TRACCIAMENTO DIGITALE DEI CONTATTI

Giorgio Resta
Dipartimento di Giurisprudenza, Università degli Studi Roma Tre

Considerazioni introduttive

A distanza di quasi tre mesi dal lancio ufficiale della App Immuni, avvenuto nel giugno 2020, è opportuno non soltanto provare a fare un primo bilancio della sua esperienza applicativa, ma anche ragionare criticamente su alcuni nodi del rapporto tra tracciamento 'analogico' e tracciamento 'digitale' dei contatti che appaiono tuttora irrisolti e che continuano a essere dibattuti, in piena emergenza pandemica, nella maggior parte dei paesi occidentali. Elencherò di seguito alcuni degli interrogativi più urgenti, ai quali le pagine che seguono tenteranno di offrire, se non una risposta, almeno un primo inquadramento teorico, muovendo dalla prospettiva del giurista:

a) quale è il rapporto tra la tutela della riservatezza e il sistema di tracciamento dei contatti?
b) quali limiti discendono, sul piano procedurale e su quello sostanziale, dal diritto fondamentale alla protezione dei dati personali?
c) sarebbe astrattamente ammissibile una misura legislativa che imponesse l'adozione di una app di tracciamento dei contatti?
d) come valutare l'esperienza italiana del tracciamento digitale e quali proposte possono essere avanzate per il suo miglioramento?

Diritti della persona, tutela della riservatezza e tracciamento dei contatti

Il primo interrogativo proposto è quello relativo al rapporto tra il tracciamento dei contatti e la tutela della riservatezza, o controllo dei dati personali: rapporto armonico o necessariamente conflittuale?

Credo sia anzitutto necessario distinguere tra tracciamento "manuale" e tracciamento "digitale", due ipotesi ben diverse per i problemi che implicano, eppure spesso sovrapposte in maniera confusoria nelle pratiche discorsive.

Come ben chiarito nel Rapporto ISS-COVID-19 n. 59/2020, *Supporto digitale al tracciamento dei contatti (contact tracing) in pandemia: considerazioni di etica e di governance,* il primo è il metodo tradizionalmente seguito per prevenire e contenere la diffusione delle malattie infettive. Esso si basa su una serie di procedure collaudate, le quali vanno dall'intervista del caso indice, all'identificazione dei contatti stretti, alla classificazione del rischio, alla comunicazione con i soggetti coinvolti e alla prescrizione di misure di sorveglianza sanitaria, sino all'effettuazione di test diagnostici in caso di insorgenza di sintomi. (1)

Il secondo è il sistema sperimentato per la prima volta da alcuni paesi asiatici all'indomani dell'epidemia MERS e oggi diffuso pressoché ovunque. Esso si avvale dei *big data* al fine di ricostruire i contatti stretti di un soggetto diagnosticato con una patologia trasmissibile come il COVID-19 ed eventualmente monitorare il loro stato di salute, controllare il rispetto delle misure

di auto-isolamento, informare il pubblico in maniera anonima circa i luoghi frequentati e gli spostamenti dei soggetti positivi (2, 3).

Se la questione del bilanciamento è riferita al tracciamento manuale, la risposta è semplice. Benché sia indubbia una compressione del diritto alla protezione dei dati personali, nessuno dubiterebbe che una siffatta limitazione sia non soltanto legittima ma socialmente desiderabile. Il diritto alla protezione dei dati personali non è stato mai concepito in Europa come una sorta di diritto dominicale sulla propria sfera privata, ma ha sempre ricevuto una configurazione a geometria variabile in funzione della natura dei dati coinvolti e delle finalità del trattamento. Quando ci si trovi in presenza di un trattamento mirato al perseguimento di finalità di sostanziale interesse pubblico, quale l'individuazione dei soggetti a rischio e il contrasto a una pandemia, la compressione della sfera individuale deve ritenersi indubbiamente fondata su un'idonea base giustificativa ai sensi degli artt. 6 e 9 Regolamento (UE) 2016/679 (*General Data Protection Regulation*, GDPR), e dunque legittima.

In tal senso basti richiamare il chiaro dettato del considerando 46 GDPR, che attesta la liceità del trattamento mirato a "tenere sotto controllo l'evoluzione di epidemie e la loro diffusione"; nonché il considerando 112, che ammette a dirittura il trasferimento di dati all'estero ai sensi dell'art. 49 GDPR "in caso di ricerca di contatti per malattie contagiose", come ha ben evidenziato lo *European Data Protection Board* (EDPB) nelle linee guida sul *contact tracing* e in quelle sulla ricerca scientifica nel contesto pandemico (4, 5). In questa linea si è mosso, inoltre, il sistema normativo italiano dell'emergenza COVID-19, e in particolare l'art. 14 del decreto-legge 14/2020, ora art. 17-bis del decreto-legge 18/2020, poi convertito in legge, che ha ammesso entro ampi margini la comunicazione dei dati personali per finalità di contrasto alla pandemia.(6) Non potrebbe essere diversamente, perché il tipo di interferenze con la sfera personale delle quali discorriamo sono non soltanto limitate sul piano temporale e di contenuto, ma anche necessarie per il perseguimento dello scopo legittimo della tutela della salute. Dunque, siamo perfettamente all'interno del parametro di proporzionalità, la vera chiave di volta del sistema europeo di tutela dei diritti fondamentali.

Se invece il discorso si sposta sul tracciamento digitale, e non semplicemente sull'uso dell'automazione per rendere più rapido ed efficiente il processo tradizionale di intervista e identificazione dei contatti stretti da parte del personale sanitario[1] (7), la valutazione deve essere necessariamente più articolata.

È ben vero che le finalità del trattamento sono sempre quelle del contrasto alla pandemia e della tutela della salute. Come tali esse non possono che ritenersi pienamente legittime sul piano degli obiettivi perseguiti. Ciò che muta, tuttavia, è la natura dello strumento utilizzato, il quale non implica unicamente una più ampia e intensa interferenza con la sfera personale, la quale è già di per sé fonte dell'applicazione di uno specifico segmento di norme (es. l'art. 35 GDPR), ma soprattutto altera sul piano sistemico la natura stessa del *contact tracing*, che da relazione interpersonale fondata sul dialogo e la comprensione reciproca tra medico (intervistatore) e paziente si trasforma in un fenomeno governato parzialmente o esclusivamente – a seconda del tipo di architettura prescelta – dall'interazione asimmetrica tra uomo e macchina (8). Ne risultano sensibilmente modificati i termini generali del problema, che non possono essere ridotti esclusivamente alla questione del bilanciamento tra privacy e salute pubblica, ma debbono essere compresi alla luce del più ampio dibattito circa la crescente incidenza delle tecnologie sul modo in cui si assumono le decisioni pubbliche e sul modo in cui definiscono le relazioni intersoggettive (9, 10).

[1] Come nel caso del software Go.Data appositamente creato dall'Organizzazione mondiale della sanità, v. WHO, *Digital tools for Covid-19 contact tracing,* 2 giugno 2020.

Come tale, l'integrazione del sistema analogico con tecniche di tracciamento digitale è un passaggio che richiede di essere discusso con attenzione, misurando con attenzione costi (non soltanto economici) e benefici attesi di una scelta che non è socialmente neutra (11).

Costi e benefici del tracciamento 'digitale'

Sul piano empirico non esiste, com'è noto, un unico modello di tracciamento digitale, né è agevole delineare in astratto una sua versione 'idealtipica'. Esistono, al contrario, molte varianti, che differiscono sia per il tipo di architettura tecnologica adottata, sia per la tipologia e l'estensione dei dati trattati, sia per l'ampiezza del loro uso, sia infine per il grado di volontarietà o obbligatorietà dell'adesione al sistema medesimo.(12) In una mappa virtuale sarebbe possibile localizzare a un estremo il modello italo-tedesco di tracciamento tramite applicazioni per Bluetooth Low Energy incentrate sulla volontarietà dell'uso, sull'anonimato, sulla minimizzazione dei dati e costruite secondo un modello rigorosamente decentralizzato; e all'estremo opposto i modelli sudcoreano e cinese che, pur con notevoli differenze interne, optano per sistemi di tracciamento a carattere obbligatorio o semi-obbligatorio, consentono l'accesso ad uno spettro molto più ampio di dati (che non si limitano ai contatti di prossimità), ammettono la conservazione centralizzata e prevedono un ruolo proattivo delle autorità sanitarie e talora di polizia nell'individuazione dei contatti a rischio[2] (13).

Facendo astrazione dalle varianti empiriche e focalizzando l'attenzione – per il momento – sul tracciamento di prossimità attraverso tecnologia Bluetooth Low Energy, il sistema di tracciamento digitale presenta alcuni vantaggi indubitabili, al cospetto di una patologia, quale è il COVID-19, che risulta ampiamente suscettibile di trasmissione anche da parte di soggetti asintomatici. Tra questi vantaggi possono annoverarsi i seguenti: a) esso promette di supplire ai vuoti di memoria del soggetto interessato, che potrebbe non ricordare tutte le persone con le quali è entrato in contatto nel periodo epidemiologicamente rilevante; b) può portare ad emersione i contatti sconosciuti, con i quali la persona ha intrattenuto un rapporto a rischio, nel senso del superamento della soglia spaziale e temporale ritenuta sicura; c) abbatte i tempi di comunicazione con i contatti a rischio, supplendo peraltro al possibile divario linguistico (cosa che è particolarmente importante in contesti etnicamente e linguisticamente non omogenei), e dunque riduce il rischio di trasmissione del virus da parte delle persone asintomatiche; d) può facilitare il follow-up dei soggetti coinvolti da parte delle autorità sanitarie; e) è un sistema che, a regime, presenta minori oneri organizzativi – in termini finanziari e di risorse impiegate – rispetto alle tecniche tradizionali e segnatamente *paper-based*.

Quanto ai costi sociali del sistema in oggetto, essi variano sensibilmente ragione dell'architettura tecnologica e istituzionale prescelta (tipo di informazioni oggetto di trattamento; modalità della loro raccolta; durata della loro conservazione; possibilità di impiego diretto e secondario). Di conseguenza, qualsiasi valutazione sia di tipo etico sia di tipo giuridico

[2] Ad esempio, rientra a tutti gli effetti nella nozione di 'tracciamento digitale' il sistema adottato in Sud-Corea a partire dal 2015, quando a seguito dell'esperienza maturata con l'epidemia MERS, si è provveduto a modificare l'*Act on Infectious Diseases Prevention and Control.* Si è quindi prevista, con i nuovi artt. 34 bis e 76 bis, la possibilità di accedere – e poi divulgare in forma anonima per segnalare al pubblico gli spostamenti dei casi indice e i luoghi a maggior rischio di contagio – a una corposa mole di dati, quali i metadati di comunicazione, e in particolare i dati che permettono la geolocalizzazione dell'individuo, i dati relativi alle transazioni finanziarie, le immagini registrate dalle videocamere di sorveglianza, i dati desunti dalle cartelle cliniche (in tema v. L. Gyooho, *Legislative and Administrative Responses to COVID-19 Virus in the Republic of Corea,* April 28, 2020).

richiederebbe a rigore una previa definizione dell'oggetto dell'analisi, sicché anche in questo caso si limiterà convenzionalmente lo sguardo sul tracciamento di prossimità attraverso tecnologia BLE (14). Fra i costi attesi di un siffatto sistema, ovviamente varianti in ciascuna dimensione in funzione della concreta tipologia di tracciamento di prossimità, vi sono almeno i seguenti: a) continuo monitoraggio della sfera relazionale della persona da parte di autorità pubbliche o poteri privati; b) rischi in termini di integrità e sicurezza dei dati relativi ai contatti di prossimità; c) falsi positivi e falsi negativi derivanti dallo screening algoritmico del rischio; d) spersonalizzazione del rapporto tra medico (intervistatore) e paziente.

La valutazione comparativa dei suddetti costi e benefici evidenzierà esiti diversi a seconda delle discipline e dei saperi assunti a punto di riferimento dell'analisi: altra è, ad esempio, la prospettiva d'indagine dell'epidemiologo, quella dell'economista, quella del bioeticista o quella del giurista. Muovendo da quest'ultimo angolo visuale, si dovrà innanzitutto notare che i fattori appena evidenziati concorrono a definire i contenuti del giudizio di proporzionalità, il quale assume giuridicamente un rilievo cruciale ogniqualvolta si discuta dell'interferenza per motivi legittimi con un diritto fondamentale. Nel caso in esame, è il diritto alla protezione dei dati personali ad essere direttamente inciso dalla messa in atto di un sistema di tracciamento digitale. Per comprendere se l'interferenza possa ritenersi oggettivamente giustificata dallo scopo legittimo perseguito, è necessario sottoporre a disamina lo specifico congegno tecnologico adottato, avendo ben chiara la consapevolezza che livelli più capillari di sorveglianza (sotto il profilo del tipo di dati trattati, degli usi possibili di tali dati, delle modalità e della durata della conservazione) potranno risultare giustificabili soltanto a fronte di una dimostrabile maggiore efficacia delle misure di contrasto all'epidemia così rese possibili e della prova dell'assenza di misure alternative meno invasive per la sfera individuale.

Limiti procedurali e sostanziali derivanti dal diritto alla protezione dei dati personali

Diversi documenti e linee guida sovranazionali delineano un quadro di principi atti a concretizzare il suddetto giudizio di proporzionalità. In particolare, le linee guida dell'EDPB stabiliscono una serie di limiti di natura procedurale e sostanziale ai quali ci si dovrebbe conformare nella messa a punto di sistemi di tracciamento digitale[3] (4).

Fra i criteri di natura procedurale rientrano:
- presenza di una base giuridica idonea ai sensi del GDPR, consistente nel consenso dell'interessato o, preferibilmente, nella norma di legge (punto 29);
- chiara definizione *ex ante* delle finalità e dell'ambito oggettivo e soggettivo del trattamento (25, 26, 31);
- trasparenza dell'intero sistema e accessibilità del codice sorgente (punto 37);
- valutazione preventiva d'impatto del trattamento (39).

Fra i criteri di natura sostanziale possono annoverarsi:
- la volontarietà delle scelte circa l'utilizzo delle app di tracciamento (punto 24);
- il rispetto dell'anonimato dei dati di contatto (punto 27);
- l'esclusione ove possibile del ricorso ai dati di localizzazione (punto 27);

[3] *vedi anche* la Risoluzione del Parlamento Europeo, 17 aprile 2020 sull'azione coordinata dell'UE per lottare contro la pandemia di CoViD-19 e le sue conseguenze (n.2020/2616(RSP))

- limitazione della durata del trattamento al periodo strettamente necessario al contrasto della pandemia (punto 31, 35);
- esclusione di decisioni a carattere interamente automatizzato ai sensi dell'art. 22 GDPR (punto 36).

Avendo ben presente una siffatta cornice regolamentare, coonestata dagli interventi formali e informali dell'Autorità garante per la protezione dei dati personali, il legislatore italiano ha stabilito per legge i punti essenziali ai quali l'app nazionale di trattamento, poi individuata nella App Immuni, avrebbe dovuto conformarsi. (6)

Innanzitutto, merita di essere enfatizzata la scelta del governo di promuovere l'introduzione di una specifica disciplina legislativa del "sistema di allerta COVID-19". A ciò si è provveduto con l'art. 6 del decreto-legge 30 aprile 2020, n. 28, poi convertito dalla legge 25 giugno 2020, n. 70. La scelta, si diceva, merita un'espressa notazione, perché riflette l'intenzione di radicare il trattamento dei dati personali sulla base giuridica dell'interesse pubblico rilevante, ai sensi degli artt. 6, p.1, lett. *d*, *e,* e 9, par. 2, lett. *i* GDPR. Si tratta di una soluzione che, pur auspicata dall'EDPB, non era tecnicamente obbligata ai sensi del Regolamento. A riprova può citarsi il caso tedesco, dove è prevalsa la diversa volontà di sviluppare una app di tracciamento federale gestita dal Robert Koch Institut, senza tuttavia definire una previa cornice legislativa e facendo invece ricorso al consenso dell'interessato quale base giuridica del trattamento.(15) Il vantaggio dell'opzione prescelta nel nostro ordinamento consiste, oltre che in una maggiore trasparenza, in una riduzione dell'incertezza circa le modalità d'uso delle app di tracciamento, e segnatamente in ordine al suo carattere necessariamente volontario e all'assenza di conseguenze pregiudizievoli per il mancato utilizzo (art. 6, c. 4)[4] (16,17).

In secondo luogo, vengono ribaditi i limiti procedurali e sostanziali precedentemente indicati, ai quali si aggiunge l'espressa definizione del termine massimo di durata del trattamento, fissato nel 31 dicembre 2020, nonché il principio per cui i dati non possono essere trattati per finalità diverse da quella dell'allerta dei soggetti a rischio contagio. L'unica deroga ammessa è per l'utilizzo "in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica", (ai sensi degli artt. 5, par.1, lett. a) e 9, par. 2, lett. i) e j), del GDPR). È opportuno notare che la norma individua nel Ministero della Salute il soggetto titolare del trattamento e chiamato a redigere la valutazione d'impatto ai sensi dell'art. 35 GDPR. Questa è stata notificata al Garante sul finire di maggio 2020, una volta definita l'architettura tecnologica della App Immuni, che come è noto si è conformata al modello decentralizzato DP-3T (2)e si è avvalsa della piattaforma di programmazione elaborata da Apple e Google.

App di tracciamento dei contatti: un primo bilancio pratico

Quali risultati ha sin qui sortito la App Immuni? Iniziamo con l'osservare che è difficile esprimere una valutazione pienamente informata in assenza di dati ufficiali aggiornati, che le istituzioni italiane competenti esitano a mettere a disposizione del pubblico e della comunità degli

[4] Non a caso in Germania il punto oggi maggiormente discusso è quello relativo alla possibile obbligatorietà dell'uso della app, specialmente in ambito lavoristico: C. Sander – S. Hilberg – S. Bings, *Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19, COVur,* 2020, 347; *Corona-Warn-App startet mit Lob und Diskussion um gesetzliche Grundlage, Becklink 2016602*.

studiosi. Compulsando i siti Internet del Ministero della Salute e del Ministero dell'Innovazione non è possibile reperire cifre aggiornate circa i download e le notifiche di allerta rilasciate da Immuni (o quanto il numero di codici di sblocco emessi dalle autorità sanitarie). Si trovano riferimenti a una risposta ad interpellanza parlamentare del Ministro Pisano, con dati ormai obsoleti. Non è diversa la situazione prendendo in esame il sito Internet di Immuni (www.immuni.italia.it), mentre le uniche statistiche aggiornate relativamente al numero dei download possono desumersi dall'account Twitter di Immuni.

Tutto ciò non va a vantaggio della trasparenza, né delle stesse chances di promozione della app di tracciamento, come può desumersi *a contrario* dalla ben diversa esperienza tedesca. Il sito Internet del Robert Koch Institut, titolare e gestore per conto del Governo della "Corona-Warn App" contiene statistiche quotidianamente aggiornate circa il numero dei download (divisi per stores di riferimento), il numero delle richieste inoltrate alla apposita hotline telefonica, nonché il numero dei codici rilasciati per l'inoltro delle notifiche di allerta[5].

Il censurabile ritardo sul piano delle politiche di comunicazione, oltre a riflettere una scarsa attenzione per il valore della trasparenza, rende altamente incerta qualsiasi valutazione sull'efficacia della app medesima. A giudicare, tuttavia, dai dati riportati nell'account Twitter di Immuni e in alcuni resoconti giornalistici, i risultati sin qui conseguiti debbono essere ritenuti insoddisfacenti. Si stima, infatti, che alla fine di Agosto 2020, dopo circa tre mesi dal lancio della app, il numero di download si aggiri intorno ai 5 milioni, cioè meno del 10% degli italiani, un risultato ben al di sotto delle aspettative. Si tratta, peraltro, di una cifra approssimata per eccesso, perché non considera gli utenti che, dopo aver effettuato il download, hanno proceduto alla disinstallazione della app dal proprio dispositivo (il che, relativamente alle app, avviene in una proporzione molto elevata di casi). Siamo in ogni caso ben lontani dalle soglie minime di utilizzazione ritenute necessarie, ad avviso di diversi studi indipendenti, al fine di assicurare l'efficacia dello strumento tecnologico.

Quali possono essere le cause di una risposta sin qui non esaltante da parte del pubblico?

Esse sono senza dubbio composite.

Mette conto notare, innanzitutto, che a livello globale i tassi di utilizzazione volontaria di tali strumenti raramente superano il 20/25% della popolazione. La Germania, che ha fortemente investito in comunicazione (la stessa Cancelliera Merkel è più volte intervenuta in proposito), ha raggiunto quota 17 milioni di download, pari a circa il 20% della popolazione. La Francia, per contro, è ferma intorno ai 2,5 milioni di download, per una quota pari a poco più del 3% della popolazione. Il nostro paese si trova in posizione mediana, ma ben lungi dal poter annoverare tale strumento tra le misure più efficaci nel contrasto all'epidemia.

Inoltre, non si può trascurare che il lancio della app è avvenuto in un periodo successivo al picco epidemico e in una fase di graduale declino dell'emergenza. Sul piano del *framing effect*, per mutuare la terminologia delle scienze comportamentali, mancavano le condizioni ottimali perché si potesse contare sull'elemento emozionale e su una più naturale propensione – dettata da altruismo o paura – all'adozione di una siffatta misura preventiva. Non è escluso che, a seguito della risalita del tasso dei contagi e nel caso in cui dovesse concretizzarsi l'ipotesi paventata di una seconda ondata, anche il numero dei download sarà destinato proporzionalmente ad aumentare.

Vi sono poi le già rilevate pecche sul piano della comunicazione pubblica, che hanno probabilmente contribuito a consolidare le già esistenti perplessità – non fugate dall'adozione di un modello iper-garantistico quale quello decentralizzato – circa i rischi derivanti da qualsiasi sistema di sorveglianza, sia esso promosso dal potere pubblico o dal potere privato.

[5] https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Kennzahlen.pdf?__blob=publicationFile

Infine, non possono sottostimarsi i difetti di natura tecnica insiti nel modello delle app per smartphone che funzionano attraverso la tecnologia BLE. Essi sono ben chiariti nel Rapporto ISS COVID-19 n. 54/2020, *Tecnologie a supporto del rilevamento della prossimità: riflessioni per il cittadino, i professionisti e gli stakeholder in era COVID-19*, e attengono sia alla scarsa precisione delle misurazioni tramite Bluetooth, sia alla necessità di disporre di sensori di ultima generazione, non sempre presenti negli smartphone di fascia più bassa, sia in generale alla limitata adattabilità dei dispositivi di telefonia mobile per i fini di allerta del rischio.

Alcune proposte di riforma

Considerata l'esperienza sin qui non esaltante delle app di tracciamento, è utile interrogarsi su quali possano essere alcune alternative praticabili, o quantomeno delle proposte migliorative rispetto al modello in atto.

Per rispondere al problema della scarsa diffusione dello strumento in oggetto, si è suggerito, nella convinzione della sua utilità, di renderlo obbligatorio, di per sé o quale precondizione per l'accesso a luoghi pubblici o aperti al pubblico. Benché gli obiettivi di una siffatta proposta siano commendevoli e non se ne possa contestare sul piano etico l'accettabilità, dal punto di vista giuridico essa non appare allo stato praticabile. Ciò per due diversi ordini di ragioni.

In primo luogo, il carattere obbligatorio della app di tracciamento implicherebbe una interferenza con il diritto fondamentale alla protezione dei dati personali. Questa sarebbe volta a perseguire scopi legittimi e potrebbe contare, per ipotesi, su una base di legge. Tuttavia, è difficile ritenere che le misure adottate siano proporzionate rispetto allo scopo legittimo perseguito, in quanto non soltanto la loro efficacia è discussa, ma sarebbero ipotizzabili misure alternative più efficaci e meno invasive per la sfera personale, come i microchip associati a dispositivi meno sensibili degli smartphone, come i *wearable*.

In secondo luogo, l'obiezione principale che potrebbe muoversi alla proposta in oggetto è quella desunta dal principio di eguaglianza. Considerato che non tutti i cittadini possiedono uno smartphone e che tra questi non tutti godono di competenze tecnologiche adeguate, subordinare l'accesso a luoghi o servizi pubblici all'utilizzo di una app di tracciamento risulterebbe irrimediabilmente in contrasto con l'art. 3 Cost.

Se si è fermamente convinti dell'utilità e dell'efficacia dello strumento (premessa che qui si esprime in senso dubitativo per le ragioni indicate dappresso), sembrerebbe più coerente con le coordinate normative del nostro ordinamento porre mano a una politica pubblica di informazione e comunicazione ben più convinta ed efficace di quella sinora posta in atto. Il paragone che mi sembra più appropriato è quello delle politiche di reperimento degli organi per trapianto: è dimostrato da diversi studi che il tasso di donazione aumenta sensibilmente per effetto di campagne comunicative mirate atte a sollecitare l'attitudine solidaristica dei soggetti coinvolti. Una strategia appropriata dovrebbe consistere da un lato nell'incremento della trasparenza generale del sistema, secondo modalità analoghe a quelle adottate in Germania, e dall'altro nell'insistenza da parte delle massime cariche istituzionali sulla necessità di un contributo proattivo del pubblico, nelle forme di una sorta di destinazione solidaristica dei dati personali. Non mi parrebbe incongrua, da questo punto di vista, la previsione di incentivi di carattere non monetario all'utilizzazione della app pubblica. Si è proposto, ad esempio, di concedere priorità nell'accesso al tampone, a parità di condizioni cliniche a coloro i quali consentano l'installazione della app di tracciamento [6].

[6] In questo senso, si veda l'intervista al Prof. A. Crisanti, in Corriere.it, 30 agosto 2020.

Direttamente connesso alla questione appena accennata, è un secondo profilo di criticità del sistema di allerta al rischio come sin qui strutturato. Fondamentalmente esso si basa sull'assunto della sostanziale indipendenza tra il sistema analogico di tracciamento dei contatti e quello digitale: il primo nella piena responsabilità delle autorità sanitarie, chiamate a interagire personalmente con un soggetto positivo, al fine di reperire tutte le informazioni utili all'identificazione dei contatti, alla valutazione del rischio di contagio, oltre che all'adozione di tutte le misure diagnostiche e terapeutiche utili alla tutela della salute dell'interessato; il secondo in larga parte rimesso al potere predittivo dell'algoritmo, programmato in modo tale da effettuare in piena indipendenza la valutazione del rischio di contagio sulla base di parametri spaziali e temporali predefiniti, nonché alla autonomia decisionale del destinatario di un alert, libero di scegliere se contattare il medico di medicina generale per l'assunzione delle misure più appropriate (le quali soltanto da quel momento acquisiranno carattere obbligatorio). Com'è evidente, nel secondo caso l'autorità sanitaria è di fatto esautorata dal processo di identificazione e comunicazione con i contatti a rischio, non avendo accesso né ai dati di prossimità conservati in maniera anonima nei dispositivi mobili di ciascun utente, né ai dati di localizzazione, per espressa scelta normativa sottratti alla raccolta. Di conseguenza viene a mancare qualsiasi filtro preventivo atto a validare, tramite l'ausilio dei dati di contesto derivanti dalla comunicazione orale e dal riscontro con altre risultanze, l'attendibilità della valutazione di rischio effettuata dal software sulla base dei parametri ab origine immessi nel sistema, senza alcuna considerazione delle circostanze specifiche del singolo contatto. Di qui la possibilità – ribadita nel Rapporto ISS COVID-19 n. 59/2020 *Supporto digitale al tracciamento dei contatti (contact tracing) in pandemia: considerazioni di etica e di governance,* p. 15 (8) – di falsi positivi, che nella consapevolezza della probabilità di misure di isolamento sino al risultato del tampone nasofaringeo, possono concretamente disincentivare l'uso della app.

Questa impostazione è comprensibile ragionando esclusivamente nell'ottica della tutela dei diritti individuali, e in particolare della tutela del diritto alla protezione dei dati personali. Essa, come si è detto, riflette le indicazioni dell'EDPB e di alcune autorità garanti nazionali, preoccupati di evitare qualsiasi forma di sorveglianza continuativa sulla sfera personale. Tuttavia, è bene porsi apertamente l'interrogativo se in questo modo non si privi il sistema sanitario di una misura potenzialmente molto efficace per l'obiettivo della tutela della vita e della salute degli altri consociati. Se i dati di prossimità o di geolocalizzazione potessero essere volontariamente e selettivamente riversati nel parco informativo a disposizione delle autorità sanitarie incaricate del tracciamento, queste avrebbero maggiori elementi per contattare rapidamente i contatti stretti, valutando con l'ausilio dell'intervista orale il grado reale di esposizione al rischio in relazione alle condizioni del contatto, quali ad esempio il luogo aperto o chiuso, il tono di voce del colloquio, l'utilizzo di dispositivi di protezione adeguati. Tutti fattori, questi ultimi, che sfuggono alle capacità d'analisi dell'algoritmo.

Il tema di fondo che emerge da queste premesse è il potenziale solidaristico insito nell'accesso ai dati personali per finalità di contrasto dell'epidemia, il quale invece rischia di risultare depotenziato nel modello decentralizzato di allerta del rischio. È chiaro che quest'ultimo persegue l'obiettivo di mantenere un livello molto alto di tutela dei dati e prevenire i rischi di violazione dell'integrità sistemi informatici contenenti informazioni estremamente sensibili. In poche parole, esso si ispira al modello della sovranità individuale sui dati, ma al prezzo di costruire un complicato congegno poco efficace sul piano operativo per le ragioni appena ricordate e incapace di soddisfare le esigenze di accesso a un parco comune di informazioni per finalità di interesse pubblico e tutela della salute (18). Che il sistema possa essere radicalmente ripensato è da escludere per molte ragioni, non ultima la posizione di ferma chiusura nei confronti di qualsiasi ipotesi di 'socializzazione' dei dati espressa dai giganti dell'informazione quali Google e Apple, che controllando il canale decisivo delle piattaforme di accesso alle app, in aggiunta ad altri fattori

decisivi per l'interoperabilità e la funzionalità delle app medesime, mantengono l'ultima parola circa le chances concrete di successo di qualsiasi soluzione tecnologica proposta. Il modo in cui in questi mesi tali multinazionali hanno letteralmente imposto ai governi nazionali il modello decentralizzato, spingendo persino la Germania a fare marcia indietro rispetto all'ipotesi iniziale della conservazione centralizzata, conferma la sostanziale impossibilità di reindirizzare su diversi binari – magari meno vantaggiosi per le imprese private sul piano dei rapporti di mercato - il sistema delle app di tracciamento su dispositivi mobili (19). Ciò non toglie che debbano essere considerate ipotesi alternative, che permettano di migliorare o sostituire il sistema esistente, sia nell'immediato sia in vista di possibili ulteriori eventi pandemici.

Dal primo punto di vista meriterebbe di essere attentamente considerato il sistema sperimentato nello stato del Rhode Island, dove è stata sviluppata una App – Crush COVID RI – che permette di tenere traccia dei dati di localizzazione comunque raccolti dallo smartphone tramite l'utilizzazione di altre funzionalità (es. app di navigazione, comunicazione o fitness) nel periodo epidemiologicamente rilevante di 20 giorni (20). In caso di accertata positività al tampone, l'individuo ha la possibilità, per libera e insindacabile scelta, di condividere tali dati con le autorità sanitarie pubbliche per fini di ricostruzione dei luoghi frequentati, dei contatti a rischio e dei possibili focolai di trasmissione del contagio. Si tratta di un modello interessante perché configura una sorta di destinazione solidaristica dei dati personali, vincolata nelle modalità e negli scopi al perseguimento dei fini di contrasto dell'epidemia e tutela della salute pubblica, e che potrebbe trovare una solida base normativa nell'art. 5 della Direttiva 2002/58/CE, che configura il consenso dell'interessato come requisito per il trattamento dei dati di comunicazione.

Dal secondo punto di vista, si moltiplicano le proposte volte a sostituire lo smartphone con dispositivi alternativi e meno invasivi per la sfera personale, come microchip e token, esclusivamente dedicati al tracciamento digitale e finalizzati a raccogliere informazioni accessibili esclusivamente dalle autorità sanitarie in caso di positività. Tale soluzione, verso cui sembra indirizzarsi Singapore dopo il fallimento dell'esperienza con la app di tracciamento[7], avrebbe il vantaggio di dissociare il tracciamento dalle altre funzionalità di uno smartphone, riducendo i problemi tecnici (quale il consumo di batteria e l'inadeguatezza dei sensori presenti sui dispositivi meno aggiornati) e la mole di dati e metadati così resi accessibili ai fornitori delle app e dei sistemi operativi. Si tratta inoltre di una soluzione economica – essendo il costo di tali dispositivi limitato a una decina di euro – e potenzialmente in grado di assicurare misurazioni più precise e attendibili.

Bibliografia

1. World Health Organization. *Contact tracing in the context of COVID-19: interim guidance.* Geneva: WHO; 2020.
2. Giansanti D, D'Avenio G, Rossi M, Spurio A, Bertinato L, Grigioni M. *Tecnologie a supporto del rilevamento della prossimità: riflessioni per il cittadino, i professionisti e gli stakeholder in era COVID-19. Versione del 31 maggio 2020.* Roma: Istituto Superiore di Sanità; 2020. (Rapporto ISS COVID-19 n. 54/2020).
3. G. Resta, *La protezione dei dati personali nel diritto dell'emergenza COVID-19.* Editoriale. *Giustizia Civile.com*. 5 maggio 2020.
4. European Data Protection Board. *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*. Brussels: EDPB; 2020. Disponibile all'indirizzo:

[7] https://health.ri.gov/covid/crush/.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; ultima consultazione 20/12/2020.

5. European Data Protection Board. *Guidance n. 3/2020 on the processing of health data for the purpose of scientific research in the context of the Covid-19 outbreak*. Brussels: EDPB; 2020. Disponibile all'indirizzo: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdata scientificresearchcovid19_it.pdf; ultima consultazione 20/12/2020.
6. Poletti D. Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza. *Persona e mercato* 2020;2:65-76. Disponibile all'indirizzo http://www.personaemercato.it/wp-content/uploads/2020/06/Poletti.pdf; ultima consultazione 20/12/2020.
7. World Health Organization. *Digital tools for COVID-19 contact tracing: annex: contact tracing in the context of COVID-19*. Geneva: WHO; 2020.
8. Gruppo di lavoro ISS Bioetica COVID-19. *Supporto digitale al tracciamento dei contatti (contact tracing) in pandemia: considerazioni di etica e di governance. Versione del 17 settembre 2020*. Roma: Istituto Superiore di Sanità; 2020 (Rapporto ISS COVID-19 n. 59/2020)
9. Rodotà S. *Tecnologie e diritti*. Bologna: Il Mulino; 1997.
10. Resta G. Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza. *Pol Dir* 2019:199.
11. Deffains B, Perroud T. L'arbitrage entre les bénéfices et les coûts semble avoir été omis ou n'a pas été rendu public. *Le Monde* 15 maggio 2020.
12. Kahn JP (Ed.). *Digital contact tracing for pandemic response. Ethics and governance guidance*. Baltimore: Johns Hopkins University Press; 2020.
13. Gyooho L. Legislative and Administrative Responses to COVID-19 Virus in the Republic of Corea. *SSRN* 2020. Disponibile all'indirizzo: https://dx.doi.org/10.2139/ssrn.3587595.
14. Cho H, Ippolito S,You WY. Contact tracing mobile apps for COVID-19: privacy considerations and related trade-offs. *arXiv 2020*; 2003.11511. Disponibile all'indirizzo: https://arxiv.org/abs/2003.11511; ultima consultazione 20/12/2020.
15. Blaeser M, Dos. Santos Firnhaber C. Corona-Warn-App. Tracking & Tracing: Fluch oder Segen der Digitalisierung des Gesundheitsmanagements? *RDG* 2020;17(4): 173-280
16. Sander C, Hilberg S, Bings S. Arbeitsschutzrechtliche Fürsorge- und Schutzpflichten sowie Haftungsrisiken für Arbeitgeber im Zusammenhang mit COVID-19. *COVuR*, 2020: 347.
17. Redaktion beck-aktuell. Corona-Warn-App startet mit Lob und Diskussion um gesetzliche Grundlage. *Beck-Aktuell Heute Im Recht* 16.6.2020 Disponibile all'indirizzo: https://rsw.beck.de/aktuell/daily/meldung/detail/corona-warn-app-startet-mit-lob-und-diskussion-um-gesetzliche-grundlage; ultima consultazione 20/12/2020.
18. Wendehorst C. Covid-19 Apps and Data Protection. In: Hondius E, *et al*. (Ed.) *Coronavirus and the law in Europe*. Cambridge: Intersentia; 2020. Disponibile all'indirizzo: https://www.comparativecovidlaw.it/2020/09/02/covid-19-apps-and-data-protection/.
19. Sharon T. Blind-sided by privacy? Digital contact tracing, the Google/Apple API and big tech's newfound role as global health policy makers, *Ethics and information technology* 2020; 18:1-30. Disponibile all'indirizzo: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7368642/; ultima consultazione 20/12/2020.
20. Geddie J, Aravindan A. Singapore plans wearable virus-tracing device for all. *Reuters* 5.6.2020. Disponibile all'indirizzo: https://www.reuters.com/article/us-health-coronavirus-singapore-tech/singapore-plans-wearable-virus-tracing-device-for-all-idUSKBN23C0FO; ultima consultazione 20/12/2020.