contact tracing, la situazione tende a complicarsi di gran lunga. Difatti, nella fase iniziale dell'implementazione di Immuni, la comunicazione istituzionale non è riuscita a costruire un ambiente recettivo, a far percepire il problema della salute pubblica come rilevante, a veicolare obiettivi realistici e ben delineati (con il rischio di alimentare progetti miracolistici o difficilmente realizzabili), ad evitare che le notizie relative al tracciamento fossero messe in discussione da fonti alternative d'informazione. Tali mancanze hanno contribuito ad una diffusione di Immuni ben al di sotto delle aspettative: arrivati al mese di ottobre 2020, gli ultimi dati disponibili parlano di un numero di download pari a circa 8 milioni.

Dal punto di vista giuridico, le obiezioni sono relative alla ingerenza delle forme tecnologiche di tracciamento, in grado di sfociare in una non sempre giustificata sorveglianza digitale ed alla conseguente violazione della normativa della privacy, con riferimento al trattamento non autorizzato dei dati personali raccolti. Buona parte delle contestazioni si sono concentrate sulla carenza di garanzie circa l'impiego legale di tali dati, richiamando l'eventualità che alcuni soggetti (persone fisiche e giuridiche) avrebbero potuto accedere ad informazioni sensibili, motivati da interessi di natura economica (profilazione utenti ai fini del marketing), criminale (furto di identità digitale e mercato clandestino delle informazioni) e politica (utilizzo improprio dei dati – per scopi di controllo delle popolazioni - da parte del governo centrale). In base ad una recente corrente di pensiero, la pandemia rappresenterebbe una ulteriore occasione per estendere e diffondere il potere di influenza sui comportamenti dei cittadini. Pur se messe in atto per far fronte ad un pericolo contingente, le misure provvisorie avrebbero la tendenza a sopravvivere alle emergenze (cfr. Harari, 2020).

Quella in atto, corrisponderebbe ad una Safetycracy, ovvero quel paradigma del potere basato sulla protezione della vita, sull'uso strumentale della scienza in campo medico e biologico da una parte e degli strumenti

tecnologici di connettività e di intelligenza artificiale dall'altra (cfr. Salerno Aletta, 2020). Ancorché legato alla salute, la costruzione di un profilo elettronico dei cittadini può favorire il mantenimento dell'ordine pubblico – attraverso l'individuazione di condotte devianti e la normalizzazione di alcuni comportamenti. Tuttavia, la sorveglianza digitalizzata ha dato vita a nuove forme di controllo sociale, cercando di orientare e influenzare le attività dei cittadini (cfr. Ragnedda, 2011). Ad oggi gli scettici del controllo digitale temono ricadute che potremmo ricondurre, operando una analogia con i famosi slogan presentati nella celebre distopia *1984* di Orwell – War is Peace, Freedom is Slavery, Ignorance is Strength – a "Libertà è Pericolo, Sorveglianza è Salute, Condividere (i dati) è Sicurezza".

Conclusioni

Con questo contributo si è cercato di ricostruire la genesi che ha spinto i governi di molti paesi ad introdurre sistemi attivi di tracciamento digitale, nella consapevolezza che tali tecnologie potessero assolvere ad alcune importanti funzioni, sia di natura preventiva (campagne informative; avvisare digitalmente gli utenti potenzialmente contagiati; fornire strumenti di auto-diagnosi) che di contrasto (diminuire o spezzare le catene di infezione in tempi più brevi). La validità di tali sistemi si sostanzia, principalmente, nella individuazione e nell'arginamento di quei focolai casuali difficilmente individuabili ricorrendo alle misure di tracciamento analogico. Tuttavia, per essere efficaci, essi devono inserirsi in un servizio sanitario ben organizzato ed integrarsi con i metodi "tradizionali" di diagnosi.

Se la prerogativa di queste misure tecnologiche è quella riuscire ad ottenere un elenco di cittadini con la salute compromessa e che devono essere posti in isolamento, la loro ovvia controindicazione rimanda alla imposizione di forme intrusive di controllo e di sorveglianza, volte a condizionare i comportamenti degli osservati in nome della preservazione della salute pubblica: una tecnologia «[…] di tracciamento collettivo (e, pertanto, non solo dei positivi) sarebbe uno strumento non tanto diretto alla prevenzione del contagio, ma piuttosto ad un – irragionevole – controllo di massa» (Miniscalco, 2020). Difatti, mentre nei paesi che attuano una politica garantista dei diritti democratici vengono proposte soluzioni di tracciamento digitale facoltative, altre realtà nazionali adottano misure obbligatorie ed intrusive, finalizzate alla raccolta indiscriminata di dati sensibili, mediante la tecnologia Geo-Tracking e la consultazione dei dati telefonici.

In un diffuso clima di timore ed incertezza, sono state introdotte misure che, solo qualche tempo fa, sarebbero state giudicate non percorribili e che

avrebbero probabilmente incontrato forti resistenze. Anche se giustificata dalla contingenza, la necessità di tracciare gli individui al fine di preservare lo stato di salute non deve rischiare di compromettere le libertà e i diritti dei cittadini e assumere la forma di una sorta di autoritarismo digitale, potenzialmente in grado di perdurare anche dopo la fine dell'emergenza sanitaria.

Bibliografia

Arcuri D. (2020), *Ordinanza n. 10/2020*, Presidenza del consiglio dei ministri, 16 aprile.

Gadotti A. (2020), *L'app Immuni non è sorveglianza di massa: un'analisi dei rischi tra fiducia e garanzie tecniche*, 17 giugno: https://www.valigiablu.it/app-immuni-coronavirus-analisi/

Greenfield A. (2017), *Tecnologie radicali*, Einaudi, Torino.

Harari Y. N. (2020), *Il mondo dopo il virus*, Internazionale, n. 1351, 27 marzo.

Li Z., Chen Q., Feng L. *et al.* (2020), *Active case finding with case management: the key to tackling the COVID-19 pandemic*, The Lancet, June 4: https://doi.org/10.1016/S0140-6736(20)31278-2.

Lisi A. (2020), Immuni, un disastro annunciato, Huffpost, 7 settembre: https://www.huffingtonpost.it/entry/il-disastro-annunciato-dellapp-immuni-e-delle-altre-app-di-tracing-dai-bug-alla-prigionia-gapple_it_5f560038c5b6946f3eb4bda3

Lombi L., Moretti V. (2020), Salute digitale e «big data» in sanità, in Cardano M., Giarelli G., Vicarelli G. (a cura di), *Sociologia della salute e della medicina*, il Mulino, Bologna.

Lyon D. (2018), *The Culture of Surveillance: Watching as a Way of Life*, Polity Press, Cambridge.

Marucci M. (2020*), Tecnologie digitali e controllo sociale ai tempi del Covid-19,* «*Menabò di Etica ed Economia*», 124 http://oa.inapp.org/xmlui/handle/123456789/672.

Melissari M., *Immuni e le altre app di contact tracing in Europa e nel mondo*, Internazionale, 25 giugno 2020, https://www.internazionale.it/notizie/laura-melissari/2020/06/25/app-immuni-contact-tracing-confronto-europa

Miniscalco M., *La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?*, Osservatorio costituzionale, Fasc. 3/2020, p. 10: https://www.osservatorioaic.it/it/osservatorio/ultimi-contributi-pubblicati/noemi-miniscalco/la-sorveglianza-attiva-per-contrastare-la-diffusione-dell-epidemia-di-covid-19-strumento-di-controllo-o-di-garanzia-per-i-cittadini

Mozure P., Zhong R., Krolik A. (2020), *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags*, New York Times, 7 agosto.
Pititto G. (2020), *La sfida delle app contro il covid-19*, GEOmedia n°1/2-2020, p.17.
Prensky M. (2001), *Digital Natives, Digital Immigrants Part 1*, «On the orizon», 9(5), pp.1-6.
Resta G. (2020), *La app 'Immuni': pregi e limiti del tracciamento digitale dei contatti*, Symposium: privacy and contact tracing, http://www.medialaws.eu/analyses/symposium-privacy-and-contact-tracing/
Salerno Aletta G., *Safetycracy, il nuovo paradigma del potere basato sulla protezione della vita*, Milano Finanza, 9 aprile 2020: https://www.milanofinanza.it/news/safetycracy-il-nuovo-paradigma-del-potere-basato-sulla-protezione-della-vita-202004091631205076.
Shwartz Altshuler T., Aridor Hershkovitz R. (2020), *Digital Contact Tracing And The Coronavirus: Israeli And Comparative Perspectives*, Foreign Policy at Brookings: https://www.brookings.edu/research/digital-contact-tracing-and-the-coronavirus-israeli-and-comparative-perspectives/.
Zunino G. (2020), *Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia)*: https://www.agendadigitale.eu/sicurezza/privacy/coronavirus-i-sistemi-per-tracciare-i-positivi-come-funzionano/