dossier

XVIII legislatura

TRACCIAMENTO DI CONTATTI

Elementi di documentazione

(aggiornato al 4 maggio 2020)

maggio 2020
n. 242/1

servizio studi del Senato

ufficio ricerche sulle questioni istituzionali, sulla giustizia e sulla cultura

SERVIZIO STUDI
TEL. 066706-2451
studi1@senato.it

I dossier del Servizio studi sono destinati alle esigenze di documentazione interna per l'attività degli organi parlamentari e dei parlamentari. I testi e i contenuti normativi ufficiali sono solo quelli risultanti dagli atti parlamentari. Il Senato della Repubblica declina ogni responsabilità per la loro eventuale utilizzazione o riproduzione per fini non consentiti dalla legge. I contenuti originali possono essere riprodotti, nel rispetto della legge, a condizione che sia citata la fonte.

XVIII legislatura

TRACCIAMENTO DI CONTATTI

Elementi di documentazione

(aggiornato al 4 maggio 2020)

maggio 2020
n. 242/1

Classificazione Teseo: Epidemie. Sanità pubblica. Tutela della riservatezza (dati sensibili e personali, privacy, sistemi informativi personali)

INDICE

Sito del Ministro per l'innovazione tecnologica e la digitalizzazione (MID)

Un aggiornamento sull'applicazione di *contact tracing* digitale per l'emergenza coronavirus https://innovazione.gov.it/un-aggiornamento-sull-applicazione-di-contact-tracing-digitale-per-l-emergenza-coronavirus/ ..... Pag. 3

Task force dati, le relazioni delle attività dei gruppi che hanno valutato le app https://innovazione.gov.it/task-force-dati-le-relazioni-delle-attivita-dei-gruppi-che-hanno-valutato-le-app/ ..... " 9

Task force, Gruppo 6 (Tecnologie per il governo dell'emergenza) si è occupato della valutazione di tecnologie per permettere la tutela della salute pubblica insieme al ripristino delle condizioni per le attività economiche e sociali e per la tutela delle libertà e dei dati personali (libertà di circolazione e privacy)

- Relazione conclusiva ..... " 11
- Sintesi della Relazione conclusiva..... " 49
- Allegato tecnico..... " 57

Task force, Gruppo 8 (Profili giuridici della gestione dei dati connessa all'emergenza) che si è occupato di valutare l'impatto delle soluzioni tecnologiche per quanto riguarda il rispetto della privacy e di altri diritti fondamentali

- Relazione conclusiva .....
- Relazione sulla proposta "CovidApp - Covid Community Alert" " 77
  del gruppo "Coronavirus Outbreak Control" ..... " 91
- Relazione sulla proposta "Immuni" di BendingSpoons ..... " 95

Sito del Garante per la protezione dei dati personali

Garante per la protezione dei dati personali. Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19. 29 aprile 2020 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9328050> ..... " 101

Garante per la protezione dei dati personali**.** Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro *data-driven* per l'emergenza COVID-19. 7 aprile 2020 <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316821#>..... " 105

Articoli

Attardi G. - Marino N. - Santus E., *Contact tracing*, perché è così importante contro il covid (anche in Italia), *Agendadigitale.eu.* 21 aprile 2020 <https://www.agendadigitale.eu/sicurezza/privacy/contact-tracing-perche-e-cosi-importante-contro-il-covid-anche-in-italia/ >..... " 111

Ballaguer Callejon F., *Social network*, società tecnologiche e democrazia. *Nomos.* [Anticipazioni n.1 del 2020 – Problemi giuridici dell'emergenza Coronavirus] <http://www.nomos-leattualitaneldiritto.it/nomos/francisco-ballaguer-callejon-social-network-societa-tecnologiche-e-democrazia/ >..... " 115

Carloni E., "Fisime per la *privacy*"? Protezione dei dati personali e interesse pubblico nella pandemia. *ASTRID*. 24 marzo 2020. *Astrid online* e *Ridiam.it* <https://ridiam.it/le-istituzioni-dopo-la-crisi/>..... " 135

Clarizia P. e Schneider E., Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19. *IRPA - Osservatorio sullo Stato digitale*. 19 aprile 2020 < https://www.irpa.eu/luci-e-ombre-sulla-procedura-di-selezione-di-immuni-lapp-del-governo-di-tracciamento-del-contagio-da-covid-19/ > " 147

*Contact tracin*g e tutela della *Privacy* al tempo del Covid-19: è giusto controllare gli spostamenti dei cittadini attraverso la rete cellulare? *dirittodell'informatica.it* (redazione). 27 marzo 2020 <http://www.dirittodellinformatica.it/privacy-e-sicurezza/contact-tracing-e-tutela-della-privacy-al-tempo-del-covid-19-e-giusto-controllare-gli-spostamenti-dei-cittadini-attraverso-la-rete-cellulare.html >..... " 151

De Falco D. e Maddalena M.L., La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia. *Federalismi.it*. 28 marzo 2020 <https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41629 >..... " 155

De Martin J.C. (Co-direttore del Centro Nexa del Politecnico di Torino), App per il tracciamento: otto regole da rispettare. *La Stampa*. 21 aprile 2020. <https://www.lastampa.it/topnews/lettere-e-idee/2020/04/21/news/app-per-il-tracciamento-otto-regole-da-rispettare-1.38742237>..... " 167

De Minico G., Virus e algoritmi. Impariamo da un'esperienza dolorosa. *laCostituzione.info*. 1° aprile 2020. <http://www.lacostituzione.info/index.php/2020/04/01/virus-e-algoritmi-impariamo-da-unesperienza-dolorosa/>..... " 168

Della Morte G., La tempesta perfetta covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa. *SIDIblog - Forum Covid-19*. 19 marzo 2020. <http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/> ..... " 172

Dominioni S., Nel ginepraio delle app di tracciabilità. *ISPI online*. 24 aprile 2020 <https://www.ispionline.it/it/pubblicazione/nel-ginepraio-delle-app-di-tracciabilita-25873 >..... " 179

Farina M., La *data protection* ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio. *BioLaw Journal – Rivista di BioDiritto* [in corso di pubblicazione] https://www.biodiritto.org/content/download/3802/45351/version/1/file/28+Farina.pdf >..... " 183

Ferla V., Per governare l'epidemia (e non uccidere il paese) serve il digitale. *Fondazione PER - Progresso Europa Riforme* [estratto da: Quaderno 6: Come si governa un'epidemia: sulle tracce del Coronavirus]. 1° aprile 2020. < https://perfondazione.eu/per-governare-lepidemia-e-non-uccidere-il-paese-serve-il-digitale/ >..... " 189

Il *contact tracing* via app: quale strategia usare. *Wired* (redazione), 20 aprile 2020 <https://www.wired.it/attualita/tech/2020/04/20/il-contact-tracing-via-app-quale-strategia-usare/>..... " 195

Micozzi F.P., Le tecnologie, la protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito *BioLaw Journal – Rivista di BioDiritto* [in corso di pubblicazione]. 15 marzo 2020.<https://www.biodiritto.org/content/download/3780/45269/version/1/file/13+Micozzi.pdf >..... " 205

Miniscalco N., La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?. *Osservatorio AIC*: 3/2020, 21 aprile 2020 < https://www.osservatorioaic.it/images/rivista/pdf/2020_3_08_Miniscalco.pdf >..... " 213

Mirabelli C, L'app per legge e a tempo. *Avvenire*. [Intervista di A. Picariello]. 24 aprile 2020. <https://www.avvenire.it/attualita/pagine/a-tempo-e-controllata-dal-parlamento-solo-cos-lapp-tuteler-salute-e-diritt >..... " 235

Schneider E., "Immuni", l'app del governo per il tracciamento del contagio da Covid-19. *IRPA - Osservatorio sullo Stato digitale*. 19 aprile 2020 < https://www.irpa.eu/immuni-lapp-del-governo-per-il-tracciamento-del-contagio-da-covid-19/ >..... " 239

Soro A., Le app degli spostamenti solo su base volontaria. *Il Mattino*. 17 aprile 2020 [Intervista di V. Di Giacomo] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9317512 >..... " 243

Soro A., "Sì al tracciamento dei contatti ma con un decreto temporaneo". *La Repubblica*. 26 marzo 2020 [Intervista di A. Iannuzzi] <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9299193 >..... " 245

Suna K. e Vibouda C., Impact of contact tracing on SARS-CoV-2 transmission. *The Lancet*. 27 aprile 2020. <https://doi.org/10.1016/S1473-3099(20)30357-1>..... " 247

Tropea G., Il *contact tracing* digitale e l'epidemia: sindrome cinese?. *laCostituzione.info*. 9 aprile 2020 <http://www.lacostituzione.info/index.php/2020/04/09/il-contact-tracing-digitale-e-lepidemia-sindrome-cinese/ >..... " 249

Tsiouras I., App Immuni, tra sicurezza e *privacy*: i presupposti per una reale efficacia del tracciamento. *Cybersecurity360*, 23 aprile 2020 < https://www.cybersecurity360.it/legal/privacy-dati-personali/app-immuni-tra-sicurezza-e-privacy-i-presupposti-per-una-reale-efficacia-del-tracciamento/>..... " 253

Zunino G., Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia). *Agendadigitale.eu.* 23 aprile 2020. <https://www.agendadigitale.eu/sicurezza/privacy/coronavirus-i-sistemi-per-tracciare-i-positivi-come-funzionano/ >..... " 263

Sito del Ministro per l'innovazione tecnologia e la digitalizzazione (MID)

Un aggiornamento sull'applicazione di contact tracing digitale per l'emergenza coronavirus

Dalla nascita della task force alla valutazione delle tecnologie: il percorso compiuto finora sull'applicazione per contrastare la diffusione del virus.

Lo scorso 31 marzo hanno preso il via i lavori del gruppo di lavoro istituito dal Ministro per l'Innovazione Tecnologica e la Digitalizzazione in accordo con il Ministero della Salute per valutare e proporre soluzioni tecnologiche basate sull'analisi dei dati e affrontare l'emergenza sanitaria, sociale e economica legata alla diffusione del virus SARS-CoV-2 in Italia. Il gruppo di lavoro è composto da un contingente multidisciplinare di 74 esperti, scelti in collaborazione con il Ministero della Salute, l'Istituto Superiore di Sanità e l'Organizzazione Mondiale della Sanità. In ragione delle rispettive autonomie, Autorità Garante della Concorrenza e del mercato, Autorità per le Garanzie nelle Comunicazioni e Autorità Garante per la protezione dei dati personali non partecipano direttamente ai lavori e forniscono pareri su questioni relative a proprie competenze. I componenti del gruppo di lavoro, diviso in otto sottogruppi con diversi campi di ricerca, sono stati individuati in base a comprovata esperienza nelle rispettive discipline di riferimento e partecipano all'attività a titolo gratuito. Il compito del gruppo di lavoro è individuare e valutare soluzioni tecnologiche basate sui dati che possano essere utili al Governo e ad alle altre istituzioni nel definire politiche di contenimento del contagio da coronavirus e da realizzare anche a emergenza terminata.

Una ricognizione preliminare sull'eventuale tracciamento dei contatti, il *contact tracing*, è stata fin dall'inizio una delle priorità identificate insieme con il Ministro della Salute. Si tratta infatti di una delle azioni di sanità pubblica utilizzate in precedenza all'estero per prevenire la diffusione di alcune malattie infettive e potrebbe rappresentare un elemento importante in una strategia post-emergenza. Qualora determinazioni di Governo e Parlamento permettessero di renderlo operativo, il *contact tracing* potrebbe aiutare a identificare individui potenzialmente infetti prima che emergano sintomi e, se condotto in modo sufficientemente rapido, potrebbe impedire la trasmissione successiva del virus dai casi secondari.

Gli standard di tracciamento manuale dei contatti forniti dall'European Center for Disease Prevention and Control (ECDC) nel marzo 2020 relativamente all'epidemia di coronavirus indicano tuttavia in 12 ore il tempo medio per ogni operazione di *contact tracing*. L'operazione richiede l'utilizzo di tre unità di personale specializzato. Il suo tasso di successo è peraltro insufficiente a identificare tutti i contatti del soggetto che ha contratto il virus o comunque a ridurre il numero di contatti secondari infettati non identificati e isolati sotto l'unità. Dunque, la soluzione manuale non assicura di interrompere la riproduzione epidemica.

L'uso della tecnologia in ambito di *contact tracing* sarebbe in grado di dare un contributo rilevante a un "tracciamento di prossimità" molto più efficiente e rapido di quello tradizionale. La tecnologia per il tracciamento dei contatti potrebbe essere adottata in modalità compatibili con le necessità di rispettare diritti e libertà fondamentali dei cittadini sanciti dalla Costituzione.

In una direzione che può soddisfare queste esigenze si sono mosse a livello europeo diverse iniziative (PEPP-PT, DP-3T, ROBERT, etc.) che mirano a definire standard tecnologici per realizzare una soluzione tecnica che renda possibile il tracciamento di contatti tramite smartphone basato su codice libero e open source, nel pieno rispetto del diritto alla privacy dei cittadini. Più recentemente anche Apple e Google hanno annunciato un'iniziativa congiunta che prevede il rilascio di un sistema di contact tracing decentralizzato ed integrato nelle loro piattaforme in linea con molti dei principi dei progetti europei.

Il 15 aprile 2020, inoltre, la Commissione europea ha pubblicato le linee guida per la realizzazione di applicazioni finalizzate al tracciamento dei contagi (Mobile applications to support contact tracing in the EU's fight against COVID-19 - Common EU Toolbox for Member States). In esse la Commissione ha affermato che "*le app mobili hanno il potenziale per rafforzare le strategie di tracciamento dei contatti personali, che sono necessarie a contenere e invertire il corso della diffusione del Covid-19*". La Commissione ha aggiunto: "*Gli Stati membri dell'Ue stanno convergendo su soluzioni efficaci, basate su app che minimizzano il trattamento dei dati personali; riconoscono inoltre che l'interoperabilità tra queste app può non solo aiutare i servizi sanitari nazionali ma anche facilitare la riapertura delle frontiere interne dell'Ue*".

Con tempestività rispetto ad altri Paesi e alla stessa Commissione Europea, il 21 marzo 2020 il Ministro della Salute ha indetto in videoconferenza una riunione con tecnici del Ministero, rappresentanti dell'Istituto Superiore di Sanità e dell'Organizzazione Mondiale della Sanità, il Ministro per l'Innovazione Tecnologica e la Digitalizzazione e tecnici ed esperti del Dipartimento della Presidenza del Consiglio per la trasformazione digitale il cui scopo era quello di definire tratti essenziali di una linea d'azione per l'introduzione di un sistema digitale di *contact tracing* da sottoporre in seguito ai dovuti passi successivi di valutazione da parte delle istituzioni.

In base alle convergenze rilevate nell'incontro è stata avviata una *fast call for contribution* nell'ambito dell'iniziativa "Innova per l'Italia: la tecnologia, la ricerca e l'innovazione in campo contro l'emergenza Covid-19" (una richiesta pubblica di offerte volta a raccogliere contributi da aziende, università, centri di ricerca e società civile nell'ambito dei dispositivi per la prevenzione, la diagnostica e il monitoraggio per il contenimento e il contrasto del diffondersi del coronavirus, promossa dai Ministri di Sviluppo Economico, Università e Ricerca e Innovazione Tecnologica e Digitalizzazione). La *fast call for contribution* si è svolta tra il 24 e 26 marzo con l'obiettivo di individuare le migliori soluzioni digitali disponibili su applicazioni di telemedicina e assistenza domiciliare dei pazienti nonché tecnologie e strategie basate sulle tecnologie per il monitoraggio "attivo" del rischio di contagio.

Le proposte di soluzioni tecnologiche sono risultate 319 per il monitoraggio e 504 per la telemedicina. Sono state sottoposte alla valutazione del "*Gruppo di lavoro data-driven per l'emergenza Covid-19*" costituito con decreto del Ministro per l'Innovazione Tecnologica e la Digitalizzazione e formato da esperti suddivisi in otto sottogruppi in ragione dell'oggetto del lavoro da svolgere.

I sottogruppi "*Tecnologie per il governo dell'emergenza*" (tenuto a individuare possibili soluzioni offerte dalle tecnologie digitali per gestire l'emergenza e contenere il contagio) e "*Profili giuridici della gestione dei dati connessa all'emergenza*" (preposto a valutare i vincoli normativi per l'utilizzazione e la condivisione dei dati personali in soluzioni tecnologiche di contenimento) hanno fornito approfondite analisi e hanno informato dei primi risultati del loro lavoro l'Autorità Garante per la protezione dei dati personali, l'Autorità Garante della concorrenza e del mercato e l'Autorità per le garanzie nelle comunicazioni.

Il 30 marzo 2020, su iniziativa del Segretario Generale della Presidenza del Consiglio dei Ministri, è stata convocata una riunione in videoconferenza di coordinamento per le eventuali iniziative governative da adottarsi a valle della selezione della soluzione tecnologica di *contact tracing*. Alla videoconferenza hanno partecipato i rappresentanti dei Ministri di Interno, Giustizia, Salute, Innovazione tecnologica e la digitalizzazione e Servizi del Comparto Sicurezza dello Stato.

Ha fatto seguito una successiva riunione di coordinamento in videoconferenza il 4 aprile 2020. In questa sede sono state espresse e valutate posizioni e suggerimenti dei partecipanti anche alla luce delle relazioni prodotte dal gruppo di lavoro, contenenti le valutazioni - sia dal punto di vista tecnico, sia dal punto di vista giuridico - delle proposte analizzate, messe a disposizione di tutti i partecipanti alle riunioni di coordinamento.

Il gruppo di lavoro ha concluso indicando, fra tutte le soluzioni esaminate, quelle maggiormente valide e idonee a essere testate per eventualmente essere adottate nell'attuale situazione emergenziale.

Il sottogruppo "Profili giuridici della gestione dei dati connessa all'emergenza" ha evidenziato che:

"Le soluzioni tecnologiche esaminate più in linea con il quadro giuridico, in generale, funzionano come segue: il segnale Bluetooth LE (Low Energy) degli utenti che hanno scelto di installare una specifica applicazione viene registrato dalle analoghe applicazioni con le quali "entrano in contatto"; quando un utente viene diagnosticato contagiato dal Covid-19 il suo dispositivo trasmette i dati al server del soggetto pubblico che gestisce il sistema [alcune delle soluzioni valutate prevedono tale

trasferimento su base sistematica e non condizionata], che provvede quindi a informare gli altri utenti - che abbiano egualmente volontariamente installato la medesima app - di essere a rischio contagio perché sono entrati in contatto con una persona risultata contagiata.

I presupposti essenziali delle valutazioni e considerazioni riassunte nel documento sono:

(a) che l'intero sistema integrato di contact tracing sia interamente gestito da uno o più soggetti pubblici e che il suo codice sia aperto e suscettibile di revisione da qualunque soggetto indipendente voglia studiarlo;

(b) che i dati trattati ai fini dell'esercizio del sistema siano "resi sufficientemente anonimi da impedire l'identificazione dell'interessato" [cfr. Considerando 26 GDPR] tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione almeno in condizioni ordinarie e salvo il verificarsi di eventi patologici o, almeno, pseudo anonimi previa adozione di idonee misure idonee a limitare il rischio di identificazione degli interessati;

(c) che la decisione di usare la soluzione tecnologica sia liberamente assunta dai singoli cittadini;

(d) che raggiunta la finalità perseguita tutti i dati ovunque e in qualunque forma conservati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, siano cancellati con conseguente garanzia assoluta per tutti i cittadini di ritrovarsi, dinanzi a soggetti pubblici e privati, nella medesima condizione nella quale si trovavano in epoca anteriore all'utilizzo della soluzione;

(e) che la soluzione adottata - nelle sue componenti tecnologiche e non tecnologiche - possa essere considerata, almeno in una dimensione prognostica, effettivamente efficace sul piano epidemiologico giacché, in difetto, diverrebbe difficile giustificare qualsivoglia, pur modesta e eventuale, compressione di diritti e libertà fondamentali".

Il sistema di *contact tracing* dovrà essere finalizzato tenendo in considerazione l'evoluzione dei sistemi di *contact tracing* internazionali, oggi ancora non completamente definiti (PEPP-PT, DP-3T, ROBERT), e in particolare l'evoluzione del modello annunciato da Apple e Google. **Il codice sorgente del sistema di contact tracing sarà rilasciato con licenza Open Source MPL 2.0 e quindi come software libero e aperto**.

L'applicazione non dovrà accedere alla rubrica dei contatti del proprio telefono, non chiederà nemmeno il numero e non manderà SMS per notificare chi è a rischio.

Inoltre sarà necessaria l'integrazione delle indicazioni e dei protocolli sanitari stabiliti dal Ministero della Salute e dalle autorità sanitarie. L'applicazione si baserà sull'installazione volontaria da parte degli utenti e il suo funzionamento potrà cessare non appena terminerà la fase di emergenza, con cancellazione di tutti i dati generati durante il suo funzionamento.

L'applicazione non conserverà i dati relativi alla geolocalizzazione degli utenti, ma registrerà esclusivamente i contatti pseudonimizzati di prossimità rilevati mediante la tecnologia *bluetooth low energy*.

Le linee generali dell'attività di ricognizione e valutazione avviata sulle possibilità di tracciamento sono state illustrate nella Camera dei Deputati dal Ministro per l'innovazione tecnologica e la digitalizzazione, chiamata in audizione l'8 aprile 2020 davanti alla Commissione Trasporti, Poste e Telecomunicazioni.

Con nota indirizzata il 10 aprile 2020 al Commissario straordinario del Governo per l'attuazione ed il coordinamento delle misure per il contenimento ed il contrasto dell'emergenza epidemiologica Covid-19, dottor Domenico Arcuri, il Presidente del Consiglio ha richiamato le osservazioni dei Ministri della Salute e per l'Innovazione Tecnologica e la Digitalizzazione. Il Presidente del Consiglio ha chiesto al Commissario di procedere rapidamente, nell'ambito dei poteri conferiti dall'articolo 122 del decreto-legge 17 marzo 2020, n. 18, a valutare le modalità con cui dare attuazione alla proposta dei due Ministri. Ha precisato che, in tali attività, il Commissario sarà supportato anche dai rappresentanti delle Amministrazioni competenti *ratione materiae* e da un rappresentante designato dal Presidente della Conferenza delle Regioni e delle Province autonome di Trento e Bolzano.

Il Commissario, raccordandosi con il Segretario Generale della Presidenza del Consiglio dei Ministri, ha quindi preso contatti con la società Bending Spoons S.p.a.. Il 16 aprile 2020, previa adozione dell'ordinanza n. 10/2020, il Commissario ha stipulato il contratto con cui la stessa società, per spirito di solidarietà e, quindi, al solo ed esclusivo scopo di fornire un proprio contributo volontario utile per fronteggiare l'emergenza da coronavirus in atto e contribuire alle azioni di contenimento che il Governo intende porre in essere, ha concesso la licenza d'uso aperta, gratuita, perpetua e irrevocabile del codice sorgente e di tutte le componenti dell'applicazione. La società si è poi impegnata, sempre gratuitamente e *pro bono*, a completare gli sviluppi software necessari per la messa in esercizio del sistema nazionale di *contact tracing* digitale.

Questo il percorso compiuto finora, in attesa dei passi ulteriori nel percorso istituzionale necessario.

Task force dati, le relazioni delle attività dei gruppi che hanno valutato le app

Pubblichiamo le relazioni conclusive dei due gruppi di lavoro della task force che si sono occupati della valutazione delle app per il monitoraggio e il contrasto dell'emergenza Covid-19.

Pubblichiamo le relazioni conclusive dei lavori del gruppo 6 e del gruppo 8 della Task force italiana per l'utilizzo dei dati contro l'emergenza Covid-19. I due gruppi si sono focalizzati:

- sulla valutazione delle tecnologie per la tutela della salute pubblica e il ripristino delle attività sociali e economiche nel Paese;
- sulla valutazione degli aspetti legati ai diritti e alla privacy di ciascuna tecnologia presa in esame.

La task force è nata a marzo su iniziativa del Ministro per l'Innovazione Tecnologica e la Digitalizzazione in accordo con il Ministero della Salute per valutare e proporre soluzioni tecnologiche data driven e affrontare l'emergenza sanitaria, sociale e economica legata alla diffusione del virus SARS-CoV-2 sul territorio italiano. Ne fanno parte 74 esperti divisi in otto gruppi di lavoro.

A questo link il Decreto Ministeriale di istituzione della task force - Pdf

Le relazioni che pubblichiamo di seguito sono frutto di autonoma valutazione dei componenti di ciascun sottogruppo di lavoro.

Le relazioni delle attività degli altri gruppi di lavoro e altri documenti prodotti dalla task force saranno pubblicati nei prossimi giorni su GitHub a questo link.

Gruppo 3 - Impatto economico

Il gruppo 3 (Impatto economico) in collaborazione con i membri del gruppo "Big Data & AI for policy" ha elaborato raccomandazioni su come gestire la "fase 2": far ripartire gradualmente attività economiche e produttive senza pregiudicare la salute e la sicurezza dei cittadini e prevenendo il rischio che l'epidemia risorga.

- A questo link è possibile leggere e scaricare la relazione conclusiva del gruppo 3 (Pdf)

Gruppo 6 - Tecnologie per il governo dell'emergenza

Il gruppo 6 (Tecnologie per il governo dell'emergenza) si è occupato della valutazione di tecnologie per permettere la tutela della salute pubblica insieme al ripristino delle condizioni per le attività economiche e sociali e per la tutela delle libertà e dei dati personali (libertà di circolazione e privacy).

- A questo link è possibile leggere e scaricare la relazione conclusiva del gruppo 6 (Pdf)
- A questo link è possibile leggere e scaricare una sintesi della relazione (Pdf)
- A questo link è possibile leggere e scaricare l'allegato tecnico alla relazione del gruppo 6 (Pdf)

Gruppo 7 - Big Data & AI for policy

Il gruppo 7 (Big Data & AI for policy) ha lavorato alla valutazione di strumenti per politiche basate sui dati, sfruttando tecnologie di big data analytics e intelligenza artificiale. Il gruppo si è occupato anche di valutare soluzioni per rendere disponibili i dati clinici e radiologici, per mettere al lavoro i centri di ricerca italiani e internazionale allo sviluppo di modelli AI predittivi e esplicativi per il decorso clinico dei pazienti Covid.

- A questo link è possibile leggere e scaricare la relazione conclusiva del gruppo 7 (Pdf)

Gruppo 8 - Profili giuridici della gestione dei dati connessa all'emergenza

Il gruppo 8 (Profili giuridici della gestione dei dati connessa all'emergenza) si è occupato di valutare l'impatto delle soluzioni tecnologiche per quanto riguarda il rispetto della privacy e di altri diritti fondamentali.

- A questo link è possibile leggere e scaricare la relazione conclusiva del gruppo 8
- A questo link è possibile leggere e scaricare la relazione del gruppo 8 sulla proposta "CovidApp - Covid Community Alert" del gruppo "Coronavirus Outbreak Control"
- A questo link è possibile leggere e scaricare la relazione del gruppo 8 sulla proposta "Immuni" di BendingSpoons

Fotografia di Sen Sathyamony su Unsplash

MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

Report sottogruppo di lavoro 6

Report sulle attività svolte dal sottogruppo di lavoro impegnato nell'individuazione di "Tecnologie per il governo dell'emergenza" (in particolare contact-tracing) mediante valutazione di 319 soluzioni tecnologiche pervenute con call for contribution dal 24 al 26 Marzo.

Coordinatori:
Fidelia Cascini, Università Cattolica S. Cuore
Paolo De Rosa, Dipartimento per la trasformazione digitale

Componenti del sottogruppo:
Francesca Bria, UCL London e Fondo Innovazione
Carlo Alberto Carnevale Maffè, Università Bocconi, Milano
Ciro Cattuto, Università di Torino
Leonardo Favario, Dipartimento per la trasformazione digitale
Alfonso Fuggetta, Politecnico di Milano
Andrea Nicolini, Fondazione Bruno Kessler
Alberto E. Tozzi, Ospedale Pediatrico "Bambino Gesù", Roma
Simone Piunno, Università Bocconi, Milano
Stefano Calabrese, Dipartimento della Protezione Civile
Umberto Rosini, Dipartimento della Protezione Civile

Premessa

Verso un modello europeo

Digital contact tracing

Il processo di valutazione
- Intervista 1 - ProteggInsieme
- Intervista 2 - TrackMyWay
- Intervista 3 - CovidApp
- Intervista 4 - Immuni
- Intervista 5 - SafeTogether
- Intervista extra - COMBAT
- Caratteristiche tecniche delle soluzioni

Realizzazione e sperimentazione

Considerazioni sulla sicurezza informatica

Privacy

Conclusioni

Bibliografia

Premessa

Le esperienze internazionali maturate in questi ultimi mesi, a partire dall'insorgenza dell'epidemia COVID-19, dimostrano che alcune soluzioni tecnologiche sono state in grado di ricostruire tempestivamente una precisa mappa dei contatti tra individui con infezione e individui sani offrendo un importante strumento operativo per azioni di prevenzione. Il tracciamento dei contatti *(contact tracing*) con adeguate tecnologie consente di ricostruire catene di potenziale contagio nel rispetto delle normative vigenti in materia di protezione dei dati personali. L'uso di queste tecnologie si è già dimostrato efficace nella strategia di contenimento dell'infezione da SARS-COV-2 in altri Paesi. In Corea del Sud, ad esempio, è stata osservata [1] - grazie all'utilizzo di Big Data nella mappatura e nel contenimento dell'epidemia - una diminuzione nel tempo del tasso effettivo di riproduzione del contagio (R_0), ottenuto individuando tempestivamente e precisamente gli *hot spot* di potenziale contagio concentrando su di esse le azioni di prevenzione. La sfida sarà quindi quella di isolare i casi confermati e i loro contatti rispettando i diritti e le libertà fondamentali proprie delle democrazie europee.
Nonostante le molte obiezioni inizialmente sollevate contro l'efficacia del *contact tracing*, le più recenti ricerche scientifiche sull'epidemia COVID-19 [2] dimostrano che la sola esecuzione di test diagnostici non è sufficiente per ridurre la trasmissione dei contagi perché il tempo necessario per il riconoscimento dei casi ritarda le altre azioni di prevenzione. Di fatto, le manifestazioni cliniche di COVID-19 possono essere assenti o impiegare alcuni giorni per esprimersi, ritardando il riconoscimento dei casi con infezione. A questo si aggiunge il tempo necessario per ricevere i risultati dei test diagnostici. Tale latenza si riflette sulla tempestività delle misure di isolamento dei soggetti infetti. La ricerca scientifica evidenzia in particolare che la malattia risulta asintomatica fino al 55% delle trasmissioni con un *generation period* molto breve (3-5 giorni). La ricostruzione della catena trasmissiva del virus a partire dal solo esito dei test diagnostici è pertanto insufficiente e tardiva (prova ne è il fatto che l'isolamento dei positivi non ha effetti risolutivi sulla riduzione di R_0 al di sotto dell'unità).

Il lavoro di Ferretti et al. [2], dimostra come anche ad elevatissimi livelli di successo nell'isolamento dei casi positivi, serva una rapida e ampia identificazione e messa in quarantena almeno dei contatti di primo livello per poter mettere sotto controllo l'epidemia. Attualmente, ricostruire "manualmente" i contatti di un malato di COVID-19 si sta rivelando un'attività lenta e farraginosa. Il Big Data Institute di Oxford propone[1] quindi un *workflow* di riferimento per lo sviluppo di soluzioni tecnologiche specificamente destinate al *contact tracing* per COVID-19, che recepisca i principali elementi etici e scientifici emersi dalle ultimissime ricerche in merito. Il modello del Big Data Institute si basa sulle migliori pratiche

[1] https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/

studiate nei modelli internazionali di contrasto all'epidemia COVID-19 e delinea lo schema di tracciabilità istantanea dei contatti di primo grado: un sistema di *alerting* su smartphone è in grado di informare gli utenti, in base alla loro matrice di contatti ed eventualmente alla loro posizione geografica, rispetto a quando possono spostarsi in sicurezza, quando devono cercare assistenza medica, quando devono evitare persone vulnerabili. Il modello proposto ha il potenziale di rallentare drasticamente la diffusione dell'epidemia se utilizzato da un numero sufficientemente ampio di persone che ne facciano uso con adeguata fedeltà.

In linea con le suddette pubblicazioni, le indicazioni fornite dall'OMS al momento della dichiarazione della pandemia sono apparse chiare ed esplicite indicando testualmente: "*Find, isolate, test and treat every case and trace every contact*". Perciò, mettere a punto processi e tecnologie allo scopo di tracciare rapidamente i contagi, è essenziale per circoscrivere e contrastare l'espandersi delle catene di trasmissione del virus, anche nei Paesi che, come l'Italia, applicano drastiche forme di contenimento generalizzato (*lockdown*).

Allineata su questi stessi obiettivi, l'attività svolta dal sottogruppo di lavoro impegnato sulla disamina di tecnologie 'data driven' per la gestione dell'emergenza in atto, è dedicata a supportare le decisioni delle autorità politiche affinché possano essere facilitate nel perseguire il triplice obiettivo di: a) provvedere alla tutela della salute pubblica, b) ripristinare il più rapidamente possibile le condizioni permissive delle attività economiche e commerciali dopo il *lockdown*, c) consentire il recupero della mobilità personale sotto monitoraggio permanente di eventuali focolai di ripresa garantendo al contempo il diritto alla riservatezza e alla protezione dei dati personali.

Verso un modello europeo

La pandemia COVID-19 rappresenta una grave minaccia per i paesi di tutto il mondo e in particolare per i paesi dell'Unione Europea, al momento tra i più colpiti. Nell'UE, infatti, il virus si è diffuso rapidamente e non conosce confini geografici o politici. Per metterlo sotto controllo, si deve agire allo stesso modo: la velocità e la cooperazione internazionale risultano quindi essenziali per contrastarne l'avanzata. In risposta al numero in rapida crescita di casi e al pericolo di sovraccaricare i sistemi sanitari, molti paesi hanno imposto vincoli agli spostamenti o adottato blocchi delle attività economiche e sociali per rallentare la diffusione del coronavirus. Poiché un blocco a lungo termine non è economicamente e socialmente sostenibile, alcuni soggetti pubblici e privati europei si sono attivati per elaborare una risposta

comune che, attraverso soluzioni tecnologiche interoperabili di *contact tracing*, consenta di mantenere una società e un'economia aperte, proteggendo la salute dei cittadini senza rischiare il collasso del sistema sanitario.

La selezione della soluzione tecnologica di riferimento a livello europeo è stata proposta dal consorzio internazionale Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[2], che conta oltre 130 membri in otto paesi europei e include eccellenze europee nel campo della ricerca scientifica e tecnologica, tra cui anche centri di ricerca italiani. PEPP-PT si basa su un approccio condiviso con le seguenti caratteristiche fondamentali:

- Procedure collaudate e consolidate per la misurazione della prossimità tra device (smartphone) su sistemi operativi e dispositivi mobili di grande diffusione.
- Protezione crittografica dei dati, anonimizzazione, conformità al GDPR ed elevata cybersecurity.
- Interoperabilità internazionale e interregionale per supportare il tracciamento delle catene locali di infezione anche se una catena si estende su più paesi o su più regioni.
- Architetture e tecnologie di back-end scalabili che possano essere implementate con l'infrastruttura IT locale.
- Un servizio di certificazione del codice open source per testare e garantire che le diverse implementazioni utilizzino i meccanismi in modo sicuro e interoperabile.
- Implementazione di riferimento disponibile sotto la licenza open source *Mozilla License Agreement.*

La tecnologia proposta dal Consorzio Europeo può dare un contributo decisivo a un tracciamento di prossimità efficiente e molto più rapido di quello tradizionale, nel rispetto dei diritti e delle libertà fondamentali dei cittadini, comprese garanzie rispetto al trattamento dei loro dati personali, in linea con i valori e le norme europee.
Per questo motivo si è attivato il processo per selezionare una soluzione tecnica che renda possibile il tracciamento della prossimità tramite *smartphone*, così che non vengano tracciate le persone fisiche e non vengano estratti i loro dati personali (es. chi siano e dove sono stati); si punta a tracciare solo le relazioni di prossimità a corto raggio che costituiscono rischio di esposizione e corrispondono a potenziali catene di trasmissione del virus. Il punto di partenza naturale per tali processi sono i telefoni cellulari poiché la maggior parte delle persone usa regolarmente questo tipo di device e anche coloro che dovessero ancora esserne privi possono essere equipaggiati in modo rapido ed economico.

Lo sviluppo di questa tecnologia si basa su tre principi di base. Innanzi tutto, è il risultato di una analisi dei *benchmark* internazionali e di un forte spirito di cooperazione europea. In secondo luogo, la tecnologia viene studiata e selezionata per essere applicabile a livello

[2] Pan-European Privacy-Preserving Proximity Tracing, PEPP-PT, https://www.pepp-pt.org

internazionale, vale a dire interoperabile oltre i confini nazionali. In tal modo, la tecnologia faciliterà la ripresa di regolari relazioni internazionali e la libertà di circolazione dei cittadini. In terzo luogo, la tecnologia individuata deve essere conforme con il regolamento generale sulla protezione dei dati (GDPR).

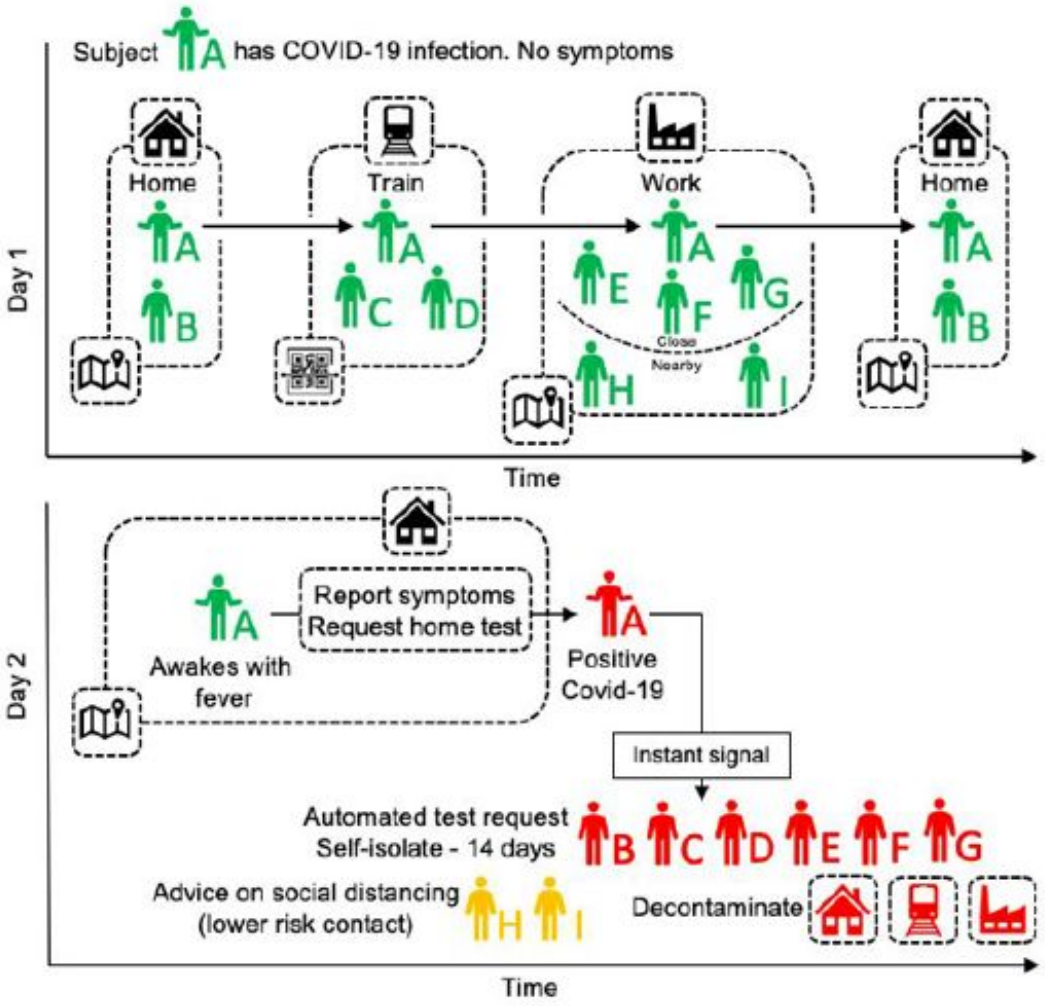
Lo sviluppo di un tale sistema è una grande sfida, ma che vale la pena raccogliere. Come è successo anni fa con la creazione dei primi standard europei per la telefonia cellulare GSM, cresciuta nell'adozione internazionale fino a diventare uno standard globale, la tecnologia di base deve fornire un meccanismo di tracciamento della prossimità applicabile in modo omogeneo anche al di fuori dei singoli confini nazionali. Sulla base di esso, ogni paese potrà sviluppare la propria versione locale di app e fornire la propria infrastruttura sicura. Ciò consentirà a ciascun paese partecipante di applicare operativamente la soluzione tecnologica in coordinamento con le autorità sanitarie locali per le esigenze della popolazione locale. Ogni paese deve anche essere in grado di informare in modo trasparente i propri cittadini così da convincerli, senza usare imposizioni autoritarie, a partecipare volontariamente a tale sistema. La tecnologia di base, sviluppata in costante confronto con autorevoli esperti di diverse discipline, dovrà fornire un contributo importante per consentire il tracciamento della prossimità, anche in modalità transfrontaliera, nel rispetto della privacy, secondo un modello scalabile e aperto, che possa essere utilizzato da qualsiasi paese.

La selezione delle soluzioni è stata quindi orientata al pieno rispetto delle leggi e dei principi europei in materia di privacy e protezione dei dati. I meccanismi e gli standard tecnici ricercati sono quindi orientati a tutelare la privacy, la trasparenza e la sicurezza nella gestione dei dati, sfruttando le possibilità della tecnologia digitale per massimizzare la velocità e la capacità in tempo reale di risposta alla pandemia. Questi meccanismi includono tecnologie di tracciamento della prossimità collaudate, anonimizzazione dei dati sicura e crittografata, meccanismi affidabili per consentire il contatto tra l'utente e i funzionari sanitari in un ambiente conforme alla protezione dei dati, interfacce di scambio di dati digitali (API) in grado di fornire catene di contatti anonimizzate e valutazione del rischio ad altre applicazioni (ad esempio per la gestione delle risorse sanitarie, la gestione del rischio privato o i sistemi di risposta alla pandemia).

L'implementazione di riferimento deve basarsi su codice open source, con servizi di backend sicuri e scalabili in grado di gestire centinaia di milioni di dispositivi registrati, servizi di supporto per l'interoperabilità transfrontaliera, la divulgazione e l'adozione da parte di una massa critica di cittadini.

Digital contact tracing

A titolo illustrativo, si descrive qui di seguito il funzionamento generale di una soluzione per il *contact tracing* digitale, in grado di valutare il rischio di trasmissione del virus attraverso monitoraggio del numero, della durata e del tipo di contatti, attraverso un normale *smartphone*. Lo schema sottostante propone un processo operativo di riferimento per le soluzioni tecnologiche destinate al *contact tracing* per COVID-19. Il modello, derivato dalle ricerche del Big Data Institute di Oxford University, si basa sulle migliori prassi studiate nei modelli internazionali di contrasto all'epidemia COVID-19 e delinea lo schema di tracciabilità istantanea dei contatti di primo grado basato su una app da installare sul proprio *smartphone* e da una infrastruttura di gestione (*backend*) sotto il controllo delle autorità sanitarie.

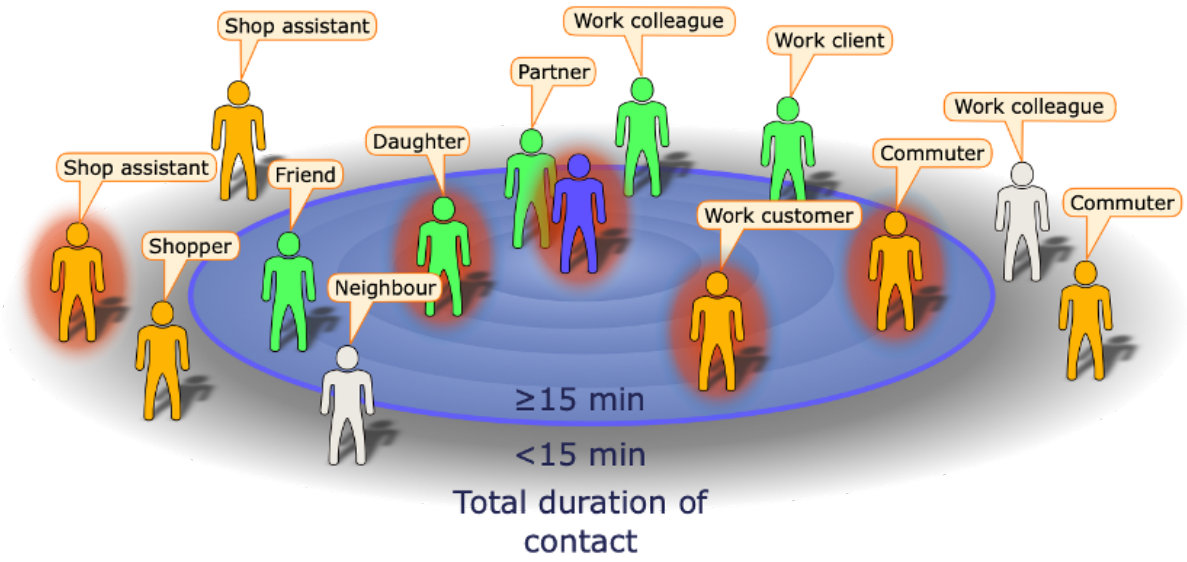


Nel pannello in alto la figura illustra i possibili contatti tra individui durante le attività quotidiane come ad esempio nei mezzi di trasporto o nell'ambiente di lavoro. Nel pannello in basso viene illustrata la

serie di interventi di isolamento e distanza sociale che possono essere messi in atto immediatamente dopo che il soggetto positivo a SARS-COV2 viene segnalato come positivo ai propri contatti dei giorni precedenti attraverso l'applicazione su smartphone. Fonte: Sustainable containment of COVID-19 using smartphones in China: Scientific and ethical underpinnings for implementation of similar approaches in other settings, David Bonsall, Michael Parker, Christophe Fraser, Big Data Institute, 16 February 2020.

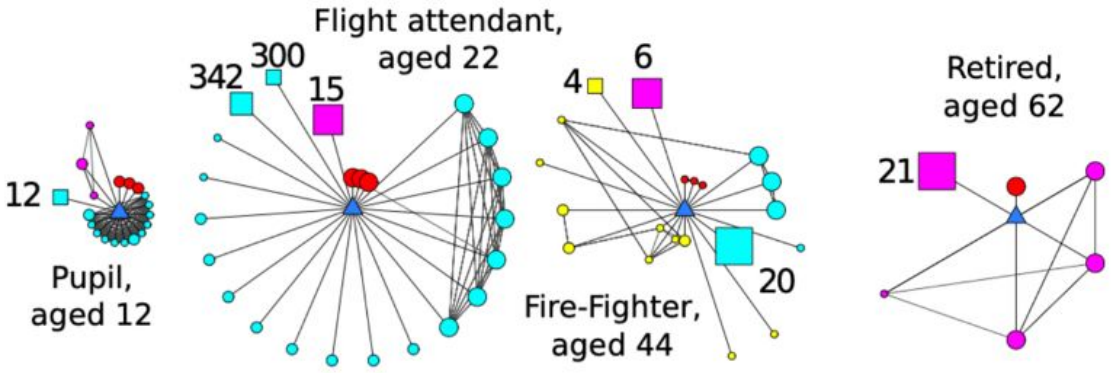
La soluzione proposta nel modello europeo, sopra indicato, non raccoglie in via ordinaria dati personali, né altri dati che consentano l'identificazione del proprietario del dispositivo mobile. La soluzione di contact tracing normalmente tiene traccia del solo numero, durata e tipo di contatti ravvicinati con altri device nei quali risulta attiva la stessa soluzione. Tuttavia sussiste il rischio che nel corso del funzionamento della soluzione vengano raccolti dati che potrebbero compromettere la natura anonima dei dati trattati in via ordinaria.
L'utente non viene necessariamente geolocalizzato (sebbene ciò possa essere tecnicamente reso possibile, purchè dietro specifica e consapevole scelta di opt-in da parte dell'utente), né viene reso riconoscibile, salvo che accetti esplicitamente tali opzioni, laddove applicabili e disponibili. In caso di contagio, le informazioni sono condivise con le sole autorità sanitarie. Utilizzando metodi di trasmissione dei dati orientati alle SAN (Small Area Network) quali ad esempio ANT, BT-LE, BT, AUDIO e WiFiP2P in funzione della sensoristica disponibile sul dispositivo e incrociando (ove possibile e sempre dietro esplicita autorizzazione dell'utente) i dati di posizione provenienti da GPS e Network Position (triangolazione basata su celle telefoniche), il telefono acquisisce un ID univoco e crittografato di tutti gli smartphone in prossimità (circa 1-2 m., ma in certi casi anche oltre) e conserva la durata e la distanza stimata di tale contatto ravvicinato. La scansione avviene a periodi programmabili di alcuni secondi, anche con l'app in *background*. Le tecnologie selezionate devono poter tracciare i contatti in prossimità del soggetto potenzialmente infetto con una precisione molto elevata, nell'ordine di poche decine di centimetri.

Con riferimento al *contact tracing* tradizionale, si veda la successiva rappresentazione grafica degli incontri fatti durante il giorno da un caso di paziente infettivo (blu) con i contatti posizionati in base alla durata totale del contatto. Nello schema sottostante, la definizione di "contatto" è relativa a qualcuno con cui il soggetto infettivo si è incontrato per 15 minuti o più. Alcuni contatti saranno tracciabili (verde), mentre altri non saranno tracciabili (arancione). Una definizione di contatto troppo restrittiva e inappropriata per l'infezione da COVID-19 implicherebbe che alcuni incontri potrebbero non riuscire a soddisfare la definizione, ma potrebbero essere comunque a rischio di infezione; a loro volta, questi contatti esclusi potrebbero essere tracciabili (grigio chiaro) o non tracciabili (arancione).



Fonte: Matt J Keeling et al., The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036

È opportuno che la soluzione tecnologica, anche tramite algoritmi di post-processing dei dati anonimi e crittografati, possa ricostruire con adeguata precisione il "grafo sociale" delle interazioni rilevanti ai fini epidemiologici. A titolo esemplificativo, nel grafico qui sotto, il soggetto infetto (ego) è il triangolo centrale blu; i cerchi rappresentano i singoli contatti, i quadrati rappresentano i gruppi di contatti (la dimensione di ciascun gruppo è indicata). I colori rappresentano le categorie sociali degli incontri (rosso = casa, ciano = lavoro / scuola, giallo = viaggio, rosa = altro). Le maggiori dimensioni dei simboli rappresentano una durata dei contatti più lunga, mentre una maggiore vicinanza all'individuo indica che il contatto è più frequente.



Fonte: Matt J Keeling et al., The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036

Va segnalato che, sulla base degli attuali vincoli tecnologici su alcuni tipi di device, in particolare quelli basati su sistema operativo iOS, il solo tracing di prossimità tramite Bluetooth rischia di non massimizzare la probabilità di identificare tutti i contatti, in quanto potrebbe non riuscire a intercettare i segnali provenienti da device dove le funzionalità Bluetooth non operano in modo coerente agli scopi dell'applicazione. Si ritiene quindi opportuno non escludere a priori la possibilità che, sotto condizione di opt-in informato e consapevole, la soluzione tecnologica da implementare possa trattare alcune puntuali e limitate informazioni geolocalizzate, non orientate a ricostruire i percorsi bensì circoscritte a specifici luoghi di potenziale contagio, specie se ad alta densità e frequenza di contatti, in quanto non tutti i contatti possibili potrebbero disporre di device (a causa di una minore penetrazione degli smartphone, specie tra la popolazione anziana) o di app installata (minore adozione/compliance da parte della popolazione). Nell'ipotesi in cui si ritenesse di utilizzare le funzionalità di geolocalizzazione dei dispositivi ancorché in ipotesi limitate occorrerebbe, ovviamente, rivedere le considerazioni sulla natura anonima dei dati trattati non risultando più possibile fare affidamento sull'effettivo anonimato.

Inoltre potrebbero essersi verificati casi di contagio ambientale e quindi potrebbe essere richiesto un intervento di sanitizzazione dei luoghi/locali. Potrebbe essere perciò giudicato opportuno che la soluzione possa conservare, oltre alla lista dei contatti di prossimità, anche un *timestamp* e una limitata cronologia delle geo-localizzazioni per i 14-21 giorni precedenti, ma la raccolta di tali dati, anche previo opt-in dell'utente, va attentamente valutata sulla base dei rischi di re-identificazione che essa comporta, in quanto l'uso della posizione vanifica - de facto - ogni forma di approccio autenticamente privacy-preserving e *può rendere più complessa e meno efficace la strategia di comunicazione pubblica e di acquisizione di utenti che volontariamente usano la suddetta app*. Si nota al riguardo che il Parlamento tedesco ha recentemente negato la possibilità di utilizzare informazioni GPS per applicazioni di contact tracing, approvando una proposta di legge in tal senso il 27 Marzo 2020.
La probabilità di contagio viene normalmente calcolata sulla base di un modello che tiene conto di durata del contatto, dei giorni trascorsi dal contatto e dal numero di questi contatti. I parametri numerici (nello schema qui sotto, indicati con c0…c3) vengono inizialmente stimati partendo dai dati presenti nella letteratura scientifica e vengono successivamente aggiornati man mano che il sistema consente di apprendere i dettagli del meccanismo di diffusione. Qui sotto si propone, a titolo esemplificativo, una forma generale e sintetica del metodo di calcolo del rischio di contagio:

$$Rischio = \sum_{i} c_0 \cdot r_i \cdot \frac{e^{(t-c_1)}}{1+e^{(t-c_1)}} \cdot e^{-\frac{(\Delta t - C_2)^2}{C_3}}$$

Fattore di rischio

Durata contatto

Giorni dal contatto

Max contagio

Rischio i

Num contatti

Tempo soglia

Larghezza gauss

Nella soluzione proposta dal consorzio europeo i dati vengono normalmente conservati solo sul device dell'utente. A seconda degli obiettivi del servizio, alcuni dati aggregati e crittografati possono eventualmente essere periodicamente salvati su un database protetto, per limitare i rischi di perdita o danneggiamento del device e dei relativi dati di contatto. Limitatamente ai casi verificati di contagio, tali dati potranno essere messi in condivisione con le autorità sanitarie per i necessari interventi di contenimento e prevenzione.

I dati acquisiti e il rischio calcolato possono essere resi accessibili in modo anonimo alle autorità sanitarie, che possono leggere i dati di rischio ed aggiornare lo stato di una persona (negativo o positivo al test). Il rischio calcolato per il singolo utilizzatore è in funzione dei dati degli altri utilizzatori. Se una persona risulta positiva al test, il rischio di ogni altra persona con la quale questa sia venuta in contatto viene aggiornato secondo una precisa procedura di "alerting". Per esempio, se una persona con la quale si ha avuto un contatto 5 giorni prima si rivela positiva, il rischio di contagio viene aggiornato sul suo cellulare. Ciascuno riceve le informazioni sul proprio stato di rischio, non su quello di altri. I cittadini possono venire informati in tempo reale e possono spontaneamente adottare misure cautelative (isolamento volontario) nei confronti delle persone più vicine. Le autorità sanitarie locali possono così disporre di uno strumento importante per concentrare i test sulle persone che hanno realmente avuto contatti a rischio contagio.

Più in dettaglio, ai fini di poter convergere con il modello di *digital contact tracing* proposto dal consorzio europeo PEPP-PT, il funzionamento desiderato della soluzione di *contact tracing* può essere sinteticamente così descritto:

1) Invio di un codice identificativo anonimo.

Ogni device abilitato trasmette un identificatore (ID) temporaneamente valido, autenticato e anonimo che non è collegato né a un utente né a un numero di telefono. La prossimità tra telefoni di altri utenti del sistema viene stimata misurando i segnali radio emessi dal device (Bluetooth, ecc.) utilizzando algoritmi testati e calibrati.

2) Registrazione della cronologia di prossimità.

Quando il device “A” si trova in prossimità epidemiologicamente rilevante del device “B” per un periodo di tempo epidemiologicamente sufficiente, come determinato dalle misurazioni empiriche e dall’euristica medica, l'ID anonimo del telefono B viene registrato nella cronologia di prossimità crittografata memorizzata localmente sul telefono A (e viceversa). Nel modello proposto da PEPP-PT, nessuna geo-localizzazione, nessuna informazione personale, nessun numero di telefono o altri dati vengono registrati, così da non consentire in alcun modo l'identificazione dell'utente. Questa cronologia di contatti di prossimità anonimi non può essere visualizzata da nessuno, nemmeno dall'utente del telefono “A”. Gli eventi più vecchi nella cronologia di prossimità vengono progressivamente eliminati quando diventano epidemiologicamente non importanti (p.es. dopo 21 giorni)

3) Utilizzo della cronologia di prossimità: due modalità operative.

Modalità 1

Se un utente non viene testato o è risultato negativo, la cronologia della prossimità anonima rimane crittografata sul telefono dell'utente e non può essere visualizzata o trasmessa da nessuno, nemmeno dalle autorità sanitarie. In qualsiasi momento, viene salvata solo la cronologia di prossimità che potrebbe essere rilevante per la trasmissione del virus e la cronologia precedente viene continuamente eliminata.

Modalità 2

Nel modello proposto da PEPP-PT, se è stato confermato che l'utente del telefono A è SARS-CoV-2 positivo, le autorità sanitarie contatteranno l'utente A e forniranno all'utente una chiave speciale crittografata, così da garantire che nessun potenziale malware possa inserire informazioni errate sull'infezione nel sistema. L'utente utilizza questa chiave speciale per fornire volontariamente informazioni al servizio sanitario nazionale che consente la notifica di app registrate nella cronologia di prossimità e quindi potenzialmente infette. Poiché questa cronologia contiene identificatori anonimi, nessuna delle due persone può essere a conoscenza dell'identità dell'altra.

4) Operazione di servizio sanitario dipendente dal paese e/o dalla regione.

Gli ID anonimi contengono meccanismi crittografici per identificare il paese e/o la regione di ogni app che utilizza il sistema. Utilizzando tali informazioni, gli ID anonimi vengono gestiti in modo specifico per paese.

Modalità 1
Se entrambi gli ID anonimi del telefono A e B provengono dallo stesso paese, l'ID anonimo della parte potenzialmente infetta può essere contrassegnato, in modo che quando l'app di questa parte chiede informazioni sul suo stato, l'app verrà informata della possibile esposizione.

Modalità 2

Se un ID anonimo del telefono B viene identificato come associato a un altro paese diverso dal telefono A, le informazioni associate all'ID anonimo del telefono B vengono trasmesse al servizio sanitario nazionale dell'altro paese. Questa trasmissione è completamente crittografata e firmata digitalmente. L'ulteriore elaborazione viene eseguita dal servizio sanitario nazionale o locale del paese/regione che ha emesso l'app.

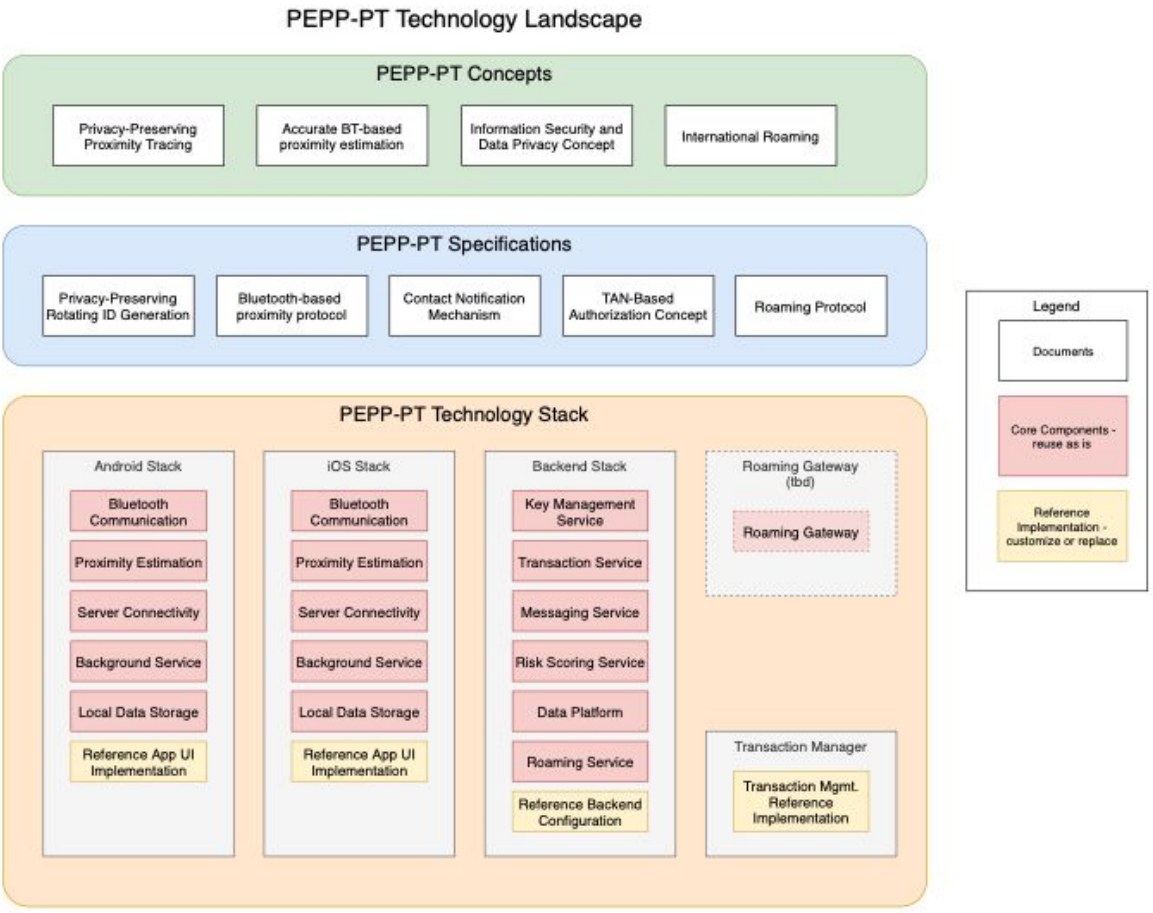
5) Elaborazione sanitaria

Il processo su come informare e gestire i contatti esposti può essere definito Paese per Paese, in modo tale da garantire comunque l'interoperabilità dei processi tra le diverse autorità sanitarie locali.

6) Informazioni e infrastrutture

Tutte le procedure, i meccanismi, gli standard e i codici del sistema vanno costantemente monitorati dal team di sicurezza. Parallelamente, le agenzie nazionali per la sicurezza informatica e le agenzie nazionali per la protezione dei dati controllano regolarmente tutte le linee di codice e le validano dal punto di vista della cybersecurity. Tutto ciò che viene rilasciato al pubblico viene controllato per prevenire effetti indesiderati nelle procedure o nel codice.

Lo schema dell'architettura tecnologica proposta dal progetto PEPP-PT è riportato nella figura seguente, che riprende i concetti, le specifiche di alto livello e la struttura degli stack tecnologici sopra sinteticamente descritti.



Il processo di valutazione

Le attività del Gruppo di Lavoro data-driven per l'emergenza COVID-19 sono state introdotte da una *fast call for contribution* della durata di tre giorni (dal 24 al 26 Marzo), nell'ambito di una iniziativa interministeriale denominata Innova per l'Italia, promossa dal Ministero dello Sviluppo Economico, dal Ministero dell'Università e della Ricerca, dal Ministero per l'Innovazione Tecnologica e la digitalizzazione, dal Ministero della Salute.

Il sottogruppo di lavoro 'Tecnologie per l'emergenza' si è dedicato all'individuazione delle tecnologie per l'identificazione dei casi di potenziale contagio (*contact-tracing*), immediatamente utilizzabili per governare l'emergenza epidemica ed eventualmente migliorabili con modifiche di facile e rapida realizzazione.[3]

[3] Le valutazioni sono state effettuate da un team composto dalla seguenti persone: Carlo Alberto Carnevale Maffè, Ciro Cattuto, Leonardo Favario, Andrea Nicolini, Alberto E. Tozzi.

Alla chiusura della *call for contribution*, il processo generale finalizzato all'individuazione delle proposte è stato articolato in cinque passaggi. In particolare:

1. creazione di una griglia di riferimento contenente i requisiti minimi indispensabili per selezionare le soluzioni tecnologiche;
2. uso di tale griglia per la selezione delle proposte da sottoporre a caratterizzazione tecnica da parte degli esperti membri del sottogruppo;
3. verifica delle soluzioni tecnologiche con riferimento alla normativa vigente in particolare in materia di privacy;
4. elaborazione di un documento di sintesi contenente la descrizione delle caratteristiche delle proposte tecnicamente meglio rispondenti all'immediato obiettivo di rispondere all'emergenza epidemica;
5. validazione del documento degli esperti tecnici da parte dei valutatori indicati nel DM del Ministro per l'innovazione tecnologica e la digitalizzazione del 31 marzo 2020

All'attenzione di componenti del sottogruppo 'Tecnologie per il governo dell'emergenza' sono pervenute in esame 319 proposte. La disamina, volta alla selezione delle proposte tecnicamente più rispondenti al bisogno di contribuire tempestivamente al governo dell'emergenza, è stata articolata in tre fasi successive. In particolare:

1. Screening generale, che ha consentito l'individuazione di 15 soluzioni rispondenti ai requisiti tecnici minimi indispensabili;
2. Caratterizzazione analitica, che ha portato alla selezione di una *short list* di 5 soluzioni tecnologiche target, tecnicamente pronte per l'uso di *contact tracing;*
3. Intervista tecnica effettuata sulla *short list* delle 5 soluzioni target, per la definizione di quelle tra queste 5 che offrissero che rispettassero nel miglior modo possibile il maggior numero di criteri definiti.

La fase 1 di screening generale è stata svolta da 5 esaminatori, sulla base di una scheda di analisi appositamente studiata e redatta dai tecnici del sottogruppo di lavoro prima della disamina delle proposte. I criteri presi come riferimento sono rappresentati in tabella 1 e sono stati considerati ciascuno secondo un valore di sufficienza (1) o insufficienza (0). Tutte le proposte che, in corso di disamina, hanno ottenuto un punteggio complessivo di tutti i criteri inferiore a 5, non sono passate alla fase 2 di caratterizzazione analitica.

Tabella 1.

	Criteri di screening	**Valore**
A	L'applicazione svolge **la funzione di digital contact tracing**?	1=si

B	**Il proponente** è una Pubblica Amministrazione, un'azienda pubblica o privata, ente o centro di ricerca pubblico o privato, associazione (che possa interagire con associati in grado di rispondere a queste esigenze), cooperativa, consorzio, fondazione o istituto?	1=si
C	La soluzione proposta risulta **concreta, già realizzata o disponibile** per l'implementazione in tempi brevi e compatibili con l'emergenza?	1=si
D	**L'approccio tecnico di rilevazione della prossimità** fisica avviene a mezzo di comunicazione diretta fra i dispositivi (ad esempio via tecnologia radio Bluetooth) ed è indipendente da informazioni altrimenti ottenute sulla posizione degli utenti nello spazio (geo-localizzazione, GPS, SSID WiFi, cella della rete mobile, etc.)?	1=si
E	**Disponibilità della soluzione tecnologica e tempi per l'attivazione dei servizi per il deployment** *(valuta la velocità con la quale la tecnologia può avere impatto; assegnare il valore 1 se si stima che i servizi possano essere attivi indicativamente entro 15 giorni, 0 altrimenti. Considerare anche l'adattamento di applicazione sviluppata per altri scopi).*	1=si
F	**Aspetti tecnici di rilevazione della prossimità** (*valuta la bontà della soluzione in termini di accuratezza nella rilevazione di parametri a valenza epidemiologica (es. risoluzione della distanza, del momento di inizio e della durata dei contatti) assegnare il valore 1 se la soluzione proposta consente misure di prossimità device-to-device passive a corto raggio e calibrazione della strategia di proximity detection, 0 altrimenti).*	1=si
G	**Aspetti tecnologici / prestazionali e di scalabilità** *(1 se la soluzione è basata su codice FLOSS, architettura scalabile e adeguate soluzioni di crittografia dei dati, protezione della privacy e data minimisation).*	1=si

La fase 2 di caratterizzazione analitica è stata svolta da 5 esaminatori con l'utilizzo dei seguenti indicatori e criteri, suddivisi in tre categorie:

Tecnologia

- Soluzione FLOSS: tutto il codice sorgente della soluzione è coperto da licenze FLOSS tra loro compatibili ed è disponibile all'interno di un repositorio pubblico completo di documentazione.
- La soluzione non ha dipendenze (software e/o architetturali) di natura proprietaria che potrebbero costituire lock-in.
- La soluzione tecnica consente misure di prossimità device-to-device passive a corto raggio.
- Calibrazione della strategia di proximity detection a corto raggio (per tenere conto delle differenze hardware tra diversi smartphones).
- Approccio massimamente distribuito: minimizzazione dei dati di contatto registrati in modo centralizzato ai soli dati strettamente necessari per le misure di contact tracing, testing e contenimento.
- Possibilità di deployment internazionale, con interoperabilità privacy-preserving di server nazionali (feature di "roaming").
- Facilità di raccordo della soluzione tecnica con il processo epidemiologico e clinico di contact tracing.
- Campionamento temporale delle relazioni di prossimità a frequenza sufficientemente alta, passivamente attivato.
- Strategie di power saving che riducono l'uso batteria e risultante churn degli utenti.
- Informazioni sul contesto dei contatti (e.g., contatto "indoors" oppure "outdoors").
- Architettura elasticamente scalabile e multi-tenant (numero limitato di interazioni con il backend, architettura backend non monolitica).
- Tecnologia privacy-preserving, con opzioni tramite consenso informato: assenza di soggetti privati con accesso ai dati individuali.
- Uso di crittografia *state of the art.*
- Possibilità di cancellazione dei propri dati locali/remoti.
- Basso debito tecnico (complessità di manutenzione, deploy, gestione)

PM & deployment

- App già rilasciata negli store, numero di download e feedback raccolti.
- Livello di testing raggiunto (maturità codebase).
- Facilità d'uso e incentivi all'adozione.
- Base di utenti già esistente e/o possibilità di refactoring della soluzione già adottata.
- Approccio internazionale. Consente scambio di best practices, testing distribuito su popolazione più vasta, riduzione di costi e rischi.
- Approccio tecnico che fa leva su esperienza di gruppi di ricerca internazionalmente riconosciuti in contact tracing con mezzi digitali. Integrazione con sistemi sanitari locali e medici di base.

Data analytics

- Capacità della soluzione di rilevare parametri di riconosciuta valenza epidemiologica per un patogeno a trasmissione aerea: risoluzione di interazioni di prossimità a corto raggio, risoluzione temporale di contatti individuali.
- Uso di ID robusto per interoperabilità con altri database in caso di decriptazione.
- Integrazione con altre informazioni da questionario contestuale integrato.
- Strategia di analisi dei dati con approccio privacy-enhancing, guidata dallo stato dell'arte della letteratura scientifica rilevante su contact tracing, outbreak investigation, high-resolution contact networks.
- Meccanismo di "scoring" del rischio individuale che faccia leva su graph analytics.
- Tecniche di machine learning a sostegno del contact tracing e dello scoring del rischio.
- Disponibilità di una piattaforma di analisi dati matura / già testata / integrata con il back end dell'applicazione.

User Experience / User Interface

- Approccio al design del progetto incentrato sull'utente finale (ricerca utenti, interaction design, visual design, architettura delle informazioni/contenuti).
- Design focalizzato su usabilità e accessibilità.

La fase 3 di intervista tecnica ai proponenti rientrati in *short list* ha permesso di approfondire alcuni aspetti tra cui:

- maturità/stage della soluzione;
- sicurezza/affidabilità;
- tecnologia di *contact tracing* utilizzata;
- approccio allo sviluppo *software*;
- architettura e approcci al *deployment*;
- analisi di potenziale *lock-in* (*software*, infrastrutturale);
- presenza di componenti critiche non rilasciabili con licenze FLOSS;
- composizione del team, delle partnership e dei ruoli;
- analisi della roadmap.

Intervista 1 - ProteggInsieme

Dall'intervista a Whatif srl, gruppo proponente della soluzione "ProteggInsieme", si evince che l'offerta è stata interamente costruita partendo dalla soluzione proposta dal Government Digital Services team di Singapore e basata sul protocollo *Bluetrace*[4]. In tal senso, lo stato di ProteggInsieme in data odierna è molto preliminare (*concept*) ovvero non esiste una versione funzionante e testabile di questo prodotto e questo è imputabile al fatto che il codice sorgente

[4] BlueTrace: https://bluetrace.io/

del *software* sviluppato dal team di Singapore non sia ancora stato reso disponibile a terzi. Inoltre, siccome *Bluetrace* è un protocollo basato sulla tecnologia Bluetooth, si ritiene opportuno sottolineare che il team di ProteggInsieme non ha un track record di esperienze pregresse per quanto riguarda questa specifica tecnologia ma potrebbe appoggiarsi alla propria rete di partner per ovviare a ciò. Infine, l'intervista ha reso evidente che la proposta ProteggInsieme necessita di ulteriore sviluppo su diversi fronti per essere pronta a rispondere pienamente alla sfida del digital contact tracing.

Intervista 2 - TrackMyWay

La soluzione "TrackMyWay", proposta da Antares Vision spa, si basa su un know-how solido del proponente nel mondo del tracking di beni di consumo (come, ad esempio, tracking di spedizioni di farmaci). In tal senso, la soluzione è fortemente incentrata sulle tecnologie di backend di proprietà di Antares Vision utili alla ricostruzione del grafo dei contatti per ogni nodo. Nel dettaglio, la proposta prevede di raccogliere una serie di informazioni attraverso un'applicazione mobile (quali, ad esempio, le coordinate GPS e l'eventuale contatto con altri device rilevato tramite Bluetooth) le quali dovranno essere successivamente inviate al backend costituito dalle summenzionate tecnologie. Ad ogni modo, dall'intervista non sono risultate chiare le scelte riguardanti le misure utili a minimizzare la quantità di informazioni da prelevare e successivamente trasferire al backend, le strategie da adottare per la gestione delle diverse risposte tra i vari dispositivi Bluetooth e le possibili modalità di rilevazione di eventi iOS-to-iOS. Inoltre, sebbene il team abbia esperienza comprovata nel campo del *tracking* digitale di oggetti in movimento tramite tecnologia GPS non vi è un track record significativo nel campo del *digital contact tracing.* Infine, l'architettura proposta risulta avere una natura centralizzata il che rappresenta un possibile problema in ottica di messa in esercizio su scala nazionale.

Intervista 3 - CovidApp

La soluzione denominata "CovidApp" è stata proposta da un team di sviluppatori indipendenti. Dall'intervista con il team si evince che il problema sia stato analizzato in modo approfondito e molti dei possibili scenari che potrebbero presentarsi anche su scala nazionale sono stati esaminati nel dettaglio. CovidApp è quindi una soluzione basata su un'applicazione mobile per la gestione del *contact tracing* attraverso la tecnologia *Bluetooth Low Energy*. In primis, l'applicazione raccoglie i dati relativi ai contatti registrati che vengono registrati all'interno del device. Successivamente, l'applicazione invia i dati raccolti al backend -ogni 4 ore- il quale li elabora per costruire il grafo dei contatti. In quest'ottica, risulta degno di nota l'approccio utilizzato per la rilevazione dei contatti tra dispositivi con sistema operativo iOS che prevede di sfruttare la triangolazione con altri device con sistema operativo Android e

successiva ricostruzione del grafo di prossimità. Un possibile svantaggio di questa soluzione è che numerose informazioni devono essere inviate al backend diverse volte al giorno il che non solo aumenta i requisiti in termini di risorse computazionali e di memorizzazione, ma potrebbe costituire un problema di scalabilità dell'intera architettura. Si noti, inoltre, che la rappresentazione del grafo di prossimità in modo centralizzato presso il backend, in cui ogni nodo ed interazione sono rappresentati indipendentemente dall'essere identificati rispettivamente come casi o come interazioni a rischio (ovvero a prescindere dal processo di *contact tracing*), comporta rischi di data protection e privacy più alti di approcci distribuiti che sono ugualmente efficaci per le strategie di *contact tracing digitale.*
Successivamente, l'intervista ha permesso di dettagliare il processo di alerting previsto da questa soluzione. Questo offre alle autorità sanitarie, a seguito della rilevazione di un caso positivo, la possibilità di attivare automaticamente e immediatamente l'alert. Inoltre, quest'ultimo è garantito essere del tutto anonimo in quanto non è necessario disporre del numero di cellulare dell'utente né del suo identificativo personale. Si noti come questa caratteristica si differenzia notevolmente dal modello PEPP-PT, che invece richiede obbligatoriamente -per attivare il processo di alerting su log dei contatti- il consenso e la collaborazione attiva da parte dell'utente riconosciuto come positivo che per procedere dovrà immettere un codice TAN sul proprio device.
Infine, durante l'intervista è stato possibile assistere ad una dimostrazione in tempo reale del prodotto che è attualmente in fase di test privato tra i membri del team.

Intervista 4 - Immuni

La proposta denominata "Immuni" è stata formulata da un pool composto da Bending Spoons, Jakala, GeoUniq e Centro Medico Santagostino. Ognuno di questi attori ha partecipato alla realizzazione del prototipo presentato.
L'intervista ha permesso di conoscere la genesi del progetto e capirne alcune scelte architetturali. Nel dettaglio, il concetto alla base di Immuni si avvicina molto a quello proposto nel protocollo BlueTrace presentato dal team di Singapore. Infatti, Immuni sfrutta la tecnologia Bluetooth Low Energy (BLE) per riconoscere le interazioni tra due device. Di conseguenza, ognuno di questi eventi è salvato nella memoria del dispositivo in modalità cifrata. Si noti che queste informazioni non lasciano mai il dispositivo a meno che il proprietario sia diagnosticato positivo al virus. In tal caso, le informazioni relative a tutti gli eventi di contatto precedentemente registrate dal dispositivo vengono inviate al backend dopo esplicita autorizzazione del proprietario. Solo a questo punto sarà possibile ricostruire a ritroso la catena di contatti e, laddove necessario, la piattaforma potrà inviare una notifica a tutti i dispositivi interessati da eventi di contatto.
Per quanto riguarda la copertura dei dispositivi mobile, il team afferma di poter tracciare correttamente il 94% dei contatti di tipo Android-Android e iOS-Android. Invece, per quanto riguarda la rilevazione degli eventi di contatto tra due device con sistema operativo iOS, il

team ha proposto due possibili alternative: la prima consiste in un artificio software mentre la seconda consiste nell'utilizzo del segnale GPS. Questa seconda strategia risulta essere particolarmente accurata grazie ad una libreria software sviluppata da GeoUniq. Si noti, però, che l'utilizzo di questa libreria proprietaria porterebbe ad un lock-in software.
Per quanto concerne il back-end, la soluzione si compone di componenti FLOSS e attualmente l'architettura di test risulta essere funzionante all'interno dell'infrastruttura di Google Cloud ma, siccome non sono stati utilizzati componenti proprietarie, si esclude il rischio lock-in.
Infine, l'intervista ha permesso di conoscere il team il quale è parso solido, con esperienza pregressa sia nel roll-out di applicazioni mobile su larga scala che di gestione di progetti software complessi anche in modalità FLOSS. Anche gli aspetti epidemiologici dell'applicazione sono stati messi a punto grazie alla partnership con il Centro Medico Santagostino.
Si noti in ultima istanza che il team ha già aderito e collabora attivamente con il Consorzio Europeo PEPP-PT. Quest'ultimo è un fattore positivo per quanto riguarda la capacità di lavorare a livello paneuropeo e nell'ottica di implementare in breve tempo una soluzione europea condivisa.

Intervista 5 - SafeTogether

La proposta SafeTogether, avanzata da Microsoft srl, ha lo scopo di realizzare una piattaforma versatile di raccolta dati relativi alla pandemia in corso. Dall'intervista con il team proponente si evince che la soluzione SafeTogether si trova in una fase molto preliminare di realizzazione (*concept*). Infatti ad oggi non esiste una vera e propria soluzione utilizzabile ma vi sono esclusivamente degli scenari di possibile utilizzo e la roadmap di progetto stima circa 4/5 settimane per la realizzazione di un oggetto preliminare da testare sul campo. Nello specifico, la proposta SafeTogether contiene diverse componenti infrastrutturali e di backend con la finalità di facilitare la raccolta e le operazioni di analisi dei dati ma non ha un frontend applicativo il che rende difficile immaginare un caso reale di utilizzo. Per quanto riguarda l'esperienza diretta con la pandemia attualmente in corso, il team di SafeTogether ha fatto presente che il modello da loro teorizzato segue quanto messo in opera dal GDS team di Singapore (TraceTogether).

Intervista extra - COMBAT

Al fine di approfondire anche alcune proposte che non hanno dichiarato esplicitamente di utilizzare le tecnologie di *digital contact tracing* più comuni, il gruppo di valutazione ha ritenuto opportuno procedere con l'intervista tecnica a Telecom Italia Spa in qualità di proponente della soluzione "COMBAT".

L'intervista ha permesso di chiarire che il framework "COMBAT" si compone di due soluzioni complementari tra di loro. La prima è prettamente rivolta allo sfruttamento di dati di celle telefoniche già disponibili al gruppo proponente mentre la seconda è basata su un'applicazione mobile.
Per quanto concerne la prima soluzione, la proposta prevede di sfruttare il database di informazioni riguardanti le celle telefoniche ed estrarne le informazioni utili per il *tracing*. Questo tipo di approccio è del tutto trasparente nei confronti dell'utente finale al quale, però, non verrebbe offerta esplicitamente la possibilità per un eventuale opt-out. Inoltre, attualmente l'accuratezza di questo approccio per la finalità del *tracing* non è paragonabile a quella offerta da altre tecnologie.
Il secondo approccio, invece, prevede di sfruttare un'applicazione mobile da realizzare *ex novo*. Questa applicazione potrebbe colmare il gap lasciato dalla soluzione presentata precedentemente in quanto consentirebbe di ottenere una risoluzione intra-cella maggiore e fornire questi dati al backend per una ricostruzione del grafo di tracing ex post. Si noti, però, che attualmente la seconda soluzione è in fase molto preliminare di realizzazione (*concept)* e quindi non è stato possibile valutarne la maturità. Infine, la roadmap dichiarata per la messa in opera della seconda soluzione è stata stimata in 4 settimane.

Caratteristiche tecniche delle soluzioni

Al termine delle tre fasi del processo di *selezione, caratterizzazione e valutazione delle proposte* è stata realizzata una tabella sinottica delle soluzioni ritenute maggiormente affidabili, per illustrarne le principali caratteristiche tecniche, i punti di forza e le possibili criticità.

Nome soluzione	**Immuni**	**CovidApp**
Tecnologia	App nativa, iOS (Swift) e Android (Kotlin).	App nativa, iOS e Android.
Program Management	Team con esperienza nel roll-out di applicazioni mobile verso milioni di utenti. Team include competenze verticali in sviluppo app mobile, data analytics, aspetti epidemiologici, geolocalizzazione.	Team distribuito creato ad hoc. Prototipo dell'applicazione realizzato e attualmente in fase di testing privato intra team di sviluppo.

	Prototipo dell'applicazione realizzato e attualmente in fase di testing privato intra team di sviluppo.	
Punti di forza	Integra la soluzione "PEPP-PT". Architettura fortemente decentralizzata. Ampio spettro di possibilità per livelli di privacy e opt-in. Le informazioni restano cifrate sull'edge e vengono rimosse progressivamente ogni 14/21 giorni. Alta scalabilità backend.	Rilevazione del contatto iOS-to-iOS tramite grafo di prossimità elaborato nel backend come triangolazione tra contatti Android.
Criticità	Rilevazione del contatto iOS-to-iOS non gestita	Architettura centralizzata: rappresentazione centralizzata del grafo di prossimità per tutti gli utenti, indipendentemente dalla diagnosi, con continuità temporale. Vincoli più forti di scalabilità e performance del backend. La rappresentazione centralizzata del grafo di prossimità nel backend implica rischi maggiori di data protection e privacy.

Realizzazione e sperimentazione

Per accompagnare l'uscita dal *lockdown* del Paese, è vitale prevedere un processo particolarmente attento ancorché veloce di validazione e messa in esercizio della soluzione prescelta che garantisca il raggiungimento degli obiettivi previsti.

Alla luce di queste considerazioni, il processo di implementazione deve essere ridondato e deve basarsi su almeno 2 soluzioni, al fine di avere la certezza di poter disporre di almeno una soluzione da mettere in campo qualora, in fase di sperimentazione concreta, una delle opzioni prescelte si rivelasse per qualunque motivo incapace di offrire le funzionalità e/o i livelli prestazionali richiesti. Per questo motivo, si propone di articolare il processo di implementazione della soluzione di *contact tracing* lungo **percorsi paralleli** in accordo al seguente modello:

a. Effettuare un approfondito *assessment* di sicurezza sull'intero codice sorgente, dell'architettura e del sistema delle soluzioni individuate, incluso risk assessment e threat modeling (a cura del comparto di *intelligence*). Inoltre sarebbe opportuno condividere il codice sorgente con la comunità scientifica dell'ambito cyber nell'ottica di avere delle review dal maggior numero di specialisti del settore possibile.
b. Effettuare una fase di *test* in campo per ciascuna soluzione preselezionata in diverse aree circoscritte del territorio (per esempio, alcuni territori urbani). Tale test potrà essere condotto su un campione di soggetti (per esempio, le forze dell'ordine e gli operatori della protezione civile) che, muovendosi sul territorio nonostante le misure restrittive degli spostamenti ancora in atto, possono già verificare il corretto funzionamento di ciascuna soluzione.

   Perché ciò avvenga, è necessario in via preliminare completare alcuni passaggi:

   i. stabilire i necessari protocolli d'uso dell'applicazione (da parte del personale medico-sanitario, delle forze di pubblica sicurezza e dei cittadini/tester);
   ii. migliorare il funzionamento dell'applicazione sulla base delle esigenze riscontrate, integrando eventuali funzionalità per meglio rispondere alle richieste emerse in fase di test;
   iii. definire il necessario coordinamento fra enti territoriali, ISS e Protezione Civile per l'uso dell'applicazione.

Questa fase di test in parallelo delle soluzioni candidate dovrebbe iniziare subito dopo la fase di validazione e scelta delle soluzioni tecnologiche da parte delle Autorità di Governo e durare indicativamente 10 giorni, così da rendere disponibile l'applicazione che presenta le

migliori prestazioni per l'impiego su larga scala sin dall'inizio del processo di uscita dal *lockdown.*

Inoltre, è necessario che, parallelamente alla messa in esercizio della soluzione tecnologica (fase di test), siano perseguiti i seguenti obiettivi:

1. delineare processi di carattere strategico-organizzativo in ambito sanitario, utili per governare il sistema di controllo dei contagi nel suo complesso e per dar seguito operativamente alle indicazioni che emergeranno dalla disponibilità delle tracciature (come ad esempio la gestione dei potenziali contagiati e il loro isolamento e cura), incluso il programma che sarà messo in campo per la comunicazione e formazione verso il personale sanitario;
2. definire gli aspetti giuridici, e tecnici relativi al tema privacy, etica e sicurezza b*y design*, inclusa la mappa del flusso dei dati, i soggetti che hanno accesso ai dati, e le condizioni di accesso;
3. definire un processo di *governance* che servirà a supervisionare l'esercizio, l'evoluzione e la valutazione del sistema di tracciatura nella sua fase operativa;
4. valutare l'integrazione con le infrastrutture tecnologiche esistenti per la gestione delle basi di dati centralizzate.

Per la gestione operativa a regime della soluzione di *contact tracing* sono necessarie sei componenti chiave:

1. Una autorità pubblica che rivesta il ruolo di *Driver* dell'esecuzione dell'intero progetto, preoccupandosi di curare la messa in opera di tutte le attività necessarie e coessenziali affinchè il *contact tracing* sia utilmente impiegato su scala nazionale (training dei medici, supporto tecnico agli utilizzatori, etc.). È fortemente raccomandabile che sia individuata una figura di *Program manager* con mandato esecutivo, in particolare per la fase iniziale del progetto.
2. Un team di sviluppo interdisciplinare che riunisca competenze tecnologiche e di sanità pubblica con una forte leadership e con le competenze digitali necessarie per guidare lo sviluppo e la manutenzione della soluzione, collaborando anche con gli stakeholder europei (queste caratteristiche andrebbero ricercate in un soggetto privato o in un consorzio di soggetti privati che supportino lo sviluppo del codice delle componenti applicative della soluzione individuata).
3. Un soggetto governativo in grado di gestire, mediante un fornitore di servizi tecnologici a controllo pubblico, l'infrastruttura tecnologica del servizio di contact tracing, garantendo massima sicurezza ed un'elevata affidabilità del servizio.
4. Una *governance* delle informazioni chiara e trasparente affidata all'autorità sanitaria nazionale e alla protezione civile.
5. Una diffusa e capillare campagna di *nudging*, comunicazione e informazione della cittadinanza, al fine di incoraggiare una partecipazione attiva e consapevole, guidata dalla Presidenza del Consiglio per massima autorevolezza.

6. La vigilanza sull'intero processo da parte della pubblica sicurezza e del comparto di *intelligence*.

La tabella seguente riassume a titolo puramente preliminare un'ipotesi di suddivisione delle competenze tra gli attori coinvolti nella realizzazione e gestione del servizio di *contact tracing*.

	Program Manager	Team di sviluppo	Gestore del servizio tecnologico	Autorità sanitaria	GPDP	PCM	DPC
Definizione Roadmap	A	R	R	C	I	C	I
Sviluppo e manutenzione della soluzione tecnologica	R	A	C	C			I
Gestione del sistema di contact tracing	R	C	A	I			C
Garantire anonimato dei dati trasmessi	R	R	A				
Gestione clinica sanitaria e attivare il contact tracing	C			RA			
Vigilanza sulla sicurezza	R	R	R			A	I
Vigilanza sulla privacy	R	R	R		A		
Campagna di comunicazione	R			C		A	I

Legenda:

- **Responsible (R)**: è il soggetto che esegue e assegna l'attività
- **Accountable (A)**: è il soggetto che ha la responsabilità sul risultato dell'attività.
- **Consulted (C)**: è soggetto che aiuta e collabora con il Responsible per l'esecuzione dell'attività.
- **Informed (I)**: è soggetto che deve essere informato al momento dell'esecuzione dell'attività.

Grande importanza assume a questo riguardo una *roadmap* di sviluppo agile che preveda una serie di rilasci scaglionati nel tempo dell'utilizzo della tecnologia, il cui proficuo impiego nel contenimento dell'epidemia e nella prevenzione di nuovi contagi richiede tempo e risorse dedicate.

Per la stima preliminare dei tempi e dei costi di sviluppo, test e roll-out nazionale, si può dividere il programma complessivo in tre fasi:

1. **Alpha** (prototipo per i primi test funzionali) + **Beta** (fase di perfezionamento e test sul campo in contesti/zone delimitati). Questa fase può richiedere circa 3 settimane di lavoro con costi derivanti principalmente dal team tecnico impegnato sui due prototipi che saranno scelti per limitare i rischi.

2. **Roll-Out su scala nazionale**. Estensione progressiva dell'adozione a tutta Italia. Questa fase può richiedere circa 3-4 settimane con i costi più rilevanti dovuti al programma di comunicazione e ai costi di setup e di progressivo allargamento dell'infrastruttura, in questo caso relativa all'unica soluzione che sarà scelta per l'uso a regime

3. **Gestione software a regime**. Questa è una fase di durata indefinita, durante la quale il sistema viene esercito e progressivamente ampliato e migliorato usando le informazioni acquisite sul campo per affinare la precisione e l'efficacia, aggiungere funzionalità ulteriori di cui - a lancio già avvenuto - si dovesse scoprire l'utilità, nonché garantire la continua integrazione con gli analoghi programmi portati avanti dagli altri paesi europei con i quali si intenderà collaborare.

Per ogni eventuale nuova versione con significative funzionalità aggiuntive, da sviluppare in modalità "agile", si può stimare prudenzialmente un monte-ore di lavoro pari allo sviluppo della versione base.

Per l'operatività immediata su **infrastrutture cloud sicure** e ad altissima affidabilità, la previsione dei costi può dipendere da molti fattori, principalmente rappresentati dal numero di persone che installeranno l'applicazione, dalla frequenza con la quale l'applicazione contatterà il sistema *backend* per aggiornamento dei dati, dalla quantità di persone che dovranno essere allertate perché entrate in contatto con positivi, dalla dimensione dei dati di tracciamento mediamente prodotti da ogni persona. Paragonando con progetti analoghi, è possibile immaginare che il costo complessivo del progetto potrebbe essere, prudenzialmente, al più nell'ordine di qualche milione di euro l'anno.

Le funzionalità software di base qui previste includono il tracciamento contatti basato su Bluetooth LE, il diario clinico, l'interfaccia utente e l'integrazione software in sicurezza con l'infrastruttura cloud, oltre alle funzionalità necessarie per far funzionare il sistema end-to-end. Non sono incluse nelle stime di costi e tempi iniziali altre funzionalità quali la georeferenziazione di alcuni dati o lo sviluppo del sistema di data analytics territoriali e l'integrazione con le basi dati sanitarie regionali e nazionali. Queste estensioni sono da ritenersi necessarie ma andranno valutate e stimate in una fase successiva all'avvio del progetto. Nel caso in cui le autorità decidano di seguire le raccomandazioni del Gruppo di Lavoro, ovvero procedere con due soluzioni in parallelo per le fasi di alpha + beta test, alla stima generale di costi di operatività andrà aggiunto un importo dovuto alla sperimentazione con l'applicazione "piano B", che sarà comunque marginale rispetto al costo totale dell'operazione.

Altri costi che andranno tenuti in considerazione saranno, a titolo esemplificativo e non esaustivo, i costi di comunicazione e pubblicità, i costi di integrazione con eventuali soluzioni internazionali, i costi per i servizi di roaming transfrontaliero del contact tracing e dell'alerting, i costi di sviluppo di dashboard specializzati per specifici scopi istituzionali o medico-sanitari.

Considerazioni sulla sicurezza delle informazioni

Una soluzione applicativa con una diffusione così ampia nella popolazione si presta con elevata probabilità a divenire oggetto di numerosi tentativi di frode e/o attacchi informatici.
Eventuali attività di compromissione potrebbero, ad esempio, essere basate su tecniche di phishing, come creazione di app o di siti "civetta" con loghi o nomi contraffatti che potrebbero essere scambiati per il servizio stesso dagli utenti finali.
E' pertanto di vitale importanza porre la massima attenzione agli aspetti di sicurezza delle informazioni dell'intero sistema di *contact tracing*, al fine di garantire la necessaria resilienza e la continuità operativa dei servizi, anche come contrasto a tentativi esterni di compromissione dei sistemi. Non è stato ad oggi possibile, dato il limitato tempo a disposizione, svolgere un approfondito audit di sicurezza del codice sorgente delle due applicazioni candidate alla fase di sperimentazione. Pertanto si raccomanda fortemente di svolgere quanto prima tale audit, nonché un approfondito *assessment* sui soggetti proponenti e sulle componenti tecnologiche di terze parti utilizzate.
Si raccomanda, altresì, una valutazione del rischio (*risk assessment*) ad ampio raggio dell'intero sistema di *contact tracing* e di tutti i soggetti coinvolti, con particolare riferimento alle differenti ipotesi implementative che potranno essere individuate.
Per questo motivo si rende necessario il coinvolgimento delle autorità preposte alla sicurezza nazionale con specifiche competenze in ambito di *cybersecurity*.
Infine, per garantire una maggiore sicurezza e trasparenza, dopo la verifica eseguita dalle autorità sopra indicate, potrebbe essere opportuno rilasciare pubblicamente il codice sorgente delle applicazioni, in modo che tutta la comunità di esperti in materia di *cybersecurity* a livello nazionale abbia la possibilità di scrutinare il sistema e segnalare eventuali problemi non ancora rilevati.
Tale scelta contribuirebbe, peraltro, ad innalzare il livello di fiducia nel progetto da parte dei cittadini.

La seguente tabella riporta, a titolo puramente indicativo, una preliminare e non esaustiva analisi del rischio (tipologia e livello di rischio associati alla soluzione, unitamente alle possibili mitigazioni), sviluppata in base alla metodologia *STRIDE (vedi legenda)*.

Tipologia	**Rischio**	**Livello**	**Possibile Mitigazione**
Information disclosure / Spoofing	Phishing mediante contraffazioni e diffusione di fake news	Alto	Distribuzione dell'app esclusivamente tramite app store e campagne di informazione
Spoofing	Inquinamento delle liste di contatto	Alto nel caso di CovidApp	Sistema di autenticazione dei client basato su certificati (certificate pinning)
Denial of Service	Attacchi DoS/DDoS agli endpoint backend	Alto	Architettura distribuita, DNS e contromisure anti-DDoS
Denial of Service	Boicottaggio della soluzione sfruttando campagne di disinformazione	Medio	Nudging e campagna di informazione, sorveglianza da parte di AGCOM
Information Disclosure	Exploit del codice o injection di trojan nell'applicazione al fine di raccogliere informazioni sulla posizione GPS, MOBILE, WiFi SSID etc.	Medio	FLOSS e community based, responsible disclosure policy, bug bounty
Elevation of Privilege	Exploit del backend al fine di segnalare possibili falsi contagi seminando panico	Alto	Hardening backend, audit frequenti e analisi logging, SOC
Tampering / Integrità del dato	Alterazione delle informazioni salvate sul device e/o inviate al backend. Renderebbero costruzione del grafo di prossimità impossibile	Medio	Audit e monitoraggio dei sistemi di crittografia e della struttura dati
Non ripudio	Dichiarazione di non aver compiuto una determinata azione (non aver avuto contatti)	Alto	Nudging/comunicazione e consenso informato
Tampering	Switch off del device BLE per non registrare i contatti	Basso	Audit dei log del device ex-post

Legenda:

STRIDE[5] è un processo metodologico che aiuta ad individuare le minacce di sicurezza in un sistema complesso,

- Spoofing (falsificazione di identità): la pretesa di essere qualcos'altro o qualcun altro che non si è.
- Tampering (alterazione dei dati): l'alterazione di qualcosa che si presuppone non sia oggetto di modifica.
- Repudiation (ripudio di una azione): significa dichiarare di non aver fatto qualcosa (indipendentemente dal fatto che sia stato fatto o meno).
- Information Disclosure (divulgazione di informazioni): riguarda l'esposizione delle informazioni a persone non autorizzate alla loro visione.
- Denial of Service (diniego di servizio): sono attacchi designati all'interruzione del servizio.
- Elevation of Privilege (elevazione dei privilegi): avviene quando un programma o un utente è tecnicamente abilitato a fare cose che si presuppone non debba fare.

Privacy

Per le considerazioni sulla protezione dei dati personali e la privacy si fa riferimento alla relazione prodotta dal sottogruppo "Profili giuridici della gestione dei dati connessa all'emergenza".

Conclusioni

Il *contact tracing* o tracciatura dei contatti è una delle azioni di sanità pubblica utilizzate per la prevenzione della diffusione di alcune malattie infettive e rappresenta un elemento importante all'interno di una strategia sostenibile post-emergenza. La sua efficacia è stata ben documentata durante la fase di contenimento della pandemia influenzale del 2009 [3]. In anni più recenti, questo metodo è stato uno strumento prezioso: nel 2014, in seguito all'importazione della malattia da virus Ebola nel Regno Unito [4] e nel 2018 nel caso di monkeypox [5]. I principali vantaggi del *contact tracing* sono che può identificare individui potenzialmente infetti prima che emergano sintomi [1] e, se condotto in modo sufficientemente rapido, può impedire la trasmissione successiva dai casi secondari.

Sulla base di stime recenti per la trasmissione COVID-19, le ricerche empiriche [6] mostrano che per rintracciare almeno l'80% dei contatti delle infezioni rilevate, è necessario prevedere un onere logistico molto elevato, con una media di 36,1 individui (95 percentili: 0-182) tracciati per ogni caso di contagio. Se si rende più larga la definizione di contatto, è possibile ridurre questo onere, ma con un corrispondente aumento del rischio di casi non tracciati; i ricercatori stimano che, per qualsiasi definizione di stretto contatto si voglia adottare, una procedura di *contact tracing* manuale che richieda più di 4 ore di ricerca è probabilmente destinata a generare una diffusione incontrollata dell'infezione. Gli standard di *contact tracing* manuale forniti dall'European Center for Disease Prevention and Control (ECDC) nel

[5] Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design:
https://www.agid.gov.it/it/sicurezza/cert-pa/linee-guida-sviluppo-del-software-sicuro

marzo 2020 relativamente all'epidemia di COVID-19 indicano tuttavia in 12 ore – con l'utilizzo di 3 risorse di personale specializzato - il tempo medio per ogni operazione di *contact tracing*, con un tasso di successo peraltro insufficiente a identificare tutti i contatti o comunque a ridurre il numero di contatti secondari infettati non identificati e isolati sotto l'unità (e quindi a interrompere la riproduzione epidemica).

L'uso della tecnologia in ambito di *contact tracing* appare promettente e in grado di dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale. La tecnologia per il *contact tracing* deve tuttavia essere approcciata in modo molto responsabile ed in linea con i diritti e le libertà fondamentali dei cittadini. Un processo di selezione verso una soluzione tecnica che renda possibile il *contact tracing* tramite *smartphone* ma senza tracciare le persone e/o accedere a dati sensibili e informazioni personali (ad esempio chi sono e dove sono state), è stato di recente avviato a livello europeo da un Consorzio che coinvolge eccellenze nella ricerca scientifica e tecnologica in Europa allo scopo di tracciare solo le relazioni di prossimità a corto raggio che costituiscono un rischio di esposizione e che corrispondono a potenziali catene di trasmissione del virus.

La soluzione paneuropea si basa su tre principi di base, in particolare: 1) è il risultato di un'analisi ben documentata dei benchmark internazionali e di un forte spirito di cooperazione europea; 2) la tecnologia è studiata e selezionata per essere applicabile a livello internazionale, vale a dire interoperabile oltre i confini nazionali; 3) la tecnologia è privacy-preserving e dunque conforme al regolamento generale sulla protezione dei dati (GDPR). Dunque la tecnologia alla base della soluzione europea, rappresenta un contributo importante per consentire il tracciamento della prossimità, anche in modalità transfrontaliera, nel rispetto della privacy, secondo un modello scalabile e aperto che possa essere utilizzato da qualsiasi paese.

Allineandosi a tali principi, questo sottogruppo di lavoro dedicato allo studio delle tecnologie per la gestione dell'emergenza in Italia, ha svolto con rigore metodologico un processo di selezione e valutazione di proposte tecnologiche, rilevate con fast-call di tre giorni dal 24 al 26 marzo u.s. La disamina delle soluzioni è stata articolata su tre livelli consecutivi che, partendo da uno screening generale di tutte le proposte, ha permesso - dopo caratterizzazione analitica e interviste tecniche e organizzative - di giungere all'individuazione di due sole soluzioni tecnologiche, ritenute teoricamente valide per essere testate a scopo di implementazione nell'attuale situazione emergenziale. Si tratta in particolare di Immuni e CovidApp.

I meccanismi e gli standard tecnici dichiarati, sono risultati coerenti con gli obiettivi di sfruttare le possibilità e le caratteristiche della tecnologia digitale per massimizzare la velocità e la capacità in tempo reale di risposta alla pandemia. Inoltre, essi sono risultati

aderenti al modello europeo e orientati al pieno rispetto delle leggi e dei principi europei in materia di privacy e di protezione dei dati personali. In particolare, queste due soluzioni tecnologiche ritenute, in base all'analisi svolta dal gruppo di lavoro, migliori per poter avanzare ad una fase di test sul campo da svolgersi in parallelo su entrambe, sembrano essere tecnologie affidabili e adeguate per il tracciamento della prossimità, per una sicura anonimizzazione dei dati, per creare un contatto tra l'utilizzatore della tecnologia e le figure sanitarie di riferimento, per interagire con interfacce di scambio di dati digitali (API).

Occorre rilevare che per entrambe le soluzioni Immuni e CovidApp sarà necessario svolgere delle attività di personalizzazione e adattamento per renderle compatibili con gli scenari operativi che verranno definiti. La soluzione Immuni utilizza la tecnologia sviluppata dal Consorzio Progetto Europeo PEPP-PT, promettendo quindi maggiori garanzie di interoperabilità e anonimizzazione dei dati personali. Tale soluzione inoltre risulta essere ad uno stadio di sviluppo più avanzato della soluzione CovidApp.

Al fine di poter adottare la soluzione tecnologica più efficace per il *contact tracing* quale componente importante dell'insieme di misure che devono essere messe in campo per la gestione della situazione emergenziale e post-emergenziale, riveste particolare importanza un processo attento ancorché veloce di validazione e messa in esercizio della soluzione tecnologica prescelta, che garantisca il raggiungimento degli obiettivi previsti. Per questa ragione, è opportuno che il processo di implementazione preveda il test in parallelo delle due soluzioni tecnologiche individuate: Immuni, come soluzione che appare all'esito di questa prima valutazione più adeguata e CovidApp, come una buona soluzione alternativa e/o di riserva.

Questo approccio prudenziale serve infatti per avere la garanzia di poter disporre di almeno una soluzione da mettere in campo, anche quando si verificasse, in una sperimentazione concreta, il fallimento per qualunque motivo della funzionalità e/o dei livelli prestazionali richiesti dell'altra opzione alternativa. La fase di test include ovviamente sia la verifica della sicurezza sull'intero codice sorgente (a cura del comparto di *intelligence*) sia la verifica del funzionamento in campo da svolgersi in diverse aree circoscritte del territorio. Si tratterà in ogni caso, indipendentemente dalla soluzione tecnologica che anche ai test di verifica dovesse risultare preferita e più affidabile, di un processo dinamico in evoluzione migliorativa che da una prima versione tecnologica passerà a versioni più avanzate e performanti dal punto di vista sia tecnico che di utilizzo concreto. Pertanto, grande importanza assume a questo riguardo una pianificazione di sviluppo agile che preveda una serie di rilasci scaglionati nel tempo dell'utilizzo della tecnologia.

La proposizione della soluzione tecnologica per il *contact-tracing* che uscirà vincente ai test, prima di essere implementata sul campo, dovrebbe infine essere calata in un quadro

strategico-organizzativo più ampio a carico del decisore politico, il quale, per controllare la trasmissione dei contagi, dovrebbe tenere in considerazione non solo altre misure di prevenzione (ad esempio il distanziamento sociale per fasce di popolazione particolarmente fragili) in aggiunta a quelle basate su soluzioni tecnologiche per il *contact tracing* ma anche strategie di azione di carattere generale. Tale strategia permette una efficiente applicazione delle azioni preventive anche verso alcuni segmenti della popolazione Italiana ad alto rischio come gli anziani e il personale sanitario. Negli scenari studiati, è evidente che l'uso di tecnologie per il contact tracing ha la maggiore efficacia prima del termine del periodo di lockdown, quando le misure di isolamento hanno consentito di ridurre il più possibile il tasso di riproduzione di base dell'infezione.

Decisioni richieste alle autorità pubbliche

Decisioni richieste alle autorità pubbliche

Per mettere in esercizio il sistema di *contact tracing*, il decisore pubblico dovrebbe:

A. **Nominare un Program Manager** con piena delega decisionale sul progetto da parte dell'autorità pubblica, al fine di garantire presidio e tempestività nell'implementazione e nel governo dei processi tecnologici.
B. **Scegliere tra le principali opzioni tecnico-organizzative** che impattano su questioni chiave di salute pubblica e di tutela della privacy. Si sollecita quindi una decisione immediata ed esplicita su ciascuno dei seguenti punti:

    1. *Policy per le tecnologie di contact tracing.* I sistemi di *tracing* e le proposte selezionate possono avvalersi di strumenti di rilevazione dei contatti che hanno diversi livelli di impatto atteso sull'efficacia degli interventi di salute pubblica e sul trattamento dei dati personali. Le opzioni proposte sono:
        a) **Solo tecnologie di prossimità senza geolocalizzazione (Bluetooth-LE)** come da modello europeo proposto da PEPP-PT (Pan-European Privacy Preserving Proximity Tracing). Vantaggi: migliore protezione dei dati grazie a codici identificativi univoci che contraddistinguono le installazioni delle applicazioni, resi sufficientemente anonimi, in aderenza al modello PEPP-PT. Svantaggi: minore copertura di situazioni con bassa presenza di device abilitati, mancata indicazione di luoghi di possibile contaminazione ambientale da sanitizzare.
        b) **Bluetooth-LE + GPS e/o altre tecnologie che consentano la geolocalizzazione** (solo dei singoli punti di potenziale contagio, non dei percorsi personali, con criptazione dei dati e dietro *opt-in* informato). Vantaggi: maggiore copertura rispetto alla base di

smartphone diffusi in Italia ed Europa, maggiore potenziale per l'identificazione di luoghi da sanitizzare. Svantaggi: uso di informazioni riconducibili a dati di carattere personale (posizione del *device*).

2. *Policy da applicare per allertamento a seguito di contagio*. Nel caso in cui un cittadino dotato di app risultasse positivo ai test, è possibile attivare due diverse procedure di allertamento:
    a. **Procedura manuale e volontaria:** (come da modello PEPP-PT) questa opzione prevede un'autorizzazione esplicita e un'azione tecnica da parte del cittadino (foto di un codice QR o immissione di un codice rilasciato dall'autorità sanitaria in caso di test positivo al virus) affinché la propria storia dei contatti anonimizzati venga trasmessa ai server delle autorità e quindi consenta di avviare il processo di allertamento. Vantaggi: i dati sui contatti risiedono solo sul *device* del soggetto. Svantaggi: maggior rischio di malfunzionamenti nella procedura di invio dati, nonché di mancato adempimento spontaneo e/o di ritardo temporale nell'adempimento da parte del cittadino, con l'effetto di ridurre l'efficacia del *contact tracing*.
    b. **Procedura pre-autorizzata automatica:** la seconda opzione prevede che la lista dei contatti anonimizzati sia a disposizione dell'autorità sanitaria, con pre-autorizzazione concessa dal cittadino al momento dell'installazione della app; Vantaggi: massima tempestività ed efficacia del processo di allertamento dei contatti. Svantaggi: i dati dei contatti risiedono sui server dell'autorità pubblica, con i rischi caratteristici della centralizzazione di una base dati, mitigabili con opportune soluzioni tecnologiche.
3. *Policy da applicare per garantire l'enforcement delle azioni di carattere sanitario conseguenti*. A seguito della rilevazione di un caso positivo e dell'allertamento dei soggetti con cui è entrato in contatto, devono seguire azioni di carattere sanitario (ad esempio la quarantena e/o l'autoisolamento per i soggetti entrati in contatto con il caso positivo), che possono essere intraprese in base alle seguenti opzioni:
    a. **Procedura volontaria**: questa opzione prevede che i contatti esposti al rischio di contagio rimangano non identificati (quindi non conosciuti alle autorità sanitarie) e che pertanto essi si assoggettino spontaneamente ai provvedimenti di contenimento indicati nel messaggio di allertamento inviato al loro *device*. Vantaggi: maggior protezione dei dati personali, anche dopo un possibile allertamento sul rischio di contagio. Svantaggi: maggiori rischi di mancata adesione e/o di ritardo temporale nell'adesione alle misure di contenimento da parte

del contatto allertato, con l'effetto di ridurre l'efficacia del *contact tracing*.

b. **Procedura proattiva**: questa opzione prevede (come da corrente prassi di *contact tracing* manuale su linee guida OMS/ECDC) che l'autorità sanitaria richieda e ottenga l'identificazione nominale da parte dei soggetti destinatari dei messaggi di allertamento a seguito di avvenuto contatto con pazienti positivi, prevedendo opportune sanzioni per le eventuali inadempienze. Vantaggi: massima tempestività ed efficacia delle azioni di contenimento dei contatti esposti a potenziale trasmissione del contagio, migliore *compliance* attesa. Svantaggi: raccolta di dati dell'app, a priori ed indipendentemente dal processo di *contact tracing*, necessità di opportuna comunicazione e coinvolgimento dei cittadini.

Bibliografia

1. Abbott S, Hellewell J, Munday J et al., *Temporal variation in transmission during the COVID-19 outbreak*. Centre for Mathematical Modelling of Infectious Disease, 2020, https://cmmid.github.io/topics/covid19/current-patterns-transmission/global-time-varying-transmission.html

2. Ferretti L, Wymant C, Kendall M et al, *Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing,* 2020, doi:https://doi.org/10.1101/2020.03.08.20032946, available at: https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/

3. McLean E, Pebody RG, Campbell C, Chamberland M, Hawkins C, Nguyen-Van-Tam JS, Oliver I, Smith GE, Ihekweazu C, Bracebridge S, Maguire H, Harris R, Kafatos G, White PJ, Wynne-Evans E, Green J, Myers R, Underwood A, Dallman T, Wreghitt T, Zambon M, Ellis J, Phin N, Smyth B, McMenamin J, Watson JM. *Pandemic (H1N1) 2009 influenza in the UK: clinical and epidemiological findings from the first few hundred (FF100) cases*. Epidemiol Infect. 2010;138:1531-41

4. Crook P, Smith-Palmer A, Maguire H, McCarthy N, Kirkbride H, Court B, Kanagarajah S, Turbitt D, Ahmed S, Cosford P, Oliver I. *Lack of Secondary Transmission of Ebola Virus from Healthcare Worker to 238 Contacts*, United Kingdom, December 2014. Emerg Infect Dis. 2017;23:2081-2084

5. Vaughan A, Aarons E, Astbury J, Balasegaram S, Beadsworth M, Beck CR, Chand M, O'Connor C, Dunning J, Ghebrehewet S, Harper N, Howlett-Shipley R, Ihekweazu C, Jacobs M, Kaindama L, Katwa P, Khoo S, Lamb L, Mawdsley S, Morgan D, Palmer R, Phin N, Russell K, Said B, Simpson A, Vivancos R, Wade M, Walsh A, Wilburn J. *Two cases of monkeypox imported to the United Kingdom*, September 2018. Euro Surveill. 2018;23
6. Matt J Keeling et al., *The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19)*, medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036

MINISTRO
PER L'INNOVAZIONE
TECNOLOGICA
E LA DIGITALIZZAZIONE

Impiego di tecnologie di digital contact tracing

Coordinatori:
Fidelia Cascini, Università Cattolica S. Cuore
Paolo De Rosa, Dipartimento per la trasformazione digitale

Componenti del sottogruppo:
Francesca Bria, UCL London e Fondo Innovazione
Carlo Alberto Carnevale Maffè, Università Bocconi, Milano
Ciro Cattuto, Università di Torino
Leonardo Favario, Dipartimento per la trasformazione digitale
Alfonso Fuggetta, Politecnico di Milano
Andrea Nicolini, Fondazione Bruno Kessler
Alberto E. Tozzi, Ospedale Pediatrico "Bambino Gesù", Roma
Simone Piunno, Università Bocconi, Milano
Stefano Calabrese, Dipartimento della Protezione Civile
Umberto Rosini, Dipartimento della Protezione Civile

Executive Summary

Il *contact tracing* o tracciatura dei contatti è una delle azioni di sanità pubblica utilizzate per la prevenzione della diffusione di alcune malattie infettive e rappresenta un elemento importante all'interno di una strategia sostenibile post-emergenza. La sua efficacia è stata ben documentata durante la fase di contenimento della pandemia influenzale del 2009 [3]. In anni più recenti, questo metodo è stato uno strumento prezioso: nel 2014, in seguito all'importazione della malattia da virus Ebola nel Regno Unito [4] e nel 2018 nel caso di monkeypox [5]. I principali vantaggi del *contact tracing* sono che può identificare individui potenzialmente infetti prima che emergano sintomi [1] e, se condotto in modo sufficientemente rapido, può impedire la trasmissione successiva dai casi secondari.

Sulla base di stime recenti per la trasmissione COVID-19, le ricerche empiriche [6] mostrano che per rintracciare almeno l'80% dei contatti delle infezioni rilevate, è necessario prevedere un onere logistico molto elevato, con una media di 36,1 individui (95 percentili: 0-182) tracciati per ogni caso di contagio. Se si rende più larga la definizione di contatto, è possibile ridurre questo onere, ma con un corrispondente aumento del rischio di casi non tracciati; i ricercatori stimano che, per qualsiasi definizione di stretto contatto si voglia adottare, una procedura di *contact tracing* manuale che richieda più di 4 ore di ricerca è probabilmente destinata a generare una diffusione incontrollata dell'infezione. Gli standard di *contact tracing* manuale forniti dall'European Center for Disease Prevention and Control (ECDC) nel marzo 2020 relativamente all'epidemia di COVID-19 indicano tuttavia in 12 ore – con l'utilizzo di 3 risorse di personale specializzato - il tempo medio per ogni operazione di *contact tracing*, con un tasso di successo peraltro insufficiente a identificare tutti i contatti o comunque a ridurre il numero di contatti secondari infettati non identificati e isolati sotto l'unità (e quindi a interrompere la riproduzione epidemica).

L'uso della tecnologia in ambito di *contact tracing* appare promettente e in grado di dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale. La tecnologia per il *contact tracing* deve tuttavia essere approcciata in modo molto responsabile ed in linea con i diritti e le libertà fondamentali dei cittadini. Un processo di selezione verso una soluzione tecnica che renda possibile il *contact tracing* tramite *smartphone* ma senza tracciare le persone e/o accedere a dati sensibili e informazioni personali (ad esempio chi sono e dove sono state), è stato di recente avviato a livello europeo da un Consorzio che coinvolge eccellenze nella ricerca scientifica e tecnologica in Europa allo scopo di tracciare solo le relazioni di prossimità a corto raggio che costituiscono un rischio di esposizione e che corrispondono a potenziali catene di trasmissione del virus.

La soluzione paneuropea si basa su tre principi di base, in particolare: 1) è il risultato di un'analisi ben documentata dei benchmark internazionali e di un forte spirito di cooperazione europea; 2) la tecnologia è studiata e selezionata per essere applicabile a livello internazionale, vale a dire interoperabile oltre i confini nazionali; 3) la tecnologia è privacy-preserving e dunque conforme al regolamento generale sulla protezione dei dati (GDPR). Dunque la tecnologia alla base della soluzione europea, rappresenta un contributo importante per consentire il tracciamento della prossimità, anche in modalità transfrontaliera, nel rispetto della privacy, secondo un modello scalabile e aperto che possa essere utilizzato da qualsiasi paese.

Allineandosi a tali principi, questo sottogruppo di lavoro dedicato allo studio delle tecnologie per la gestione dell'emergenza in Italia, ha svolto con rigore metodologico un processo di selezione e valutazione di proposte tecnologiche, rilevate con fast-call di tre giorni dal 24 al

26 marzo u.s. La disamina delle soluzioni è stata articolata su tre livelli consecutivi che, partendo da uno screening generale di tutte le proposte, ha permesso - dopo caratterizzazione analitica e interviste tecniche e organizzative - di giungere all'individuazione di due sole soluzioni tecnologiche, ritenute teoricamente valide per essere testate a scopo di implementazione nell'attuale situazione emergenziale. Si tratta in particolare di Immuni e CovidApp.

I meccanismi e gli standard tecnici dichiarati, sono risultati coerenti con gli obiettivi di sfruttare le possibilità e le caratteristiche della tecnologia digitale per massimizzare la velocità e la capacità in tempo reale di risposta alla pandemia. Inoltre, essi sono risultati aderenti al modello europeo e orientati al pieno rispetto delle leggi e dei principi europei in materia di privacy e di protezione dei dati personali. In particolare, queste due soluzioni tecnologiche ritenute, in base all'analisi svolta dal gruppo di lavoro, migliori per poter avanzare ad una fase di test sul campo da svolgersi in parallelo su entrambe, sembrano essere tecnologie affidabili e adeguate per il tracciamento della prossimità, per una sicura anonimizzazione dei dati, per creare un contatto tra l'utilizzatore della tecnologia e le figure sanitarie di riferimento, per interagire con interfacce di scambio di dati digitali (API).

Occorre rilevare che per entrambe le soluzioni Immuni e CovidApp sarà necessario svolgere delle attività di personalizzazione e adattamento per renderle compatibili con gli scenari operativi che verranno definiti. La soluzione Immuni utilizza la tecnologia sviluppata dal Consorzio Progetto Europeo PEPP-PT, promettendo quindi maggiori garanzie di interoperabilità e anonimizzazione dei dati personali. Tale soluzione inoltre risulta essere ad uno stadio di sviluppo più avanzato della soluzione CovidApp.

Al fine di poter adottare la soluzione tecnologica più efficace per il *contact tracing* quale componente importante dell'insieme di misure che devono essere messe in campo per la gestione della situazione emergenziale e post-emergenziale, riveste particolare importanza un processo attento ancorché veloce di validazione e messa in esercizio della soluzione tecnologica prescelta, che garantisca il raggiungimento degli obiettivi previsti. Per questa ragione, è opportuno che il processo di implementazione preveda il test in parallelo delle due soluzioni tecnologiche individuate: Immuni, come soluzione che appare all'esito di questa prima valutazione più adeguata e CovidApp, come una buona soluzione alternativa e/o di riserva.

Questo approccio prudenziale serve infatti per avere la garanzia di poter disporre di almeno una soluzione da mettere in campo, anche quando si verificasse, in una sperimentazione concreta, il fallimento per qualunque motivo della funzionalità e/o dei livelli prestazionali richiesti dell'altra opzione alternativa. La fase di test include ovviamente sia la verifica della

sicurezza sull'intero codice sorgente (a cura del comparto di *intelligence*) sia la verifica del funzionamento in campo da svolgersi in diverse aree circoscritte del territorio. Si tratterà in ogni caso, indipendentemente dalla soluzione tecnologica che anche ai test di verifica dovesse risultare preferita e più affidabile, di un processo dinamico in evoluzione migliorativa che da una prima versione tecnologica passerà a versioni più avanzate e performanti dal punto di vista sia tecnico che di utilizzo concreto. Pertanto, grande importanza assume a questo riguardo una pianificazione di sviluppo agile che preveda una serie di rilasci scaglionati nel tempo dell'utilizzo della tecnologia.

La proposizione della soluzione tecnologica per il *contact-tracing* che uscirà vincente ai test, prima di essere implementata sul campo, dovrebbe infine essere calata in un quadro strategico-organizzativo più ampio a carico del decisore politico, il quale, per controllare la trasmissione dei contagi, dovrebbe tenere in considerazione non solo altre misure di prevenzione (ad esempio il distanziamento sociale per fasce di popolazione particolarmente fragili) in aggiunta a quelle basate su soluzioni tecnologiche per il *contact tracing* ma anche strategie di azione di carattere generale. Tale strategia permette una efficiente applicazione delle azioni preventive anche verso alcuni segmenti della popolazione Italiana ad alto rischio come gli anziani e il personale sanitario. Negli scenari studiati, è evidente che l'uso di tecnologie per il contact tracing ha la maggiore efficacia prima del termine del periodo di lockdown, quando le misure di isolamento hanno consentito di ridurre il più possibile il tasso di riproduzione di base dell'infezione.

Decisioni richieste alle autorità pubbliche

Decisioni richieste alle autorità pubbliche

Per mettere in esercizio il sistema di *contact tracing*, il decisore pubblico dovrebbe:

A. **Nominare un Program Manager** con piena delega decisionale sul progetto da parte dell'autorità pubblica, al fine di garantire presidio e tempestività nell'implementazione e nel governo dei processi tecnologici.
B. **Scegliere tra le principali opzioni tecnico-organizzative** che impattano su questioni chiave di salute pubblica e di tutela della privacy. Si sollecita quindi una decisione immediata ed esplicita su ciascuno dei seguenti punti:

    1. *Policy per le tecnologie di contact tracing.* I sistemi di *tracing* e le proposte selezionate possono avvalersi di strumenti di rilevazione dei contatti che

hanno diversi livelli di impatto atteso sull'efficacia degli interventi di salute pubblica e sul trattamento dei dati personali. Le opzioni proposte sono:

a) **Solo tecnologie di prossimità senza geolocalizzazione (Bluetooth-LE)** come da modello europeo proposto da PEPP-PT (Pan-European Privacy Preserving Proximity Tracing). Vantaggi: migliore protezione dei dati grazie a codici identificativi univoci che contraddistinguono le installazioni delle applicazioni, resi sufficientemente anonimi, in aderenza al modello PEPP-PT. Svantaggi: minore copertura di situazioni con bassa presenza di device abilitati, mancata indicazione di luoghi di possibile contaminazione ambientale da sanitizzare.

b) **Bluetooth-LE + GPS e/o altre tecnologie che consentano la geolocalizzazione** (solo dei singoli punti di potenziale contagio, non dei percorsi personali, con criptazione dei dati e dietro *opt-in* informato). Vantaggi: maggiore copertura rispetto alla base di smartphone diffusi in Italia ed Europa, maggiore potenziale per l'identificazione di luoghi da sanitizzare. Svantaggi: uso di informazioni riconducibili a dati di carattere personale (posizione del *device*).

2. *Policy da applicare per allertamento a seguito di contagio*. Nel caso in cui un cittadino dotato di app risultasse positivo ai test, è possibile attivare due diverse procedure di allertamento:

   a. **Procedura manuale e volontaria:** (come da modello PEPP-PT) questa opzione prevede un'autorizzazione esplicita e un'azione tecnica da parte del cittadino (foto di un codice QR o immissione di un codice rilasciato dall'autorità sanitaria in caso di test positivo al virus) affinché la propria storia dei contatti anonimizzati venga trasmessa ai server delle autorità e quindi consenta di avviare il processo di allertamento. Vantaggi: i dati sui contatti risiedono solo sul *device* del soggetto. Svantaggi: maggior rischio di malfunzionamenti nella procedura di invio dati, nonché di mancato adempimento spontaneo e/o di ritardo temporale nell'adempimento da parte del cittadino, con l'effetto di ridurre l'efficacia del *contact tracing*.

   b. **Procedura pre-autorizzata automatica:** la seconda opzione prevede che la lista dei contatti anonimizzati sia a disposizione dell'autorità sanitaria, con pre-autorizzazione concessa dal cittadino al momento dell'installazione della app; Vantaggi: massima tempestività ed efficacia del processo di allertamento dei contatti. Svantaggi: i dati dei contatti risiedono sui server dell'autorità pubblica, con i rischi

caratteristici della centralizzazione di una base dati, mitigabili con opportune soluzioni tecnologiche.

3. *Policy da applicare per garantire l'enforcement delle azioni di carattere sanitario conseguenti*. A seguito della rilevazione di un caso positivo e dell'allertamento dei soggetti con cui è entrato in contatto, devono seguire azioni di carattere sanitario (ad esempio la quarantena e/o l'autoisolamento per i soggetti entrati in contatto con il caso positivo), che possono essere intraprese in base alle seguenti opzioni:
    a. **Procedura volontaria**: questa opzione prevede che i contatti esposti al rischio di contagio rimangano non identificati (quindi non conosciuti alle autorità sanitarie) e che pertanto essi si assoggettino spontaneamente ai provvedimenti di contenimento indicati nel messaggio di allertamento inviato al loro *device*. Vantaggi: maggior protezione dei dati personali, anche dopo un possibile allertamento sul rischio di contagio. Svantaggi: maggiori rischi di mancata adesione e/o di ritardo temporale nell'adesione alle misure di contenimento da parte del contatto allertato, con l'effetto di ridurre l'efficacia del *contact tracing*.
    b. **Procedura proattiva**: questa opzione prevede (come da corrente prassi di *contact tracing* manuale su linee guida OMS/ECDC) che l'autorità sanitaria richieda e ottenga l'identificazione nominale da parte dei soggetti destinatari dei messaggi di allertamento a seguito di avvenuto contatto con pazienti positivi, prevedendo opportune sanzioni per le eventuali inadempienze. Vantaggi: massima tempestività ed efficacia delle azioni di contenimento dei contatti esposti a potenziale trasmissione del contagio, migliore *compliance* attesa. Svantaggi: raccolta di dati dell'app, a priori ed indipendentemente dal processo di *contact tracing*, necessità di opportuna comunicazione e coinvolgimento dei cittadini.

Sommario finale delle decisioni dell'autorità politica:

A) Program manager designato: _____

B) Policies tecnico-operative:

Policy	**Opzione a)**	**Opzione b)**

Tecnologie di contact tracing	non geolocalizzate:___	anche geolocalizzate:___
Allertamento in seguito a contagio	manuale:___	automatica:___
Enforcement sanitario per contatti a rischio contagio	volontaria:___	proattiva:___

Allegato tecnico

Il contact tracing - nella sua modalità tradizionale - è una prassi consolidata nei processi di contenimento di malattie contagiose. La cronologia dei contatti personali di un soggetto infetto è normalmente oggetto di procedure manuali basate su interviste da parte di personale dedicato, di fronte alle cui domande il paziente è legalmente tenuto a fornire risposte puntuali e circostanziate. Gli standard di processo indicati dall'European Center for Disease Prevention and Control (ECDC) prevedono (vedi tabella qui sotto) un tempo medio per le operazioni di *contact tracing* che risulta tuttavia eccessivo rispetto ai cicli di riproduzione epidemiologica fatti registrare nei casi di COVID-19.

Total time needed to manually assess the contact history for ONE case of COVID19 + delay in interviewing contacts

(3 specialized staff involved)

Table 1. Estimated resources needed for contact tracing

Activity	Human resources			Material
	Staff profile	Number of staff	Time (per staff)	
Interview case (*)	HCW/public health staff	One	Two hours	• Phone • Questionnaire • Translation services (if necessary)
Create contact list and retrieve personal information. This may require collaboration with other entities, including transport authorities, companies, and hospitals.	Administrative or other services	One	Six hours	
Enter interview in the system (e.g. electronic information system or excel file)	HCW/ public health staff	One	One hour	• Database
Classification of contacts as high or low-risk exposure; including prioritisation of whom to contact.	Two HCW/ public health staff One administrative or other services	Three	Two hours	
Initial interview by phone with contacts. Through this interview, staff will establish the contacts' level of exposure, ask about symptoms and other personal information. Staff will also provide information about infection control measures, symptom monitoring and other precautionary measures.	HCW/ public health staff	One	45 min.	• Phone • Questionnaire
Enter information from interview into database	HCW/ public health staff	One	15 min.	• Database
			12 hours	

Fonte: ECDC; Marzo 2020

A ridurre tale grave ritardo nella identificazione dei contatti, nonché alla strutturale imprecisione dovuta alla ricostruzione orale e mnemonica della possibile catena trasmissiva, vuol offrire un contributo rigoroso ed efficace proprio l'adozione di tecnologie di contact tracing digitale, come meglio descritto nel presente allegato tecnico.

Va fin da subito segnalato, in merito alle pur doverose analisi ai fini di garantire la tutela dei dati personali, che con il contact tracing digitale non si riscontrerebbe uno specifico differenziale in termini di trattamento delle informazioni relative ai luoghi visitati: le stesse

informazioni vengono infatti già raccolte oralmente oggi, solo che richiedono tempi, costi e risorse incompatibili con la gestione dell'emergenza e le specifiche caratteristiche epidemiologiche del COVID-19. Inoltre, l'attuale livello di protezione contro i rischi di copia, diffusione o modifiche non autorizzate dei dati personali, come nel processo correntemente applicato in Italia, ovvero di informazioni di contact tracing raccolte oralmente e su moduli cartacei, è da ritenersi non adeguato e certamente inferiore a quanto si può ottenere con il trattamento dei dati in modalità digitale protetta e crittografata.

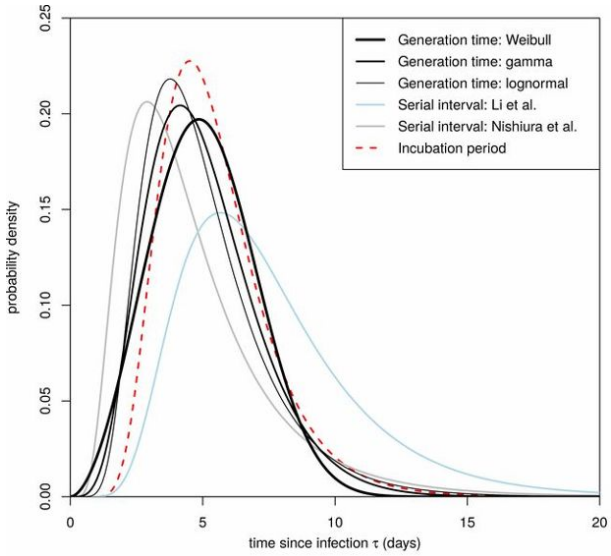
Per meglio comprendere che l'attuale livello di trattamento dei dati personali per i processi di contact tracing manuale è meno tutelante per i cittadini rispetto al processo di contact tracing digitale, basta riferirsi al "data dictionary" (vedi tabella qui sotto) pubblicato dalle Technical Guidelines dell'OMS (https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance) per la reportistica dei casi di contagio. Le informazioni richieste al paziente, annotate prima sul modulo cartaceo e poi copiate – con relativo rischio di errori di imputazione - su una tabella elettronica, riguardano precisi dettagli di luoghi, orari e identità delle persone con le quali si sono verificati contatti, anche accidentali, nelle 2 settimane precedenti.

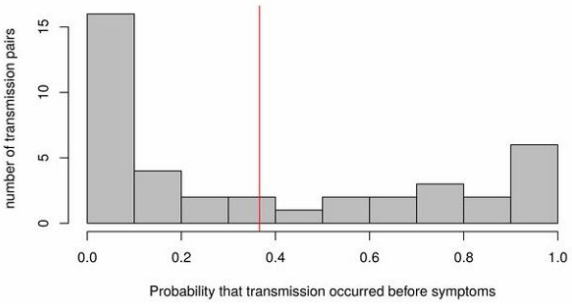
Tx section	Variable name	Short label EN	Format
Exposure and travel information	patinfo_occuhcw	Health care worker	Coded variables
Exposure and travel information	patinfo_occuhcw_country	Healthcare worker country	Free text
Exposure and travel information	patinfo_occuhcw_city	Healthcare worker city	Free text
Exposure and travel information	patinfo_occuhcw_name	Healthcare worker facility name	Free text
Exposure and travel information	expo_travel	Has the patient travelled in the 14 days prior to symptom onset?	Coded variables
Exposure and travel information	expo_travel_country1	Specify country travelled to 1	Free text
Exposure and travel information	expo_travel_city1	Specify city travelled to 1	Free text
Exposure and travel information	expo_travel_date1	Specify date departed from 1	DD/MM/YYYY
Exposure and travel information	expo_travel_country2	Specify country travelled to 2	Free text
Exposure and travel information	expo_travel_city2	Specify city travelled to 2	Free text
Exposure and travel information	expo_travel_date2	Specify date departed from 2	DD/MM/YYYY
Exposure and travel information	expo_travel_country3	Specify country travelled to 3	Free text
Exposure and travel information	expo_travel_city3	Specify city travelled to 3	Free text
Exposure and travel information	expo_travel_date3	Specify date departed from 3	DD/MM/YYYY
Exposure and travel information	expo_visit_healthcare	Has the patient visited any health care facilities in the 14 days prior to symptom onset	Coded variables
Exposure and travel information	expo_contact_case	Has the patient had contact with a confirmed case?	Coded variables
Exposure and travel information	expo_case_setting_detail	Explain contact setting	Free text
Exposure and travel information	expo_ID1	ID number of confirmed case 1	Free text
Exposure and travel information	expo_ID2	ID number of confirmed case 2	Free text
Exposure and travel information	expo_ID3	ID number of confirmed case 3	Free text
Exposure and travel information	expo_ID4	ID number of confirmed case 4	Free text
Exposure and travel information	expo_ID5	ID number of confirmed case 5	Free text
Exposure and travel information	expo_case_date_first1	Date of first exposure to confirmed case 1	DD/MM/YYYY
Exposure and travel information	expo_case_date_first2	Date of first exposure to confirmed case 2	DD/MM/YYYY
Exposure and travel information	expo_case_date_first3	Date of first exposure to confirmed case 3	DD/MM/YYYY
Exposure and travel information	expo_case_date_first4	Date of first exposure to confirmed case 4	DD/MM/YYYY
Exposure and travel information	expo_case_date_first5	Date of first exposure to confirmed case 5	DD/MM/YYYY
Exposure and travel information	expo_case_date_last1	Date of last exposure to confirmed case 1	DD/MM/YYYY
Exposure and travel information	expo_case_date_last2	Date of last exposure to confirmed case 2	DD/MM/YYYY
Exposure and travel information	expo_case_date_last3	Date of last exposure to confirmed case 3	DD/MM/YYYY
Exposure and travel information	expo_case_date_last4	Date of last exposure to confirmed case 4	DD/MM/YYYY
Exposure and travel information	expo_case_date_last5	Date of last exposure to confirmed case 5	DD/MM/YYYY
Exposure and travel information	expo_case_location	Likely country for exposure to case?	Free text

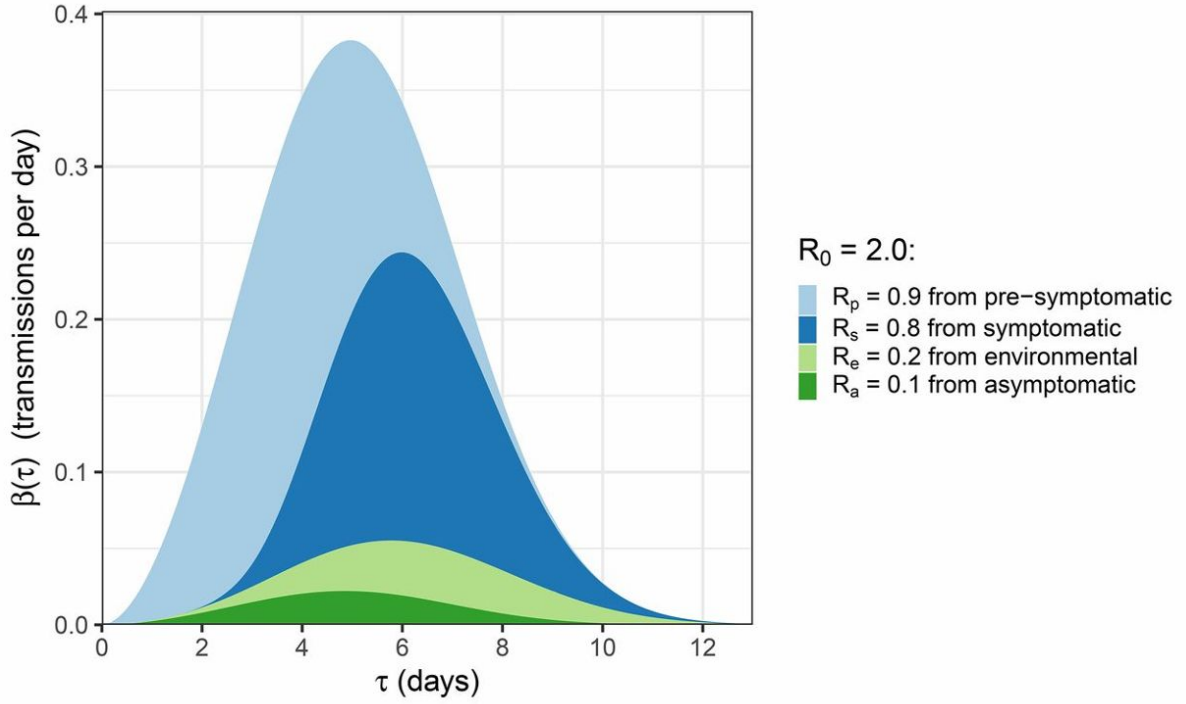
Fonte: OMS, Technical Guidelines for COVID-19, March 2020

Con il contact tracing digitale, quindi, sarà possibile automatizzare gran parte del processo di compilazione dei record, diminuendo tempi e rischio di errori e consentendo massima portabilità dei dati aggregati e anonimi.

L'efficacia del contact tracing digitale nel contribuire al contenimento del contagio è supportata dalle più recenti ricerche scientifiche sull'epidemia di COVID-19. Secondo una ricerca della Oxford University pubblicata su Science (Ferretti et al, 2020, citato nel grafico qui sotto), i tradizionali processi di contact tracing manuale successivi all'esecuzione di test biologici non risultano essere abbastanza tempestivi ed efficaci, a causa del ritardo di insorgenza dei sintomi rispetto all'infettività e della tardiva disponibilità dei risultati e dei successivi allarmi e interventi di isolamento dei positivi e quarantena dei contatti. La ricerca empirica evidenzia che in media il 55% (intervallo di confidenza: 37% - 72%) delle trasmissioni avviene prima dell'insorgenza dei sintomi, con un *generation period* molto breve (circa 5 giorni di media, con circa 2 giorni di deviazione standard, vedi grafici qui sotto, tratti dall'articolo di Ferretti et al. su Science). Il grafico superiore riporta diverse rappresentazioni del *generation period* e la probabilità di trasmissione pre-sintomatica. Il grafico inferiore riporta il modello di infettività utilizzato nella ricerca.

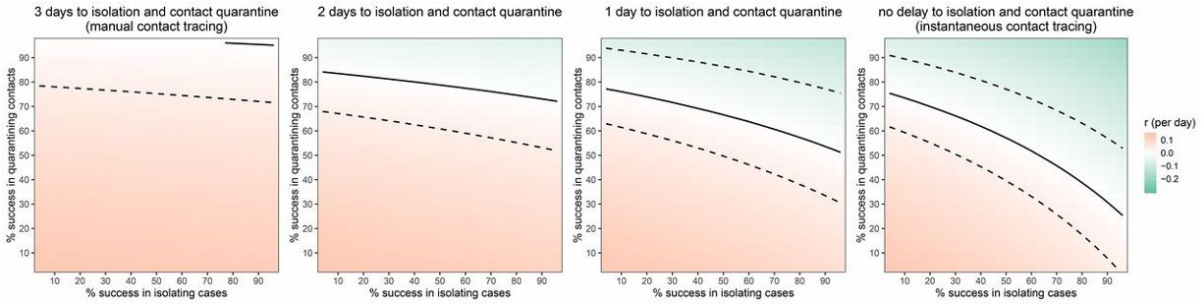






Fonte: Quantifying SARS-CoV-2 transmission suggests epidemic control digital with contact tracing, Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, David GBonsall, Christophe Fraser. Science, 31 Mar 2020: eabb6936, DOI: 10.1126/science.abb6936

Quindi la ricostruzione della catena trasmissiva a partire dal solo esito dei test diagnostici risulta insufficiente e tardiva. Infatti, l'isolamento dei positivi non ha effetti risolutivi sulla riduzione di R_0 al di sotto dell'unità. Il modello del Big Data Institute – che dispone anche di un motore di calcolo on-line di sensitivity analysis sui diversi parametri epidemiologici e scenari di contenimento reperibile a questo link: https://045.medsci.ox.ac.uk - mostra come sia necessario individuare e mettere tempestivamente in quarantena una significativa percentuale dei contatti di primo livello, da tracciare con adeguate soluzioni tecnologiche ricostruendo la cronologia dei contatti nelle precedenti giornate. I grafici seguenti mostrano come anche ad elevati livelli di successo nell'isolamento dei casi positivi (in ascissa), serva una significativa quota di rapida identificazione e messa in quarantena almeno dei contatti di primo livello (in ordinata) per poter mettere sotto controllo l'epidemia. Inoltre, come evidenziato dalla comparazione dei diversi grafici, risulta particolarmente critica la variabile temporale per l'efficacia dell'intero processo: nel grafico più a destra, a fronte dell'immediato intervento di isolamento e/o quarantena dei contatti a seguito di digital tracing, la curva nera piena - che rappresenta R=0 nelle diverse combinazioni di isolamento e quarantena che interrompono il diffondersi dell'epidemia - si presenta più bassa e quindi più controllabile. A mano a mano che cresce il tempo di intervento (1, 2 o 3 giorni di ritardo, negli altri grafici più a sinistra), la soglia di efficacia del contact tracing si sposta più in alto. Le implicazioni di questa analisi sono chiarissime: mentre con il contact tracing digitale si possono ridurre i tempi di intervento in modo tale da contrastare efficacemente l'epidemia, con il contact tracing tradizionale si scontano ritardi tali da compromettere gravemente l'efficacia delle misure di quarantena dei contatti.



Fonte: Quantifying SARS-CoV-2 transmission suggests epidemic control digital with contact tracing, Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, David GBonsall, Christophe Fraser. Science, 31 Mar 2020: eabb6936, DOI: 10.1126/science.abb6936

Più specificamente, la sequenza di grafici (modello "mappa di calore") mostra il tasso di crescita esponenziale dell'epidemia "r" in funzione del tasso di successo dell'isolamento dei casi sintomatici (asse x) e del tasso di successo del tracing del contatto (asse y). I valori positivi di "r" (rosso) implicano un'epidemia crescente; valori negativi di "r" (verde) implicano un'epidemia in declino, con valori negativi maggiori che implicano un declino più rapido. La linea nera piena mostra r = 0, cioè la soglia per il controllo dell'epidemia. Le linee tratteggiate mostrano l'incertezza nella soglia dovuta all'incertezza in R0. I diversi grafici mostrano la variazione dell'efficacia del tracing in seguito alle variazioni nel ritardo associato all'intervento, dall'avvio dei sintomi all'isolamento del caso e alla quarantena dei contatti.

Il grafico successivo, tratto da un paper scientifico pubblicato su The Lancet il 28/2/2020 (vedi citazione qui sotto), illustra un processo simulato di contagio utilizzabile per la modellazione matematica del "contact tracing".

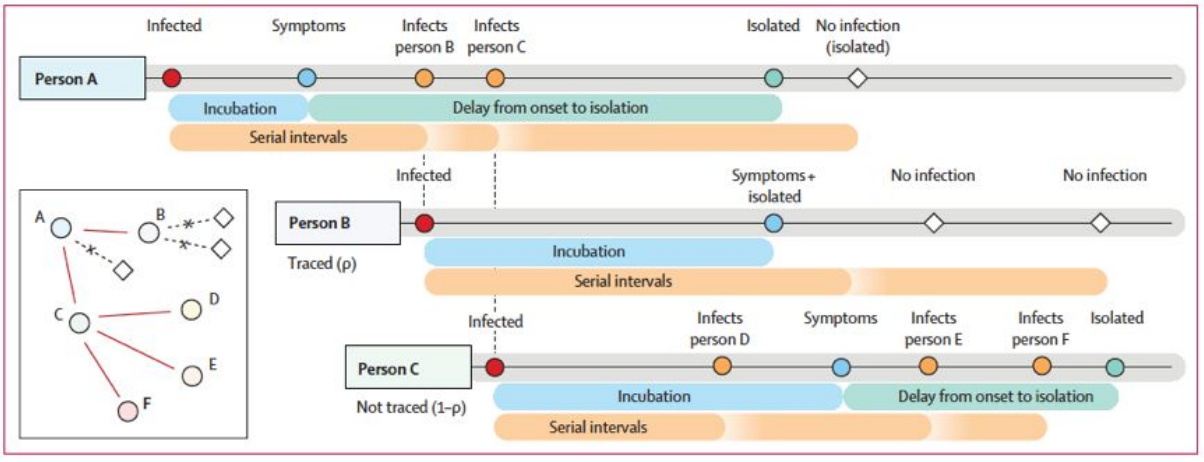


Figure 1: Example of the simulated process that starts with person A being infected

Dopo il periodo di incubazione, la persona A manifesta sintomi e viene isolata a un certo tempo coerente con la tabella di distribuzione del ritardo. Uno schema basato su una distribuzione negativa binomiale e con il tasso di riproduzione di base e un parametro di distribuzione determina quante persone vengono potenzialmente infettate dall'individuo A. Per ciascuno di questi casi, viene descritta una serie di intervalli. Due di queste esposizioni avvengono prima che l'individuo A venga isolato. Ogni contatto viene tracciato con una probabilità p; mentre 1-p indica la probabilità di essere persi al tracciamento. L'individuo B viene tracciato con successo, il che significa che viene isolato senza alcun ritardo quando sviluppa sintomi. Tuttavia, l'individuo B può infettare altre persone prima che venga isolato. L'individuo C non viene riconosciuto dal contact tracing. Il risultato è che viene identificato solo se e quando manifesta sintomi, e viene isolato dopo

l'insorgenza dei sintomi. Dato che l'individuo C non viene riconosciuto, questo infetta 2 o più altri individui (E e F), oltre l'individuo D, evento evitabile se C fosse isolato all'insorgenza dei sintomi.
Source: Hellewell, J. et al., Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts, The Lancet, 28/2/2020, DOI:https://doi.org/10.1016/S2214-109X(20)30074-7

Con un tasso di riproduzione di base (R_0) pari a 1.5, il focolaio si dimostra controllabile con meno del 50% dei contatti tracciati con successo. Per controllare la maggior parte dei focolai, con R0 di 2.5 è necessario tracciare più del 70% dei contatti, mentre per R0 di 3.5 serve ricostruire puntualmente oltre il 90% dei contatti. Il grafico qui sotto evidenza gli effetti di controllo dell'epidemia in diversi scenari di casi iniziali, ritardo nell'isolamento, trasmissione prima dell'insorgenza di sintomi e infezioni subcliniche, al variare della percentuale di "contact tracing". Negli scenari studiati, è evidente che l'uso di tecnologie per il contact tracing ha la migliore ragion d'essere al termine del periodo di lockdown, quando le misure di isolamento hanno consentito di ridurre il più possibile il tasso di riproduzione di base dell'infezione.

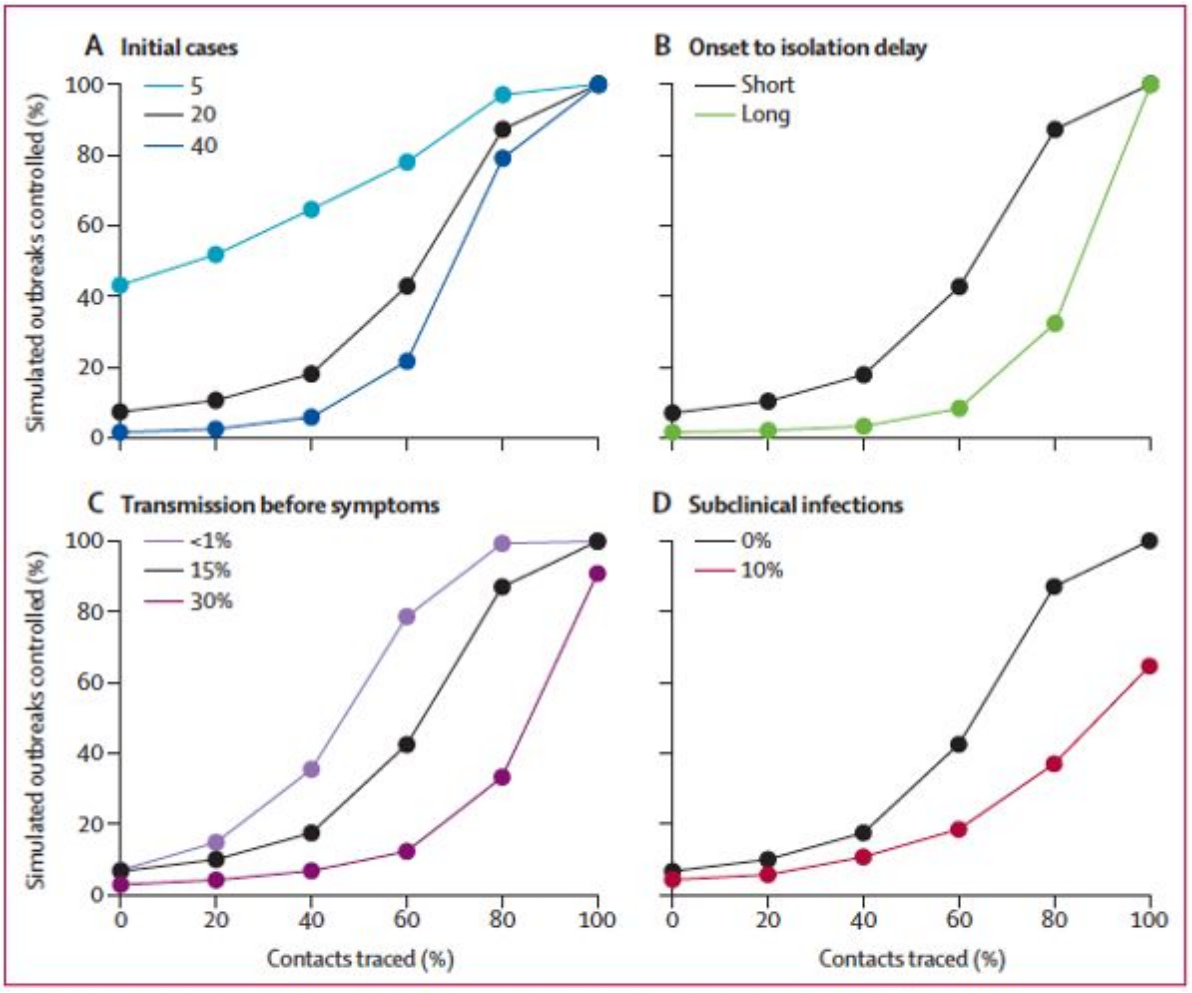


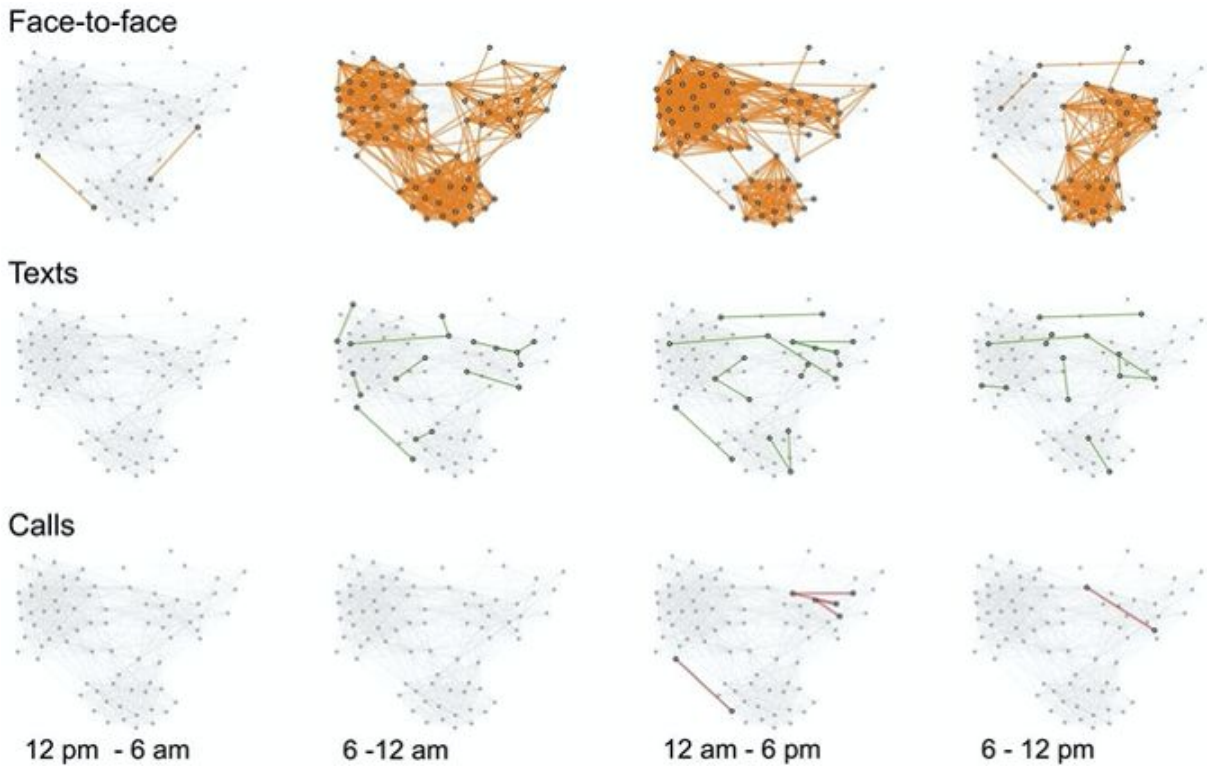
Figure 4: **Achieving control of simulated outbreaks under different transmission scenarios**
The percentage of outbreaks controlled for the baseline scenario, and varied number of initial cases (A), time from onset to isolation (B), percentage of transmission before symptoms (C), and proportion of subclinical (asymptomatic) cases (D). The baseline scenario is a reproduction number (R_0) of 2·5, 20 initial cases, a short delay to isolation, 15% of transmission before symptom onset, and 0% subclinical infection. Results for R_0=1·5 and 3·5 are given in the appendix. A simulated outbreak is defined as controlled if there are no cases between weeks 12 and 16 after the initial cases.

Source: Hellewell, J. et al., Feasibility of controlling COVID-19 outbreaks by isolation of cases and contacts, The Lancet, 28/2/2020, DOI:https://doi.org/10.1016/S2214-109X(20)30074-7

In termini di modelli teorici, la letteratura scientifica ha prodotto un'ampia gamma di esperimenti che consentono la puntuale ricostruzione delle relazioni di prossimità tra soggetti dotati di device in grado di ricostruire i contatti a distanza ravvicinata, e quindi fornire modelli di analisi per la definizione delle possibili catene di trasmissione del virus.

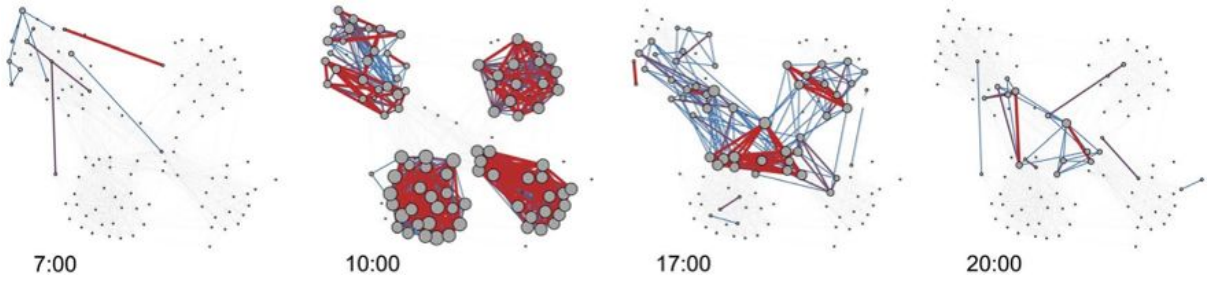
In questo tipo di modelli (si veda ad esempio Stopczynski, A., 2014, citato qui sotto) si descrive lo studio su larga scala volto a misurare le interazioni umane attraverso una varietà di canali di comunicazione, con un'alta risoluzione e un'estesa durata temporale. Questo genere di modelli integrano la raccolta di dati di prossimità con altri dati, per esempio tratti da sistemi di telecomunicazione, da social network, da geolocalizzazioni e da informazioni di

base (personalità, dati demografici, salute, cultura, etc.) per una popolazione densamente connessa di migliaia individui, utilizzando smartphone come sensori sociali, illustrando l'importanza dell'approccio multicanale ad alta risoluzione nel processo di raccolta dei dati.
Il grafico qui sotto, tratto dal paper sopra citato, propone a scopo illustrativo una comparazione dei processi di relazione (face-to-face, messaggistica, chiamate telefoniche) su diverse reti in diverse fasce della giornata.



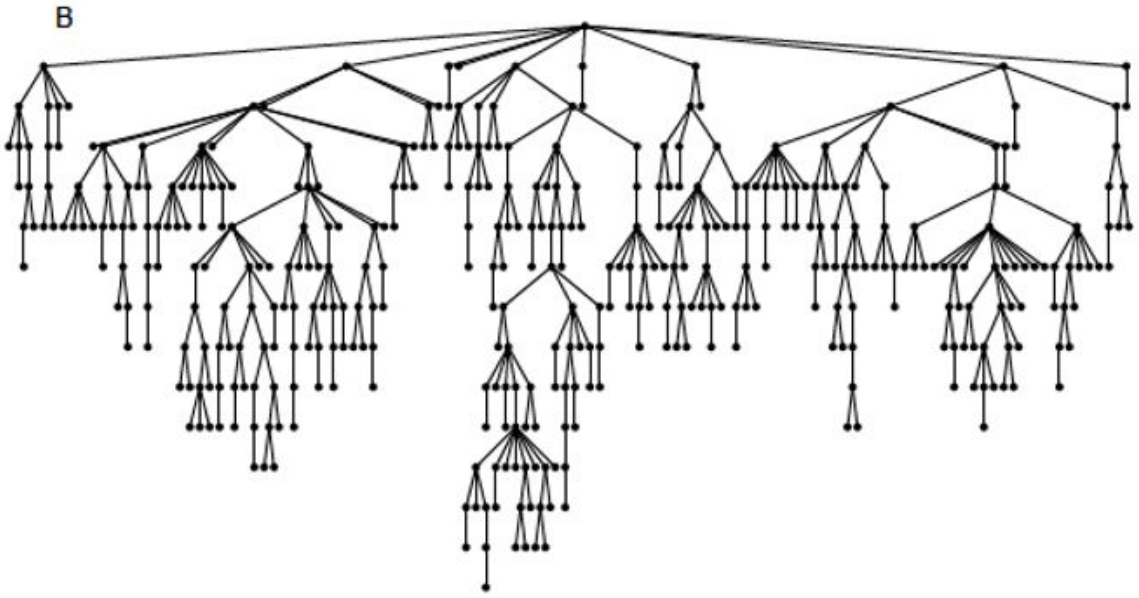
Fonte: Stopczynski A, Sekara V, Sapiezynski P, Cuttone A, Madsen MM, et al. (2014) Measuring Large-Scale Social Networks with High Resolution. PLoS ONE 9(4): e95978. doi:10.1371/journal.pone.0095978

Nella dinamica delle interazioni faccia a faccia, il modello evidenzia (vedi grafico qui sotto) i pattern di comportamento dei soggetti che, nell'esperimento in oggetto, si incontrano al mattino, frequentano le lezioni in quattro diverse linee di studio e la sera interagiscono. I bordi sono colorati in base alla frequenza di osservazione, che varia da basso (blu) ad alto (rosso). Con 24 possibili osservazioni all'ora, le soglie di colore sono rispettivamente: blu (osservazioni 0v f6), viola (osservazioni 6v f12) e rosso (osservazioni v12). La dimensione del nodo viene ridimensionata linearmente in base al grado.



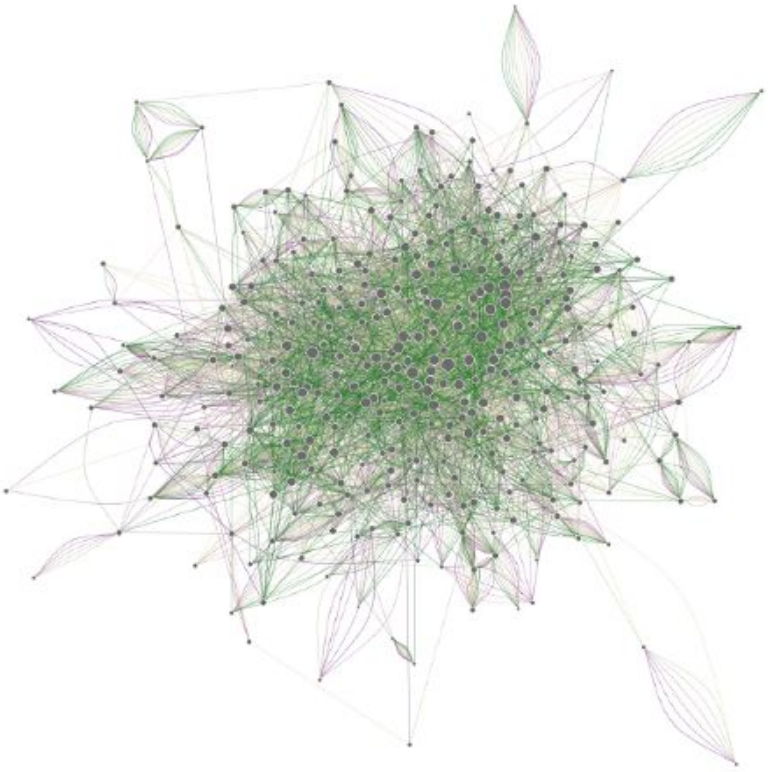
Fonte: Stopczynski A, Sekara V, Sapiezynski P, Cuttone A, Madsen MM, et al. (2014) Measuring Large-Scale Social Networks with High Resolution. PLoS ONE 9(4): e95978. doi:10.1371/journal.pone.0095978

Nel grafico qui sotto, tratto a titolo meramente esemplificativo da un modello matematico realizzato sul test di Haslemere (UK) pubblicato su BioRXiv nel 2018 (cfr. Stephen M. Kissler, Sparking "The BBC Four Pandemic": Leveraging citizen science and mobile phones to model the spread of disease, bioRxiv 6 november 2018. https://www.biorxiv.org/content/10.1101/479154v1, articolo non peer-reviewed), è riportato l'albero raffigurante le infezioni dirette in un processo di epidemia simulato in una città inglese. Ogni riga rappresenta una nuova generazione dell'epidemia, dall'alto verso il basso. Si noti che le infezioni che si allineano su una riga non si sono necessariamente verificate contemporaneamente, ma rappresentano invece "generazioni" dell'epidemia.



Source: Stephen M. Kissler, Sparking "The BBC Four Pandemic": Leveraging citizen science and mobile phones to model the spread of disease, bioRxiv 6 november 2018. https://www.biorxiv.org/content/10.1101/479154v1

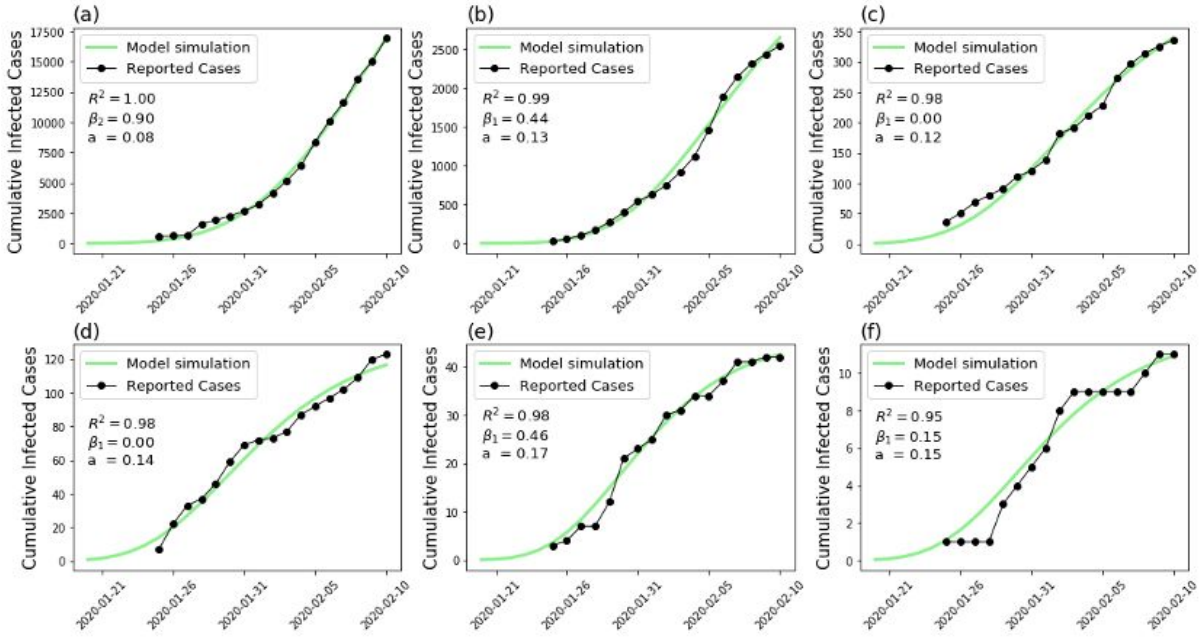
Il grafico seguente (sempre tratto dal lavoro di S. Kissler sopra citato) rappresenta un possibile esempio di modello di rete di incontri personali a coppie nel tempo per il 75% delle persone, nel set di dati testato nell'esperimento di Haslemere (UK), che trascorrono il maggior tempo entro 20 m da un'altra persona (vale a dire con il maggior numero totale di "ore-persona" di contatto). Un incontro è definito come la prima volta che due individui si trovano entro una specifica distanza (qui 20 mt) l'uno dall'altro durante un arco di tempo. Ogni nodo rappresenta un individuo e ogni riga rappresenta un incontro che si è verificato durante una particolare fascia oraria di un giorno. I quarti di giorno sono costituiti dalle ore 7: 00-11: 00, 11: 00-15: 00, 15: 00-19: 00 e 19: 00-23: 00. Nell'esempio riportato, le giornate dello studio erano tre e quindi ci sono al massimo dodici linee che possono collegare due nodi qualsiasi. Le linee sono colorate in base al quarto di giorno in cui si è verificato l'incontro, che va da giovedì quarto 1 (viola) a sabato quarto 4 (verde). L'area del nodo è proporzionale al numero totale di incontri unici per quell'individuo in tutti e tre i giorni.



Source: Stephen M. Kissler, Sparking "The BBC Four Pandemic": Leveraging citizen science and mobile phones to model the spread of disease, bioRxiv 6 november 2018. https://www.biorxiv.org/content/10.1101/479154v1

Le best practices analizzate evidenziano come la metodologia di "contact tracing" possa consentire di circoscrivere con elevata precisione le aree a rischio di diventare un focolaio infettivo, fornendo preziose indicazioni per il contenimento dell'epidemia ma anche evitando di applicare restrizioni su aree eccessivamente estese, e mitigando così gli impatti negativi sulla vita sociale ed economica. I grafici sotto riportati, tratti da una ricerca pubblicata su

MedRxiv il 9 febbraio 2020 (Xiaolin Zhu & al, Spatially Explicit Modeling of 2019-nCoV Epidemic Trend Based on Mobile Phone Data in Mainland China, MedRxiv, 9 February 2020), mostrano come i processi di "contact tracing" digitale abbiano consentito, pur nello specifico contesto epidemico cinese, di delimitare con accuratezza le aree di contagio e prevedere con grande precisione le evoluzioni epidemiche.



Comparison between the number from model simulation and reported cases in cities with representative severity of disease spreading: (a) Wuhan, (b) Xiaogan, (c) Beijing, (d) Chengdu, (e) Kunming, and (f) Datong - Source: Xiaolin Zhu & al, Spatially Explicit Modeling of 2019-nCoV Epidemic Trend Based on Mobile Phone Data in Mainland China, MedRxiv, 9 February 2020

Le soluzioni di contact tracing digitale possono inoltre contribuire a mitigare l'impatto sulle attività sociali ed economiche, facilitando la progressiva ripresa operativa, tramite strumenti di autodiagnostica e di auto-profilazione del rischio di esposizione ai contatti e ai focolai, che facilitino l'applicazione delle misure di "social distancing" e la progressiva riapertura di tutte le filiere produttive, distributive e di servizi, riducendo al minimo gli interventi restrittivi per cittadini e imprese.

Una volta consolidate, le tecnologie di contact tracing possono supportare la creazione di un "**passaporto sanitario digitale**" che misuri sistematicamente il livello individuale di rischio epidemico, così da consentire la progressiva ripresa delle attività economiche e sociali, complementando l'attuale modulo cartaceo di autodichiarazione con una soluzione rigorosa, oggettiva e verificabile, che consenta sia alle autorità sia alle imprese di disporre di una base informativa certificata per le indirizzare le scelte organizzative e di monitoraggio. Tale soluzione tecnologica, anch'essa basata su app installata su smartphone, è sostanzialmente un certificato medico digitale ad aggiornamento dinamico, e viene utilizzata regolarmente a Taiwan e in Corea del Sud come "titolo di accesso" a locali pubblici e privati, sistemi di

trasporto (treni, aerei, navi, trasporto pubblico locale), aree pubbliche ad accesso regolamentato, ecc. In tali luoghi viene solitamente previsto un semplice sistema di "check-in", basato su un QR-code da far leggere allo smartphone, così da verificare la congruenza tra stato di salute/livello di rischio del soggetto e il contesto spaziale nel quale intende recarsi. Il passaporto sanitario digitale viene periodicamente verificato dalle autorità sanitarie competenti in caso di modifica e/o evoluzione delle condizioni cliniche ed epidemiologiche del soggetto. Nel caso dei pazienti guariti dal COVID-19 che hanno evidenziato una condizione di immunità, tale "passaporto" permette una circolazione libera da vincoli. Nei casi internazionali sopra citati, quale azione ha contribuito a circoscrivere molto più precisamente sia le aree di contenimento sia il numero degli individui assoggettati a limitazioni nella circolazione, e quindi di ridurre i costi sociali dell'emergenza, favorendo una migliore organizzazione del lavoro e della logistica, grazie all'accesso diretto e immediato - tramite canali digitali - alle opportune indicazioni di risk management personalizzato messe a disposizione degli operatori di trasporto, delle aziende e dei cittadini, riducendo nel contempo il carico burocratico su autorità e cittadini. Rimane da stabilire se le misure che si sono dimostrate efficaci in altri paesi siano trasferibili nel contesto italiano che ha caratteristiche socio-demografiche e culturali specifiche e una situazione epidemiologica per COVID-19 nella quale sono fortemente rappresentati gli anziani e il personale sanitario.

Supporto alle public policies per l'uscita dal lockdown

Per poter esprimere al meglio le proprie potenzialità, le soluzioni tecnologiche identificate dovranno prestarsi a supportare, grazie alla raccolta e all'elaborazione di informazioni logistiche ed epidemiologiche puntuali, le decisioni relative a politiche pubbliche da applicare per il contenimento dell'emergenza sanitaria. In termini epidemiologici, per pianificare gli interventi necessari, è opportuno basarsi su un semplice modello:

(1) **R0 = [N(h)*SAR(h)]+[N(c)*SAR(c)]**

Dove:

- **R0** = basic reproduction number (indice effettivo di riproduzione)
- **N(h)** = number of household persons (numero conviventi/famigliari)
- **SAR(h)** = Secondary Attack Rate within household (indice di infettività per conviventi)
- **N(c)** = number of community persons (numero contatti sociali/professionali)
- **SAR(c)** = Secondary Attack Rate within household (indice di infettività per conviventi)

Per fermare l'epidemia, R0 deve scendere sotto il valore standard di 1. Dall'equazione (1) sopra rappresentata, si può dedurre che entrambi i fattori, ovvero [N(h)*SAR(h)], ovvero il contagio "domestico" e [N(c)*SAR(c)], ovvero il contagio "sociale", devono scendere fino ad avere una somma inferiore all'unità.

Il parametro N(h) è un dato relativamente statico e conoscibile ex ante, può essere estratto da DB pubblici (stato di famiglia, INPS) o dedotto grazie alle soluzioni di contact tracing (dietro opt-in, e.g. tramite dichiarazione spontanea, geolocalizzazione tramite cellulare, ecc.). Ai fini della gestione dell'emergenza, può costituire un attributo permanente di ogni soggetto, così da rappresentare un parametro di riferimento immediato in caso di allertamento da contagio in uno qualsiasi dei membri dell'insieme N(h).

In un lockdown totale, la variabile "c" viene minimizzata se non azzerata, mentre si induce un effetto di crescita sui parametri N(h) e SAR(h), a causa della stretta convivenza forzosa e prolungata. Secondo alcune valutazioni (cfr. paper dell'Imperial College del 16/3/2020), aver indicato la quarantena domestica a molti positivi ha in realtà favorito la propagazione del contagio a livello familiare.
Al contrario, la creazione di "fever clinics" dove circoscrivere e monitorare attivamente i quarantenati e i positivi è stato un pilastro essenziale delle azioni di contenimento applicate in Cina e in South Korea. In quarantena solitaria o in isolamento, infatti, anche il parametro N(h) viene sostanzialmente azzerato, di fatto annullando i rischi di ulteriore contagio.

In un lockdown pubblico parziale, come quello applicato in Italia e in molti Paesi occidentali, gli effetti del limiti alla mobilità e del social distancing forzoso si riflettono sui parametri N(c) e SAR(c).

Il parametro N(c) viene ridotto dalle limitazioni alla circolazione, alla concentrazione di persone e dalla chiusura di specifici outlet commerciali/sociali. Tale parametro tuttavia è quello a più alta variabilità e richiede un monitoraggio attivo per essere quantificato e analizzato. E' quindi necessario predisporre processi e tecnologie per quantificare e se necessario identificare e allertare tempestivamente ogni soggetto che, anche solo temporaneamente o accidentalmente, si trovi a far parte di tale insieme.
Le soluzioni di "near-real time digital contact tracing" indirizzano l'insieme N(c). L'obiettivo da raggiungere non è necessariamente tracciare il 100% dei contatti, bensì identificarne un numero sufficiente a rallentare e poi interrompere le catene trasmissive.

Il parametro SAR(c) viene abbattuto con diverse misure di sicurezza e di protezione, quali ad esempio l'introduzione di distanze minime negli spazi pubblici, l'utilizzo di DPI (Dispositivi Protezione Individuale), la sanitizzazione degli ambienti, ecc.

A sua volta, possiamo articolare N(c) in diversi cluster (fuzzy set a funzioni di appartenenza continue), in parte sovrapposti:

- **N(t)** = number of encounters during transportation/travel (incontri in viaggio)
- **N(w)** = number of encounters during work/school (incontri per lavoro/scuola)
- **N(r)** = number of encounters during retail/commerce (incontri per spese/commercio)
- **N(s)** = number of encounters during social activities (incontri in attività sociali)

Analogamente, è possibile distinguere i relativi parametri SAR [SAR(t), SAR(w), SAR(r) e SAR(s)] che caratterizzano i fenomeni di trasmissione nei rispettivi contesti. Questa classificazione, che non viene normalmente proposta nei tradizionali modelli epidemici (per i quali ogni contatto umano, indipendentemente dal contesto, è sostanzialmente equivalente ai fini della trasmissione del virus), è invece estremamente importante nella prospettiva della ripresa delle attività sociali ed economiche, in quanto implica interventi di natura normativa, tecnologica e organizzativa molto diversi a seconda dei casi.

Le soluzioni tecnologiche per il contact tracing potranno prevedere la generazione di dati che supportino una lista di interventi raccomandati, i quali intervengano nel ridurre, singolarmente presi, tutti i singoli parametri sopra elencati, prima stimandone teoricamente gli effetti e successivamente misurandone sperimentalmente e/o empiricamente i risultati grazie alle applicazioni digitali.

Tale verifica empirica può essere supportata dall'utilizzo di BigData e da soluzioni tecniche che rilevino in tempo reale il livello di esposizione al rischio di contagio tramite smartphone o altri device di prossimità. La ricostruzione accurata, anche utilizzando più fonti informative (p.es., sulla base del profilo familiare, professionale e comportamentale del soggetto) del «grafo sociale» relativo al contagiato consente di individuare non solo i contatti diretti rilevati dalla app, ma anche di inferire possibili contatti non rilevati o «nascosti», relativi a persone non dotate di app (si pensi ad anziani, disabili o bambini) ma associabili al soggetto. Ciò consente una migliore protezione attiva e l'individuazione di «hot spot» di possibile contagio ambientale, sui quali pianificare adeguati interventi di decontaminazione.

Nella tabella qui sotto si riporta, a titolo puramente illustrativo, un esempio della possibile disaggregazione dei parametri sopra descritti, la cui quantificazione può essere determinata empiricamente - addirittura a livello di singolo soggetto, invece che come media di un aggregato di casi - grazie all'analisi dei dati derivanti dal contact tracing digitale.
Laddove l'adozione di soluzione di contact tracing digitale dovesse raggiungere un'adeguata massa critica, infatti, sarebbe possibile stimare - con ridotti livelli di errore rispetto ai processi manuali - sia il numero **N(x)** di contatti nei diversi contesti ambientali (famiglia, lavoro, trasporto, ecc.), sia - ex post, a seguito di opportune analisi epidemiologiche sulla catena di trasmissione del contagio - il fattore **SAR(x)** di ciascun contesto specifico, in base per

esempio alla distanza e alla durata del contatto stesso, oltre che di eventuali fattori di contagio ambientale.

Parameter	Contrib. to R0	Description
Nh	1,00	• **N(h)** = number of household persons (numero conviventi/famigliari)
Nc	***1,00***	• **N(c)** = number of extended community persons (numero contatti sociali/professionali)
Nt	0,10	• **N(t)** = number of encounters during transportation/travel (incontri in viaggio)
Nw	0,30	• **N(w)** = number of encounters during work/school (incontri per lavoro/scuola)
Nr	0,10	• **N(r)** = number of encounters during retail/commerce (incontri per spese/commercio)
Ns	0,50	• **N(s)** = number of encounters during social activities (incontri in attività sociali)
SARh	1,00	• **SAR(h)** = Secondary Attack Rate within household (indice di infettività per conviventi)
SARc	***1,00***	• **SAR(c)** = Secondary Attack Rate within extended community
SARt	0,10	• **SAR(t)** = Secondary Attack Rate for transportation/travel
SARw	0,20	• **SAR(w)** = Secondary Attack Rate within working environment
SARr	0,10	• **SAR(r)** = Secondary Attack Rate for retail activities/commerce
SARs	0,60	• **SAR(s)** = Secondary Attack Rate for social activities
R0	***2,00***	• **R0** = basic reproduction number (indice effettivo di riproduzione)
Delta R(day)	0-100	• Effect of intervention on R0(daily)

Questa analisi consentirebbe di migliorare notevolmente l'attuale modello di classificazione del rischio di esposizione al contagio, rilasciato dall'ECDC nel report del 31.3.2020. In tale documento (vedi tabella qui sotto) il rischio di contagio è classificato secondo 2 soli livelli discreti (Alto vs Basso), definiti in base a una soglia fissa di durata (maggiore o minore di 15 minuti) e a una misura fissa di distanza (minore o maggiore di 2 metri), oltre a una casistica di prossimità e modalità del contatto stesso (p. es., permanenza in un ambiente chiuso, occupazione di un posto a sedere su un mezzo di trasporto, ecc.).

Table 1. Classification of contact based on level of exposure

High-risk exposure (close contact)	Low-risk exposure
A person: • having had face-to-face contact with a COVID-19 case within 2 metres for more than 15 minutes • having had physical contact with a COVID-19 case • having unprotected direct contact with infectious secretions of a COVID-19 case (e.g. being coughed on) • who was in a closed environment (e.g. household, classroom, meeting room, hospital waiting room, etc.) with a COVID-19 case for more than 15 minutes • in an aircraft, sitting within two seats (in any direction) of the COVID-19 case, travel companions or persons providing care, and crew members serving in the section of the aircraft where the index case was seated [23] (if severity of symptoms or movement of the case indicate more extensive exposure, passengers seated in the entire section or all passengers on the aircraft may be considered close contacts) • A healthcare worker or other person providing care to a COVID-19 case, or laboratory workers handling specimens from a COVID-19 case, without recommended PPE or with a possible breach of PPE [24]	A person: • having had face-to-face contact with a COVID-19 case within 2 metres for less than 15 minutes • who was in a closed environment with a COVID-19 case for less than 15 minutes • travelling together with a COVID-19 case in any mode of transport* • A healthcare worker or other person providing care to a COVID-19 case, or laboratory workers handling specimens from a COVID-19 case, wearing the recommended PPE [24]

* *Except* if sitting in an aircraft as specified in the relevant point in the left column.

Fonte: ECDC, 31 March 2020 - https://www.ecdc.europa.eu/sites/default/files/documents/Public-health-management-persons-contact-novel-coronavirus-cases-2020-03-31.pdf

Per ciascun soggetto infetto, infatti, il contact tracing digitale può consentire di ricostruire puntualmente una estesa casistica di contatti e di stimare, ex post, un livello di contagiosità specifica in modo molto più accurato rispetto al dato attuale, supportando così sia la ricerca medica sia l'indirizzo delle opportune politiche di contenimento, protezione individuale, e distanziamento sociale, che invece oggi vengono decise sulla base di informazioni molto più imprecise e aggregate.

A tale proposito, nella tabella qui sotto si riporta un esempio di classificazione degli interventi di policy proposto da Imperial College nel paper di policy recommendation per il Governo UK del 16.3.2020, dove vengono evidenziati anche gli effetti attesi in termini di riduzione dei contatti potenziali. Tale tabella è stata alla base delle raccomandazioni di public policies fornite al governo britannico da parte del team dell'Imperial College.

Label	**Policy**	**Description**
CI	Case isolation in the home	Symptomatic cases stay at home for 7 days, reducing non-household contacts by 75% for this period. Household contacts remain unchanged. Assume 70% of household comply with the policy.
HQ	Voluntary home quarantine	Following identification of a symptomatic case in the household, all household members remain at home for 14 days. Household contact rates double during this quarantine period, contacts in the community reduce by 75%. Assume 50% of household comply with the policy.
SDO	Social distancing of those over 70 years of age	Reduce contacts by 50% in workplaces, increase household contacts by 25% and reduce other contacts by 75%. Assume 75% compliance with policy.
SD	Social distancing of entire population	All households reduce contact outside household, school or workplace by 75%. School contact rates unchanged, workplace contact rates reduced by 25%. Household contact rates assumed to increase by 25%.
PC	Closure of schools and universities	Closure of all schools, 25% of universities remain open. Household contact rates for student families increase by 50% during closure. Contacts in the community increase by 25% during closure.

Source: Imperial College, March 16, 2020

Come si può notare dal testo delle descrizioni relativo ad ogni singola policy di contenimento suggerita dagli studiosi dell'Imperial College, le stime degli effetti attesi sono necessariamente alquanto grossolane (sono misurate in quartili dei soli volumi di contatti attesi: 25%, 50% o 75%) e non contengono stime disaggregate degli effetti su R0 di ogni specifica misura, a causa dell'indisponibilità di un modello di tipo analitico con dati reali.

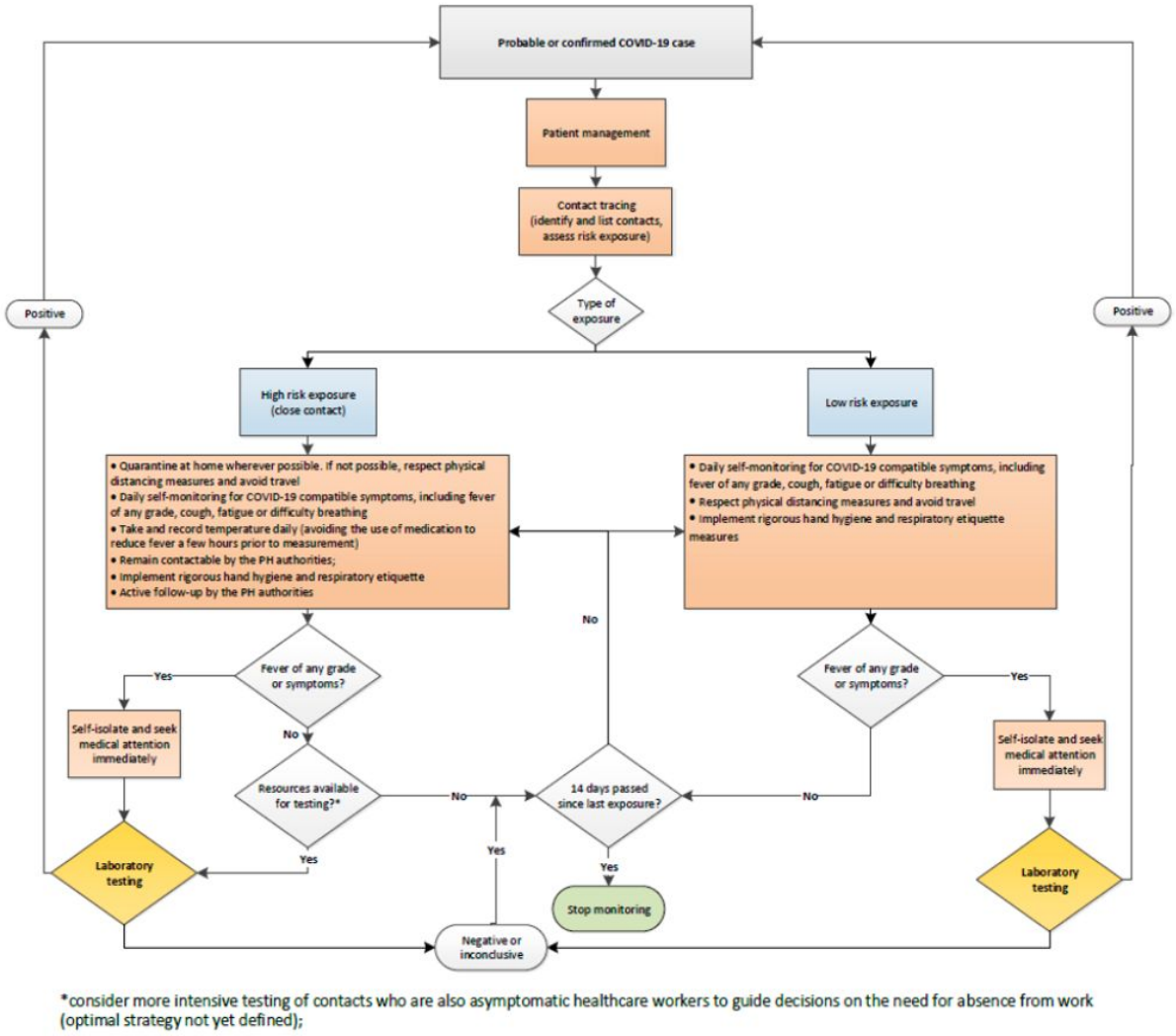
Le soluzioni tecnologiche raccomandate per il digital contact tracing possono contribuire a migliorare notevolmente l'accuratezza di tali stime, in quanto consentono la raccolta di dati empirici e la possibilità di svolgere analisi su BigData ai fini di alimentare e supportare in

termini quantitativi i modelli epidemiologici e le analisi di impatto e le valutazioni costi/benefici delle politiche pubbliche di gestione dell'emergenza e del post-emergenza.
Qui sotto si riporta, a puro titolo illustrativo e con numeri esemplificativi senza valenza reale, una possibile tabella di classificazione analitica degli interventi di public policy. A ciascuna voce di possibile intervento (p.es. quarantena in struttura isolata, adozione di DPI, social distancing in scuole e università, ecc.) può essere associato un periodo di applicazione, un effetto atteso sui rilevanti parametri epidemiologici, un livello di compliance attesa da parte della popolazione e quindi un possibile impatto specifico su R0, oltre che una eventuale stima dei costi economici - diretti e indiretti - dell'intervento stesso, al fine di giungere a una possibile analisi costi/benefici per ciascuna decisione da adottare.

Parametro	Label	Intervento	Intervento Y/N	Delta R(day) min	Delta R(day) max	Durata (giorni)	Compliance attesa %	Impatto R(day)	Impatto totale R0
Nh	RFC	Ricovero in fever clinic	0	80	100	45	100%	0	0,00
Nh	QDI	Quarantena domestica in isolamento	1	60	90	45	90%	68	0,30
Nh	QDF	Quarantena domestica in famiglia	1	0	30	45	80%	12	0,05
Nh	QSI	Quarantena in struttura isolata con supporto di servizi	0	70	100	45	95%	0	0,00
SARh	CFF	Coabitazione forzata in famiglia	1	-50	-20	45	80%	-28	-0,13
SARh	ADD	Adozione DPI per uso domestico	0	20	40	90	70%	0	0,00
SARh	TAS	Teleassistenza sanitaria	0	40	60	90	60%	0	0,00
SARh	CDG	Consegna domestica grocery	0	10	20	90	10%	0	0,00
Nc	LGN	Lockdown generale nazionale	1	70	90	45	85%	68	0,31
Nw	RAS	Restrizione attività scuole e università	0	20	40	30	100%	0	0,00
Nw	RAE	Restrizione attività economiche (da disaggregare per settore/filiera)	0	30	50	30	50%	0	0,00
Nt	RTPU	Restrizione trasporti pubblici	0	50	70	15	40%	0	0,00
Nt	RTPR	Restrizione trasporti privati	0	10	20	30	75%	0	0,00
Nr	RAC	Restrizione attività commerciali (da disaggregare per merceologia)	0	30	50	30	70%	0	0,00
Ns	RAS	Restrizione attività sociali (da disaggregare per tipologia)	0	40	60	30	80%	0	0,00
SARc	SDGN	Social distancing generale nazionale	1	60	80	45	85%	60	0,27
SARc	ADUE	Adozione DPI per uso extradomestico	0	70	90	90	20%	0	0,00
SARw	SDSU	Social distancing scuole e università	0	20	50	90	90%	0	0,00
SARw	SDLL	Social distancing luoghi di lavoro	0	40	60	90	80%	0	0,00
SARt	SDTPU	Social distancing nel trasporto pubblico	0	60	80	90	80%	0	0,00
SARt	SDTPR	Social distancing nel trasporto privato	0	10	20	90	80%	0	0,00
SARr	SDRC	Social distancing nel retail/commerce	0	30	50	90	90%	0	0,00
SARs	SDAS	Social distancing nelle attività sociali	0	40	70	90	70%	0	0,00
SARw	CISU	Check-in per strutture scuola/università	0	30	50	90	100%	0	0,00
SARw	CILL	Check-in per luoghi di lavoro	0	50	80	90	80%	0	0,00
SARt	CITPU	Check-in per trasporto pubblico	1	40	60	45	95%	48	0,21
SARt	CITPR	Check-in per trasporto privato	1	10	20	45	80%	12	0,05
SARr	CIAR	Check-in per accesso a retail/horeca	0	50	70	90	90%	0	0,00
SARs	CISE	Check-in per social events	0	60	80	90	60%	0	0,00
		Totale impatto su R0							**1,07**

Questo genere di approccio tende a rafforzare quanto più volte ribadito nei documenti redatti dal Gruppo di Lavoro, ovvero che le risultanze derivanti dall'applicazione di tecnologie di contact tracing non possono essere considerate in isolamento, ma vanno collocate all'interno del processo integrato raccomandato da OMS e ECDC, sintetizzato con le "3T" dell'espressione "Trace, Test & Treat", e correttamente utilizzate sia per supportare i processi di test e trattamento dei casi di contagio, sia a sostegno e indirizzo delle scelte di medicina pubblica. Per quanto riguarda il collegamento tra i dati raccolti con il digital contact tracing e gli altri elementi dell'approccio "3T", si può in conclusione far riferimento al workflow proposto dall'ECDC per la gestione dei contatti rilevati relativi a un caso di COVID-19 probabile e/o confermato (vedi schema qui sotto).

Figure 1-A. Algorithm for the management of contacts of probable or confirmed COVID-19 cases



Fonte: ECDC, 31 March 2020 - https://www.ecdc.europa.eu/sites/default/files/documents/Public-health-management-persons-contact-novel-coronavirus-cases-2020-03-31.pdf

Come evidenziato dai suggerimenti di ECDC, il workflow del contact tracing prevede una forte integrazione dei processi tecnologici e sanitari, nella logica delle «3T»: Trace, Test & Treat. Lo schema qui rappresentato è peraltro tuttora riferito a una classificazione binaria del livello di rischio (high/low): il contact tracing digitale basato su tecnologie di prossimità, come sopra discusso, consente invece di disporre di una misura precisa e continua - e non arbitrariamente discretizzata ex ante - dei diversi fattori di rischio, rendendo il processo di trattamento più specifico e personalizzato. In conclusione, quindi, va rimarcato che l'interoperabilità tra soluzioni digitali di contact tracing, autodiagnosi remota, monitoraggio delle azioni di contenimento, teleassistenza per quarantena e gestione dell'isolamento risulta essenziale per garantire la piena integrazione dei processi sanitari, logistici e operativi e, in ultima analisi, una maggiore efficacia delle azioni di contenimento dell'epidemia.

Bibliografia

1. Abbott S, Hellewell J, Munday J et al. *Temporal variation in transmission during the COVID-19 outbreak.* Centre for Mathematical Modelling of Infectious Disease, 2020 (available at: https://cmmid.github.io/topics/covid19/current-patterns-transmission/global-time-varying-transmission.html)

2. Ferretti L, Wymant C, Kendall M et al, Quantifying dynamics of SARS-CoV-2 transmission suggests that epidemic control and avoidance is feasible through instantaneous digital contact tracing 2020; doi:https://doi.org/10.1101/2020.03.08.20032946 (available at: https://bdi-pathogens.shinyapps.io/covid-19-transmission-routes/)

3. McLean E, Pebody RG, Campbell C, Chamberland M, Hawkins C, Nguyen-Van-Tam JS, Oliver I, Smith GE, Ihekweazu C, Bracebridge S, Maguire H, Harris R, Kafatos G, White PJ, Wynne-Evans E, Green J, Myers R, Underwood A, Dallman T, Wreghitt T, Zambon M, Ellis J, Phin N, Smyth B, McMenamin J, Watson JM. Pandemic (H1N1) 2009 influenza in the UK: clinical and epidemiological findings from the first few hundred (FF100) cases. Epidemiol Infect. 2010;138:1531-41

4. Crook P, Smith-Palmer A, Maguire H, McCarthy N, Kirkbride H, Court B, Kanagarajah S, Turbitt D, Ahmed S, Cosford P, Oliver I. Lack of Secondary Transmission of Ebola Virus from Healthcare Worker to 238 Contacts, United Kingdom, December 2014. Emerg Infect Dis. 2017;23:2081-2084

5. Vaughan A, Aarons E, Astbury J, Balasegaram S, Beadsworth M, Beck CR, Chand M, O'Connor C, Dunning J, Ghebrehewet S, Harper N, Howlett-Shipley R, Ihekweazu C, Jacobs M, Kaindama L, Katwa P, Khoo S, Lamb L, Mawdsley S, Morgan D, Palmer R, Phin N, Russell K, Said B, Simpson A, Vivancos R, Wade M, Walsh A, Wilburn J. Two cases of monkeypox imported to the United Kingdom, September 2018. Euro Surveill. 2018;23

6. Matt J Keeling et al., The Efficacy of Contact Tracing for the Containment of the 2019 Novel Coronavirus (COVID-19), medRxiv doi: https://doi.org/10.1101/2020.02.14.20023036)

Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19

Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza"

Sintesi del documento

Il presente documento riassume talune considerazioni di carattere giuridico - con particolare riferimento al diritto alla protezione dei dati personali e altri diritti fondamentali - relative all'eventuale utilizzazione di una soluzione integrata di *contact tracing* finalizzata esclusivamente a consentire ai cittadini che abbiano scelto liberamente di installare un'applicazione sui propri dispositivi e che siano risultati contagiati all'esito di diagnosi medica di informare - in forma anonima - altri cittadini - che a loro volta abbiano liberamente scelto di utilizzare la medesima applicazione - del rischio di contagio dovuto a un contatto e dell'opportunità di adottare talune cautele.
Il presente documento non si occupa, invece, di ogni eventuale diversa utilizzazione secondaria di tali soluzioni tecnologiche avente finalità diversa dal semplice *contact tracing* nei termini appena riassunti.
Le considerazioni che seguono sono basate sull'analisi della documentazione relativa a un subset di soluzioni tecnologiche tra quelle presentate nell'ambito della call lanciata dal Ministro per l'innovazione tecnologica e la digitalizzazione d'intesa con il Ministero della Salute ritenute dagli esperti tecnico-epidemiologici, sotto i profili di loro competenza, idonee a garantire gli obiettivi di contenimento della diffusione del virus e la progressiva revoca di taluni limiti e divieti adottati al medesimo fine nelle scorse settimane.
Le soluzioni tecnologiche esaminate più in linea con il quadro giuridico, in generale, funzionano come segue: il segnale Bluetooth LE (Low Energy) degli utenti che hanno scelto di installare una specifica applicazione viene registrato dalle analoghe applicazioni con le quali "entrano in contatto"; quando un utente viene diagnosticato contagiato dal COVID-19 il suo dispositivo trasmette i dati al server del soggetto pubblico che gestisce il sistema [alcune delle soluzioni valutate prevedono tale trasferimento su base sistematica e non condizionata], che provvede quindi a informare gli altri utenti - che abbiano egualmente volontariamente installato la medesima app - di essere a rischio contagio perché sono entrati in contatto con una persona risultata contagiata.
I presupposti essenziali delle valutazioni e considerazioni riassunte nel documento sono:
(a) che l'intero sistema integrato di *contact tracing* sia interamente gestito da uno o più soggetti pubblici e che il suo codice sia aperto e suscettibile di revisione da qualunque soggetto indipendente voglia studiarlo;
(b) che i dati trattati ai fini dell'esercizio del sistema siano "resi sufficientemente anonimi da impedire l'identificazione dell'interessato" [cfr. Considerando 26 GDPR] tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione almeno in condizioni ordinarie e salvo il verificarsi di eventi patologici o, almeno, pseudoanonimi previa adozione di idonee misure idonee a limitare il rischio di identificazione degli interessati;
(c) che la decisione di usare la soluzione tecnologica sia liberamente assunta dai singoli cittadini;
(d) che raggiunta la finalità perseguita tutti i dati ovunque e in qualunque forma conservati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, siano cancellati con conseguente garanzia assoluta per tutti i cittadini di ritrovarsi, dinanzi a soggetti pubblici e privati, nella medesima condizione nella quale si trovavano in epoca anteriore all'utilizzo della soluzione;
(e) che la soluzione adottata - nelle sue componenti tecnologiche e non tecnologiche - possa essere considerata, almeno in una dimensione prognostica, effettivamente efficace sul piano epidemiologico giacché, in difetto, diverrebbe difficile giustificare qualsivoglia, pur modesta e eventuale, compressione di diritti e libertà fondamentali.

(f) che la soluzione adotti misure tecniche ed organizzative che minimizzino i rischi di reidentificazione in ogni fase di vita del sistema (a titolo esemplificativo con variazione periodica e casuale dell'ID anonimo dell'applicazione).

Le analisi - parziali in quanto basate esclusivamente sulla documentazione acquisita nell'ambito della call e su alcune interviste telefoniche - e le valutazioni - preliminari e sommarie in considerazione del ridotto lasso di tempo avuto a disposizione - svolte nel corso dei lavori suggeriscono che una soluzione di *contact tracing* sia implementabile nel rispetto dei presupposti che precedono e che il suo utilizzo sia sostenibile nel rispetto del diritto alla protezione dei dati personali e degli altri diritti e libertà fondamentali.
Nel presente documento si forniscono taluni spunti di riflessione e raccomandazioni che, pur senza alcuna pretesa di esaustività, si auspica possano risultare utili al Governo nell'assunzione delle decisioni di propria competenza in relazione all'opportunità di adozione di una soluzione di *contact tracing e alle competenti Autorità amministrative indipendenti per lo svolgimento delle analisi e valutazioni* di propria competenza.

1. Il contesto di riferimento

Nel quadro delle azioni finalizzate al contrasto al COVID-19 il Governo intende esplorare l'eventualità di utilizzare idonee soluzioni tecnologiche al duplice scopo di contenere la diffusione del virus e consentire la progressiva eliminazione dei limiti, vincoli e divieti alla libertà di movimento e all'esercizio di attività professionali, commerciali e produttive che ci si è visti costretti ad adottare nelle ultime settimane.
In tale contesto il Ministro per l'innovazione tecnologica e la digitalizzazione, d'intesa con il Ministro della Salute, ha promosso una call pubblica finalizzata alla ricognizione delle soluzioni esistenti e affidato a un gruppo interdisciplinare di esperti (informatici, data scientist, epidemiologi, economisti e giuristi), tra l'altro, il compito di supportare il Dipartimento per l'innovazione tecnologica e la digitalizzazione della Presidenza del Consiglio dei Ministri e il Ministero della Salute nell'analisi e valutazione delle diverse soluzioni tecnologiche così identificate.

Il presente documento redatto dai componenti di un sottogruppo del predetto gruppo di lavoro dedicato allo studio e alla valutazione dei profili giuridici connessi al trattamento dei dati – personali e non – nell'attuale periodo di emergenza ha il duplice scopo di:

(a) identificare le principali questioni connesse al diritto alla protezione dei dati personali e, più in generale, ai diritti fondamentali che verrebbero in rilievo qualora il Governo decidesse di adottare soluzioni di c.d. *contact tracing*;
(b) svolgere un'analisi preliminare – sulla sola base delle informazioni fornite dai proponenti – dell'impatto privacy e sul versante degli altri diritti fondamentali di quelle tra le soluzioni tecnologiche identificate nell'ambito della citata call che siano risultate idonee, sotto il profilo tecnico-epidemiologico, al raggiungimento degli obiettivi perseguiti dal Governo.

Il presente documento non intende, invece, naturalmente, anticipare in alcun modo le valutazioni che, qualora il Governo decidesse di utilizzare una o più delle soluzioni tecnologiche identificate nell'ambito della call e della successiva attività del Gruppo di lavoro, competeranno al Garante per la protezione dei dati personali e/o all'Autorità per le Garanzie nelle Comunicazioni e/o all'Autorità Garante per la concorrenza e il mercato nell'esercizio dei relativi poteri.

2. L'obiettivo perseguito attraverso le soluzioni tecnologiche oggetto di valutazione e le loro funzionalità generali

La situazione attuale

Quando un cittadino viene identificato come contagiato - o anche solo potenzialmente contagiato - gli viene chiesto di segnalare con quali persone sia entrato in contatto nelle precedenti due/tre settimane e di informarle del rischio di essere state, a loro volta, contagiate affinché contattino gli operatori sanitari allo scopo di verificare l'eventuale contagio e, medio tempore, adottino misure idonee a evitare ulteriori contagi.

Tale processo sconta una serie di limiti:

(i) il soggetto contagiato può non conoscere [es: sconosciuti con i quali ha condiviso una corsa su un mezzo pubblico o la permanenza in un esercizio commerciale] o non ricordare i soggetti con i quali è entrato in contatto nel periodo di riferimento e/o non essere in grado di contattarli;

(ii) i soggetti eventualmente contagiati, possono non conoscere, non ricordare o non essere comunque in grado di contattare le ulteriori persone con le quali sono, a loro volta, entrate in contatto;

(iii) il soggetto contagiato - o come si è detto potenziale contagiato - è costretto a informare il personale sanitario dei nominativi delle persone con le quali è entrato in contatto nelle due/tre settimane precedenti e a informare tali persone del suo stato di contagiato e/o potenziale contagiato;

(iv) l'informazione relativa alla possibile esposizione a un rischio di contagio non è tempestiva perché affidata a un sistema manuale e volontario nonché all'utilizzo di informazioni di contatto non necessariamente utili [quelle in possesso del contagiato o potenziale contagiato o recuperate da questi e/o dagli operatori sanitari].

Si tratta di limiti che minano in maniera rilevante l'efficacia del processo e comprimono sensibilmente la privacy degli interessati mettendo in circolazione dati particolari (sanitari) al di fuori delle regole e garanzie previste dalla disciplina vigente.

Le soluzioni di contact tracing oggetto di valutazione

I limiti evidenziati nell'attuale approccio sembrano astrattamente superabili attraverso il ricorso a adeguate soluzioni tecnologiche di c.d. *contact tracing* già utilizzate - con formule e declinazioni sensibilmente diverse - in taluni Paesi stranieri.

Le più efficaci - a parere del sottogruppo che le ha valutate sotto il profilo tecnico-epidemiologico - tra le soluzioni individuate nell'ambito della call di cui si è detto dispongono - o potrebbero disporre all'esito dell'adozione di taluni correttivi emersi nel corso delle valutazioni degli scriventi - presentano le seguenti caratteristiche:

(a) identificazione delle istanze di installazione delle applicazioni su dispositivi dei cittadini che hanno preventivamente scaricato e installato l'app attraverso l'utilizzo di codici anonimi di identificazione delle singole installazioni dell'app [gli identificativi sono o, almeno, dovrebbero essere privi di qualsivoglia potenzialità identificativa dei cittadini possessori dei dispositivi];

(b) registrazione continua di un "diario dei contatti" con gli altri dispositivi con i quali entrano in contatto in un raggio compatibile con l'eventuale contagio nonché del dato relativo alla durata del contatto [tali informazioni sono o dovrebbero essere inaccessibili, in quanto registrate in forma crittografata, allo stesso titolare del dispositivo] ;

(c) indifferentemente

c.1) trasferimento dei dati archiviati nel citato “diario dei contatti” presente sul dispositivo del soggetto contagiato a un server gestito dal gestore del servizio solo a seguito dell’accertamento da parte degli operatori sanitari dello status di contagiato previo invio sul dispositivo del soggetto in questione di un apposito codice;
c.2) trasferimento sistematico di tutti i “diari dei contatti” degli utenti dell’app sul server del gestore del servizio a prescindere dal verificarsi di una specifica condizione;
(d) identificazione, attraverso un apposito algoritmo, ad opera del gestore del servizio, di un elenco di dispositivi posseduti da soggetti esposti a rischio contagio in quanto entrati in contatto, in circostanze di spazio e di tempo idonee a consentire il contagio, con il dispositivo del soggetto contagiato e, dunque, presumibilmente con quest’ultimo;
(e) invio intra-app a tali dispositivi di un messaggio contenente un’informazione relativa al rischio di contagio - senza alcuna menzione di dati identificativi del soggetto contagiato - con contestuale invito a adottare misure idonee a evitare ulteriori eventuali contagi e a contattare gli operatori sanitari preposti [il messaggio in questione dovrebbe essere instradato utilizzando esclusivamente l’identificativo che contraddistingue ciascuna installazione della app e non richiedere l’incrocio di tali informazioni non direttamente identificative con alcuna altra informazione di recapito];
(f) cancellazione di tutti i dati non anonimi o aggregati oggetto di trattamento - sia dai dispositivi dei singoli che dal server centrale - successivamente alla fine dell’emergenza .
(g) variazione periodica e casuale dell’ID anonimo dell’applicazione.

Le soluzioni tecnologiche in questione, inoltre, prevedono a volte una funzionalità di “diario clinico” attraverso la quale l’utente può annotare e tenere traccia di eventuali sintomi - anche lievi - e essere avvisato sull’opportunità di contattare gli operatori sanitari o adottare eventuali diversi accorgimenti.
I dati registrati nel diario clinico, tuttavia, restano all’interno del dispositivo, nell’esclusiva disponibilità del possessore - come fossero annotati su un taccuino completamente indipendente dall’app quale attività a carattere esclusivamente personale o domestico - e non sono in nessun caso condivisi con terzi.
I trattamenti di dati personali anche particolari connessi a tale funzionalità, pertanto, non formano oggetto di valutazione nel presente documento in quanto non appaiono suscettibili di evidenziare questioni peculiari rispetto a quelle caratteristici del rapporto tradizionale tra paziente e operatori sanitari.
Le stesse soluzioni, inoltre, generalmente dispongono di potenzialità di geolocalizzazione degli utenti che, tuttavia, nell’impostazione di base sono disattivate ed in ogni caso attivabili volontariamente solo dall’utente.
Sul punto si tornerà nel prosieguo per formulare alcune considerazioni di carattere generale.
L’implementazione di una soluzione tecnologica avente le caratteristiche qui sopra sinteticamente riassunte consentirebbe, in astratto di ovviare ai limiti evidenziati nel paragrafo precedente in relazione ai processi attualmente in uso in quanto, tra l’altro:

(a) sottrae la ricostruzione dei contatti del soggetto contagiato alla sua conoscenza e/o memoria;
(b) permette la diffusione immediata del messaggio relativo al potenziale contagio e alla necessità di adottare specifiche cautele a tutti i soggetti esposti a rischio contagio;
(c) consente che l’informazione di cui sub (b) sia comunicata in forma anonima e senza conoscere i destinatari.

Le soluzioni in questione, peraltro, se opportunamente configurate - e previa eventuale adozione di idonee misure tecnico-organizzative di minimizzazione dei trattamenti - appaiono capaci di garantire il risultato attraverso il trattamento di dati in forma anonima o, comunque, dotati di una ridottissima capacità identificativa, peraltro solo eventuale e indiretta, nella sola ipotesi in cui si verifichino eventi patologici.
In particolare, sulla base delle informazioni acquisite nell'ambito della call e nel corso delle interviste con taluni tra i soggetti proponenti di alcune delle soluzioni, sembra possibile affermare che il sistema integrato - app da installarsi sui dispositivi degli utenti, server centrale destinato allo storage del "diario dei contatti" e all'identificazione delle istanze di installazione dell'applicazione dei soggetti esposti a rischio di contagio, sistema di comunicazione di una positività di contagio al server e propagazione dell'allerta alle istanze di installazione dei dispositivi dei soggetti a rischio contagio - non necessiti, per il suo funzionamento, di alcun trattamento di dati personali potendo funzionare attraverso una rete nell'ambito della quale tutti i dispositivi coinvolti sono contraddistinti da identificativi completamente autonomi.

È, peraltro, evidente che le considerazioni che precedono circa il carattere normalmente anonimo o, almeno, pseudoanonimo dei dati trattati nell'esercizio del sistema verrebbero meno qualora si decidesse di attivare le funzionalità/potenzialità di geolocalizzazione delle quali sono dotate diverse tra le soluzioni esaminate: in questo caso, infatti, sussisterebbero tutta una serie di ipotesi nelle quali l'identificativo ancorché anonimo del dispositivo sul quale è installata un'app associato a dati di geolocalizzazione potrebbe consentire l'identificazione del possessore del dispositivo.
Ai fini del presente documento, tuttavia, non si prende in considerazione tale eventualità non essendo per un verso proposta come necessaria ai fini del funzionamento della più parte delle soluzioni tecnologiche esaminate e non apparendo, per altro verso, opportuna sotto il profilo della tutela dei diritti fondamentali la sua attivazione in questa fase.

Raccomandazioni
Preferenza per una soluzione che contempli il trattamento di soli dati anonimi

È evidente - ed è risultato palese in occasione della diffusione delle prime notizie relative alla circostanza che il Governo sta valutando l'eventuale adozione di una soluzione tecnologica di contact tracing - l'esistenza di una diffusa preoccupazione nella popolazione per l'eventualità che l'attuale emergenza sia in qualche modo utilizzata per introdurre nel Paese forme di monitoraggio o controllo di massa della popolazione ispirate a modelli in uso in altri ordinamenti.
È egualmente evidente che tale preoccupazione - peraltro fondata su solide basi costituzionalistiche - rischia di minare il successo dell'iniziativa disincentivando una parte potenzialmente anche rilevante della popolazione dall'utilizzo della soluzione in questione.
In tale contesto si raccomanda di valutare con particolare attenzione la possibilità di scegliere, tra le diverse opzioni disponibili, quella che appare capace di garantire un risultato in linea con gli obiettivi perseguiti previa utilizzazione di dati anonimi o, almeno, dotati di capacità identificativa degli interessati nella sola ipotesi di episodi patologici quali incidenti o attacchi malevoli.
In questa prospettiva si suggerisce altresì di astenersi dall'associare alle soluzioni tecnologiche qui considerate qualsivoglia funzionalità di geolocalizzazione soddisfacendo, eventualmente, la diversa esigenza di monitoraggio dei focolai di diffusione persistente del virus così come delle zone a rischio diffusione calante mediante il ricorso a sistemi e soluzioni autonomi e distinti.
L'anonimato - assoluto o quasi assoluto - dell'interessato nell'utilizzo della soluzione tecnologica eventualmente prescelta si presenta come un valore irrinunciabile da garantire sia sul piano del

bilanciamento dei diritti fondamentali sia ai fini del successo dell'iniziativa che ha nell'adesione convinta e spontanea dei cittadini un fattore strategico.
Non sembra lecito aprire la porta a eventuali compressioni della privacy e di altri diritti fondamentali laddove il perseguimento dell'obiettivo appaia possibile anche attraverso il ricorso a tecnologie che non impongono tale compressione

3. Principali questioni di diritto sottese all'implementazione delle soluzioni tecnologiche individuate

(A) Ragionevole probabilità di efficacia della soluzione

Sotto il profilo giuridico – tanto che si guardi al diritto alla protezione dei dati personali, tanto che si guardi a qualsiasi altro diritto fondamentale – la questione della sostenibilità del ricorso a una soluzione avente le funzionalità descritte nei paragrafi precedenti va, innanzitutto, affrontata e risolta in una logica di bilanciamento dei diritti, considerando sostenibile la parziale compressione di taluni diritti in vista della tutela di altri in ossequio a un criterio di necessità e proporzionalità.
Com'è noto, le norme in materia di protezione dei dati personali sono quelle attualmente vigenti e precisamente, per l'Italia, il Regolamento UE 2016/679 (GDPR) e il Decreto Legislativo 196/2003 (nel testo modificato dal D.Lgs. 101/2018), mentre per la Repubblica di San Marino, la Legge 171/2018. Inoltre, restano sempre valide le norme sovranazionali in subiecta materia e, in particolare, quelle contenute nella nota "Convenzione 108+", così come, per l'Europa, la Carta dei Diritti Fondamentali dell'Unione Europea che qualifica i diritti alla riservatezza e alla protezione dei dati personali come diritti fondamentali, nonché la legislazione europea.
In tale contesto normativo è evidente che, laddove non sussistessero sufficienti elementi a supporto dell'efficacia della soluzione tecnologica ipotizzata in termini di tutela della salute pubblica, difficilmente potrebbe accedersi a un giudizio di sostenibilità delle necessarie limitazioni e compressioni del diritto alla protezione dei dati e/o di altri diritti fondamentali per quanto esse possano risultare modeste e contenute previa adozione delle soluzioni oggetto della raccomandazione che precede.
In questa prospettiva, prima ancora di addentrarsi nell'esame delle questioni giuridiche connesse alla progettazione e sviluppo di talune specifiche soluzioni tecnologiche, sembra essenziale affrontare la questione della sussistenza di idonei elementi utili a ritenere che l'app eventualmente prescelta come componente del sistema integrato di contact tracing possa effettivamente essere scaricata e utilizzata regolarmente da una percentuale rilevante della popolazione da identificarsi sulla base degli studi epidemiologici in corso.
Nella medesima prospettiva, peraltro, appare altresì opportuno tenere presente che il solo presupposto che precede sarebbe, comunque, scarsamente produttivo degli effetti sperati qualora l'adozione di un'idonea soluzione tecnologica non fosse accompagnata da un'efficace organizzazione dei necessari presidi sanitari e dell'attività logistica necessaria, tra l'altro, alla distribuzione e esecuzione dei test tra i cittadini.
Al riguardo occorre tener presente - come risulta chiaro anche dall'esame delle esperienze straniere - che la componente tecnologica è, in ogni caso, "solo" una delle componenti di un sistema di contact tracing, inidonea, isolatamente considerata, a garantirne l'efficacia.
In assenza dei presupposti che precedono, pertanto, l'adozione delle soluzioni tecnologiche ipotizzate risulterebbero improduttive di benefici significativi in termini di contenimento della diffusione del contagio.
Al riguardo non si dispone, allo stato, di elementi idonei a fondare alcuna valutazione sul punto con specifico riferimento alle soluzioni oggetto della call.
Sul versante economico-sociale, peraltro, si è consapevoli che il nostro Paese, pur collocandosi al 24º posto fra i 28 Stati membri dell'UE nell'indice di digitalizzazione dell'economia e della società (DESI) della Commissione europea per il 2019, come indicato nel medesimo rapporto, "[...]è in buona posizione, sebbene ancora al di sotto della media dell'UE, in materia di connettività e servizi

pubblici digitali. I servizi pubblici online e open data sono prontamente disponibili e la diffusione dei servizi medici digitali è ben consolidata".
Si segnala, quindi, al riguardo, che, proprio tenendo conto delle condizioni di scarsa digitalizzazione del Paese sia sul versante infrastrutturale che culturale e educativo, l'obiettivo di ampia diffusione dell'app, specie qualora il download e l'utilizzo fossero affidati esclusivamente a una scelta volontaria del singolo cittadino, appare estremamente ambizioso.

Raccomandazioni
Alla luce delle considerazioni che precedono si raccomanda di anteporre a qualsivoglia valutazione relativa all'adozione di una specifica soluzione tecnologica, analisi e valutazioni relative agli strumenti - comunicativi, regolamentari e tecnologici - utilizzabili al fine di rendere raggiungibile il predetto obiettivo di diffusione e utilizzo della soluzione da parte della necessaria percentuale minima di popolazione.
Tale raccomandazione ha, peraltro, un duplice riflesso giuridico:
(a) come si è detto dalla potenziale efficacia della soluzione in termini di tutela della salute pubblica dipende ampiamente la sua sostenibilità in termini di impatto su altri diritti e libertà fondamentali;
(b) taluni degli strumenti utilizzabili per aumentare la diffusione della soluzione e il suo utilizzo da parte dei cittadini potrebbero incidere sulla base giuridica del trattamento dei dati personali.

(B) Esclusione dell'obbligo e adozione di strumenti di incentivazione all'utilizzo della soluzione tecnologica

Il conseguimento dell'obiettivo di effettivo utilizzo della soluzione tecnologica da parte di una adeguata percentuale della popolazione potrebbe essere difficilmente conseguibile qualora ci si limiti a promuoverne il download e l'uso attraverso un'idonea campagna di comunicazione, lasciando poi la decisione completamente affidata alla scelta individuale del singolo cittadino. Tuttavia, la strada della previsione ex lege di un obbligo di utilizzo dell'app, pur non preclusa, appare costituzionalmente non agevole (cfr. Corte cost., sent. n. 5/2018) e controindicata da ragioni di ordine pratico-giuridico.
La soluzione che appare più perseguibile è una incentivazione al download e all'uso della soluzione tecnologica in questione fondata sulle elevate garanzie da essa prestate.

Ragioni di ordine pratico e giuridico suggeriscono questa raccomandazione.
A solo titolo esemplificativo si rileva che:
- non sussisterebbero efficaci strumenti di *enforcement* nell'ipotesi di inadempimento anche diffuso all'obbligo e/o di artificiosa sottrazione all'obbligo medesimo [es: utenti che potrebbero scaricare l'app ma utilizzare poi in maniera anomala il dispositivo spegnendolo in taluni momenti o separandosene];
- un obbligo o un incentivo che impatti sull'esercizio di diritti e libertà rischierebbe di essere percepito dai cittadini come un'ingerenza eccessiva dello Stato in scelte di carattere personale e, probabilmente, considerata una "forzatura" normativa finalizzata a consentire forme di controllo di massa della popolazione;
- talune fasce della popolazione, probabilmente, si troveranno in una condizione di oggettiva difficoltà di utilizzo della soluzione non disponendo di uno smartphone o non essendo in grado di usare la soluzione per questioni anagrafiche, legate al proprio stato di salute (ipovedenti o portatori

di altri handicap, detenuti), culturali o economiche. Peraltro, queste annoverebbero fasce già vulnerabili della popolazione esacerbando un digital divide e discriminazioni inammissibili

- nella loro versione di base, le soluzioni tecnologiche esaminate non tengono traccia di eventuali disattivazioni del bluetooth e/o di usi anomali dello smartphone con la conseguenza che sussisterebbe il rischio di garantire benefici a cittadini che installino e usino l'app per il tempo strettamente necessario alla "conquista" del beneficio;
- è difficilmente aggirabile, praticamente prima che giuridicamente, il problema delle conseguenze dell'eventuale violazione dell'obbligo\impegno incentivato da parte del cittadino: ipotizzare una sanzione per l'ipotesi in cui il cittadino, ad esempio, spenga lo smartphone durante determinate fasce orarie o non lo porti con sé, sembra piuttosto difficile anche alla luce della difficoltà di accertamento del carattere doloso o anche solo gravemente colposo della condotta [es: lo smartphone può spegnersi per incolpevole esaurimento della carica, può essere dimenticato a casa, può trovarsi in una posizione di assenza di campo ecc.].

Peraltro, sotto il profilo della disciplina sulla protezione dei dati personali taluni sistemi di incentivazione all'utilizzo della soluzione e, dunque, alla prestazione dell'eventuale consenso ai connessi trattamenti di dati personali rischierebbero di compromettere la libertà della prestazione del consenso e, conseguentemente, la sua validità, rendendo necessario identificare una diversa base giuridica per i trattamenti di dati personali [cfr sul punto si veda il paragrafo (C) che segue].

Raccomandazioni

Si sconsiglia, di introdurre qualsivoglia obbligo legale di utilizzo della soluzione tecnologica.
Si suggerisce di affidare il ricorso a tale soluzione ad una adesione libera, ancorché incentivata, del singolo utente.
Sono assolutamente sconsigliate, perché di dubbia costituzionalità, forme di incentivo che graduino\limitino l'accesso dei cittadini a servizi altrimenti fruibili secondo principi di parità di trattamento o che vincolino l'esercizio di diritti di libertà all'adozione dell'app.
Alla luce delle considerazioni precedenti e volendo evitare incentivi tali da far venir meno il carattere volontario della decisione, l'adozione massiva della soluzione prescelta pare meglio essere affidata ad una campagna informativa per l'adesione volontaria capace di sviluppare fenomeni di incentivazione dolce tali però da non comprimere se non addirittura violare diritti e libertà fondamentali.
Valido esempio concreto potrebbe essere l'invio per sms a tutti i cittadini iscritti ai servizi di alert della protezione civile locale o nazionale del link per scaricare l'app con messaggio del tipo "Oggi salvo vite umane , oggi salvo la mia vita, installo "….". Analoga campagna push potrebbe essere aggiunta nella messaggistica di fatturazione e pubblicitaria dei soggetti privati che aderiscono all'iniziativa.

(C) Implementabilità del sistema attraverso trattamento di dati esclusivamente anonimi o base giuridica del trattamento dei dati personali eventualmente sotteso al funzionamento dell'app

Alcune delle soluzioni tecnologiche oggetto di valutazione sembrerebbero implicare - il condizionale è necessaria conseguenza dell'assenza di informazioni sufficientemente puntuali nella documentazione sin qui acquisita - un trattamento di dati personali ancorché in misura estremamente contenuta e, anzi, in alcuni casi ai limiti - previa adozione di talune possibili misure di minimizzazione dei trattamenti - della definizione di dato personale e, conseguentemente dell'applicabilità della vigente disciplina nazionale e europea in materia di privacy.
Il funzionamento di base delle soluzioni tecnologiche prese in esame - o almeno di quelle risultate più rispondenti ai requisiti tecnico-epidemiologici - prevede la circolazione di soli dati non identificativi scambiati tra dispositivi contraddistinti da identificativi insuscettibili di rivelare, almeno direttamente, l'identità dei possessori; più correttamente, probabilmente – salvo miglior verifica tecnica – dati pseudoanonimi.
I due unici momenti dell'intero processo di *contact tracing* identificati come astrattamente idonei a impattare - pur senza annullarla - sulla validità di tale assunto appaiono essere rappresentati dal dialogo tra il dispositivo dell'utente e il server centrale ai fini del trasferimento - eventuale e episodico oppure sistematico a seconda delle soluzioni prescelte - del "diario dei contatti" e dal dialogo tra il dispositivo dell'operatore sanitario e il server del gestore del sistema finalizzato all'attivazione del processo di contatto dei soggetti a rischio contagio.
Nel primo momento, infatti, il server centrale, come si è anticipato, è tecnicamente nella condizione - peraltro necessaria ai fini del funzionamento del protocollo di comunicazione TCP/IP - di identificare l'indirizzo IP dal quale proviene il "diario dei contatti" preso in carico.
Analogamente nel secondo momento l'operatore sanitario, evidentemente, all'atto della trasmissione del codice per l'attivazione del processo di contatto dei soggetti a rischio contagio ha preventivamente identificato anagraficamente il proprio paziente e, pertanto, disponendo altresì (sebbene anche qui in modo istantaneo e transitorio) dell'identificativo univoco della installazione sul dispositivo del paziente medesimo potrebbe ricondurre tale ultimo dato a una specifica identità anagrafica.
In entrambi i casi, peraltro, appare possibile fare in modo che il gestore del sistema di *contact tracing* non raccolga alcun dato identificativo diretto o indiretto [indirizzo IP del dispositivo del soggetto dal quale provengono le informazioni archiviate nel diario dei contatti nel primo caso e dati anagrafici del soggetto contagiato nel secondo] e che pertanto, come si è anticipato, il suo trattamento possa sostanzialmente considerarsi, salvo quanto si dirà nel prosieguo, un trattamento di dati anonimi.

In particolare:
(a) in relazione al primo dei due momenti, come si è anticipato sopra, potrebbe ipotizzarsi l'interposizione di un proxy gestito da una terza parte fidata che raccolga la comunicazione cifrata dei diari dei contatti dai possessori dei dispositivi e la inoltri al server del gestore del sistema dopo aver proceduto alla definitiva cancellazione dell'indirizzo IP identificativo del mittente; in questo modo al gestore del sistema, titolare del trattamento, perverrebbero esclusivamente dati resi sufficientemente anonimi da impedire l'identificazione dell'interessato tenuto conto dell'insieme di fattori obiettivi tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione;
(b) in relazione al secondo dei due momenti, come pure si è anticipato, potrebbe ipotizzarsi che l'operatore sanitario, nella sua qualità di titolare autonomo o di responsabile nominato da un autonomo - rispetto al gestore del sistema di contact tracing - titolare del trattamento dei dati acquisiti nell'ambito del rapporto con il paziente - incidentalmente utente dell'app - qualora accerti il verificarsi della condizione idonea a giustificare l'invio dell'alert ai dispositivi entrati in contatto

con quello del soggetto contagiato proceda alla comunicazione al server del gestore del sistema dell'input all'invio del predetto alert. In tal caso sarebbe sufficiente che contestualmente all'invio, il sistema utilizzato dall'operatore sanitario eliminasse definitivamente ogni associazione tra l'identificativo dell'installazione dell'app e l'identità anagrafica del paziente dell'operatore sanitario.

Tali accortezze farebbero sì che il gestore del sistema si trovi anche in questo flusso di input a ricevere esclusivamente "dati resi sufficientemente anonimi da impedire l'identificazione dell'interessato" tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione. Ovviamente anche in questo caso con la sola eccezione di eventuali incidenti o attacchi idonei a consegnare nelle mani di un medesimo soggetto la pluralità di elementi informativi necessari al fine di realizzare l'associazione tra dati anonimi e dati direttamente o indirettamente personali.

Si tratta di un'ipotesi remota ma ineliminabile in ragione della quale, nel prosieguo, si preferisce considerare il trattamento posto in essere dal gestore del sistema come un trattamento comunque rientrante, sebbene solo in una dimensione cautelativa, nell'ambito di applicazione della disciplina in materia di protezione dei dati personali.

In tale contesto la principale questione da affrontare nel valutare l'impatto privacy è, evidentemente, quella relativa alla base giuridica del trattamento di dati personali che viene in rilievo nell'esercizio del sistema.

In linea di principio tale base giuridica potrebbe essere identificata nel consenso dell'interessato, trattandosi di una soluzione astrattamente compatibile con la circostanza che presupposti necessari per l'inizio di ogni trattamento sono il download dell'app, l'installazione sul dispositivo dell'interessato e l'utilizzo dell'app medesima sebbene in modalità "passiva" ovvero in background.

L'identificazione nel consenso della base giuridica del trattamento in questione, peraltro, potrebbe essere quella meglio capace di tener conto anche dell'eventualità - remota ma ineliminabile per quanto si è detto - che i dati oggetto di trattamento, al verificarsi di un evento patologico, siano in grado di reidentificare un interessato e associargli un dato particolare quale l'aver effettuato un tampone con un determinato esito.

Tale soluzione, tuttavia, presenta taluni limiti:
1) la libertà del consenso, come è noto necessario presupposto per la sua validità, rischia di essere compromessa dagli eventuali meccanismi di incentivazione all'uso dell'app e, dunque, al connesso trattamento di dati personali;
2) la libera revoca del consenso potrebbe avere implicazioni sul funzionamento dell'intero sistema;
3) a seguito della duplice manifestazione di volontà relativa all'installazione e all'utilizzo dell'app - eventualmente da far constare attraverso accettazione di termini d'uso - tutti i trattamenti strumentali al funzionamento del sistema di contact tracing appaiono necessari con la conseguenza che l'eventuale consenso risulterebbe, di fatto, obbligatorio risultando impossibile, in difetto, il funzionamento dell'applicazione per le finalità sue proprie.

Anche in considerazione delle perplessità emerse con riferimento all'identificazione del consenso come base giuridica dei trattamenti connessi al funzionamento del sistema di contact tracing si suggerisce di affidare l'eventuale adozione di tale sistema a un decreto legge che, con riferimento ai profili oggetto del presente documento, potrebbe stabilire:

(a) che il gestore del proxy e quello del sistema, rispettivamente con riferimento, alla raccolta, anonimizzazione e all'inoltro al gestore del sistema nonché alla raccolta e alla conservazione sono legittimati a trattare i dati degli utenti - come si è detto "sufficientemente anonimi" ai sensi del GDPR - a condizione che gli utenti medesimi abbiano manifestato liberamente l'adesione ai termini d'uso dell'applicazione i quali dovranno chiarire i trattamenti posti in essere da ciascun soggetto;
(b) che gli operatori sanitari sono obbligati a inserire i dati relativi all'eventuale diagnosi di contagio nel sistema di contact tracing attivando così l'alert destinato ai soggetti a rischio di contagio [art. 9.2.h Regolamento].

O, in alternativa, stabilire:

(a) che il gestore del proxy, con riferimento alla raccolta, anonimizzazione e inoltro dei dati, e il gestore del sistema, con riferimento alla raccolta e alla conservazione, sono legittimati al trattamento dei dati medesimi sulla base dell'eventuale consenso dell'interessato;
(b) che gli operatori sanitari sono obbligati a inserire i dati relativi all'eventuale diagnosi di contagio nel sistema di contact tracing attivando così l'alert destinato ai soggetti a rischio di contagio [art. 9.2.h Regolamento].

Nella sostanza si tratta di scegliere se identificare o meno la base giuridica del trattamento nel consenso degli interessati, anche se solo in misura parziale e limitatamente al solo trattamento da parte del gestore del server proxy e del gestore del sistema dei dati riconducibili all'interessato tramite l'IP di invio. In ogni caso si muoverebbe dal presupposto che, probabilmente, tale scelta non è indispensabile sotto un profilo tecnico-giuridico ma indiscutibilmente potrebbe risultare - ove la si ritenga legittima in applicazione della disciplina vigente nonostante le perplessità sopra evidenziate - a rendere più facilmente sostenibile sul versante politico-mediatico l'eventuale decisione di adozione di una soluzione di contact tracing.
Si tratta di due opzioni tra cui appare difficile identificarne una ideale e da preferire certamente sull'altra.
Si tratta, quindi, di due distinte opzioni che portano a qualificare diversamente la natura giuridica del consenso prestato.
In un'ottica di obbligo legale, il consenso dell'utente è una condizione per l'applicabilità della legge; il consenso è, perciò, un evento, assimilabile all'atto giuridico in senso stretto.
In un'ottica negoziale, il consenso dell'utente è una manifestazione di volontà ad aderire alle condizioni previste dalla legge per usufruire della prestazione; il contesto è qui assimilabile ai negozi a fonte eteronoma, cioè ai negozi che sono disciplinati non dalla volontà delle parti, ma dalla legge.
Il precipitato giuridico, ossia la portata pratica, di tale distinzione, ad esempio, si può riscontrare nell'ipotesi di scaricamento dell'app da parte di soggetto incapace naturale. Quid iuris? Nel primo caso (atto giuridico in senso stretto), si ritiene che l'attività non impedirebbe la raccolta dei dati, laddove, nel secondo caso (atto negoziale) il vizio del consenso renderebbe, invece, revocabile (ex nunc)/annullabile (ex tunc) il trattamento successivo del flusso di informazioni inviate.
Ma l'analisi giuridica si deve arrestare dinnanzi alle superiori scelte di politica legislativa.
Il medesimo decreto legge dovrebbe altresì precisare, sempre limitatamente ai profili oggetto del presente documento: 1) l'obbligo del gestore del server proxy di procedere alla immediata cancellazione di ogni associazione tra ID dell'applicazione e IP di invio dei dati; 2) l'obbligo di adozione di misure tecniche ed organizzative tali da impedire la memorizzazione dell'associazione tra identità della persona fisica e ID dell'installazione dell'app all'atto dell'inserimento delle positività da parte del personale sanitario.

GRUPPO DI LAVORO 8 – PROFILI GIURIDICI

RELAZIONE PROPOSTA n. 71

Nome soluzione

CovidApp - Covid Community Alert.

Soggetto proponente

L'app viene proposta dal team denominato "Coronavirus Outbreak Control", che non risulta possedere personalità giuridica.

Tipologia di dati trattati dall'app

In base alla descrizione fornita, il funzionamento dell'app garantirebbe il trattamento di dati in forma anonima o comunque il trattamento di informazioni con una ridottissima capacità identificativa, peraltro solo eventuale e indiretta nell'ipotesi in cui si verifichino eventi patologici. In due soli frangenti sembrerebbe ravvisabile un trattamento di dati personali, pur con limitate possibilità di re-identificazione: anzitutto, in relazione all'indirizzo IP dell'utente al momento della trasmissione delle informazioni registrate in locale al server; in secondo luogo, in riferimento alla attività di sblocco del diario clinico di un paziente da parte del personale medico, che implica necessariamente (e inevitabilmente) l'associazione tra l'ID randomico attribuito al paziente che utilizza l'app e l'identità del paziente medesimo, nota all'operatore sanitario che lo ha precedentemente visitato (e derivante da una precedente, autonoma e separata attività di trattamento di dati relativi alla salute).
Sotto il primo profilo, tuttavia, i dati inerenti agli indirizzi IP non formano comunque oggetto di memorizzazione e sono comunque proposte misure idonee di mitigazione.
Quanto al secondo versante, il rischio connesso alla inevitabile cognizione dell'associazione tra paziente visitato e ID inserito nel sistema potrebbe parimenti essere contenuto imponendo l'immediata cancellazione delle informazioni all'operatore sanitario.
Al di fuori di queste circostanze, le informazioni immagazzinate riguardano le interazioni spaziali anonime registrate mediante tecnologia Bluetooth con altri dispositivi nel periodo antecedente e la relativa durata temporale (funzionali a rivelare il rischio di esposizione con il dispositivo appartenente di un paziente riscontrato clinicamente positivo).
L'installazione dell'app non richiede il trattamento del numero telefonico del dispositivo. All'utente, all'atto del login, è infatti assegnato un ID generato pseudo-randomicamente e soggetto su base costante a un processo di *shuffling* volto a ridurre qualsiasi rischio di tracciamento dei dispositivi sulla base del segnale Bluetooth.
Se l'utente lo desidera, su base volontaria, è consentita l'attivazione del segnale GPS, che comunque non comporta un tracciamento generalizzato dell'utente e si limita a registrare

esclusivamente le interazioni con altri dispositivi (non operando, cioè, quando il dispositivo risulta in stato di "isolamento").

Modalità del trattamento

L'app procede alla generazione di codici identificativi anonimi correlati ai device (smartphone) su cui è installata al fine di verificarne l'interazione spaziale con altri dispositivi che potrebbero successivamente risultare appartenenti a individui di cui sia riscontrata la positività al virus. In caso di disinstallazione e successiva reinstallazione dell'app il codice randomico è generato *ex novo*. L'app è in grado di riscontrare l'associazione tra l'ID randomico originale e quelli successivamente assegnati all'esito del processo di *shuffling* conservando i dati per finestre di tempo limitate. La comunicazione dei dati relativi alle interazioni registrate da ciascun dispositivo su cui l'app sia stata installata comporta in ogni caso il trattamento dell'indirizzo IP, che può tuttavia essere accompagnato da idonee misure di mitigazione del rischio come segnalato in relazione generale.
Su base periodica, i dati registrati mediante tecnologia Bluetooth e salvati in locale, relativi all'interazione con altri dispositivi e indicativi degli spostamenti effettuati dai rispettivi proprietari, sono trasmessi al server e archiviati in modalità *cloud*.
Al contempo, in caso di visita, mediante un'apposita interfaccia dedicata (CoviDoc), gli operatori sanitari, con il consenso dell'utente *in loco*, provvedono, tramite la scansione del QR code associato al dispositivo in essere ai pazienti, ad aggiornare il diario clinico, segnalando eventuali casi di contagio. Si precisa che l'attività di trattamento dei dati relativi alla salute effettuata dal personale medico che successivamente adoperi l'app risale invece a una autonoma e separata fase diagnostica e a un trattamento separato e autonomo dei dati (pare in ogni caso opportuno che l'operatore sanitario proceda all'immediata cancellazione dell'identificativo, prevenendone così la conservazione, onde minimizzare ogni rischio di re-indentificazione collegato alla sua personale conoscenza del paziente cui si riferisce il codice randomico anonimo utilizzato).
Una volta aggiornato lo status clinico di un utente, l'app è in condizione di individuare all'interno del database i dispositivi (identificati da ID anonimo) con i quali il dispositivo appartenente al paziente dichiarato positivo (o sospetto positivo) si sia trovato in una rilevante prossimità spaziale (tale da rendere apprezzabile il rischio di contagio) nell'arco dei quattordici giorni antecedenti così da inviare loro notifiche push (con misure tecniche e organizzative atte a impedirne la identificazione) contenenti l'informazione circa l'esposizione a rischio e possibili istruzioni sul comportamento da adottare.
Il funzionamento dell'app presuppone una previa definizione della distanza e della durata della interazione spaziale tra dispositivi rilevanti al fine di ritenere apprezzabile il rischio di contagio.
Il processo di continua memorizzazione su base periodica delle interazioni registrate tra dispositivi consente di rimediare a un *gap* tecnico dovuto alla impossibilità dei dispositivi iOS di trasmettere segnali Bluetooth in modalità *background*. Con questa soluzione tecnica, l'interazione tra dispositivi Android e dispositivi iOS consente di rimediare alla limitazione

tecnica dei dispositivi Apple che ricevono il segnale ma non lo trasmettono e garantire una percentuale di copertura del 98,9%, che sarebbe altrimenti limitata al 71,5%.

Uso di soluzioni di terze parti

L'app utilizza la tecnologia di tracciamento contatti basata sul Bluetooth Low Energy (LE). La componente server del progetto utilizza invece i servizi *cloud* della piattaforma Amazon AWS, così come progettata, ma può essere dispiegata su strutture autonome e proprietarie del titolare del trattamento.

Privacy by design - Privacy by default

Dall'esame della documentazione, la soluzione tecnologica appare fortemente improntata al rispetto dei principi di *privacy by design* e *privacy by default*. Nella definizione delle caratteristiche e delle modalità operative dell'app, si è tenuto conto dello stato dell'arte, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per i diritti e le libertà delle persone fisiche. Questa certosina attenzione emerge nella dettagliata presentazione tecnica dell'app, ove si documenta l'implementazione delle misure tecniche e organizzative adeguate, tra cui la minimizzazione del trattamento di dati e la pseudonimizzazione.

Misure di sicurezza

Sotto il profilo tecnico, la documentazione non è corredata da report che dimostrino l'esecuzione di test di sicurezza sulle app e sui server utilizzati. Non è quindi dato formulare una compiuta valutazione in relazione agli aspetti di sicurezza informatica e di resistenza a possibili attacchi informatici. Si segnala tuttavia l'impegno a una continua implementazione dell'applicazione grazie a un team di sviluppatori del codice *open source*. I proponenti dichiarano altresì di aver dato corso ad attività quali *penetration test e reverse engineering* di cui non hanno ancora prodotto la relativa documentazione, come sopra specificato.
Nella descrizione, si segnala che tutte le comunicazioni tra app e server utilizzano protocolli HTTP su Transport Layer Security (HTTPS), avvalendosi pertanto di cifratura mediante crittografia asimmetrica. I relativi certificati sono gestiti da Amazon AWS, che fornisce la piattaforma di *cloud*.
Non è precisata la localizzazione dei *data center* di archiviazione delle informazioni, tuttavia la documentazione dichiara la conformità dell'app alla legislazione applicabile nell'Unione europea.

Analisi dei rischi per le libertà e i diritti degli interessati

Non si ravvisano, sulla base delle informazioni rappresentate dal proponente, particolari rischi per le libertà e i diritti degli interessati legati al fisiologico funzionamento dell'app.

L'obiettivo perseguito dall'app non è quello di permettere l'individuazione di un paziente infetto, bensì di notiziare ai suoi utenti le possibili interazioni spaziali entro l'arco temporale dei 14 giorni antecedenti con dispositivi appartenenti a utenti le cui connotazioni cliniche siano state esaminate dal personale medico, con conseguente riscontro di positività al Coronavirus e aggiornamento del diario sanitario. Si potrebbero tuttavia registrare, in condizioni "patologiche" che prescindono dalla normale operatività dell'app e dal suo fisiologico funzionamento, attacchi informatici in grado di comportare il rischio di una re-identificazione degli utenti precedentemente "anonimizzati" con annessa, possibile, esposizione dei dati relativi alla salute (quali l'aggiornamento dello stato clinico del paziente all'esito dell'effettuazione di un tampo, positivo o negativo che sia).
La ricerca di modalità volte ad assicurare in ogni fase l'anonimato, frutto di una adesione apprezzabile ai principi di *privacy by design* e *privacy by default*, costituisce senza dubbio un punto di forza della soluzione proposta, le cui modalità tecniche appaiono congegnate in modo da limitare al massimo il rischio di identificazione dei titolari dei dispositivi. L'app presenta inoltre una possibile implementazione legata all'utilizzo della tecnologia GPS, la cui attivazione sarebbe eventualmente rimessa all'utente, e dunque previo consenso, ma che si consiglia in ogni caso di valutare in relazione al suo possibile impatto sui diritti e le libertà degli individui. In ogni caso, il tracciamento è circoscritto all'evenienza in cui il dispositivo dell'utente interagisca con lo spazio, non attivandosi invece in fasi di "isolamento".
Non sono precisate le misure volte a consentire la distruzione automatica delle informazioni, sebbene il riferimento cronologico appaia legato alle interazioni occorse nei quattordici giorni antecedenti lo sblocco del diario clinico del paziente.
La presentazione dell'app non è corredata da una valutazione di impatto, ma dà conto dell'*endorsement* di un team di esperti in materie giuridiche, informatiche e ingegneristiche. Il proponente dichiara che è comunque in fase di finalizzazione e di revisione legale il "documento privacy".

RELAZIONE PROPOSTA n. 100

Nome soluzione

Immuni

Soggetto proponente

Bending Spoons S.p.A..
L'iniziativa è presentata unitamente a Arago, GeoUniq, Centro Medico Santagostino e Jakala.

Tipologia di dati trattati dall'app

Alla luce dei chiarimenti forniti dalla proponente in data 02/04/2020, pare che l'app non tratti dati personali fino al momento in cui, a seguito di diagnosi da parte di un operatore sanitario, non venga contattato l'utente.
All'utente all'atto del login viene assegnato un codice generato pseudo-randomicamente, dal sistema Bluetooth LE, circostanza che non permette di identificare l'utente dello specifico dispositivo. Non viene richiesto alcun numero di telefono in fase di login.
L'App consente pertanto una minimizzazione di tutti i dati personali e particolari fino all'eventuale e futuro contatto con l'operatore.
Non sono previsti dati di geolocalizzazione essendo sufficiente allo scopo il contatto di prossimità con i terzi soggetti attraverso la memorizzazione dei Bt_ID (bluetooth Identification), ma è possibile aggiungere anche il georeferenziamento (che potrebbe rimanere su base volontaria).
L'applicazione consente altresì la memorizzazione sul device personale dei dati di familiari/conviventi in relazione ai quali - fino all'implementazione di dispositivi wearable - può essere attivata solo la funzione di "diario clinico" con le stesse garanzie di minimizzazione dei dati implementate per l'utente principale dell'App.

Modalità del trattamento

I dati inerenti lo stato di salute che vengono memorizzati ed elaborati esclusivamente in locale sul device dell'utente non vengono associati ad un'identità o a dati anagrafici. Neanche in fase di Login. L'applicazione, basata esclusivamente su tecnologia Bluetooth LE, consente di gestire una funzione di *contact tracing* basata su una serie di ID (temporanei) non associati ad una identità dell'utente sia sul device sia in modalità tracing di prossimità. Al momento l'app non usa tecnologie di geolocalizzazione, nonostante il proponente dichiari che è possibile implementarla successivamente.
L'app fornisce una funzione di alerting nel caso ad un utente venga richiesto, a seguito di diagnosi da parte di un operatore sanitario, o per volontà dell'utente stesso di provvedere

ad inviare al server centrale una copia del database locale al server remoto contenente i Bt_ID crittografati dei dispositivi degli altri utenti con cui il paziente è stato in prossimità (max 50 mt) nel lasso di tempo di riferimento. Ove poi risulti necessario, dal server - su input dell'operatore sanitario - attraverso l'app, è possibile inviare (con modalità notifiche push) opportuni messaggi ai dispositivi che si sono trovati in prossimità di quello dell'utente positivo; tutto ciò senza che all'operatore sia noto alcun dato personale dei destinatari della notifica push. Tutto ciò avviene sfruttando un'applicazione mobile specifica per gli operatori sanitari che permette a questi ultimi di fornire all'utente un codice da inserire nell'applicazione installata sul proprio device e che consente di effettuare il dump remoto dei dati del diario clinico dell'utente e dei dati di prossimità rilevati.
Non sono previste né l'acquisizione di dati di geolocalizzazione né di metadati associati alle informazioni salvo la condizione di salute dell'utente diagnosticata dall'operatore sanitario in virtù delle misurazioni di temperatura inserite dallo stesso utente.

Dalla documentazione trasmessa è possibile ricavare che il rilevamento dei contatti di prossimità avviene con una precisione nell'ordine di 1 metro senza l'acquisizione di altri dati che non sia il codice bt_ID, la durata dell'interazione e la potenza di segnale (da cui è possibile inferire la distanza tra i dispositivi).

Per quanto riguarda il trattamento dei dati degli operatori sanitari viene effettuata la memorizzazione dei dati personali di quegli operatori sanitari che accedono al sistema, solo ai fini di autorizzazione/autenticazione sul sistema stesso.

Uso di soluzioni di terze parti

L'app utilizza la tecnologia di tracciamento contatti basate sul Bluetooth Low Energy (LE) di Arago.
Per la parte server del progetto, invece, viene utilizzata la piattaforma Google Cloud Platform.

Privacy by design – Privacy by default

Dall'esame della documentazione esaminata, emerge che nella progettazione di quest'applicazione si sono tenuti presenti i principi di privacy by design e by default in quanto è stato tenuto conto dello stato dell'arte, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per i diritti e le libertà delle persone fisiche.
Dalla documentazione prodotta e dalla descrizione delle misure di protezione implementate si evince come siano state messe in atto misure tecniche e organizzative adeguate, quali la pressoché totale minimizzazione dei dati e la pseudonimizzazione degli stessi lasciando

soltanto nella fase finale e all'operatore sanitario l'attività di identificazione dell'utente successivamente all'accertamento della positività.
Inoltre le tecnologie utilizzate consentono di acquisire soltanto gli ID degli altri dispositivi presenti ad una distanza inferiore ai 50 metri.

Misure di sicurezza

Sotto il profilo della sicurezza informatica la società proponente non ha fornito report in merito a test di sicurezza sulle applicazioni o sui server in uso. Anche per quest' App, come per le altre esaminate, non si possono pertanto valutare in modo adeguato gli aspetti relativi alla cybersecurity e alla resistenza o meno ad attività di *reverse engineering* o ad altre tipologie di attacco informatico sia sull'app sia anche sui flussi di dati intercorrenti tra gli smartphone e il server.
Dalla documentazione fornita è stato dichiarato ed è stato possibile accertare la presenza di cifratura dei dati solo sui server del cloud provider (Google Cloud Platform) con algoritmi AES256 o AES128. Inoltre è stato dichiarato che il Cloud pro Google Cloud Platform è certificato ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.
È stato dichiarato inoltre che i dati utilizzati nell'ambito del progetto verranno memorizzati esclusivamente in datacenter collocati all'interno dell'Unione Europea.
Si suggerisce di richiedere ulteriori informazioni in merito alle misure di sicurezza effettivamente implementate.

Analisi dei rischi per le libertà e i diritti degli interessati

Sulla base della documentazione prodotta dalla proponente e della descrizione del funzionamento dell'app ivi contenuta, non si ravvisano particolari rischi per la libertà e i diritti degli interessati.
Non vi è la possibilità di ricostruire i movimenti degli utenti, la lista dei loro contatti/incontri e nemmeno di acquisire in un unico punto le informazioni memorizzate nei diari clinici (destinate a rimanere sui dispositivi).
Queste caratteristiche rappresentano un punto di forza della soluzione proposta. Conseguentemente, se non indispensabile, si raccomanda di non implementare la funzione di geolocalizzazione che - al contrario - consentirebbe la raccolta dei dati sulla posizione degli interessati e, quindi, la ricostruzione dei loro movimenti con evidenti rischi per i diritti e libertà dei cittadini. Si precisa che anche ove la geocalizzazione rimanesse una opzione volontaria ed eventuale anche un'adesione minima espone a rischi di reidentificazione che andrebbero comunque apprezzati sia ai fini della tutela dei diritti e libertà fondamentali sia quale serio disincentivo all'adozione.
In ogni caso, vista la rilevanza e il numero di utenti che utilizzerebbero l'applicazione, si raccomanda di:

- effettuare robusti test di sicurezza informatica sull'applicazione prima del rilascio definitivo all'autorità pubblica;

- condurre una valutazione d'impatto ai sensi dell'art. 35 Reg. UE 2016/679.

Sito del Garante per la protezione dei dati personali

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020 [9328050]

[doc. web n. 9328050]

Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020

Registro dei provvedimenti
n. 79 del 29 aprile 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, alla quale hanno preso parte il dott. Antonello Soro, presidente, la dott.ssa Augusta Iannini, vice presidente, la prof.ssa Licia Califano e la dott.ssa Giovanna Bianchi Clerici, componenti e il dott. Giuseppe Busia, segretario generale;

Vista la richiesta di parere della Presidenza del Consiglio dei Ministri;

Visti gli articoli 36, par. 4, e 57, par. 1, lett. c), 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, di seguito Regolamento).

Visto il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 (decreto legislativo n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice) e, in particolare, l'articolo 154, comma 5;

Vista la documentazione in atti;

Viste le osservazioni del segretario generale ai sensi dell'articolo 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

PREMESSO

1. La Presidenza del Consiglio dei Ministri ha richiesto il parere del Garante su una proposta normativa per il tracciamento dei

contatti fra soggetti mediante apposita applicazione su dispositivi di telefonia mobile nell'ambito delle strategie di contenimento dell'epidemia Covid-19.

L'intervento normativo - si legge nella relazione illustrativa – è volto a disciplinare il trattamento di dati personali nel contesto dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del Covid-19 per finalità di tracciamento dei contatti tra i soggetti che, a tal fine, abbiano volontariamente installato un'apposita applicazione sui dispositivi mobili.

Al comma 1 si precisa che il titolare del trattamento è il Ministero della salute e che il trattamento riguarda il tracciamento effettuato tramite l'utilizzo di un'applicazione, installata su base volontaria e destinata alla registrazione dei soli contatti tra soggetti che abbiano parimenti scaricato l'applicazione. Ciò, al solo fine di adottare le adeguate misure di informazione e prevenzione sanitaria nel caso di soggetti entrati in contatto con utenti che risultino, all'esito di test o diagnosi medica, contagiati. Si prevede, in particolare, che il Ministero si coordini, anche ai sensi dell'articolo 28 del Regolamento, con i soggetti operanti nel Servizio nazionale della protezione civile e i soggetti cc.dd. "attuatori" di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché con l'Istituto superiore di sanità, le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID-19. Si chiarisce, infine, che la modalità di tracciamento dei contatti tramite la piattaforma informatica di cui al predetto comma è complementare alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale.

Al comma 2 si prevede che, all'esito di una valutazione di impatto effettuata ai sensi dell'articolo 35 del Regolamento il Ministero della salute adotti misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante, assicurando, in particolare, che: gli utenti ricevano, prima dell'attivazione dell'applicazione, un'idonea informativa; i dati personali raccolti dall'applicazione siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, individuati secondo criteri stabiliti dal Ministero della salute; il trattamento effettuato per il tracciamento dei contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati, con esclusione di ogni forma di geolocalizzazione dei singoli utenti; siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento; i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo, stabilito dal Ministero della salute, strettamente necessario al tracciamento e cancellati in modo automatico alla scadenza del termine; i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento possano essere esercitati anche con modalità semplificate.

Il comma 3 prevede che i dati raccolti attraverso l'applicazione non possono essere utilizzati per finalità diverse da quella di cui al medesimo comma 1, salvo in forma aggregata o anonima per finalità scientifiche o statistiche.

Il successivo comma 4 stabilisce che il mancato utilizzo dell'applicazione non comporta conseguenze in ordine all'esercizio dei diritti fondamentali dei soggetti interessati ed è assicurato il rispetto del principio di parità di trattamento, mentre il comma 5 prevede che la piattaforma informatica utilizzata è realizzata esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite da amministrazioni o enti pubblici o in controllo pubblico.

Infine il comma 6 chiarisce che ogni trattamento di dati personali dovrà cessare al termine del periodo di emergenza secondo la tempistica espressamente indicata, con conseguente cancellazione dei dati trattati.

RILEVATO

2. La norma tiene conto di molte delle indicazioni fornite dal Presidente del Garante nell'audizione tenuta in data 8 aprile u. presso la IX Commissione trasporti e comunicazioni della Camera dei deputati (in www.gpdp.it, doc. web n. 9308774), dal Segretario generale in riscontro alle ipotesi avanzate all'interno del Gruppo di lavoro "data-driven" per l'emergenza Covid-19, istituito presso la Presidenza del Consiglio dei ministri (nota del 7 aprile 2020, doc. web. n. 9316821).

Essa appare conforme, per quanto dalla stessa disciplinato e nelle sue linee generali, ai criteri indicati dalle Linee guida del Comitato europeo per la protezione dei dati del 21 aprile scorso (doc. web n. 9321621)a proposito dei sistemi di contact tracing, che possono sintetizzarsi nei termini seguenti, raffrontandovi la disposizione in esame:

a) volontarietà: in ragione del rilevante impatto individuale del tracciamento, l'adesione al sistema deve essere frutto di una scelta realmente libera da parte dell'interessato. La mancata adesione al sistema non deve quindi comportare svantaggi né rappresentare la condizione per l'esercizio di diritti. Si apprezza, in tal senso, la previsione di cui al comma 4 dell'articolo, che appare sufficientemente esaustiva, salvo la necessità di precisare, per fugare ogni possibile dubbio interpretativo, che il mancato utilizzo dell'applicazione non comporta conseguenze pregiudizievoli, adottando dunque una locuzione più ampia di quella riferita al solo esercizio dei diritti fondamentali;

b) previsione normativa: il presupposto può individuarsi nell'esigenza di svolgimento di un compito di interesse pubblico, in particolare per esigenze di sanità pubblica, in base a "previsione normativa o disposizione legislativa" dell'Unione europea o degli Stati membri. Sotto questo profilo, in particolare, la scelta di una norma di rango primario soddisfa i requisiti di cui all'articolo 9, par. 2, lett. i) del Regolamento e agli articoli 2-ter e 2-sexies del Codice, con garanzie ulteriori che potranno essere stabilite con il previsto provvedimento del Garante da adottare ai sensi dell'articolo 2-quinquiesdecies del medesimo Codice;

c) trasparenza: è necessario assicurare il pieno rispetto degli obblighi di trasparenza previsti dal Regolamento nei confronti degli interessati. In linea con tale esigenza è la previsione di cui all'articolo 1, comma 2, lett. a), della norma che assicura agli interessati un'idonea informazione sul trattamento e in particolare sulla pseudonimizzazione dei dati, mentre si raccomanda all'Amministrazione interessata di sottoporre la valutazione di impatto cui è tenuta al più ampio regime di conoscibilità e di prevedere, anche nella norma, il carattere libero e aperto del software da rilasciare con licenza open source;

d) determinatezza ed esclusività dello scopo: il tracing dev'essere finalizzato esclusivamente al contenimento dei contagi, escludendo fini ulteriori, ferme restando le possibilità di utilizzo a fini di ricerca scientifica e statistica, purché nei soli termini generali previsti dal Regolamento;.

e) selettività e minimizzazione dei dati: i dati raccolti devono poter tracciare i contatti stretti e non i movimenti o l'ubicazione del soggetto. Devono essere raccolti solo i dati strettamente necessari ai fini della individuazione dei possibili contagi, con tecniche di anonimizzazione e pseudonimizzazione affidabili. Anche la conservazione deve limitarsi al periodo strettamente necessario, da valutarsi sulla base delle decisioni dell'autorità sanitaria su parametri oggettivi come il periodo di incubazione. A tal riguardo le disposizioni dello schema di norma su tali aspetti è opportuno che siano ulteriormente articolate in sede di attuazione dal Ministero della salute ai sensi del comma 2, anche con riferimento alla sorte dei dati raccolti sul dispositivo di chi, in un momento successivo all'installazione dell'applicazione, abbia poi deciso di disinstallarla;

f) non esclusività del processo algoritmico e possibilità di esercitare in ogni momento i diritti di cui agli articoli da 15 a 22 del Regolamento;

g) interoperabilità con altri sistemi di contact tracing utilizzati in Europa. Tali caratteristiche di interoperabilità potranno essere assicurate in sede applicativa e, ancor prima, nell'ambito dei provvedimenti di competenza del Ministero;

h) reciprocità di anonimato tra gli utenti dell'app, i quali devono peraltro non essere identificabili dal titolare del trattamento, dovendo la identificazione ammettersi al limitato fine dell'individuazione dei contagiati. La norma, alla lettera e), non specifica chiaramente se si intenda optare per la conservazione dei dati in forma centralizzata ovvero decentrata. In ogni caso, la centralizzazione richiederebbe in sede attuativa la previsione di misure di sicurezza rafforzate, adeguate alla fattispecie.

RITENUTO

3. In estrema sintesi, dunque, il sistema di contact tracing prefigurato non appare in contrasto con i principi di protezione dei dati personali in quanto:

a) è previsto da una norma di legge sufficientemente dettagliata quanto ad articolazione del trattamento, tipologia di dati raccolti, garanzie accordate agli interessati, temporaneità della misura;

b) si fonda sull'adesione volontaria dell'interessato, escludendo ogni forma di condizionamento della determinazione individuale e, quindi, di disparità di trattamento basate sulla scelta di consentire o meno il tracciamento;

c) è preordinato al perseguimento di fini di interesse pubblico indicati con sufficiente determinatezza ed escludendo il trattamento secondario dei dati così raccolti per fini diversi, salva la possibilità (nei termini generali previsti dal Regolamento) di utilizzo, in forma anonima o aggregata, a fini statistici o di ricerca scientifica;

d) appare conforme ai principi di minimizzazione e ai criteri di privacy by design e by default, nella misura in cui prevede la raccolta dei soli dati di prossimità dei dispositivi, il loro trattamento in forma pseudonima, sempre che non sia possibile in forma del tutto anonima, escludendo il ricorso a dati di geolocalizzazione e limitandone la conservazione al tempo strettamente necessario ai fini del perseguimento dello scopo indicato, con cancellazione automatica alla scadenza del termine;

e) si conforma al principio di trasparenza nei confronti dell'interessato, garantendone la dovuta informazione;

f) ammette l'ulteriore precisazione delle caratteristiche di dettaglio del trattamento e delle misure di sicurezza adeguate da parte del Ministero della salute ai sensi del comma 2 e, per quanto concerne il vaglio di questa Autorità, mediante l'atto di cui all'art. 2-quinquiesdecies del Codice. In tali sedi potranno, inoltre, essere previste le modalità di intervento umano sulla decisione algoritmica, così da soddisfare anche i requisiti di cui all'articolo 22, par. 2, lett. b) - del Regolamento.

L'Autorità auspica che tale misura sia idonea anche a superare il proliferare di iniziative analoghe in ambito pubblico, difficilmente compatibili con il quadro giuridico vigente.

4. Quanto al testo della norma, il Garante non ha particolari perfezionamenti da suggerire, salvo - per le ragioni esplicitate al punto 2 – richiamare l'attenzione sull'opportunità di sostituire, al comma 4, la locuzione "conseguenza in ordine all'esercizio dei diritti fondamentali dei soggetti interessati" con il più ampio "conseguenza pregiudizievole" e di integrare il comma 3 con i riferimenti normativi pertinenti (artt. 5, par. 1, lett. a) e 9, par. 2, lett. j), del Regolamento) e sostituendola parola utilizzati con "trattati".

In conclusione, quindi, il Garante esprime parere favorevole sullo schema di norma in esame, auspicando, ove condivisi, i mirati interventi integrativi e specificativi dell'Amministrazione interessata in sede applicativa, nei termini prospettati ai punti 2 e 3, e riservandosi ogni valutazione dei profili tecnici del progetto in sede di esame ai sensi dell'articolo 2-quinquiesdecies del Codice.

IL GARANTE

ai sensi dell'articolo 57, par. 1, lett. c), del Regolamento, esprime parere favorevole, nei termini di cui in motivazione, sulla proposta normativa concernente il tracciamento dei contatti fra soggetti tramite apposita applicazione sui dispositivi di telefonia mobile, con le osservazioni di cui ai punti 2, 3 e 4.

Roma, 29 aprile 2020

IL PRESIDENTE
Soro

IL RELATORE
Soro

IL SEGRETARIO GENERALE
Busia

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Garante per la protezione dei dati personali - Primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro data-driven per l'emergenza COVID-19

Preg.mo Avv. Valter Campanile
Capo di Gabinetto
Ministro per l'Innovazione Tecnologica e Digitalizzazione

Roma, 7 aprile 2020

OGGETTO: primi riscontri alle ipotesi avanzate all'interno del Gruppo di lavoro data-driven per l'emergenza COVID-19

Premessa

Con la presente si intende in primo luogo porgere un cordiale ringraziamento al Gruppo di lavoro data-driven per l'emergenza COVID-19 e a tutti i soggetti coinvolti nell'iniziativa, rappresentando un profondo apprezzamento per il lavoro e gli approfondimenti svolti, tutti volti a ricercare la soluzione che meglio concilia la scelta di soluzioni tecniche per il contrasto dell'emergenza epidemiologica con tutti i diritti fondamentali coinvolti.

Al fine di coadiuvare il gruppo di lavoro nelle proprie riflessioni, si inviano alcune osservazioni informali, che in tale veste non anticipano né sostituiscono quelle del Garante sulle scelte definitive.

1. Volontarietà dell'utilizzo dell'app e trasparenza del trattamento

Si prende favorevolmente atto che è stata prevista la volontarietà della partecipazione, in primo luogo perché, l'efficacia dello strumento richiede inevitabilmente la collaborazione attiva del singolo, il quale deve essere sensibilizzato sul fatto che l'uso di tale applicazione può contenere il contagio (proprio e altrui). È indispensabile, a tal fine, che il singolo possa confidare nella trasparenza e nella correttezza delle caratteristiche del servizio nonché nell'assenza del perseguimento di scopi ulteriori e incompatibili con tale finalità. L'idea che lo strumento possa essere utilizzato anche per altri scopi potrebbe infatti disincentivare il suo utilizzo, pregiudicando la primaria finalità di salute pubblica che esso dovrebbe perseguire.

Il rispetto del principio di trasparenza e correttezza, inoltre, è una condizione essenziale per l'attivazione di un circuito fiduciario nei confronti delle istituzioni che impiegheranno la soluzione tecnologica prescelta, fornendo agli interessati un'informativa chiara, con modalità che ne garantiscano la massima pubblicità e diffusione, anche mediante i mezzi di comunicazione, e che, fra gli altri elementi, sia in grado di spiegare le particolari finalità del trattamento, le sue possibili implicazioni e modalità, e affronti anche il tema dell'esercizio dei diritti degli interessati.

2. Base giuridica del trattamento

Occorre precisare che la base giuridica del trattamento non può essere individuata nel consenso dell'interessato perché non sussistono i requisiti previsti dal Regolamento UE 2016/679 (cfr. cons. 42, 43 e 46, di seguito, "Regolamento"); ma deve essere ricondotta all'esecuzione di un compito di interesse pubblico, rispetto al quale sarà comunque prevista la volontarietà di adesione da parte dell'interessato, sulla base di disposizioni normative idonee, che costituiscano una misura necessaria e proporzionata in una società democratica (art. 6, parr. 1, lett. e), 3 e 4; art. 9, par. 2, lett. g) e i) del Regolamento).

È pertanto necessario che il relativo utilizzo sia fondato su un'idonea base normativa. Questa, oltre a dover specificare la finalità perseguita e limitare il trattamento al perdurare dello stato di emergenza, precisando che i dati personali dovranno essere in ogni caso cancellati una volta raggiunto lo scopo per il quale sono stati raccolti e non potranno essere utilizzati per finalità diverse e ulteriori, rispetto a quelle stabilite dalla norma e rese note all'interessato dovrà prevedere misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato. Allo stato, tale base normativa non è desumibile da alcuna disposizione vigente e dovrà quindi essere elaborata ex novo o integrando le fonti esistenti, acquisito il parere del Garante, cosi da precisare normativamente almeno la finalità in concreto perseguita, il titolare del trattamento e le conseguenze per gli interessati.

L'individuazione di una chiara ed esplicita base giuridica, oltre che costituire una necessità, potrà determinare un maggiore tasso di accettazione e adesione alla soluzione tecnologica offerta da parte della collettività, in un contesto di ancora maggiore trasparenza e fiducia.

3. Privacy by design

La puntuale individuazione delle finalità per le quali si vorrebbe ricorrere all'utilizzo di una app è essenziale, non solo per rispettare il principio di privacy by design, ma proprio per progettare, nel dettaglio, soluzioni in grado di soddisfare le diverse esigenze correlate all'emergenza e per la valutazione della proporzionalità delle misure che si intendono adottare, tenendo conto dei gravi rischi per le libertà e i diritti degli interessati che potrebbero derivare dal trattamento.

Tali rischi, che dovranno essere accuratamente individuati e valutati nell'ambito di una valutazione di impatto, non riguardano solo quelli relativi alla perdita di riservatezza, ma comprendono anche quelli derivanti dall'utilizzo di informazioni non esatte, che potrebbero determinare alte percentuali di errore, con conseguenze pregiudizievoli sia sui diritti e sulle libertà dei singoli individui (falsi positivi o falsi contatti), sia sulle scelte dei decisori pubblici.

Nel fare ciò, occorre valutare, nel rispetto del principio di precauzione, l'adeguatezza del complesso delle misure di contenimento che si intendono introdurre, sia in relazione ai risultati prefissati, che alle risorse e agli strumenti a disposizione per raggiungerli, sulla base di indicatori qualitativi e ove possibile, quantitativi volti a dimostrarne in modo inequivoco l'efficacia.

Attesi i predetti margini di errore, occorrerà in ogni caso evitare sistemi basati su decisioni interamente automatizzate che si fondano esclusivamente sui dati raccolti attraverso l'applicazione, prevedendo sempre la possibilità di un intervento umano in grado di valutare i risultati e, se del caso, correggerli, affiancando le attuali modalità di ricostruzione della catena epidemiologica che richiedono l'intervento degli operatori sanitari per determinare le misure di sanità pubblica da adottare nei confronti degli interessati.

4. Finalità del trattamento e conseguenze per gli interessati

Da un primo esame dei documenti di sintesi trasmessi non emerge con chiarezza come si configuri il trattamento dei dati che si intende porre in essere nel ricostruire i contatti interpersonali di possibile contagiato, attraverso le applicazioni in esame, con particolare riferimento alle conseguenze per la filiera dei contatti di un soggetto risultato positivo.

In sostanza, non si comprende se, ricostruiti i contatti, si intenda:

- avvisare tali soggetti dell'avvenuta esposizione al rischio di contagio, oppure,
- attivare nei loro confronti iniziative di sanità pubblica.

Nel primo caso si tenderebbe a ricostruire i contatti per allertare la popolazione interessata di una possibile esposizione al rischio contagio, rimettendo agli stessi soggetti avvisati il compito di procedere, in via autonoma e secondo la propria coscienza, a contattare il personale sanitario preposto, secondo le indicazioni nazionali fornite nelle ultime settimane. In tal caso è

assolutamente necessario definire puntualmente il contenuto del messaggio inviato tramite l'applicazione, sia con riferimento ai dettagli dell'esposizione al potenziale contagio; sia in merito ai comportamenti che il soggetto avvisato dovrà tenere dopo aver ricevuto il messaggio (es. chi contattare, adozione di misure di prevenzione ulteriori, ecc.). In tal caso, la finalità perseguita sembrerebbe essere riconducibile a quella preventiva di allerta pubblica per finalità di protezione civile e autoprotezione. Nel secondo caso, una volta riscostruiti i contatti del contagiato, dovrebbe essere previsto l'intervento di un operatore di sanità pubblica che procederebbe a intervistare tali soggetti, al fine di programmare, sulla base di quanto appreso dagli stessi, le misure di sanità pubblica necessarie (tampone, isolamento, ricovero, ulteriori iniziative nei confronti di altri soggetti, ecc.). Come previsto dalle disposizioni vigenti, non sarebbe lasciata all'interessato la decisione di rivolgersi alle strutture sanitarie deputate al controllo dell'epidemia da COVID 19, essendo le stesse strutture di sanità pubblica a interpellare i contatti stretti del contagiato. In tale ipotesi, l'attività dovrebbe essere coordinata dalle strutture sanitarie a ciò deputate (asl, servizi di prevenzione, ISS).

In tale ultima ipotesi, riconducibile a una finalità di tutela della sanità pubblica, l'app costituirebbe pertanto un ausilio per gli operatori sanitari nella ricostruzione della filiera dei contatti, che si affianca alle metodologie, utilizzate fino a oggi, per includere tutti i potenziali soggetti a rischio eventualmente anche non rilevati dall'app.

In questa prospettiva appare necessario aver preventivamente organizzato modalità efficaci e rapide per consentire agli operatori di attivare tempestivamente le misure necessarie nei confronti dei soggetti esposti al rischio.

5. Ruoli e responsabilità dei soggetti coinvolti nel trattamento

Dalla documentazione fornita non emerge quali siano i soggetti coinvolti nel trattamento (titolare, contitolare, responsabile) e i dati personali effettivamente trattati da ciascuno di essi.

Per valutare i profili di protezione dei dati personali, è di fondamentale importanza individuare correttamente la titolarità del trattamento che dovrebbe essere ricondotta, proprio in relazione alle specifiche finalità, a uno o più soggetti pubblici (es.: ISS, ASL, Regioni, ecc.).

Assai rilevante, in considerazione dell'elevato rischio dei trattamenti in questione, si rivelerà l'oculata scelta e individuazione dei partner tecnologici (responsabili del trattamento), indispensabili per una gestione adeguata della complessa infrastruttura IT a cui l'app si dovrà appoggiare, alla quale occorrerà prestare la massima attenzione, tanto più se questi fossero stabiliti al di fuori dell'UE, avendo cura di privilegiare, piuttosto, nel rispetto del principio di precauzione, soggetti situati in territorio italiano, affidabili e dotati di proprie infrastrutture IT, organizzati anche in forma societaria, ma in partecipazione o in controllo pubblico, con esperienza pluriennale nella gestione di piattaforme complesse, che comportano la raccolta di dati, anche relativi alla salute, dalle app installate sui dispositivi degli utenti, e si interfacciano già con un elevato numero di enti e operatori pubblici garantendo un accesso selettivo ai dati (es. Sogei).

È necessario, inoltre, definire con chiarezza, fin dall'inizio, il ruolo e le responsabilità del soggetto fornitore dell'app, precisando se lo stesso si limiti a cedere la tecnologia per i successivi utilizzi ovvero sia chiamato a svolgere taluni trattamenti, che andrebbero in tale caso precisati, che ricadrebbero comunque sotto la responsabilità del titolare.

6. Alcune osservazioni sulle caratteristiche delle app in esame

La documentazione fornita non consente di valutare puntualmente gli aspetti di sicurezza del trattamento, sia in relazione alle app che in relazione ai sistemi di backend, né le specifiche misure di garanzia, comprese la minimizzazione, la pseudonimizzazione e la cifratura dei dati, controllo e tracciamento degli accessi, che invece dovranno essere rigorosamente individuati, una volta chiarite le modalità di utilizzo degli strumenti tecnologici, prevedendo meccanismi automatici di cancellazione dei dati personali – sia sui sistemi di backend e sui sistemi intermedi eventualmente previsti e da chiunque gestiti sia, infine, sul dispositivo mobile dell'utente – alla conclusione dei tempi di conservazione necessari al contenimento del contagio.

A prescindere dalla soluzione che verrà preferita dal Gruppo di lavoro, si ritiene indispensabile che qualsiasi app debba poter essere rimodulata in base alle esigenze in concreto individuate dai decisori pubblici, prevedendo soluzioni flessibili e suscettibili di essere modificate all'occorrenza, consentendo l'integrazione nel trattamento dei principi della protezione dei dati. Ciò anche perché le esigenze di contenimento potrebbero cambiare nel tempo.

In tale prospettiva, sulla base della documentazione fornita, si rileva che entrambe le soluzioni ritenute maggiormente affidabili dal

Gruppo di lavoro si basano sull'uso della tecnologia BT-LE che, nelle modalità in cui se ne prefigura l'utilizzo, appare essere quella più idonea a raggiungere l'obiettivo prefisso, in un'ottica privacy-oriented, poiché consente di individuare la catena dei contagi, rilevando con sufficiente accuratezza la distanza tra soggetti che, avendo con sé uno smartphone o altro tipo di dispositivo su cui è attiva e funzionante la app, entrano nella reciproca sfera di rilevamento con quella tecnologia. Tale tipo di rilevamento non produce nelle modalità in cui è proposto nelle soluzioni prospettate, una raccolta sistematica e centralizzata dei dati personali.

Occorre tuttavia prestare attenzione alla corretta definizione della distanza di rilevamento e del tempo di esposizione (durata del contatto), parametri che determinano la selezione dei contatti a reale rischio di contagio, perché una metrica spazio-temporale troppo ampia potrebbe amplificare il numero dei contatti da tracciare in assenza di un vero rischio e penalizzando l'efficienza del sistema nel suo complesso, mentre delle metriche eccessivamente ristrette potrebbero viceversa sottrarre dei contatti significativi.

Un'altra osservazione riguarda il fatto che le proprietà di maggiore o minore compliance alla disciplina di protezione dei dati personali dovrebbero riferirsi al sistema di tracciamento nel suo complesso e, più in generale, al sistema informativo di back-office a cui i dati raccolti vengono, in certe condizioni, conferiti.

Sarà importante quindi che le caratteristiche tecniche e organizzative del sistema informativo forniscano, unitamente a quelle delle singole componenti applicative, sufficienti garanzie in ordine alla protezione dei dati trattati, compreso il profilo della sicurezza, anche a garanzia della maggiore accettabilità sociale della soluzione prescelta.

Dal punto di vista tecnico, si confida nella possibilità che gli sviluppatori delle soluzioni prescelte possano individuare opportune misure tecniche per sopperire ad alcuni deficit di interoperabilità tra i due principali ambienti operativi (Apple iOS e Android) usati su dispositivi smartphone, che attualmente appaiono condizionare l'efficacia di applicazioni basate sulla tecnologia BT-LE per via di limitazioni presenti in particolare, nell'ambiente iOS a scopi di sicurezza e che, se non superate, rischiano di rendere meno efficace il rilevamento dei contatti, considerata l'attuale ripartizione dell'utenza che vede una forte presenza di dispositivi basati su quell'ambiente operativo (circa il 30%, a fronte del 70% di utenza Android in Italia sul totale degli smartphone).

Rispetto a quanto indicato nella relazione sui profili giuridici, occorre precisare che, in ogni caso, i dati raccolti e successivamente trattati dalle app in esame non possono essere considerati anonimi. Infatti, a determinate condizioni, potrebbe essere possibile/necessario che l'autorità pubblica competente identifichi nuovamente l'interessato.

Pertanto è corretto ricondurre i dati trattati alle seguenti categorie:

a) dati personali, in quanto sono considerati tali anche gli "identificativi online prodotti dai dispositivi, quali gli indirizzi IP, marcatori temporali (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza" (cfr. cons. 30 e art. 4, par. 1, punto 1), del Regolamento);

b) dati personali sottoposti a pseudonimizzazione, ossia data personali che "potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni" (cfr. cons. 26 e 29, e art. 4, par. 1, punto 5), del Regolamento), ad esempio nel caso di utilizzo di identificativi dinamici dei dispositivi.

L'Ufficio del Garante è in ogni caso a disposizione per collaborare e fornire soluzioni tecnico-giuridiche su ogni dubbio e/o criticità emerse o che dovessero emergere in materia di protezione dei dati personali da qualunque soluzione adottata.

Avv. Giuseppe Busia
Segretario generale del Garante per la protezione dei dati personali

Articoli

Contact tracing, perché è così importante contro il covid (anche in Italia)

Perché anche l'Italia ha deciso di puntare sul contact tracing per contenere la diffusione del covid-19 nella fase 2 e come funzionano le tecnologie – come il bluetooth – che consentiranno di garantire trasparenza e tutela della riservatezza

21 Apr 2020
Giuseppe Attardi professore di Informatica all'Università di Pisa
Nicola Marino Co-fondatore INTECH e consulente in materia di sanità digitale
Enrico Santus Senior Data Scientist a Bayer, esperto di AI nella Salute

Si ripete da tempo che la più efficace soluzione per contrastare la diffusione del **coronavirus** sia il vaccino, ma, come è noto, lo sviluppo di un vaccino richiede tempi troppo lunghi per poter attendere in una condizione di lock down generalizzato.

Altri strumenti devono quindi essere adottati. Tra essi, oltre a sistemi già adottati nel nostro Paese – quali l'isolamento dei focolai e il distanziamento sociale tra le persone – si fa strada anche il contact tracing. Grazie all'utilizzo di app ad hoc – in Italia il Governo ha scelto **Immuni di Bending Spoon** – è infatti possibile infatti gestire l'epidemia (non reprimerla), riducendo lo stress delle istituzioni sanitarie.

Proviamo quindi ad approfondire, di seguito, i principi del **contact tracing**, con il supporto di alcuni studi che ne dimostrano l'efficacia.

Indice degli argomenti

- Come funzionano le app di contact tracing
- Efficacia dell'app
- La soluzione di Apple e Google
- Perché la tecnologia bluetooth
- Immuni, la soluzione italiana

Come funzionano le app di contact tracing

Tutte le **app** finora sviluppate per il contact tracing si avvalgono di un **algoritmo semplice** che sfrutta funzionalità diffuse su tutti gli smartphone, quali il Bluetooth (BT) e il Global Positioning System (GPS). Queste app si poggiano su un server centrale, in cui l'autorità sanitaria salva – previo consenso degli interessati e dopo anonimizzazione dei dati – i contatti registrati dagli smartphone dei soggetti positivi al coronavirus. Questo server centrale comunica poi con i dispositivi di tutti gli altri utenti (o in locale o inoltrando i dati anonimizzati e aggregati agli smartphone) per permettere loro di verificare di non aver avuto contatti con soggetti positivi. Qualora dei contatti vi fossero stati, gli utenti

sarebbero informati che il contatto è avvenuto senza rivelare né dove è avvenuto né chi sia il soggetto positivo.

Per comprendere quanto sia importante conoscere se una persona sia stata a contatto con un soggetto positivo al Covid-19, potremmo dividere i soggetti contagiati in tre categorie:

- chi ha già sviluppato i sintomi,
- coloro che li hanno sviluppati in modo lieve (paucisintomatici) e
- i cosiddetti "asintomatici", ovvero quel gruppo di persone che non riporta alcuna sintomatologia sebbene sia positivo.

Gran parte dei contagi non monitorati avvengono nel periodo in cui chi è positivo non ne è ancora consapevole e pertanto non prende precauzioni di sorta (quali la quarantena). Questo è stato confermato da un recentissimo studio condotto da Ferretti et al., e pubblicato su Science.

Gli studiosi hanno mostrato che l'alta incidenza della **trasmissione pre-sintomatica** (quella in cui i sintomi non sono ancora evidenti) può rendere inefficaci gli interventi di isolamento nel controllo dell'epidemia, sostenendo che le tradizionali **procedure di localizzazione manuale** dei contatti non siano sufficientemente veloci per contrastare la diffusione del SARS-CoV-2. A rafforzare tale tesi lo studio pubblicato sulla rivista Nature, il quale, analizzata la patogenesi virale ed osservato il picco di carica virale nei tamponi oro-faringei al momento dell'insorgenza dei sintomi, ha stimato che il 44% dei casi secondari di infezione avviene durante lo stadio presintomatico dei casi primari.

Da qui, si conclude che **un'app di tracciamento ricoprirebbe un ruolo decisivo qualora fosse affiancata all'isolamento sociale** (le metodiche adottate singolarmente non garantirebbero lo stesso effetto preventivo). Tale app dovrebbe fornire agli utenti la possibilità di ricevere **una notifica istantanea qualora ad un soggetto con il quale sono entrati in contatto fosse stata fatta una diagnosi di infezione da Covid-19 entro i 2-3 giorni precedenti** (garantendo la massima privacy) ed inducendo tali utenti all'autoisolamento.

Efficacia dell'app

L'efficacia della app è proporzionale alla sua diffusione e alla rapidità con cui essa informa i partecipanti di contatti sensibili (potenziali contagiati). In questo modo si possono precocemente indurre all'isolamento nuovi potenziali infetti, riducendo la diffusione della patologia durante uno stadio di assenza di sintomi. Inoltre, la app risolve il problema legato all'incertezza del ricordo (ovvero la difficoltà di ricordare tutti gli spostamenti degli ultimi 14 giorni) o alla non conoscenza diretta dei contatti (difficilmente un soggetto conosce tutti coloro che ha incontrato, ad esempio i passeggeri di un bus). Infine, considerando che la app può consentire di somministrare questionari di analisi dello stato di salute con cadenza giornaliera, si ridurrebbe drasticamente lo sforzo dell'autorità sanitaria nel reperire tali informazioni.

I benefici legati all'uso di una app, tra l'altro, non sono solo sanitari, **ma anche economici (micro e macro), psicologici e sociali**. La consapevolezza di essere soggetti a rischio, senza temere che tale informazione raggiunga altre persone, permette infatti agli individui di agire responsabilmente nei confronti delle persone vicine, responsabilizzando di conseguenza l'intera comunità.

La soluzione di Apple e Google

Il 10 Aprile 2020 Apple e Google hanno annunciato di aver avviato una collaborazione al fine di trovare una soluzione alla diffusione del Coronavirus. Le due multinazionali hanno dichiarato che, già a maggio, rilasceranno una API (Application Programming Interface) che permetterà – agli sviluppatori di app supportati da autorità riconosciute – di sfruttare la tecnologia Bluetooth per tracciare i contatti usando un'unica interfaccia per entrambe le piattaforme, iOS e Android. Al centro di questa decisione, Apple e Google hanno posto l'attenzione su privacy, trasparenza e consenso. E difatti dovranno essere gli utenti stessi a decidere se attivare o meno tale sistema, che sarà comunque reso disponibile di default su tutti i dispositivi.

La scelta di sfruttare il Bluetooth da parte dei due colossi americani deriva dal fatto che questa tecnologia – diversamente dal GPS – non permette di identificare la posizione dei soggetti, ma solo la prossimità tra dispositivi. Il Bluetooth, infatti, sfrutta onde radio a corto raggio, permettendo la comunicazione tra dispositivi a distanza di pochi metri.

Perché la tecnologia bluetooth

Immaginiamo che due persone si incontrino in un parco e scambino una rapida conversazione. Se le loro app di tracciamento sono attivate, i loro dispositivi inizieranno a scambiarsi dei codici a vicenda. Tali codici non identificano il dispositivo stesso, ma sono numeri generati in maniera casuale (con seme fisso – per la riproduzione) ogni 15 minuti. Quando gli individui si allontaneranno, i loro dispositivi conterranno dei codici anonimi che non sono associabili ad alcun soggetto fisico.

Se dopo qualche giorno uno dei due individui coinvolti nel contatto viene trovato positivo al coronavirus, il personale sanitario può procedere con un lungo questionario/una lunga intervista, oppure può chiedere di condividere i numeri casuali che il dispositivo del soggetto ha memorizzato negli ultimi giorni. Se si procede con la condivisione, questi numeri vengono caricati – in forma anonima – in un server centrale, al quale le app di tutti gli altri utenti possono accedere per verificare che non abbiano esattamente lo stesso codice. Se l'app di un utente trova un codice nel database della sanità, **l'utente riceverà un avviso, che lo informerà di essere stato a contatto con un soggetto infetto per un certo periodo di tempo**, e che dovrà pertanto prendere delle precauzioni. È garantito sia l'anonimato dell'infetto che dell'altro partecipante al contatto, poiché i numeri seriali non sono in alcun modo riconducibili agli identificativi dei due, e perché i luoghi di contatto non sono mai salvati. Né il personale sanitario né Apple o Google potranno mai identificare l'utente.

Immuni, la soluzione italiana

In Italia, giovedì scorso, il commissario straordinario all'Emergenza CoVid-19, Domenico Arcuri, ha scelto di adottare la soluzione *Immuni* di Bending Spoons, una delle 319 proposte arrivate durante la fast call del Ministero per l'Innovazione Tecnologica e la Digitalizzazione.

La app della software house milanese potrà essere adottata su base volontaria e sarà sperimentata prima in alcune Regioni, prima della diffusione nazionale. La app non solo rileva i contatti come abbiamo già descritto sopra, ma permette di memorizzare anche un diario che analizza la storia clinica del paziente, nonché informazioni sui farmaci assunti dallo stesso. **Dettagli che potrebbero rivelarsi fondamentali qualora venisse diagnosticato il CoViD-19.** Limite di Immuni è il fatto che non sia open source, un vero peccato se si considera che analoghe app sviluppate in tutto il mondo lo sono – si pensi a Safe Paths del MIT o TraceTogether di Singapore.

NOMOS
Le attualità nel diritto

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale

SOCIAL NETWORK, SOCIETÀ TECNOLOGICHE E DEMOCRAZIA[1*]

di Francisco Balaguer Callejón[**]

SOMMARIO: Introduzione. 1.- Il contesto della globalizzazione. 1.1- Accelerazione del tempo e estensione dello spazio pubblico. 1.2.- Attori globali e Stato. 2.- Trasformazione dei modelli culturali e cambio di paradigma. 3.- Costituzione, democrazia e social network. 3.1- Costituzione e social network. 3.2- Processi democratici e social network. 4.- Le società tecnologiche e le reti. Aspetti problematici. 4.1- Incidenza sui diritti fondamentali. 4.2- Tendenza al monopolio e impatto sulla concorrenza. 4.3- La pressione sui mezzi di comunicazione tradizionali. 5.- I processi comunicativi e di costruzione dello spazio pubblico. 5.1- Il precedente substrato, globalizzazione e crisi economica. 5.2- La frammentazione e radicalizzazione dello spazio pubblico. 6.- I processi elettorali. 6.1- Notizie false e disinformazione. 6.2- Interventi di attori esterni e di gruppi organizzati. 6.3- Profili individuali e propaganda subliminale. 7.- Possibile aree di azione. 7.1- Diritti fondamentali. 7.2- Concorrenza, pubblicità e mezzi di comunicazione. 7.3- Processi elettorali. 7.4- Misure fiscali. 7.5- Sanzioni. Conclusioni/Sintesi. Parole chiave. Abstract. Keywords.

Introduzione

I *social network* hanno suscitato grandi aspettative in relazione alla promozione dei processi democratici di fronte ai regimi dittatoriali e alle possibilità di migliorare la qualità democratica dei sistemi costituzionali. Tuttavia, il modo in cui vengono gestiti dalle grandi società tecnologiche ha messo in discussione il loro funzionamento dal punto di vista della loro compatibilità con i diritti costituzionali, la loro incidenza negativa nei processi democratici, specialmente nei processi elettorali e il rispetto delle regole della concorrenza da parte di queste società, tra gli altri ambiti. Nel titolo di questo contributo si fa riferimento alle società tecnologiche come un fattore che deve essere attualmente inserito nella relazione tra *social network* e la democrazia per comprendere la natura dei problemi che

[1] Traduzione dal castigliano di Tommaso Nicola Poli.

[*] Relazione presentata al Convegno "70 anni di Costituzione", Università di Salerno, in corso di pubblicazione. Contributo sottoposto a *double blind peer review*.

[**] Catedrático de Derecho Constitucional de la Universidad de Granada e Catedrático Jean Monnet *ad personam* de Derecho Constitucional Europeo y Globalización

ISSN 2279-7238

affrontiamo. L'inerzia dello sviluppo tecnologico, che è nel secolo XXI uno strumento di legittimazione molto potente, conduce a volte a riflettere, in maniera incosciente, che i *social network* sono poco meno di un fenomeno naturale, non collegato al mercato e non correlato con l'interesse, molte volte spurio, delle società tecnologiche che le gesticono. Queste società stanno costruendo un nuovo mondo e lo fanno in funzione delle loro prospettive di vantaggi economici, senza apparire preoccupate della lesione di diritti che questo orientamento verso la redditività economica sta generando e l'impatto negativo che la loro attività sta avendo sui processi democratici e sui sistemi costituzionali.

Di fronte a queste società tecnologiche, i governi degli Stati e specialmente l'Amministrazione nordamericana, che è la principale responsabile del loro controllo, stanno reagendo in maniera molto lenta, quando lo fanno, senza intervento alcuno in relazione ai problemi costituzionali che stanno generando o attraverso interventi minimi che non servono per correggere i problemi. In maniera apparentemente paradossale, è l'Unione europea insieme con alcuni Stati europei, ad affrontare i maggiori eccessi di queste società. Un paradosso apparente se teniamo conto che la permissività dei regolatori nordamericani può avere come contropartita un interesse strategico nell'accumulazione dei dati a livello mondiale da parte di questi regolatori e la loro utilizzazione da parte delle agenzie di sicurezza nordamericane. Qualcosa che è già stato in grado di contrastare con riferimento all'ambiente di Cambridge Analytica che, nel momento in cui interveniva in maniera fraudolenta nei processi elettorali nel Regno Unito, manteneva anche relazioni in ambiti come la difesa o i servizi di intelligence e di sicurezza[2].

Per comprendere la portata dei problemi possiamo effettuare una comparazione con la forma nella quale si sviluppavano (e continuano a svilupparsi in parte) i processi di comunicazione, tanto privati quanto pubblici, prima dell'apparizione dei *social network* e delle grandi piattaforme di internet. Le comunicazioni private erano e continuavano ad essere sottoposte ad una protezione costituzionale: la corrispondenza o le conversazioni telefoniche non possono essere intercettate se non con un'autorizzazione giudiziale. I mezzi di comunicazione sono plurali e devono dare un'informazione obiettiva, differenziata delle opinioni diverse che si diffondono attraverso gli stessi. La pubblicità è sottoposta ad alcune regole e deve essere offerta in maniera differenziata nei media senza che sia ammissibile la pubblicità subliminale.

Tenendo in conto le precedenti condizioni, immaginiamo ora che qualcuno abbia la possibilità di conoscere la nostra corrispondenza, che possa sentire tutto quello che diciamo in qualsiasi momento e sapere anche quello che stiamo leggendo sul periodico ogni giorno, il tempo che dedichiamo a ciascuna notizia così come il tipo di notizie o di articoli che ci interessano o non ci piacciono e la reazione che ci provoca la loro lettura. Immaginiamo anche che, con tutti questi dati, qualcuno ha la capacità di elaborarli, di definire per il tramite di algoritmi quali sono i nostri gusti e di offrirci quelle cose che ci piacerebbe propriamente comprare, attraverso una pubblicità personalizzata. Facciamo un ulteriore passo in avanti e

[2] Cfr. House of Commons, Digital, Culture, Media and Sport Committee, DCMS. *Disinformation and 'fake news': Final Report*. Published on 18 February 2019 by authority of the House of Commons, p. 78:

ISSN 2279-7238

pensiamo che questi dati sono utilizzati per conoscere non solo le nostre preferenze ma anche le nostre fobie e le nostre paure e che con questi è elaborato un profilo psicologico individualizzato che rende possibile l'invio di propaganda politica subliminale orientata a cambiare il significato del nostro voto alle elezioni o disincentivare la nostra partecipazione al processo elettorale.

Quindi, questo è successo esattamente in alcune delle ultime tornate elettorali che sono state celebrate nel mondo, cominciando dal referendum sulla Brexit e continuando con le elezioni presidenziali negli Stati Uniti. Nel loro aspetto più serio, quello che hanno fatto alcune piattaforme che gestiscono *social network* non è provare a convincere apertamente i votanti a cambiare i loro voti, ma utilizzare profili psicologici precedentemente creati attraverso algoritmi per generare una reazione contro un particolare candidato. Ad esempio, se da tutti i dati che sono elaborati è determinata una fobia particolare per i cani, a quella persona sono inviate foto di un candidato o di una candidata che accarezzano cani, per creare istintivamente e in modo inconsciente una sensazione di rifiuto. Se questa propaganda subliminale si combina con altre operazioni similari, attraverso *fake news* e messaggi scoraggianti nei confronti di quella candidatura, forse un cambio di voto non può essere raggiunto ma è possibile che si ottenga come risultato l'astensione della persona alla quale tutti questi messaggi sono diretti. Quando questo è fatto in maniera massiccia e personalizzata su mille o milioni di persone, la destabilizzazione del processo elettorale è più probabile. Nel caso delle elezioni presidenziali nordamericane è comprovato che è stato fatto in Stati decisivi su gruppi molto ampi di elettori e che hanno potuto cambiare il senso dell'elezione in questi Stati.

Naturalmente, se facciamo comparazioni storiche possiamo affermare sempre che nei sistemi dittatoriali del XX secolo, per esempio, sono stati utilizzati mezzi tecnologici per diffondere propaganda di massa, manipolare l'opinione pubblica, imporre false narrazioni e fare credere alla gente notizie false. Molti di questi fenomeni, con diverse varianti derivate dall'epoca concreta nella quale sono stati prodotti, sono tanto antichi come la storia dell'Umanità. Ciò che risulta nuovo, nell'attività che stanno realizzando alcune società che gestiscono *social network*, è che non si tratta di propaganda massiccia inviata con carattere generale ad un pubblico più o meno ampio o con carattere settoriale ad un insieme di persone concrete delle quali si conoscono le loro preferenze politiche o eventualmente i dati che sono pubblici. Al contrario, ora ci troviamo davanti a propaganda politica individualizzata inviata ad ogni persona in ragione dei profili psicologici che sono stati elaborati con algoritmi mediante l'elaborazione di dati privati, che non dovranno né essere conosciuti né utilizzati da queste piattaforme. Se a questo aggiungiamo che questa propaganda può arrivare ad essere subliminale e cambiare la nostra intenzione di voto senza che possiamo renderci conto della manipolazione che stiamo subendo, avremmo avuto già un'idea della gravità di quello che può succedere ed è successo in alcune delle ultime tornate elettorali che sono state celebrate in diversi paesi.

Per comprendere la natura e la portata delle sfide alle quali è di fronte attualmente il sistema democratico, sarebbe conveniente realizzare alcune precisazioni:

ISSN 2279-7238

1.- Una parte dei problemi non sono collegati necessariamente con i *social network* come tali ma con l'attività delle società tecnologiche che gestiscono le reti e il modello di business sul quale le stesse sono basate. Trattandosi di un modello di business che è orientato a conseguire entrate pubblicitarie, è fondamentale per queste attirare l'attenzione del pubblico con la finalità di ottenere maggiori vantaggi[3]. La instabilità politica, la radicalizzazione dello spazio pubblico e la conflittualità permanente generano entrate molto superiori a quelle che offre un clima di stabilità e di consenso.

2.- Altri problemi riguardano l'attività degli attori globali e nazionali differenti dalle società tecnologiche, che utilizzano le reti con propositi simili di promozione di instabilità, in funzione di altri interessi che non sono necessariamente economici ma politici e geostrategici. La questione che è affrontata è che questa attività favorisce gli interessi economici delle società che gestiscono reti. Per questo motivo i controlli che queste realizzano, quando lo fanno, sono meno efficaci di quelli che applicano in funzione di altre limitazioni che considerano più necessarie per la loro immagine pubblica, secondo l'ideologia che stimano più generalizzata tra i loro utenti, per esempio.

3.- C'è un terzo tipo di problemi che possono essere collegati al tipo di supporto comunicativo e allo sviluppo tecnologico, che potrebbero essere considerati strutturali, almeno nell'attuale stato di sviluppo delle piattaforme. La capacità di intervento pubblico su questi è più ridotta. Tuttavia, è fondamentale stabilire i limiti reali perché queste società tendono ad utilizzare la tecnologia come un ostacolo permanente di fronte a qualsiasi controllo, affermando abitualmente che ci sono limitazioni tecniche che impediscono che questi controlli siano realizzati.

D'altra parte, è importante analizzare anche l'impatto dei *social network* in un contesto più ampio che quello dei processi elettorali (sebbene siano stati questi processi quelli che hanno sollevato, a ragione, l'attenzione del pubblico) poiché stanno generando nuovi paradigmi, non solamente comunicativi ma anche politici, e una trasformazione dei modelli culturali in molti ambiti. La percezione del tempo e dello spazio sta cambiando in maniera radicale nel secolo XXI, condizionando in maniera molto rilevante i processi politici e costituzionali. Alcuni di questi cambiamenti non sono sicuramente reversibili. La società di oggi è sottoposta a stimoli che sono percepiti ogni volta in modo più urgente e volatile allo stesso tempo. Rimane poco dell'idea di programmazione per il futuro propria delle nostre costituzioni e dei nostri processi costituenti[4]. I problemi sono attuali (forse anche della mattina di oggi, nemmeno del pomeriggio) e la percezione generalizzata è che devono essere risolti immediatamente. Allo stesso modo, la frammentazione e la radicalizzazione dello spazio pubblico ostacola la possibilità di articolare consensi costituzionali e democratici. La

[3] Come indicavano, Deb, Anamitra/Donohue, Stacy/Glaisyer, Tom, 2017. "Is Social Media a Threat to Democracy?", 1° ottobre 2017, https://www.omidyargroup.com/wp-content/uploads/2017/10/Social-Media-and-Democracy-October-5-2017.pdf

[4] Francisco Balaguer Callejón, "Las dos grandes crisis del constitucionalismo frente a la globalización en el siglo XXI" in Nomos. Le attualità nel diritto, 2018. Anticipazioni Convegno: Passato, presente e futuro del costituzionalismo e dell'Europa: http://www.nomos-leattualitaneldiritto.it/wp-content/uploads/2018/09/Balaguer_Costituzionalismo.pdf. Vi è una versione italiana: "Le due grandi crisi del costituzionalismo di fronte alla globalizzazione nel XXI secolo", attualmente in corso di stampa.

ISSN 2279-7238

falsificazione delle notizie forma parte di questo scenario. Uno scenario nel quale i mezzi di comunicazione tradizionali vengono ogni volta più indeboliti per la tendenza delle grandi piattaforme di internet a monopolizzare il mercato pubblicitario[5].

Delimitare in quale misura l'attivazione di meccanismi costituzionali e democratici di controllo può contribuire a ripristinare le tendenze più disfunzionali che le società tecnologiche di internet e di reti stanno creando è fondamentale per fare fronte a questi processi. Non si può affermare, in assoluto, che i *social network* e le piattaforme sono neutrali e che si limitano a rispecchiare tendenze sociali. Quanto meno, risulta abbastanza chiaro che stanno potenziando esattamente le tendenze più problematiche per i diritti costituzionali, la stabilità del sistema democratico e la limpidezza dei processi elettorali. Lo stanno facendo, inoltre, attraverso attività che colpiscono direttamente i diritti fondamentali e per creare maggiori entrate attraverso un modello di business al quale risulta specialmente favorevole l'instabilità politica. Sono molti gli ambiti nei quali possono essere adottate misure di controllo a livello statale e europeo per impedire che il sistema democratico continui ad essere deteriorato. Dall'intervento sul proprio modello di affari di queste piattaforme fino alla regolazione del mercato pubblicitario, per impedire che terminino monopolizzando a detrimento delle misure di comunicazione tradizionali. Nell'ambito specifico dei processi elettorali queste misure dovrebbero avere una maggiore portata, attivando tutte le misure che siano necessarie per impedire la manipolazione elettorale e garantire che le elezioni siano limpide e pienamente democratiche.

1.- Il contesto della globalizzazione.

1.1- Accelerazione del tempo e estensione dello spazio pubblico.

Ci sono due fenomeni che convergono nella tematica che stiamo affrontando e che sono, da un lato, l'accelerazione del tempo storico e, dall'altro, l'estensione dello spazio pubblico. Quello che sta succedendo nel secolo XXI, nel contesto della globalizzazione, è che stanno cambiando tutti i termini del gioco politico e costituzionale, come conseguenza dello sviluppo tecnologico[6]. Sono nati nuovi paradigmi, specialmente nei processi comunicativi, che esprimono una trasformazione di modelli culturali di grande portata. La globalizzazione non solo ha accelerato lo sviluppo tecnologico (fino al punto che è calcolato che solo i primi dieci anni del secolo XXI equivalgono in progressi scientifici e tecnologici a tutto il secolo XX) ma ha anche cambiato la relazione tra gli esseri umani con la dimensione di spazio e tempo precedentemente conosciuta. La progressiva estensione degli spazi a livello globale ha prodotto una correlativa accelerazione del tempo. Stiamo parlando, pertanto, dei parametri essenziali nei quali sono stati sviluppati movimenti, attività e istituzioni sociali che ora si trovano di fronte ad un contesto molto diverso da quello che li ha generati.

[5] Cfr. Pitruzzella, Giuseppe, "La libertà di informazione nell'era di Internet", in G. Pitruzzella, O. Pollicino, S. Quintarelli. *Parole e potere: Libertà d'espressione, hate speech e fake news*. Italian Edition. Egea, 2017.

[6] Con le parole di D. Rousseau, "Au-delà même de la question du numérique, ce qui se joue en ce début de siècle, c'est la fin d'un monde fabriqué au xixe siècle et relookée au xxe."Dominique Rousseau, "Le numérique, nouvel objet du droit constitutionnel", *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, p. 9.

ISSN 2279-7238

Questo è quello che succede con il costituzionalismo. La sua relazione genetica con lo spazio e il tempo è molto differente da quella che è stata creata nel contesto della globalizzazione. Con riferimento allo spazio, il costituzionalismo moderno è stato collegato storicamente allo Stato. Sorge storicamente come un movimento che tenta di limitare e controllare il potere dello Stato ed è stato adattato ai cambiamenti sociali e politici sempre all'interno di questo livello dello Stato nazionale. La proiezione del costituzionalismo a livello sovranazionale sta generando trasformazioni importanti tanto per quanto riguarda il concetto di Costituzione quanto per quanto riguarda gli stessi Stati nazionali e i loro sistemi costituzionali interni[7]. Tuttavia, oltre queste trasformazioni che potrebbero dare luogo nel futuro ad una rivitalizzazione del costituzionalismo nella sfera sovranazionale, è certo che molte delle funzioni che la Costituzione potrebbe compiere all'interno dello Stato risultano oggi in grande misura inefficaci di fronte ai grandi attori globali[8]. In particolare, quest'inefficacia risulta evidente di fronte a speculatori finanziari e alle società tecnologiche di comunicazione di Internet, che agiscono a livello globale e che non incontrano alcun freno nelle politiche o nelle legislazioni statali.

Con riferimento al tempo, il nuovo ritmo che sta segnando lo sviluppo tecnologico ha creato una percezione del tempo che risulta incompatibile con alcune delle funzioni storiche del costituzionalismo. Pensiamo, ad esempio, ai processi costituenti, con la loro vocazione di stabilire norme fondamentali stabili con capacità di integrazione politica e sociale. L'immediatezza nella risposta ai problemi politici e sociali, che è una caratteristica specifica dello spazio pubblico che è stata generata attraverso i *social network*, rende difficile pensare nei termini nei quali si sono sviluppati tradizionalmente i processi costituenti o di riforma costituzionale. Ogni volta è più difficile programmare nel tempo in termini di stabilità, che era una delle funzioni specifiche delle costituzioni. Il tempo delle costituzioni, tale e come lo abbiamo conosciuto fino ad ora, non è coerente con le caratteristiche dello spazio pubblico che si è configurato da pochi anni attraverso i *social network*[9].

1.2.- Attori globali e Stato.

[7] Cfr. Francisco Balaguer Callejón, *El Tratado de Lisboa en el Diván. Una reflexión sobre constitucionalidad, estatalidad y Unión Europea*, in *Revista Española de Derecho Constitucional*, núm. 83, mayo-agosto de 2008 e Francisco Balaguer Callejón "Constitución y Estado en el contexto de la integración supranacional y de la globalización", in Miguel Carbonell, Héctor Fix-Fierro, Luis Raúl González Pérez y Diego Valadés (Coordinadores), *Estado constitucional, Derechos humanos, Justicia y vida universitaria. Estudios en homenaje a Jorge Carpizo*, UNAM, México, 2015, Tomo IV, Volumen 1, páginas 197-211.

[8] Con le parole di D. Rousseau, "La nouvelle civilisation du numérique signe, en effet, la fin de l'État souverain national, la fin du contrôle de l'État sur l'économie et la société", D. Rousseau, "Le numérique, nouvel objet du droit constitutionnel", *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, p. 9.

[9] Inoltre i *social network* offrono anche possibilità di partecipare nei processi costituenti e in quelli legislativi. Cfr. sui primi, Eric Sales, "La transformation de l'écriture de la Constitution, l'exemple islandais", *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, pp. 45-57 e sui secondi, Ariane Vidal-Naquet, "La transformation de l'écriture de la loi: l'exemple de la loi sur la République numérique" *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, pp. 59-68.

ISSN 2279-7238

Nel contesto della globalizzazione, lo Stato è sempre più incapace di controllare i grandi attori globali. Questa incapacità la vediamo ora con le società tecnologiche ma l'abbiamo vista prima negli anni della crisi economica con le politiche economiche che potevano risultare contrarie ai principi o ai diritti costituzionali. Egualmente in questo caso una nuova legittimità è stata sollevata di fronte a una Costituzione sempre più marginalizzata nello spazio pubblico, perché non serviva come strumento di controllo del potere né permetteva di garantire i diritti incorporati nel documento costituzionale. Anche sul piano economico ci sono elementi strutturali derivati dal processo di globalizzazione che creano una tensione costante con l'ordine costituzionale la cui soluzione non è facile. Tuttavia, anche qui c'erano possibilità di affrontare politiche economiche egualmente efficaci e più coerenti con la cornice costituzionale (che non erano basate quasi esclusivamente nella riduzione progressiva dei costi sociali, come quelle che sono state imposte durante la crisi in alcuni paesi europei) che non furono possibili per l'imposizione di una narrativa basata sulla legittimità economica, che terminò spostando la Costituzione fuori dallo spazio pubblico del dibattito e della decisione.

Lo stesso si può dire in relazione alla democrazia pluralista. La narrativa economica che è prevalsa durante la crisi ha totalmente stravolto la democrazia pluralista, forzando l'esecuzione di certe politiche pubbliche, indipendentemente dall'esito delle elezioni. Fino a tale punto che, quando i governanti nazionali non rispettarono queste politiche, furono sostituiti da altri attraverso una pressione economica che obbligò i parlamenti nazionali a cambiare governi in alcuni Stati. Si può parlare, da questa prospettiva, di una esternalizzazione del potere politico statale durante il periodo della crisi, che permise agli speculatori finanziari globali, in ultima istanza, di determinare le politiche statali[10].

Quando la crisi economica ha cominciato ad essere superata, abbiamo potuto vedere, a partire dalla Brexit e dalle elezioni nordamericane (alle quali hanno seguito altre tornate elettorali egualmente influenzate) qualcosa ancora più grave: l'internazionalizzazione del potere politico delle grandi società tecnologiche che gestiscono *social network*, che sono intervenute nelle elezioni, con tecniche assolutamente incompatibili con le regole democratiche, per favorire determinati candidati. A queste società si aggiungono attori molto potenti, interni ed esterni, che agiscono nei *social network* fomentando la radicalizzazione e la frammentazione progressiva dello spazio pubblico e l'orientamento delle tendenze politiche e del voto verso gli estremi dello spettro politico.

In realtà, entrambi i fenomeni, l'esternalizzazione del potere statale e l'internazionalizzazione del potere dei grandi attori globali sono autoalimentati. Da un lato, la crisi economica ha favorito la creazione di un substrato sociale sempre più radicalizzato di fronte alla globalizzazione e più frustrato davanti all'incapacità dello Stato e, pertanto, del sistema rappresentativo e democratico interno, per risolvere i problemi sociali. D'altro lato, le grandi piattaforme che gestiscono *social network* hanno promosso questa

[10] Cfr. Francisco Balaguer Callejón, "Las dos grandes crisis del constitucionalismo frente a la globalización en el siglo XXI" precedentemente citato.

ISSN 2279-7238

radicalizzazione[11] utilizzando tutti gli strumenti alla loro portata non per un orientamento ideologico proprio di queste piattaforme, ma per incrementare i loro utili con l'attuale modello di business nel quale esercitano la loro attività. Come già abbiamo indicato, per questo modello di business è vitale richiamare l'attenzione del pubblico e fomentare la polemica e l'instabilità, quello che determina un aumento delle entrate pubblicitarie[12].

2.- Trasformazione dei modelli culturali e cambio di paradigma.

Alcune delle tendenze prodotte dallo sviluppo tecnologico non provocano il cambiamento in modo prevedibile in un senso più coerente con i requisiti del costituzionalismo perché esprimono una trasformazione di modelli culturali che attualmente sembra inarrestabile. In queste la tensione tra costituzionalismo e sviluppo tecnologico è strutturale e ha una difficile soluzione. In relazione ad altre tendenze, tuttavia, è possibile e desiderabile una regolazione che, partendo dai principi e valori costituzionali, garantisce i diritti fondamentali e la limpidezza dei processi elettorali, minacciati entrambi attualmente dalle società tecnologiche. Tuttavia, è qui che la nuova legittimazione tecnologica si oppone radicalmente al costituzionalismo, perché fa appello in maniera permanente a ragioni tecniche per impedire qualsiasi regolamentazione delle attività di queste piattaforme. Nella narrativa che queste società stanno riuscendo ad imporre, la Costituzione e i diritti sono un ostacolo per il progresso che queste offrono.

In ogni caso, è percepibile un cambio di modelli culturali con lo sviluppo di Internet e i *social network* che ha una dimensione storica. La dipendenza crescente della tecnologia, le trasformazioni dei modelli comunicativi interpersonali e sociali, la frammentazione dello spazio pubblico, l'effetto bolla, la radicalizzazione dei dibattiti, la difficoltà di stabilire consensi, sono tra gli ambiti nei queli questi cambiamenti sono percepiti. Sul piano comunicativo e politico possiamo vedere un progressivo orientamento del parlamento verso atteggiamenti e pratiche che tendono a convertirlo in uno scenario che dopo si proietta sui *social network*. Egualmente succede con i partiti politici e la loro crescente dipendenza dalle agende che dettano i *social network* per le tematiche da discutere e per le strategie da seguire. I limiti di questa evoluzione non sono chiaramente definiti e la possibilità di ripristinare alcune di queste tendenze nemmeno è percepibile attualmente.

3.- Costituzione, democrazia e social network.

3.1- Costituzione e social network.

Sul piano specificatamente costituzionale possiamo apprezzare una trasformazione delle condizioni strutturali di sviluppo del costituzionalismo e della medesima nozione di

[11] Come afferma Idris Fassassi "Les réseaux ne font qu'accentuer les tendances lourdes de l'environnement dans lequel ils opèrent", I. Fassassi, "Les effets des réseaux sociaux dans les campagnes électorales américaines", *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, p. 86.

[12] Cfr. Deb, Anamitra/Donohue, Stacy/Glaisyer, Tom "Is Social Media a Threat to Democracy?", precedentemente citato.

ISSN 2279-7238

Costituzione prima della nuova configurazione dello spazio e del tempo politico. Con riferimento al tempo, possiamo parlare di una difficoltà per sviluppare processi costituenti o di riforma che riguarda la scomparsa del consenso come formula di soluzione del conflitti, con l'impossibilità di realizzare una programmazione a lungo termine propria delle costituzioni, con l'abbandono dei diritti costituzionali nel dibattito politico, con la debolezza dei mezzi di comunicazione tradizionali, etc.

Con riferimento specificatamente allo spazio pubblico nazionale, che era l'ambito nel quale il costituzionalismo si era sviluppato sino ad ora, i cambiamenti che lo sviluppo tecnologico sta introducendo, specialmente attraverso Internet e i *social network*, sono molto rilevanti[13]. La frammentazione progressiva dello spazio pubblico che è stata creata o, quanto meno, potenziata dalle società tecnologiche che gestiscono *social network*, ostacola la possibilità di avere consensi sociali ampi destinati ad ordinare in maniera globale l'insieme della società per il tramite di strumenti costituzionali. La lesione dei diritti attraverso le reti è un'altra delle questioni nelle quali lo sviluppo tecnologico sollecita la cornice costituzionale nazionale[14]. Tuttavia la più rilevante si manifesta attualmente nella medesima qualità democratica dello Stato dovuta all'attività di manipolazione elettorale che hanno sviluppato alcune società tecnologiche che gestiscono *social network* nei processi elettorali recenti[15].

3.2- Processi democratici e social network.

Il modello di business con il quale sono state costruiti i *social network* dalle società che le gestiscono e la loro dipendenza dalla pubblicità ha creato una necessità permanente di attrarre l'attenzione del pubblico, di fomentare l'uso dei *social network* e delle applicazioni di Internet. Nella loro traslazione dal piano della comunicazione politica, questa attenzione permanente è conseguita sul piano politico generando dibattito, radicalizzazione e instabilità politica.

D'altro lato, questo modello, che è costruito dalla vendita pubblicitaria, mediante l'utilizzazione massiccia di dati personali e la configurazione di profili attraverso algoritmi, cominciò ad essere utilizzato successivamente nella propaganda politica. La loro applicazione alla propaganda politica ha creato nuove lesioni di diritti, utilizzando questi profili psicologici

---

[13] Sicuramente, non è possibile valutare questi cambiamenti solamente da una prospettiva negativa poiché, come indicano Julien Bonnet e Pauline Türk "Les technologies numériques n'étant qu'un outil, c'est la façon dont elles vont être utilisées, développées et encadrées qui déterminera, dans l'avenir, leurs effets bénéfiques ou délétères, à moyen et long terme, sur la démocratie", J. Bonnet e Pauline Türk, "Le numérique : un défi pour le droit constitutionnel", *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, p. 18. Per valutare questi effetti, bisogna distinguere anche, come fa Coralie Richaud, tra la pratica collettiva e quella individuale nei *social network*. Cfr. C. Richaud, "Les réseaux sociaux: nouveaux espaces de contestation et de reconstruction de la politique ?, *Les Nouveaux Cahiers du Conseil constitutionnel*, 2017/4 N° 57, pp. 29-44.

[14] Come indica D. Rousseau, "Le discours anti-droits de l'homme est devenu le discours dominant" *Libération*, 6 décembre 2018, https://www.liberation.fr/auteur/8617-dominique-rousseau.

[15] Cfr. Scott, Mark, "Cambridge Analytica helped 'cheat' Brexit vote and US election", *Politico*, 29/3/2018:https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook/. Cfr. egualmente, Ferguson, Niall, "Social networks are creating a global crisis of democracy", 2018, in: https://www.theglobeandmail.com/opinion/niall-ferguson-social-networks-and-the-global-crisis-of-democracy/article37665172/

ISSN 2279-7238

per elaborare e diffondere propaganda subliminale particolarizzata. Questa propaganda subliminale è inserita all'interno di un contesto di radicalizzazione, frammentazione dello spazio pubblico, creazione di effetto bolla, disinformazione e falsificazione di notizie, che contribuiscono a potenziare la loro efficacia.

Le società di Internet hanno favorito fino ad ora le opzioni più radicali e populiste nei processi elettorali per differenti motivi. Tra questi dovrebbe essere evidenziato, in primo luogo, che la creazione di instabilità favorisce il conseguimento di maggiori entrate con il loro attuale modello di affari. In secondo luogo, il deterioramento e il potenziale blocco della politica ostacola il controllo che i poteri pubblici dovevano realizzare su queste società di internet e sulle reti. Da questa prospettiva le società tecnologiche vincono sempre con la radicalizzazione e l'instabilità politica, tanto dal punto di vista economico come dalla prospettiva dell'estensione del loro potere davanti all'assenza di limiti e di controlli generata dall'instabilità politica che le stesse provocano.

4.- Le società tecnologiche e le reti. Aspetti problematici.

4.1- Incidenza sui diritti fondamentali.

Sfortunatamente è sempre più chiaro che i *social network* non sono gestiti da mere piattaforme statiche che agiscono come intermediari senza avere nessun tipo di responsabilità. Al contrario, si tratta di società che gestiscono *social network* e non mere piattaforme, alle quali deve essere attribuita la responsabilità delle cattive pratiche che sono sviluppate in queste quando non fanno nulla per evitarle, o anche le favoriscono. Controllare le società che gestiscono i *social network* e il loro modello di business è fondamentale per invertire l'involuzione democratica e civilizzatrice che attualmente stiamo vivendo.

Un ambito specificatamente sensibile all'azione di queste società è quello della lesione dei diritti fondamentali come il diritto alla *privacy* o la protezione dei dati personali. La lesione massiccia del diritto alla protezione dei dati personali da alcune di queste società tecnologiche è stata una costante ed anche l'incapacità degli attori politici di proteggere la cittadinanza. Il problema è che da questa lesione massiccia ne sono derivate altre, molte come conseguenza dell'utilizzazione dei dati ottenuti per fini molto diversi attraverso *algoritmi* che utilizzano queste società e che incidono su uno spettro molto ampio di diritti fondamentali. Un aspetto specialmente problematico è la lesione dei diritti politici come conseguenza dell'interferenza delle società che gestiscono *social network* nei processi elettorali.

4.2- Tendenza al monopolio e impatto sulla concorrenza.

ISSN 2279-7238

Uno dei problemi più gravi che stanno affrontando le società tecnologiche è la posizione di monopolio che stanno occupando in alcune delle attività che sviluppano[16]. Questa posizione è stata conseguita senza che ci sia stata alcuna reazione significativa da parte degli organismi regolatori. Come indica nel rapporto *Unlocking digital competition*: "Over the last 10 years the 5 largest firms have made over 400 acquisitions globally. None has been blocked and very few have had conditions attached to approval, in the UK or elsewhere, or even been scrutinised by competition authorities"[17].

L'esempio di Facebook è rivelatore. In base a quello che è indicato in *Disinformation and 'fake news': Final Report*, questa società concentrò in maniera illecita una grande quantità di dati personali che dopo vendette o cedette ad altre applicazioni (in cambio dei dati che fornivano le altre società). Tutti i dati, quelli raccolti da questa società e quelli delle altre, si concentrarono su Facebook. Una volta concentrati, Facebook, attraverso una applicazione disegnata inizialmente per proteggere i dati degli utenti in Internet, che aveva comprato precedentemente, realizzò un tracciato dell'evoluzione di queste applicazioni. Queste, che avevano un potenziale di crescita importante e potevano competere nel futuro, avevano offerte per l'acquisto di Facebook. Le società che non accettarono le offerte di acquisto e quelle alle quali Facebook attribuiva loro una possibilità di concorrenza futura tuttavia non avevano interesse ad acquistarla, furono disattivate da Facebook ritirando l'accesso ai dati personali che costituiva la base dei loro affari e provocando la loro rovina[18].

4.3- La pressione sui mezzi di comunicazione tradizionali.

Il modello di business delle società che gestiscono *social network* sta generando una trasformazione importante del mercato pubblicitario con una tendenza al monopolio, occupando una percentuale sempre maggiore di questo mercato. Come indica *The Cairncross Review. A sustainable future for journalism*, i mezzi di comunicazione stanno riducendo in maniera significativa le loro due fonti tradizionali di entrate: la circolazione e la pubblicità[19]. L'informazione viene distribuita sempre di più in misura maggiore attraverso i *social*

---

[16] Cfr. Frosini, Tommaso Edoardo, "Internet e democrazia", *Il diritto dell'informazione e dell'informatica*, Anno XXXII, 2017, Fasc. 4-5, pp. 657-671.

[17] *Unlocking digital competition. Report of the Digital Competition Expert Panel*, March 2019, Jason Furman and others, p. 12. "The largest digital companies have made extensive use of mergers, as their market shares have grown. Acquisitions have included buying businesses that could have become competitors to the acquiring company (for example Facebook's acquisition of Instagram), businesses that have given a platform a strong position in a related market (for example Google's acquisition of DoubleClick, the advertising technology business), and data-driven businesses in related markets which may cement the acquirer's strong position in both markets (Google/YouTube, Facebook/WhatsApp*)", Ibidem*, p. 11.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

[18] House of Commons, Digital, Culture, Media and Sport Committee, DCMS. *Disinformation and 'fake news': Final Report*, cit., pp. 26 e ss.

[19] *The Cairncross Review. A sustainable future for journalism*, 12 February 2019: "The news publishing business is undergoing an extraordinary period of contraction in both of its main traditional sources of revenue: advertising and circulation", p. 5.

ISSN 2279-7238

network[20] e vi è evidenza di una battuta di arresto permanente dei mezzi di comunicazione tradizionali[21].

La crescente debolezza dei mezzi di comunicazione sta provocando la scomparsa di mezzi e l'indebolimento della loro funzione pubblica di formazione di opinione a partire da un'informazione obiettiva e veritiera[22]. Allo stesso tempo, i mezzi stanno subendo anche una dipendenza crescente dai dibattiti e dall'agenda politica che sono impostate nei *social network*. Tuttavia mentre i mezzi di comunicazione tradizionali sono aperti e trasparenti, nei *social network* intervengono gruppi e attori anonimi che condizionano i dibattiti e alimentano quelli che possono creare più conflitto e instabilità.

Il cambiamento di modelli culturali nell'ambito dell'informazione favorisce anche la frammentazione e la radicalizzazione. L'informazione nelle reti si mostra disaggregata e condizionata dagli algoritmi, in modo che non c'è una visione ampia di tutti i temi di attualità come nei mezzi di comunicazione tradizionali ma anche si accede all'informazione in maniera frammentata e selettiva[23].

5.- I processi comunicativi e di costruzione dello spazio pubblico.

5.1- Il precedente substrato, globalizzazione e crisi economica.

Le società di *social network* agiscono su un precedente substrato di malcontento sociale generato dalla globalizzazione e dalla crisi economica. Questo malcontento corrisponde ad una crescente sensazione di precarietà in ampi strati della popolazione e nell'aumento della diseguaglianza tra i settori della minoranza che accumulano sempre più ricchezza e il resto della società.

Fino ad ora, queste società hanno contribuito a potenziare il malcontento invece di canalizzarlo per offrire soluzioni, che è una delle funzioni essenziali dei sistemi costituzionali e democratici. I problemi sociali che sono stati creati dovuti alla globalizzazione e che sono stati incrementati come conseguenza della crisi non hanno facile soluzione, ma devono essere

[20] "In 2018, the Reuters Institute for the Study of Journalism reported that 74% of UK adults used some online method each week to find news, and 91% of 18-24 year olds. Most online news is available for free and much of it is carried by aggregators such as Google News or Apple News, posted on Facebook's news feed, or sent from one person to another at the tap of a finger", *Ibidem*, p. 6.

[21] "sales of both national and local printed papers have plunged: they fell by roughly half between 2007 and 2017, and are still dropping. In addition, print advertising revenues, which used to carry much of the cost of producing news, have fallen even faster, declining in a decade by 69%. Small wonder so many news groups are struggling, including digital-only groups like HuffPost and Buzzfeed, as well as many local newspaper publishers. To cut costs, there have been mergers, as well as heavy cuts in staffing: the number of full-time frontline journalists in the UK industry has dropped from an estimated 23,000 in 2007, to 17,000 today, and the numbers are still swiftly declining", *Ibidem*, p. 6.

[22] Come indica Anna Papa, si fa più attenzione al dato isolato e non al loro inserimento in un processo complesso di formazione di coscienza, nel quale il dato deve essere contestualizzato per essere convertito in informazione e unito con altre informazioni con le quali si confronta, creare coscienza. Cfr. Anna Papa, "Il diritto ad essere informati nella tutela multilivello della libertà di espressione", in corso di stampa.

[23] "Social feeds and search results show snippets and single articles. This creates a more disaggregated news experience than traditional news media." Ciò significa che gli utenti non accedono che ad una parte delle informazioni: "Online content is effectively "unbundled". The different sections of a print newspaper are brought together into one product. Online, readers can select only the articles they wish to view, without necessarily being exposed to other content. So, they may be less likely to read public interest news". *Ibidem*, p. 7.

ISSN 2279-7238

affrontati mediante il dialogo e la negoziazione attraverso i processi democratici nell'ambito degli Stati nazionali e nelle strutture sovranazionali.

Si può affermare, pertanto, che le società che gestiscono *social network* stanno ostacolando funzioni essenziali dell'ordinamento costituzionale e dei processi democratici. Non solo non contribuiscono alla circostanza che queste funzioni siano realizzate ma anche le ostacolano anche aumentando la radicalizzazione e favorendo i conflitti invece di offrire una soluzione pacifica e democratica a questi conflitti.

5.2- La frammentazione e radicalizzazione dello spazio pubblico.

La frammentazione dello spazio pubblico è uno degli effetti più disfunzionali che è stato generato attraverso i *social network* con il loro attuale modello di business. Colpisce il nucleo medesimo della democrazia pluralista poiché ostacola il riconoscimento degli altri, il rispetto della diversità, la possibilità di articolare dibattiti produttivi e la capacità di offrire soluzioni globali per l'intera società.

La radicalizzazione è favorita dalla frammentazione dello spazio politico e dall'effetto bolla[24]. L'autoalimentazione permanente delle proprie idee genera fondamentalismo. La radicalizzazione impedisce il dibattito, converte l'avversario politico in nemico e trasforma la politica in una lotta per imporre le proprie idee che è incompatibile con il concetto di democrazia costituzionale proprio delle costituzioni normative, per le quali non esiste democrazia senza Stato di Diritto e senza rispetto dei diritti delle minoranze.

La trasformazione della democrazia nella semplice volontà della maggioranza parlamentare o sociale suppone un'involuzione storica che ci riporta al periodo tra le due guerre, nel quale questa concezione della democrazia era la base dell'implementazione di regimi fascisti.

6.- I processi elettorali.

6.1- Notizie false e disinformazione.

La disinformazione generata attraverso notizie false non è qualcosa di nuovo nella storia. Ciò che è nuovo è la capacità che hanno i *social network* di convertire queste notizie false in tendenze maggioritarie in contesti democratici, occupando una parte fondamentale dello spazio pubblico[25].

È anche una novità il fatto che queste notizie si trasmettono in un ambito privato e intimo (per esempio, attraverso WhatsApp) che ne aumenta straordinariamente la loro efficacia perché elimina la distanza dal mittente del messaggio.

[24] Pariser, Eli, *The Filter Bubble. What the Internet Is Hiding from You*, Penguin Books, 2011.

[25] Cfr. Pitruzzella, Giuseppe, "La libertà di informazione nell'era di Internet" in G. Pitruzzella, O. Pollicino, S. Quintarelli. *Parole e potere: Libertà d'espressione, hate speech e fake news*. Italian Edition. Egea, 2017.

ISSN 2279-7238

Le notizie false stanno distruggendo lo spazio pubblico e alterando le condizioni strutturali dei processi democratici. Favoriscono lo sviluppo della frammentazione e radicalizzazione e l'accesso al potere di movimenti populisti poco rispettosi con le regole democratiche.

6.2- Interventi di attori esterni e di gruppi organizzati.

L'intervento di attori esterni e di gruppi organizzati nel dibattito pubblico e specificatamente nei processi elettorali è una manifestazione di più dell'interesse interno e esterno per generare instabilità e bloccare il sistema democratico.

Sfortunatamente, questo interesse è congruente con quello della società che gestiscono *social network*. Per questo motivo, oltre al vantaggio economico diretto che questi gruppi interni ed esterni (mediante la contrattazione di propaganda politica) queste società hanno favorito inizialmente questo intervento.

Successivamente ai grandi scandali che sono stati generati dal referendum sulla Brexit e le elezioni presidenziali negli Stati Uniti, queste società hanno agito con efficacia relativa e diversa per controllare l'intervento esterno ma, in ogni caso, in maniera insufficiente.

6.3- Profili individuali e propaganda subliminale.

La creazione di profili individuali mediante l'utilizzazione massiccia di dati personali e la loro utilizzazione specifica per la distribuzione personalizzata di propaganda subliminale è l'azione più grave che può essere attribuita alle società che gestiscono *social network* dalla prospettiva della loro incidenza nei processi democratici.

Questa attività presenta segnali chiari di criminalità in quanto impone un'infrazione delle norme che regolano i processi elettorali, suscettibile di alterare il risultato delle elezioni.

Queste pratiche possono supporre la distruzione dei processi democratici. Di fronte a queste la cittadinanza è assolutamente inerme perché nessuno è cosciente del fatto che la loro volontà di votare a favore di un'opzione politica può essere manipolata e alterata attraverso la propaganda subliminale.

7.- Possibile aree di azione.

Per fare fronte ai problemi che le società che gestiscono *social network* stanno generando nei processi democratici non sono sufficienti misure che colpiscono unicamente i processi democratici, per esempio. È necessario partire da una visione di insieme di tutti questi problemi, che implica affrontare anche la questione del modello di business che hanno queste società. Questo modello di business è attualmente incompatibile con quello che i *social network* intendevano essere: un spazio di partecipazione civica, di promozione di cause giuste e di approfondimento democratico.

Alcune società che sono state costruite sul modello di business basato sull'attrazione dell'attenzione del pubblico per creare più entrate pubblicitarie e che hanno tendenza al

ISSN 2279-7238

monopolio o all'oligopolio, difficilmente potranno apportare strumenti di partecipazione democratica. Non si può offrire ciò che non si ha. Le società che non sono democratiche né per loro struttura né per la finalità delle loro attività, non possono configurare meccanismi reali di democratizzazione.

Le misure che sono proposte quindi sono fondamentalmente esterne, ma anche è possibile pensare ad una regolamentazione dei propri *social network* che renda possibile il cambiamento di alcuni dei modelli che sono stati introdotti e sono risultati pregiudiziali per la configurazione dello spazio pubblico dei processi comunicativi. Sarebbe il caso, ad esempio, dell'implementazione di procedimenti che ritardino le risposte ora immediate che, per loro propria naturalezza, tendono a logorare e radicalizzare i processi comunicativi.

7.1- Diritti fondamentali.

Le misure che dovrebbero essere adottate in questo ambito sono di ampio respiro: dall'educazione della cittadinanza nell'ambito digitale affinchè controllino le lesioni ai loro diritti, fino alle sanzioni di ogni tipo contro le lesioni più gravi che possono prodursi.

In particolare, l'educazione digitale deve contemplare dai processi tecnici che favoriscano la comprensione di come funzionano le reti e Internet fino ai meccanismi giuridici di regolazione e, in particolare, i diritti che riguardano gli utenti così come l'insieme di diritti suscettibile di essere leso e le misure che l'ordinamento giuridico offre per garantirli.

La protezione dei dati personali deve estendersi ai modelli che sono utilizzati per il loro trattamento. L'elaborazione dei profili deve essere sottoposta alle limitazioni stabilite nella normativa europea. L'elaborazione di profili psicologici deve essere oggetto di attenzione speciale per evitare che sia uno strumento di manipolazione delle coscienze che incide negativamente nei processi democratici.

7.2- Concorrenza, pubblicità e mezzi di comunicazione.

Il controllo della concorrenza per evitare che le società di internet consolidino posizioni di monopolio è fondamentale. Le cattive pratiche seguite fino ad ora non devono essere permesse nel futuro. Al contrario, sarebbe conveniente seguire le proposte che già sono state fatte da alcuni responsabili politici (come la Senatrice Elizabeth Warren negli Stati Uniti) nel senso di rompere gli attuali monopoli, come già si fece prima in questo paese con altre società in epoche precedenti, per preservare la libera concorrenza.

La regolazione del mercato pubblicitario sarebbe anche necessaria per evitare che queste società tecnologiche continuino ad aumentare la loro quota di partecipazione in questo mercato, indebolendo sempre di più i mezzi di comunicazione tradizionali.

Secondo le raccomandazioni della relazione *Unlocking digital competition*, gli organismi regolatori dovrebbero cambiare i loro metodi di lavoro per affrontare adeguatamente le condizioni del mercato digitale, in maniera che non si limitino a controllare gli effetti a breve

ISSN 2279-7238

termine delle possibili fusioni e degli acquisti di società che analizzano anche la loro prevedibile evoluzione successiva per evitare che si consolidino monopoli[26].

7.3- Processi elettorali.

È necessaria una nuova normativa elettorale che tenga in conto il contesto tecnologico, tanto per quanto riguarda la propaganda elettorale quanto per gli altri aspetti che possono provocare un'alterazione del normale sviluppo di questi processi. In particolare, la propaganda subliminale deve essere proibita e penalizzata con tutti i mezzi alla portata dello Stato di Diritto.

Abbiamo un caso recente in Spagna che ci serve come esempio dell'importanza del fatto che gli organi giurisdizionali prendano coscienza dell'entità dei problemi e della necessità di darle una risposta rapida ed effettiva. In concreto, la recente approvazione della Ley organica 3/2018, del 5 dicembre, di Protezione dei Dati Personali e garanzia dei diritti digitali, che nella sua Disposizione Addizionale Terza modificava la Legge Organica del Regime Elettorale Generale, incorporando un articolo 58 bis nel quale si permetteva ai partiti politici di raccogliere dati personali relativi alle opinioni politiche delle persone nella cornice delle loro attività elettorali "con le garanzie adeguate". I partiti potrebbero utilizzare dati personali ottenuti su pagine Web e altre fonti di accesso pubblico per la realizzazione di attività politiche durante il periodo elettorale. Questa riforma è stata dichiarata incostituzionale solo alcuni mesi dopo, mediante la STC 76/2019 del 22 maggio. La sentenza basa la dichiarazione di incostituzionalità e nullità "en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el art. 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear".

7.4- Misure fiscali.

Le misure fiscali sono una questione fondamentale dell'azione contro le cattive pratiche delle società che gestiscono *social network*. Quando queste società sono orientate al profitto economico, le misure fiscali possono essere un elemento di compensazione che renda

[26] "Decisions on whether to approve mergers, by the CMA and other authorities, have often focused on short-term impacts. In dynamic digital markets, long-run effects are key to whether a merger will harm competition and consumers. Could the company that is being bought grow into a competitor to the platform? Is the source of its value an innovation that, under alternative ownership, could make the market less concentrated? Is it being bought for access to consumer data that will make the platform harder to challenge? In principle, all of these questions can inform merger decisions within the current, mainstream framework for competition, centred on consumer welfare", *Unlocking digital competition* cit., p. 12.

ISSN 2279-7238

possibile l'utilizzazione dei fondi ottenuti per stabilire istituzioni e meccanismi di controllo così come di educazione digitale della cittadinanza.

Queste misure fiscali possono anche essere il meccanismo che permette di controllare gli effetti disfunzionali dell'attività di queste piattaforme sui mezzi di comunicazione tradizionali se sono accompagnati da benefici fiscali che rendano possibile la permanenza e stabilità di questi mezzi.

7.5- Sanzioni.

Le sanzioni economiche sono molto importanti per lottare contro le cattive pratiche delle società tecnologiche, precisamente perché colpiscono i loro profitti, che costituiscono la base del loro attuale modello di affari. È raccomandabile che queste sanzioni corrispondano all'entità dei danni causati, potendo raggiungere percentuali del loro volume totale di affari globali annui (come è già stato previsto da legislazioni settoriali come quella europea in materia di protezione dei dati).

Le sanzioni penali sono sempre l'ultimo strumento, ma saranno necessarie per le cattive pratiche che si producono in relazione con i processi elettorali, come è il caso della propaganda subliminale particolarizzata in funzione di profili psicologici precedentemente elaborati attaverso algoritmi. Questo tipo di interventi nei processi elettorali non sono una questione minore e richiedono una risposta molto ferma dell'ordinamento giuridico per evitare una denaturalizzazione completa dei processi democratici.

Conclusioni/Sintesi

Nella relazione tra i *social network* e la democrazia è necessario considerare un mediatore fondamentale come sono le società tecnologiche che gestiscono le reti. Questo mediatore è stato occulto per molto tempo, fino al punto che è stato abituale pensare ai *social network* come uno strumento di comunicazione politica senza mediatori (a differenza dei mezzi di comunicazione tradizionali) il quale evidentemente non è certo. I *social network* non sono un fenomeno naturale che è apparso nei processi sociali e politici in maniera spontanea. Sono il risultato di scelte di impresa che hanno configurato un modello di business che è basato nell'attirare l'attenzione del pubblico per ottimizzare i rendimenti pubblicitari mediante l'utilizzazione continua delle reti. Questo modello di affari sta provocando problemi importanti nei processi di comunicazione politica perché fomenta la frammentazione dello spazio pubblico e la loro radicalizzazione con la finalità di incrementare l'uso delle reti e ottenere così più vantaggi. A questa finalità economica si unisce la politica di generare instabilità per indebolire le istituzioni democratiche e ostacolare così il controllo che dovrebbero realizzare queste istituzioni sulle medesime società tecnologiche.

Sono molti gli ambiti nei quali i *social network* stanno creando disfunzioni dal punto di vista costituzionale e democratico. Dai diritti fondamentali ai processi elettorali, passando per la configurazione stessa dell'ordine costituzionale, in un contesto nel quale le condizioni dello

ISSN 2279-7238

spazio e il tempo si sono trasformate come conseguenza della globalizzazione e dello sviluppo tecnologico. Nuovi modelli culturali e nuovi paradigmi stanno nascendo e la loro incidenza sul costituzionalismo è molto ampia. Alcuni dei cambiamenti che hanno portato i *social network* possono essere strutturali e si manteranno prevedibilmente nel futuro. Altri, tuttavia, possono considerarsi direttamente vincolati agli interessi delle società tecnologiche e dovranno essere oggetto di revisione per evitare che conducano ad un'involuzione democratica. L'intervento dei poteri pubblici, statali e sovranazionali, è sempre più necessario per controllare queste società.

Le misure che possono essere prese sono molto diverse. Dal rafforzare la protezione dei diritti fondamentali fino a promuovere l'educazione digitale della cittadinanza, passando da azioni destinate ad evitare che le società tecnologiche consolidino posizioni di monopolio, così come misure fiscali e sanzionatorie, etc. Di particolare importanza è la regolazione dei processi elettorali per evitare che continuino a produrre interferenze attraverso delle notizie false e per mezzo della propaganda subliminale particolarizzata. L'orizzonte si sta muovendo, in ogni caso, nella misura in cui avanza lo sviluppo tecnologico e che altre società disegnano nuove strategie. Pertanto, è necessario tenere conto che le caratteristiche non sono solamente quelle che oggi conosciamo ma dobbiamo avere un'atteggiamento vigile per evitare che siano generati nuovi effetti disfunzionali nel futuro.

ABSTRACT

In the relationship between social networks and democracy it is necessary to consider a fundamental mediator such as the technological companies that manage the networks. That mediator has been hidden for a long time, to the point that it has been usual to think of social networks as an instrument of political communication without mediators (as opposed to traditional media), which is obviously not true. Social networks are not a natural phenomenon that has appeared in social and political processes spontaneously. They are the result of business options that have set up a business model based on attracting the public's attention to optimize advertising performance through the continuous use of networks. This business model is causing significant problems in the processes of political communication because it promotes the fragmentation of public sphere and its radicalization in order to increase the use of networks and thus obtain more benefits. To this economic purpose we must add the advantages for these companies of generating instability to weaken democratic institutions what hinder the control that these institutions should perform over the technology companies.

There are many areas in which social networks are generating dysfunctions from a constitutional and democratic point of view. From fundamental rights to electoral processes, through the configuration of the constitutional order, in a context in which the conditions of space and time have been transformed as a result of globalization and

ISSN 2279-7238

technological development. New cultural patterns and new paradigms are being generated and their impact on constitutionalism is very broad. Some of the changes that social networks have brought can be structural and will be predictably maintained in the future. Others, however, can be considered directly linked to the interests of technology companies and should be subject to revision to prevent a democratic involution. The intervention of public, state and supranational authorities is more and more necessary to control these companies.

The measures that can be taken are very diverse. From strengthening the protection of fundamental rights to promoting the digital education of citizens, as well as actions aimed at preventing technology companies from consolidating monopoly positions or fiscal and sanctioning measures, etc. Particular importance has the regulation of electoral processes to avoid interferences through fake news and targeted subliminal propaganda. The horizon is moving, in any case, as technological development advances and these companies design new strategies. Therefore, it is necessary to bear in mind that the risks are not only those we know today but that we must have a vigilant attitude to impede generating new dysfunctional effects in the future.

Parole chiave: Social network, società tecnologiche, Fake News, democrazia.

Keywords: Social Network, Technological Companies, Fake News, Democracy.

ISSN 2279-7238

24 marzo 2020

"Fisime per la privacy"? Protezione dei dati personali e interesse pubblico nella pandemia.

Enrico Carloni

Contributo pubblicato nel blog *ridiam.it*

"Fisime per la privacy"? Protezione dei dati personali e interesse pubblico nella pandemia

di
Enrico Carloni

1. Premessa

La gestione dell'epidemia Covid-19 richiede risposte non solo di tipo medico, ma anzitutto sociale tramite strategie (in larga parte obbligatorie) di "distanziamento". Eppure, la soluzione in grado di frenare completamente la circolazione del virus, vale a dire il totale isolamento della popolazione, risulta di difficile percorribilità: la scelta attuale, di una generale chiusura di scuole ed attività economiche, è ancora accompagnata da deroghe in parte inevitabili (il personale sanitario, i servizi essenziali, la distribuzione dei farmaci, i generi alimentari: attività che pure potrebbero essere in larga parte svolte in modalità più sicura, in particolare prevedendo maggiori controlli ed imponendo condizioni più robuste di sicurezza per gli operatori impegnati in questi settori). E da deroghe ulteriori, ampie, giustificate da esigenze di contemperamento tra beni costituzionalmente protetti, quali quelle che comportano l'attività lavorativa di banche, assicurazioni, fabbriche, agricoltura, edicole, financo tabaccherie, ecc.

Probabilmente l'equilibrio sin qui trovato non è adeguato a contenere la pandemia nelle zone del paese in cui il numero di contagiati è più alto, il che chiama in causa altre scelte di politica dell'emergenza. In attesa di soluzioni farmacologiche, di trattamento e prevenzione, è sempre più avvertita la possibilità di uno sviluppo di medio periodo delle strategie di gestione della crisi, in un arco di tempo di svariati mesi nei quali sarà sempre più difficile mantenere l'opzione di chiusura completa o semi completa delle attività sociali ed economiche.

Questo scenario sollecita a maggior ragione l'utilizzo di un armamentario non solo (pure indispensabile) di vigilanza attiva di tipo epidemiologico "tradizionale", ma anche tecnologico, tramite soluzioni di tracciamento dei dati delle persone infette (ancorché asintomatiche). Il che, in termini più complessivi, comporta il trattamento dei dati, anche sensibili, delle persone, posto che può risultare necessario ripercorrere i contatti di soggetti che non hanno contratto il virus o che solo successivamente mostreranno sintomi o comunque saranno riconosciuti come positivi (e quindi contagiosi) al Covid-19. Cosicché il "tracciamento" va inteso, in sintesi, come trattamento massivo di dati storici di localizzazione in forma (di norma) non anonimizzata.

Tra le leve di cui si discute per contribuire a gestire il problema, ipotesi di questo genere si fanno sempre più spesso strada nel dibattito pubblico: "il ricorso alle più avanzate tecnologie disponibili (big data, geolocalizzazione, Intelligenza artificiale e Blockchain) per tracciare gli spostamenti dei soggetti positivi e le possibili occasioni di contagio" (Coronavirus: l'appello dei docenti…, in La Repubblica, 19 marzo 2020).

La qual cosa "pone, ovviamente, il problema della privacy". Obiettivo di questo breve intervento è quello di riflettere su come la privacy si ponga effettivamente come ostacolo ad una soluzione auspicabile, ammettendo sul modello coreano e di altre realtà dell'estremo oriente, alcune delle quali di diversa tradizione democratica, che una strategia di tracciamento ed in particolare di ricostruzione epidemiologica dei contatti assistita dall'utilizzo dei dati. E su come, al contrario, sia possibile, necessario ed opportuno, per tutti i valori in gioco (non ultimo, la stessa protezione dei dati personali) cercare una soluzione che definisca un equilibrio, proprio per evitare che le esigenze di protezione dei dati personali siano percepite, e vengano trattate, come "fisime", riprendendo l'espressione utilizzata dal virologo Burioni, insostenibili nel momento attuale.

2. Privacy e interesse pubblico

In un recente intervento a Radio Radicale, proprio commentando le esigenze di contemperamento tra diritti fondamentali, e libertà, che caratterizza l'attuale fase di emergenza, l'ancora attuale Garante per la protezione dei dati personali, Soro, ha rimarcato il carattere "non dispotico" del diritto alla privacy, che si pone al fianco degli altri diritti fondamentali. Affermazioni dello stesso tenore ricorrono in altre dichiarazioni ed interviste dello stesso Garante: "in momenti come questo, certamente eccezionale, ci sono naturali e dovute limitazioni alla privacy. E alle nostre libertà. Tutto ciò va valutato bilanciando le limitazioni con un altro fondamentale diritto individuale e interesse collettivo: quello alla salute" (intervista a Tiscali News, 19 marzo 2020).

L'emergenza mostra la necessità di coesistenze e contemperamenti che in situazioni ordinarie erano parse meno evidenti, per quanto il principio di ricerca di adeguate soluzioni di bilanciamento tra valori e principi fosse già presente nell'ordinamento, proprio con riferimento ad un diritto spesso interpretato in termini di ineludibile prevalenza come il diritto alla protezione dei dati personali. Dello stesso avviso era stata, ad esempio, la Corte costituzionale, che nel bilanciare le esigenze di protezione dei dati con quelle di trasparenza aveva evidenziato l' "eguale valore" dei due principi, da porre in equilibrio attraverso soluzioni proporzionate.

Traendo forza dal fatto di essere posta da fonti europee (e quindi, ora rinforzata dal "contenitore-regolamento"), e dal fatto di essere fatta oggetto di tutela attraverso l'azione di un'autorità dedicata dai poteri particolarmente incisivi e penetranti, la protezione dei dati personali ha però spesso mostrato tratti meno moderati, ponendosi come meta-valore in grado di prevalere sugli altri. In questo percorso, marcato nel corso del mandato dell'attuale collegio anche in virtù dell'entrata in vigore del regolamento europeo (Gdpr), è emersa con particolare forza la difficoltà di contemperamento tra esigenze contrapposte date da altri interessi pubblici. Non è qui possibile ricostruire con attenzione i diversi profili, per quanto alcune specifiche declinazioni saranno evidenti nel prosieguo, ma è abbastanza evidente che il sistema di protezione dei dati costruito dal regolamento europeo è nel suo complesso particolarmente esigente nei confronti delle autorità pubbliche, mentre lo è molto meno rispetto ai soggetti privati.

Il sistema si nasconde infatti dietro il velo del "consenso", trascurando il carattere spesso puramente formale delle autorizzazioni ai trattamenti che quotidianamente prestiamo per accedere ai servizi della società dell'informazione, e non solo. Chi di noi ha letto con attenzione il disclaimer che accompagna i vari siti (quando ci viene chiesto di accettarne o meno i cookies), o i servizi di un provider, o anche solo quelli della nostra banca o del fornitore di una carta fedeltà? Però tutti questi dati sono trattati da soggetti privati sulla base del consenso prestato, mentre alle amministrazioni si richiedono non solo autorizzazioni attraverso la legge, ma anche specifiche condizioni che le rendono legittime: questo, soprattutto, nella società dell'informazione.

La crisi mostra in modo purtroppo plastico i limiti di un modello che nel corso dell'ultimo ventennio ha progressivamente modificato il punto di equilibrio tra diritti individuali (sempre più assolutizzati) ed esigenze della comunità (sempre più destinate a declinare a fronte dei primi). All'interno di un approccio che mostra la corda nel momento in cui emerge con forza l'esigenza di proteggere diritti che sono ad un tempo prerogativa individuale ed interesse collettivo, come è per il caso della salute nella pandemia ma già prima nel testo dell'art. 32 della Costituzione.

Nel momento in cui vecchie e nuove libertà arretrano di fronte alla imprescindibile esigenza di salvaguardare la vita e la salute dei cittadini, questo sacrificio viene da più parti richiesto anche per la protezione dei dati personali.

Il momento, nella sua drammaticità e complessità, pone un punto di svolta anche per le amministrazioni, e gli interpreti: come rimarcato da Azzariti, tra i diritti va cercato un equilibrio proporzionato, ma giunti al limite "su tutto prevale il diritto alla vita, nella forma essenziale del diritto alla salute. Di fronte

a questo tutti gli altri diritti devono essere limitati" (intervista a Il Fatto quotidiano, 11 marzo 2020). In questo senso l'affermazione del Premier Conte, che riconosce il diritto alla salute quale obiettivo prioritario, un diritto che è di ciascuno e di tutti, cui fa seguito un'adesione unanime parlamentare (nelle limitate occasioni in cui anche il Parlamento è intervenuto) e soprattutto popolare, va interpretato come fatto di rilievo costituzionale, se non addirittura come fatto normativo costituzionale, che impone una lettura conseguente dell'ordinamento.

Una lettura che involge la Costituzione, nei suoi diritti e nelle sue libertà esplicite ed implicite, il modello costituzionale di equilibrio di spesa radicato negli articoli 81 e 97 della Costituzione, i vincoli derivanti dall'appartenenza al sistema eurounitario, lo stesso ordinamento europeo. Senza arrivare a chiamare in causa i controlimiti, è necessario orientare fin che possibile la risposta in coerenza con questi principi, all'interno di un quadro ordinamentale che deve contenere fin quando si riesca soluzioni derogatorie ed emergenziali quando capaci di incidere il nucleo dei diritti fondamentali. Una rilettura della quale sarà forse necessario tenere conto anche a medio termine, quando la tensione potrà porsi tra i diritti di proprietà intellettuale e lo stesso diritto alla salute.

3. Privacy ed emergenza sanitario-epidemiologica

L'emergenza pone ora in fibrillazione il sistema di protezione dei dati personali, perché chiama in causa ipotesi di risposta, richieste con crescente insistenza e forza, che coinvolgono forme di trattamento particolarmente invasive, perché condotte attraverso utilizzo di reti telematiche, soluzioni di trattamento automatizzato e di profilazione, con riferimento ai dati oggetto di maggiore protezione, quelli relativi allo stato di salute. Né è escluso l'utilizzo di intelligenze artificiali e forme robotizzate di trattamento dei dati raccolti.

La tensione tra contrasto della pandemia e protezione dei dati si pone anche su altri versanti (pensiamo a quello dei controlli del datore di lavoro), ma trova dunque uno sviluppo specifico e particolare nella dimensione digitale, dove il (sinteticamente definito) "modello coreano" comincia a trovare non solo sostenitori nel dibattito pubblico, ma già prime sperimentazioni locali e tentativi di sviluppo di politiche nazionali.

In termini generali, la questione diventa, nel sistema della protezione dei dati personali, quella della legittimità dello specifico trattamento, nonché del rispetto dei principi cardine del sistema della privacy, primi tra tutti quelli di proporzionalità e minimizzazione.

Una prima risposta può passare attraverso la via del consenso, tramite la promozione di applicazioni volontariamente utilizzate dai cittadini, come nel modello di cui si avvia la sperimentazione in Umbria, una soluzione che insieme ad altre è stata percorsa nella stessa esperienza coreana. Più complesso, ma forse necessario per il contenimento e la vigilanza sulla pandemia, il ricorso anche a soluzioni diverse, prescindendo dal consenso degli interessati.

Nel Regolamento generale, un esplicito riferimento ad epidemie, quale specifico fattore in grado di giustificare trattamenti mirati, è contenuto nel considerando 46 (mentre l'art. 23 parla più genericamente di "altri importanti obiettivi di interesse pubblico" anche in materia "di sanità pubblica e sicurezza sociale").

In questi termini, ai sensi del considerando, trattamenti necessari a gestire la "pandemia" può considerarsi lecita, derivando dall'esigenza di salvaguardare un "interesse essenziale", che non si limita solo all'interessato od altra persona fisica ma assume una dimensione collettiva, che è al contempo di interessi individuali e interessi collettivi. Infatti, secondo il considerando 46, "alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana".

Il considerando 46 consente di illuminare una serie di previsioni del Gdpr, permettendo di offrire una lettura maggiormente "aperta" delle sue previsioni: ne conseguirà, in particolare, la necessità di una interpretazione (anzitutto da parte del Garante) non stretta dell'art. 6 e quindi delle condizioni di liceità dei trattamenti anche laddove non basati sul consenso, e quindi in particolare laddove "il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica" od "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Qui, evidentemente, la protezione dai rischi epidemici (di più, pandemici), consente di legittimare un trattamento sia ai sensi dell'una che dell'altra ipotesi.

Il che non esime, però, dall'esigenza di una disciplina che regoli queste ipotesi, in particolare quando ciò che si va a delineare non è solo un trattamento particolarmente esteso, ma un trattamento nuovo, specie nelle forme invasive che sono proprie dei trattamenti massivi relativi a dati sensibili o super-sensibili. Il tutto, peraltro, all'interno di un quadro di significativi limiti e condizioni, cosicché il trattamento, risulti legittimo in termini formali e sostanziali, seppure particolarmente pervasivo sulla base di esigenze straordinarie.

Il tutto richiede dunque un'adeguata copertura normativa già ai sensi del Gdpr: una disciplina nazionale che "persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito", ferma (in assenza del consenso) sempre una valutazione del fatto che queste autorizzazioni legislative al trattamento costituiscano "una misura necessaria e proporzionata in una società democratica" (art. 23).

4. La protezione dei dati, tra Gdpr ed ePrivacy

Il quadro va completato, in relazione alle ipotesi sul campo, tenendo conto del fatto che la disciplina del Gdpr fa espressamente salva, in termini di "specialità", le specifiche norme previste a livello nazionale sulla base della direttiva ePrivacy, per gli aspetti da questa regolate. In rapporto tra ePrivacy e Gdpr è a ben vedere comunque complesso: da un lato, la normativa sulle comunicazioni elettroniche (datata ed in corso di revisione, ma tuttora vigente) "precisa ed integra" la disciplina generale contenuta nel (successivo) regolamento.

In questo senso può leggersi in termini di specialità, esplicitato dall'art. 95 del regolamento europeo che disciplina appunto il rapporto con la direttiva 2002/58/CE (il regolamento "non impone obblighi supplementari per quanto riguarda le materie che sono soggette a obblighi specifici fissati dalla direttiva"). La qual cosa è confermata anche dal considerando 173 dello stesso Gdpr ("è opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo" della direttiva ePrivacy).

Questo rileva anche nei casi in cui è la direttiva del 2002 ad imporre una specifica base giuridica per legittimare determinati trattamenti, in questo caso quindi in deroga a quanto altrimenti previsto dall'art. 6 del regolamento europeo. Per gli aspetti non specificamente regolati dalla direttiva (e a valle dalla normativa attuativa, in Italia in particolare, limitatamente a questi aspetti, il d.lgs. n. 196 del 2003), troverà in ogni caso applicazione il Gdpr.

Le disposizioni della direttiva, e quindi le relative norma applicative, prevalgono su quelle del Gdpr limitatamente a quei trattamenti che specificamente attengono alla materia delle comunicazioni elettroniche, e tra questi rientrano quelli all'ubicazione ed all'utilizzo dei mezzi di comunicazione. Qui, come rimarcato anche recentemente dal Comitato europeo per la protezione dei dati personali, "in linea di principio, i dati relativi all'ubicazione

possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli" (EDPB, Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di Covid-19, 19 marzo 2020).

La direttiva consente però di adottare disposizioni legislative che autorizzino trattamenti necessari, tra l'altro, per salvaguardare la sicurezza pubblica. Infatti, ai sensi dell'art. 15, "gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica". Una formulazione, si noti, sostanzialmente non dissimile da quella posta in termini generali dal Gdpr.

Trovandoci di fronte a una situazione di (straordinaria ed invero inusuale) emergenza, la presenza di queste esigenze pare difficilmente contestabile. La questione in termini di presupposti sostanziali è dunque data da una valutazione di tipo epidemiologico, tecnologico e politico, che valuti la capacità effettiva di contenimento dell'epidemia, le concrete modalità tecnologiche di realizzazione (e quindi, in particolare, l'eventuale possibilità di prescindere dall'utilizzo di dati personali), la necessità in un'ottica di bilanciamento tra valori (quindi, in particolare, l'esigenza di controllo remoto per ridurre le attuali condizioni di limitazione di altre libertà personali), l'effettiva utilità dei dati così raccolti.

4. Condizioni di percorribilità delle ipotesi di tracciamento

La discussione più che sul "se" deve dunque concentrarsi sul "come" sia possibile comprimere la privacy per esigenze vitali di tipo epidemiologico. Vale a dire, attraverso quali forme legali, attraverso quali garanzie sostanziali. C'è, e residua comunque sia pure per scelte che dilatano i poteri emergenziali, un'esigenza insopprimibile di "forme" che sono anche sostanza.

Forme che si declinano intorno a tre principi che richiedono di essere valorizzati pure a fronte di una scelta di questo tipo.

Legalità, proporzionalità, responsabilità.

In termini di legalità, la questione attiene al ricorso ad un avente valore di legge che preveda e disciplini nei suoi tratti essenziali la logica del trattamento, le

modalità generali, le finalità, i tempi di conservazione dei dati. Definendo, in primo luogo, il carattere straordinario, contingibile e urgente di queste misure: la loro stretta temporaneità è la prima condizione di compatibilità, si può dire in termini più complessivi di costituzionalità, delle misure adottate. Per quanto in altri ambiti faccia pregio l'esigenza di provvedere su criteri di stretta legalità, e si sia quindi giunti ad ammettere un sistema di regole che si reggono su una "vera e propria 'cascata' di fonti normative", in questo caso pare ineludibile l'esigenza di un atto avente valore di legge, in concreto auspicabilmente un decreto legge (evitando non solo il ricorso in questo campo agli ormai consueti dPCM, ma anche, ad esempio, per quanto possibile, la soluzione di un emendamento in sede di conversione di altri provvedimenti già adottati). Questo, per una questione di assunzione consapevole e responsabile di un atto destinato a determinare una compressione straordinaria di diritti fondamentali proprio nel loro nucleo più intimo (quello, appunto, dei dati sensibili).

Proporzionalità: è chiaro che una soluzione di tracciamento dei "potenziali" positivi, dei contatti intercorsi, richiede soluzioni particolarmente invasive in larga parte refrattarie ad esigenze di minimizzazione. Se per finalità di monitoraggio degli assembramenti, ad esempio, una minimizzazione (intesa come anonimizzazione, aggregazione dei dati) pare possibile. Più difficile nell'ottica epidemiologica di monitoraggio attivo: solo per esemplificare, dovrà essere possibile risalire non solo ai contatti diretti (tramite tecniche di geoposizionamento), ma anche ai contatti intercorsi nell'ambiente familiare, lavorativo, incrociando dunque più dati che sono attinenti ad aspetti diversi della sfera personale. La proporzionalità va assicurata attraverso soluzioni di pseudo-anonimizzazione che evitino in modo assoluto trattamenti (e diffusione di notizie) che esulino dai compiti e dalle responsabilità di tipo epidemiologico. La proporzionalità consiste però, soprattutto (e di nuovo) nel carattere assolutamente temporaneo del trattamento, coerentemente con lo stesso presupposto, emergenziale, che giustifica misure straordinarie ma è idonea a sorreggerle solo nei termini più stretti della fase critica della pandemia. Il che implica anche uno stretto rispetto del principio di limitazione della finalità. Proporzionalità che significa anche necessario approntamento di misure alternative, in grado di determinare il più rapido abbandono di queste soluzioni. In ultima istanza, con queste cautele, misure invasive come il "tracciamento", come riconosciuto dal Comitato europeo per la protezione dei dati, "possono essere considerate proporzionate in circostanze eccezionali e in funzione delle modalità concrete del trattamento". Proporzionalità che si lega all'utilizzo che di questi dati verrà fatto: un sistema di "tracciamento" ha senso, ed è quindi ammissibile, solo ove si inserisca in una strategia di vigilanza attiva sull'epidemia che consista anche nel controllo tramite tamponi dei soggetti potenziali positivi non sintomatici. Diversamente, il semplice "tracciamento"

perde il suo senso e la sua utilità epidemiologica, e con questo la sua legittimazione in termini di finalità e proporzionalità.

Responsabilità. Una responsabilità che va intesa in termini forse più ampi, ed in parte diversi, da quanto previsto nel Gdpr (che pure per questa parte regge la materia della privacy). Responsabilità come accountability politico-governativa, a partire dalla chiara scelta da assumere con decreto legge, da parte del Governo, passando per l'ineludibile ruolo del Parlamento. Né nuocerebbe l'esplicita previsione di un dovere del Governo di riferire al Parlamento al termine dell'emergenza rispetto alle misure adottate, all'utilizzo fatto dei dati, ai dati conservati o destinati ad esserlo. Responsabilità che non si esaurisce nel mero adempimento: già nel senso che ne sottintende il Gdpr (dove "responsabilizzazione" è la traduzione, solo parzialmente fedele, della nozione di "accountability"): non si tratta solo di assicurare la conformità delle attività di trattamento con il regolamento e nel dare prova solo di questo adempimento, ma ad esempio "dimostrare l'efficacia delle misure", con un atteggiamento proattivo e sostanziale. Responsabilità come chiara individuazione dei soggetti chiamati a svolgere un ruolo sostanziale nei trattamenti, ma anche come effettività del controllo che compete in particolare al Garante della privacy: un controllo che, mutuando un modello che avuto buon esito nel campo dei contratti pubblici, dovrebbe assumere forme per quanto possibile collaborative (ma non co-decisionali) nella fase dell'emergenza. Responsabilità in termini di pieno controllo giurisdizionale sulle forme di trattamento e sulla loro legittimazione, specie decorso il momento emergenziale.

6. Proteggere la privacy nell'emergenza

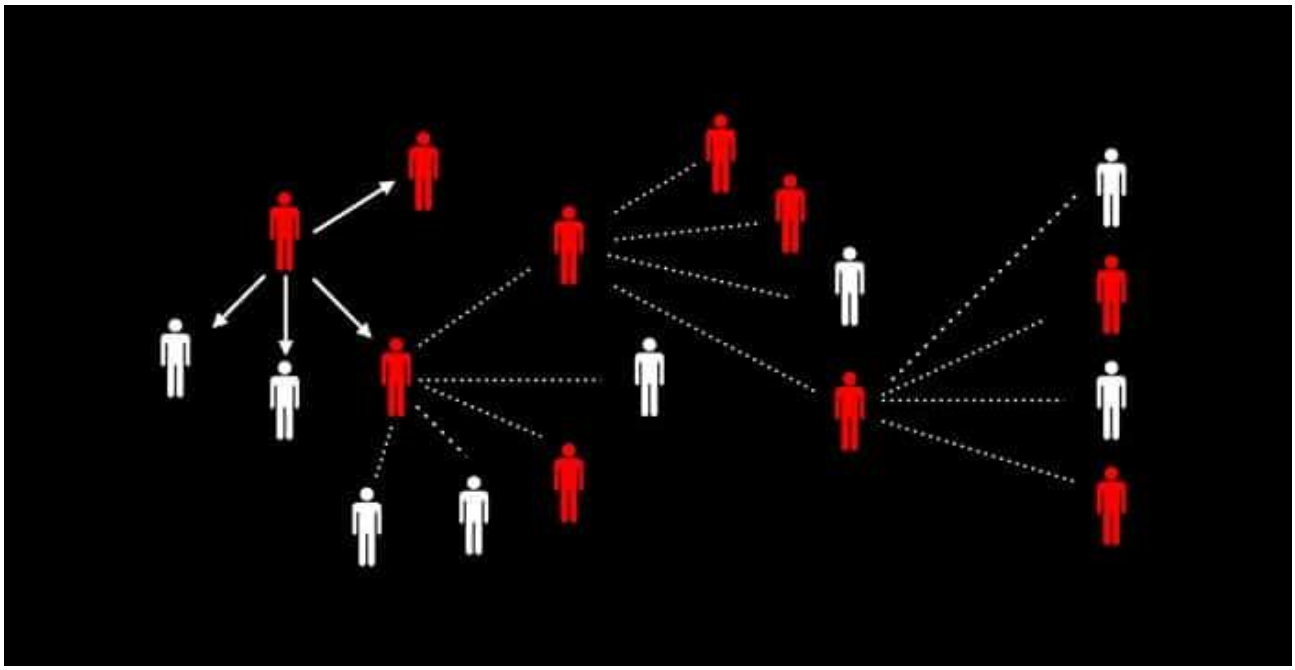
Trovandoci in circostanze eccezionali, in un momento in cui disposizioni di varia fonte e natura impongono limiti importanti alle nostre libertà per condivisibili e meritorie esigenze di salute, individuali e collettive, non pare ragionevole, né utile per i diversi interessi in gioco, mettere in campo contrapposizioni tra protezione dei dati e governo della pandemia.

D'altra parte, come si è detto in apertura, il diritto alla protezione dei dati di carattere personale "non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità" Considerando 4 del citato Regolamento UE 2016/679): il sistema della protezione dei dati personali presenta al suo interno meccanismi e soluzioni di flessibilità che lo rendono idoneo a porre una griglia di principi validi anche in queste fasi eccezionali.

Perché le condizioni di eccezione non divengano stato di eccezione, è necessario che l'ordinamento operi modulando e bilanciando i diritti e gli interessi tenendo in debita considerazione la situazione straordinaria che stiamo vivendo. Con intelligenza, la privacy va protetta accettandone la compressione, ma richiedendo che questa avvenga nel rispetto di principi di legalità, proporzionalità e responsabilità, forse in grado di traghettarci attraverso questi mesi difficili che abbiamo di fronte.

Il tutto senza banalizzazioni e semplificazioni (come ricondurre le esigenze di privacy a "fisime"), ma anche senza arroccamenti controproducenti non solo per le legittime esigenze di contrasto della pandemia, ma anche della stessa protezione dei dati. Il momento che stiamo vivendo richiede e suggerisce robuste parentesi entro cui circoscrivere e contenere lo stato di eccezione. Con le dovute cautele, ma senza dimenticare il fatto che il terrore del tiranno che spesso aleggia dietro alcune letture delle potenzialità dei sistemi di tracciamento non è stato sin qui accompagnato da un corrispondente allarme rispetto alle forme di profilazione e tracciamento che da tempo gli operatori privati dei servizi di comunicazione hanno predisposto e sviluppato sulla base del nostro irriflesso consenso.

Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19



"Immuni" è stata selezionata, tra le oltre 300 soluzioni proposte da privati, società ed enti, per il tracciamento dei positivi al coronavirus tramite procedure e figure contrattuali atipiche. Il procedimento avviato con una fast call for contribution adottata dai Ministeri dello Sviluppo Economico, della Salute e per l'Innovazione Tecnologica e la Digitalizzazione sembra essersi concluso con un'ordinanza del Commissario straordinario su richiesta del Presidente del Consiglio dei Ministri. Il rapporto è stato configurato poi come un contratto di appalto gratuito privo della necessaria sinallagmaticità. Inoltre, la violazione del principio di legalità, determinata dall'assenza di una base giuridica legale, non trova rimedio neppure in una congrua motivazione della scelta del Commissario in ordine ai vantaggi e ai requisiti dell'app.

Lo scorso 23 marzo, il Ministro dello Sviluppo economico, il Ministro della Salute e il Ministro per l'innovazione tecnologica e la digitalizzazione hanno indetto una ***fast call for contribution***, chiusa il 26 marzo 2020, rivolta a privati, società ed enti, diretta a individuare le migliori soluzioni digitali e tecnologiche disponibili per il **monitoraggio "attivo" del rischio di contagio** da Covid-19.

Il 31 marzo 2020, il Ministro per l'innovazione tecnologica e la digitalizzazione ha, quindi, nominato il "***Gruppo di lavoro data-driven per l'emergenza Covid-19***" con il compito di effettuare attività di analisi e studio degli impatti del fenomeno epidemiologico in atto, nonché di procedere in tempi rapidi alla valutazione delle proposte formulate dai partecipanti alla *fast call*, al fine di selezionare la proposta più efficace e idonea a essere implementata in tempi rapidi a livello nazionale.

All'esito delle valutazioni effettuate dal Gruppo di lavoro e comunicate al Ministro per l'innovazione tecnologica e la digitalizzazione, la soluzione denominata "**Immuni**", proposta dalla società **Bending Spoons S.p.a.** è stata ritenuta 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 (Pan-European Privacy-Preserving Proximity Tracing,** realizzato da un gruppo di 130 scienziati e 32 fra aziende e istituti di ricerca di 8 Paesi, tra cui la Fondazione ISI di Torino, sul quale stanno convergendo Francia e Germania), nonché per le garanzie che offre in ordine al **rispetto della *privacy***.

A seguito della richiesta del Presidente del Consiglio dei Ministri di procedere rapidamente a dare attuazione alla proposta di implementazione del sistema di *contact tracing* digitale, con l'ordinanza n. 10/2020, del 16 aprile scorso, il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19 ha disposto di procedere alla stipula del contratto di concessione gratuita della licenza d'uso sul *software* di *contact tracing* e di appalto di servizio gratuito con la società Bending Spoons S.p.a.

la procedura e lo strumento utilizzati dal Commissario per acquisire l'app, nonostante l'urgenza, lasciano alcuni dubbi, in ordine all'atipicità degli strumenti utilizzati e all'assenza di una congrua motivazione in ordine ai criteri di scelta e alle effettive caratteristiche dell'app.

Innanzitutto, il Commissario straordinario ha sottoscritto con la Bending Spoons S.p.A., titolare dell'app, un contratto di concessione gratuita della licenza d'uso sul software di *contact tracing* e di appalto di servizio gratuito. È compatibile la gratuità con la configurazione del rapporto in termini di appalto, contraddistinto dalla necessaria onerosità e sinallagmaticità delle prestazioni? Il rapporto sembrerebbe piuttosto configurabile come una sponsorizzazione (se si valorizza il ritorno di immagine e la possibilità di acquisire vantaggi nella fase di sviluppo e attuazione dell'app), ovvero una donazione (nei limiti della possibilità di donazione di cosa futura).

In secondo luogo, non appare chiaro l'*iter* procedimentale utilizzato. La stipula del contratto, infatti, è presentata nell'Ordinanza del Commissario Straordinario come conclusione della *fast call* indetta dai Ministeri dello Sviluppo Economico, della Salute e per l'Innovazione Tecnologica della Salute. Tuttavia, il Commissario Straordinario non è mai citato negli atti della procedura e la fast call non prevedeva che le soluzioni tecnologiche sarebbero state acquisite a titolo gratuito.

In ultimo, non sono state esplicitate le motivazioni in virtù delle quali tra tutte le app e i software proposti sia stato scelto proprio Immuni, che tra l'altro non sembra rispettare tutti i criteri individuati nell'avviso pubblicato. L'obiettivo dichiarato nella *fast call*, pubblicata sul sito del Ministero, era di "*individuare soluzione tecnologiche **già realizzate***". Tra i requisiti e i criteri per la partecipazione, lo stesso Ministero aveva specificato che sarebbero state considerate soltanto "*proposte **già realizzate e disponibili per l'implementazione** in tempi estremamente brevi e compatibili con l'emergenza*".

In particolare, secondo quanto chiarito dal Ministro Paola Pisano, in audizione alla Camera, l'app, secondo quanto previsto dalle raccomandazioni dell'Ue, avrebbe dovuto essere connotata da requisiti specifici, quali la **volontarietà** della partecipazione, la **gestione pubblica e open source** del sistema integrato di *contact tracing*, **la suscettibilità ad essere revisionato** da qualunque soggetto indipendente, l'**anonimità dei dati trattati** e la **minimizzazione** dei **rischi di reidentificazione**.

Eppure, nell'ordinanza del Commissario non è fornito alcun dettaglio sull'effettiva disponibilità dell'app (che anzi necessiterà di uno sviluppo informativo per consentire la messa in esercizio e di una fase di sperimentazione), sull'efficacia concreta della soluzione tecnologica scelta (che affinché possa funzionare – secondo le stime del governo – deve essere scaricata e usata da almeno il 60%

della popolazione), sul rispetto del **principio di minimizzazione** alla **mappatura** (che si auspica vastissima), ovvero sulla **cessione dei dati,** trattati e memorizzati – pare – su un unico ***server* ministeriale**.

La crisi epidemiologia determinata dalla propagazione del Covid-19 costituisce senz'altro un'ipotesi imprevedibile di estrema urgenza suscettibile di giustificare il ricorso a procedure in deroga ai principi concorrenziali, come del resto chiarito dalla Commissione con gli Orientamenti sull'utilizzo del quadro in materia di appalti pubblici nella situazione di emergenza connessa alla crisi della Covid-19.

Tuttavia la compressione dei principi di trasparenza, imparzialità e *par condicio* degli operatori deve essere, comunque, proporzionata e ampiamente giustificata soprattutto se si considera che, nonostante il Governo, con decretazione d'urgenza, abbia introdotto strumenti *ad hoc* per la fornitura di beni e servizi informatici, la procedura utilizzata dal Commissario non trova alcun fondamento giuridico nella normativa vigente.

La scelta dell'operatore, anche al fine di recuperare il *vulnus* al principio di legalità, avrebbe dovuto essere quindi comunque motivata adeguatamente in ordine alla procedura seguita, al rispetto dei requisiti individuati nella *fast call* e ai criteri che hanno determinato l'individuazione dell'app Immuni, soprattutto in considerazione dei possibili vantaggi pubblicitari, tecnologici e di posizionamento del mercato che potrebbero conseguire all'aggiudicazione.

Published on marzo 27th, 2020 | *by dirittodellinformatica.it*

Contact tracing e tutela della Privacy al tempo del Covid-19: è giusto controllare gli spostamenti dei cittadini attraverso la rete cellulare?

La drammatica emergenza sanitaria di questi mesi, scaturita dalla rapida diffusione del virus Covid-19, ha radicalmente inciso sulle vite dei cittadini di tutto il mondo e continua a condizionarle pesantemente. La necessità di limitare il più possibile la diffusione del contagio, e quindi di evitare il sovraccarico delle strutture sanitarie, ha richiesto misure sempre più stringenti e strumenti di controllo più efficaci per vigilare sulla loro attuazione. Tra questi ha fatto discutere la scelta della Regione Lombardia, area drammaticamente travolta dal c.d. Coronavirus. La Regione ha chiesto e ottenuto dai principali operatori di telefonia mobile dati in grado di tracciare gli spostamenti dei possessori di telefoni cellullari. Questa scelta, giustificata dall'aggravarsi dell'emergenza, ha comunque suscitato diverse perplessità, specie perché sembra replicare in scala ridotta la sorveglianza imposta dai governi cinese e sudcoreano.

Il telefono cellulare ha ereditato il suo nome proprio dalla rete cellulare che permette la telecomunicazione. Semplificando, questa rete si basa sulla suddivisione del territorio in piccole aree chiamate "celle", ciascuna delle quali è collegata e servita da una diversa stazione di telecomunicazione. Quando uno smartphone si sposta, questo varca gli invisibili confini delle celle, rendendo possibile la localizzazione del suo possessore.

Questa tecnica, assieme al riconoscimento facciale dei cittadini e all'adozione di applicazioni mobile in grado di indicare e segnalare i potenziali contagiati, rappresentano solo alcuni dei possibili impieghi della tecnologia per contrastare la diffusione del Coronavirus.

IL SISTEMA EUROPEO DI TUTELA DELLA PRIVACY ALLA PROVA DELL'EMERGENZA

Simili misure, che potrebbero presentare diverse utilità nell'attuale contesto emergenziale, comportano diversi rischi dal punto di vista della tutela dei dati personali dei soggetti interessati. Se è pur vero che la pandemia ha carattere globale e coinvolge tutti gli Stati ad ogni latitudine, diverse sono le caratteristiche ed i principi dei singoli ordinamenti giuridici che devono affrontare l'emergenza. Nell'Occidente democratico e liberale, ed in particolare in Europa, si pone il problema dell'attento bilanciamento tra la tutela della salute pubblica e le libertà individuali e, tra queste, la tutela della privacy.

Come noto, il diritto dell'Unione europea fonda il suo meccanismo di tutela della privacy sul Regolamento n. 679/2016, il c.d. GDPR, completato dalla normativa attuativa dei singoli Stati

membri e dalla vigilanza delle singole Autorità di controllo. Tale complesso normativo, generalmente ritenuto un sistema in grado di offrire una efficace tutela alla privacy dei cittadini europei, è sottoposto ora alla notevole pressione dell'attuale emergenza, tale da creare diversi rischi alla sua tenuta complessiva.

COVID-19 E TRATTAMENTO DEI DATI: LA DICHIARAZIONE DEL COMITATO EUROPEO

Il Comitato europeo per la Protezione dei Dati, l'organismo garante della corretta applicazione del GDPR, ben consapevole di tale problema, ha recentemente pubblicato una specifica Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia Covid-19. L'incipit di questo documento è chiaro: «le norme in materia di protezione dei dati (come il regolamento generale sulla protezione dei dati) non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus». Tuttavia, il Comitato si affretta a precisare che «anche in questi momenti eccezionali, titolari e responsabili del trattamento devono garantire la protezione dei dati personali degli interessati». Si pone quindi la necessità di tutelare la salute pubblica garantendo comunque la liceità del trattamento dei dati personali e la generale tutela della Privacy.

Il GDPR, in effetti, prevede specificamente la base giuridica sulla quale fondare il trattamento dei dati suddetti in situazioni emergenziali. Il Considerando 46 del Regolamento indica esplicitamente il controllo dell'evoluzione delle epidemie e della loro diffusione come uno dei presupposti per i quali il trattamento di dati personali deve essere ritenuto lecito. Inoltre, l'art. 9, co. 2, lett. i, del GDPR prevede, come deroga al divieto di trattamento di alcuni particolari categorie di dati, l'evenienza che questo sia «necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici […]». Il Comitato evidenzia che, con riferimento ai dati delle telecomunicazioni e quelli relativi all'ubicazione degli interessati, il trattamento in linea di principio potrebbe essere lecito se si basasse su dati resi anonimi o per i quali i singoli avessero prestato il loro consenso. Quindi, con riferimento all'utilizzo dei dati personali relativi ai telefoni cellulari e alla geolocalizzazione degli interessati, il Comitato invita le autorità pubbliche a trattare tali dati in forma anonima, così da impedire la successiva re-identificazione delle persone. Si deve infatti precisare che la normativa atta a garantire la privacy non si applica in caso di dati anonimizzati. D'altra parte, se non fosse possibile elaborare solo dati anonimi, il Comitato richiama quanto disposto dall'art. 15 della direttiva 2002/50/CE, c.d. Direttiva e-Privacy. Tale disposizione consente agli Stati membri di implementare misure legislative eccezionali per salvaguardare la sicurezza pubblica, ma ciò è possibile solo se tale legislazione si basa su misure necessarie, adeguate e proporzionate. Queste devono comunque essere «soggette al controllo giurisdizionale della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo. In presenza di situazioni di emergenza, le misure in questione devono essere rigorosamente limitate alla durata dell'emergenza». Potrebbero dunque essere ammissibili tecniche di localizzazione ed applicazioni mobile con lo scopo di fornire alle autorità sanitarie dati utili per il contenimento del contagio. Devono, però, sempre essere privilegiate tecniche in grado di garantire l'anonimato e, solo qualora ciò non fosse possibile, bisognerebbe predisporre un sistema di garanzie adeguate, quali il diritto ad un ricorso giurisdizionale.
In ogni caso, gli Stati membri devono agire nel rispetto del principio di proporzionalità e favorire l'impiego di tecniche meno intrusive possibili: solo così facendo potrà essere garantita la tutela della privacy anche nel delicato contesto attuale.

L'INTERVENTO DEL GARANTE DELLA PRIVACY

Sul c.d. contact tracing digitale e sui rischi che questo può comportare per le libertà individuali dei cittadini, è stata interpellata anche la nostra Autorità Garante per la protezione dei dati personali. Nei numerosi interventi pubblici degli ultimi giorni, il Garante ha confermato la possibilità di ricorrere alla mappatura e al tracciamento dei soggetti entrati in contatto con persone contagiate nonché all'utilizzo della rete cellulare per un controllo generalizzato degli spostamenti. Non esisterebbero, pertanto, divieti assoluti all'impiego della tecnologia in tal senso: ciononostante devono essere valutate modalità opportune e proporzionate alle esigenze di prevenzione. Lo stato d'emergenza potrebbe richiedere inevitabilmente la compressione di alcuni diritti e alcune libertà in nome della tutela della salute pubblica ed individuale. Tuttavia, la disciplina a tutela della privacy non deve essere ritenuta solo un mero e superficiale ostacolo, essendo uno degli aspetti che più caratterizzano l'ordinamento giuridico italiano ed europeo. Trasparenza, proporzionalità e coerenza tra obiettivo perseguito e strumenti utilizzati devono rappresentare le linee guida dell'Esecutivo nel fronteggiare l'emergenza Coronavirus.

Il Garante, peraltro, ha auspicato che l'implementazione di ulteriori tecniche di contact tracing, che potrebbero riguardare milioni di cittadini, venga prevista da una normativa ad hoc. A tal proposito, l'Autorità ha sollecitato l'emanazione di un Decreto Legge, che, seppure adottato dal Governo, verrebbe successivamente sottoposto ad un profondo e reale confronto parlamentare, ritenendolo lo strumento normativo più adeguato per la delicatezza dei temi in questione. Anche in prospettiva di tutela del diritto alla privacy, viene quindi evidenziata l'inadeguatezza di atti meramente amministrativi, come i decreti ministeriali e i d.p.c.m., per la predisposizione di un sistema di tecniche preventive sicuramente utili, ma potenzialmente pericolose per altri diritti fondamentali dei cittadini.

Redazione Diritto dell'informatica

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

OSSERVATORIO EMERGENZA COVID-19
PAPER – 28 MARZO 2020

La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia

di Domenico De Falco e Maria Laura Maddalena
Magistrati di Tribunale Amministrativo Regionale

La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia *

di Domenico De Falco e Maria Laura Maddalena
Magistrati di Tribunale Amministrativo Regionale

Sommario: Premessa. **1.** Il quadro internazionale sulle politiche di "sorveglianza attiva" nel contenimento dell'epidemia Covid-19. **2.** La situazione in Italia con particolar riferimento alle linee guida del Ministero della salute per l'effettuazione dei test per covid 19. **3.** Le criticità emerse e le possibili soluzioni. **4.** L'uso di strumenti di data tracing e di intelligenza artificiale per l'individuazione dei contatti dei soggetti positivi e la tutela della privacy. **5.** Compatibilità delle misure di sorveglianza attiva con il quadro costituzionale. **6.** L'applicazione del principio di proporzionalità nella adozione delle misure di contenimento del virus.

Premessa

Questo breve scritto vuole tentare di offrire una chiave di lettura, dal punto di vista del giurista, di due tematiche tra loro strettamente connesse e molto dibattute a livello scientifico e politico: la politica dei test per covid 19 e l'uso di strumenti di intelligenza artificiale per concretizzare per sistema di sorveglianza attiva sui contatti dei soggetti risultati positivi, secondo uno schema che – in modo semplicistico- definiremo "modello coreano".

Gli autori, in quanto giudici amministrativi, non intendono certo addentrarsi nelle controverse questioni scientifiche sottese a questi temi, ma – cercando di mettere a frutto la loro esperienza come giudici dell'azione amministrativa, anche in caso di sindacato sulla discrezionalità tecnica– proprio nel momento in cui da più parti si richiede una rivisitazione dell'atteggiamento del Governo su questi temi[1], ritengono di poter offrire il loro contributo, senza pretese di esaustività, alla luce del quadro normativo vigente e delle indicazioni fornite dagli organi ufficiali (prima fra tutte l'OMS), per fornire spunti di riflessione in ordine alla adozione di decisioni così delicate ed importanti da parte delle autorità preposte.

* Paper non sottoposto a referaggio.

[1] Si pensi alla recentissima richiesta del Presidente della Giunta delle regione Lombardia al ministero di rivedere le linee guida sui test per covid 19, alle istanze dei 18 sindaci dei comuni dell'interland milanese, alle numerose sollecitazioni da parte di medici del territorio e di illustri esperti tutte volte a sollecitare un diverso approccio governativo su tali temi.

1. Il quadro internazionale sulle politiche di "sorveglianza attiva" nel contenimento dell'epidemia Covid-19.

Contemporaneamente al drammatico aggravarsi della situazione in Italia, la Cina e la Corea del Sud, che pure precedevano l'Italia quanto a diffusione dell'infezione, sembrano essere uscite dal tunnel, con un numero di nuovi infetti oramai nullo o poco significativo.

Secondo quanto è dato di desumere, tale successo nel contenimento del virus deriva non solo dalle misure di distanziamento sociale, adottate peraltro anche nel nostro Paese, ma da quelle che vengono definite misure di "sorveglianza attiva" ovvero di isolamento dei focolai del virus, attraverso il tracciamento dei contatti dei soggetti positivi e la sottoposizione di essi ai test anche se trovati asintomatici, procedendo così a ritroso fino a definire una platea di soggetti, sicuramente molto numerosi, da mettere in quarantena e ai quali praticare i tamponi[2]. E' da chiarire subito che tali misure non prevedono di praticare test di massa a tappeto, cosa che sarebbe insostenibile oltre che inutile, ma di effettuare i test ai contatti dei contagiati e ad alcune categorie di soggetti più a rischio di essere portatori di infezione (sanitari, assistenti degli anziani, personale delle case di riposo, ecc.).

Tali modalità sono state seguite anche dalla Cina, al fine di contenere il contagio fuori dell'area della provincia dell'Hubei. Ed infatti, raccomandazioni volte a sostenere tali misure emergono proprio dal rapporto della missione congiunta OMS-Cina sulla malattia del Coronavirus (covid-19), del 16-24 febbraio 2020, reso pubblico il 27 febbraio 2020[3]). A pag. 21, tra le raccomandazioni più importanti per i Paesi con casi di Covid-19 importati, si legge al punto 2: "*Dare priorità alla ricerca attiva di casi, con immediata somministrazione di test e isolamento, tracciamento accurato dei contatti e quarantena rigorosa per i contatti stretti*;" al punto 4: "*Espandere immediatamente la sorveglianza per rilevare le catene di trasmissione COVID-19, testare tutti i pazienti con polmoniti atipiche, conducendo lo screening in alcuni pazienti con malattie respiratorie alle vie aeree superiori e/o recente esposizione a COVID-19, e aggiunta di test per il virus COVID-19 ai sistemi di sorveglianza esistenti*".

Inoltre, le ultime linee giuda OMS del 13 marzo 2020 (Considerations in the investigation of cases and clusters of COVID-19 Interim guidance 13 March 2020[4]) espressamente prevedono che debba essere effettuato il tracciamento di tutti i contatti dei soggetti risultati positivi, da due giorni prima dell'insorgere dei sintomi, e che i test debbano essere eseguiti su tutti i contatti dei pazienti risultanti positivi, a prescindere se essi abbiano sintomi. In particolare, dette linee guida prevedono che il test debba, comunque, sempre effettuato alla fine della quarantena.

[2] Cfr. il sito del ministero della salute coreano, in inglese, dove si riporta giorno per giorno lo sviluppo delle attività di tracciamento dei link epidemiologici https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030

[3] https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf

[4] https://www.who.int/publications-detail/considerations-in-the-investigation-of-cases-and-clusters-of-covid-19

Tale approccio, fondato su di uno sforzo di sorveglianza attiva da parte delle istituzioni pubbliche che "ricercano" il virus e lo isolano, è stato ancora fortemente raccomandato pubblicamente dal Direttore Generale dell'Organizzazione Mondiale della Sanità che nella dichiarazione del 16 marzo scorso ha invitato tutti i Paesi a moltiplicare i test da praticare, secondo l'OMS, in misura crescente e con risposte sempre più rapide.

Secondo quanto ha dichiarato al Washinton Post Reinhard Busse, capo del dipartimento per la tutela della salute presso l'università di Berlino, la medesima strategia è stata da subito adottata dalla Germania, identificando e isolando le aree del contagio nella popolazione, come dimostra lo scarso tasso di letalità tra gli ammalati. Il metodo tedesco prevede il tracciamento di tutti i contatti dei positivi, la somministrazione del test e l'isolamento[5]. La Francia ha, qualche giorno fa, dichiarato di voler anch'essa applicare tale strategia e in questa direzione si muove anche la Regione Veneto.

2. La situazione in Italia con particolar riferimento alle linee guida del Ministero della salute per l'effettuazione dei test per covid 19.

In Italia, tuttavia, non risulta che le ultime raccomandazioni indicate dall'OMS per quanto riguarda le più incisive modalità di sorveglianza attiva e la politica del test siano pienamente seguite, in quanto i test sono somministrati ai soli soggetti gravemente sintomatici e che abbiano avuto comprovati contatti con soggetti infetti. E ciò anche nelle zone del Centro-Sud di Italia in cui il contagio non è ancora molto diffuso e potrebbero essere quindi più facilmente identificate e isolate le catene di contagio.

Sul punto, infatti, risulta ancora vigente la Circolare del Ministero della Salute, del 9 marzo 2020[6] che continua a richiedere per l'effettuazione di un test per la ricerca del covid-19 (il c.d. caso sospetto) che il paziente presenti una infezione respiratoria acuta grave non altrimenti spiegabile oppure un'infezione acuta anche non grave unitamente a possibili contatti con soggetti positivi o in aree in cui è segnalata la diffusione locale del virus. Pertanto in Italia il solo fatto che vi siano certi "contatti" con soggetti infetti non è ritenuta condizione da sola sufficiente per eseguire il test.

In senso difforme, come accennato, sembrano porsi tuttavia le indicazioni del citato report della missione Cina OMS del febbraio 2020, secondo cui la sintomatologia e i contatti con soggetti positivi sono considerati come condizioni alternative e non necessariamente cumulative ("*conducting screening in some patients with upper respiratory illnesses and/or recent COVID-19 exposure*" cfr. pag. 21, punto 4).

[5] Al momento in cui si scrive, la Germania ha già superato l'Italia nel numero di test effettuati, oltre 400.000, pur avendo un numero assai inferiore di contagi e pur essendo il contagio sviluppatosi solo molti giorni dopo rispetto all'Italia.
[6] http://www.trovanorme.salute.gov.it/norme/renderNormsanPdf?anno=2020&codLeg=73669&parte=1%20&serie=null

In Italia, invece, dopo i primi giorni dalla scoperta del primo caso certificato di covid-19 a Codogno, in cui si è seguita la via del tracciamento dei contatti dei positivi con somministrazione di test anche a soggetti asintomatici, dal 27 febbraio 2020, le autorità sanitarie hanno annunciato che i test sarebbero stati effettuati solo sui pazienti sintomatici nonché che fossero stati in contatto con le persone positive, con un criterio, come visto, previsto dalla Circolare 9 marzo 2020 del Ministero della Sanità tutt'ora vigente.

Tale decisione sarebbe stata adottata perché il rischio di contagio sarebbe marcatamente più basso per i soggetti asintomatici oltre che al fine di ridurre il panico e proteggere l'immagine del Paese, in un momento di rapidissima crescita dei dati dei contagiati in Italia rispetto al resto dell'Europa e dell'occidente [7]. Essa si fonda sulle risultanze del "Documento relativo ai criteri per sottoporre soggetti clinicamente asintomatici alla ricerca d'infezione da SARS-CoV-2 attraverso tampone rino-faringeo e test diagnostico", redatto in data 26 febbraio 2020 dal gruppo di lavoro permanente del Consiglio superiore di sanità circa il ruolo degli asintomatici nella dinamica della diffusione epidemica di COVID-19.

Tuttavia, dopo la redazione di tale rapporto, in molti studi è stata evidenziata la circostanza che anche i soggetti asintomatici possano trasmettere il virus. Si pensi ad esempio al recentissimo studio cinese *Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus* (SARS-CoV2)[8] secondo il quale l'86% di tutti i positivi non sono stati documentati e che le infezioni non documentate (che avevano sintomi lievi, limitati o assenti), sebbene meno contagiose, sono state la fonte di trasmissione per il successivo 79% dei casi certi.

Inoltre, anche lo studio eseguito proprio in Italia in relazione al comune di Vo', sotto la supervisione di Andrea Crisanti, direttore dipartimento di medicina molecolare e professore di epidemiologia e virologia Università di Padova, conferma, secondo il professore ordinario di Immunologia clinica dell'Università di Firenze Sergio Romagnani, che "*la grande maggioranza delle persone che si infetta, tra il 50 e il 75%, è completamente asintomatica, ma rappresenta comunque una formidabile fonte di contagio*" [9]).

D'altro canto, anche l'ECDC (*European Centre for Disease Prevention and Control*) ha affermato che nel corso dell'infezione, il virus è stato identificato in campioni del tratto respiratorio 1-2 giorni prima della comparsa dei sintomi.

[7] cfr. sole 24 ore, 27 febbraio 2020, "La giravolta comunicativa del coronavirus, meno tamponi e contare solo i casi gravi" di Nicola Barone e Marzio Bartoloni

[8] https://science.sciencemag.org/content/early/2020/03/13/science.abb3221

[9] da https://www.repubblica.it/salute/medicina-e-ricerca/2020/03/16/news/coronavirus_studio_il_50-75_dei_casi_a_vo_sono_asintomatici_e_molto_contagiosi-251474302/ ; cfr. anche intervista al prof. Andrea Crisanti, direttore dipartimento di medicina molecolare e professore di epidemiologia e virologia Università di Padova del 22 marzo 2020 su www.globalist.it

Ciò nonostante, anche la recentissima circolare 20 marzo 2020 sul rintraccio dei contatti in ambito di sorveglianza sanitaria del ministero continua a far riferimento al documento redatto in data 26 febbraio 2020 dal gruppo di lavoro permanente del Consiglio superiore di sanità che esclude la necessità di testare gli asintomatici, pur riconoscendo però la necessità di effettuare il tracciamento dei contatti dei positivi fino a 2 giorni prima del manifestarsi dei sintomi (così implicitamente ammettendo la possibilità che soggetti al momento asintomatici possano infettare).

3. Le criticità emerse e le possibili soluzioni.

L'effetto della decisione di somministrare i test solo ai gravemente sintomatici, oltre a non contribuire a limitare la diffusione dell'epidemia, ha portato anche ad una evidente sottovalutazione del numero reale dei contagiati, come ammesso recentemente anche dallo stesso Capo del Dipartimento della Protezione civile, Borrelli, il quale ha dichiarato che il numero dei contagiati potrebbe essere ragionevolmente il decuplo di quelli rilevati, in linea del resto con l'alto tasso di mortalità registrato in Italia rispetto al numero ufficiale dei contagiati, che non appare coerente con le statistiche mondiali. Inoltre, la non idoneità del criterio di effettuazione dei test finora seguito a conteggiare il reale numero dei contagiati determina ora evidenti criticità nella verifica circa i reali effetti delle misure adottate. Infine, non è da sottovalutare l'effetto negativo sulla tempestività del ricorso alle cure appropriate che viene rimandato fino a che la malattia non assuma caratteri di evidente gravità, giacché solo dopo gli esiti del test possono attivarsi i protocolli per la cura del Civid-19, con evidenti ritardi nella gestione di situazioni spesso critiche.

Inoltre, nonostante l'applicazione di misure di tracciamento dei contatti, la circostanza che i tamponi vengano effettuati solo ai gravemente sintomatici limita il numero di persone che possono essere rintracciate ai soli contatti del primo soggetto testato positivamente al virus, senza estendersi ai contatti di ulteriori soggetti che vengano rintracciati e che potrebbero essere positivi, ma che non mostrando (al momento) sintomi, non vengono testati.

Tale approccio ha riguardato anche i sanitari ai quali non vengono praticati i test, se non quando vi siano gravi sospetti di positività (e ciò nonostante il personale sanitario rappresenti circa il 10% dei contagiati totali) e non risulta in questo momento che sia stato adottato uno specifico protocollo sul punto, anche se vi sono state su questo tema recentissime aperture da parte di alcune autorità sanitarie.

Di contro, il Rapporto sulla missione congiunta OMS -Cina del 16-24 febbraio 2020 a pag. 11, lett. a), sottolineava l'importanza di prestare grande attenzione alla prevenzione dell'infezione tra i sanitari mediante misure di sorveglianza. Le linee guida OMS del 13 marzo 2020, inoltre, espressamente richiedono che tutti gli operatori sanitari venuti in contatto con un soggetto positivo, in assenza di adeguate protezioni, siano testati, a prescindere dal manifestarsi dei sintomi.

E' evidente, infatti, che la diffusione del contagio tra i sanitari non solo mina ulteriormente le capacità di risposta del sistema sanitario, colpendo proprio i soggetti che sono in prima linea nell'attuale "guerra" sanitaria, ma soprattutto trasforma gli ospedali e gli studi professionali dei medici di famiglia in focolai dell'infezione, come avvenuto inizialmente a Codogno e come sta avvenendo tutt'ora in molti altri casi. Analogo gravissimo problema si pone per le case di riposo, i conventi, le carceri e tutti i luoghi in cui vi sono forme di convivenza di comunità di persone. Probabilmente, per il personale sanitario e soprattutto ospedaliero, al fine di evitare che essi siano vettori di contagio anche delle rispettive famiglie, potrebbe essere opportuno prevedere la possibilità di risiedere in luoghi diversi delle proprie abitazioni (in questa direzione va la recente iniziativa della Regione Toscana e delle ASL locali per il reperimento, tra le strutture turistiche ricettive, di alloggi da destinare a residenza del personale sanitario).

Né sembra possa essere opposto che l'incremento del numero di test conseguente ad un mutamento delle linee guida nella indicazione del "caso sospetto" non sarebbe economicamente sostenibile o che non vi sarebbero abbastanza reagenti o laboratori accreditati. Infatti, potrebbe comunque farsi ricorso ad ulteriori strutture, come peraltro già previsto dalla nuova circolare del 20 marzo 2020 del ministero della salute[10], la quale pure opportunamente e finalmente prevede (anche se solo per le regioni in cui il contagio sia diffuso) che non sia necessario effettuare sempre anche il doppio test, a meno che non si tratti di campioni in cui il risultato è difficilmente interpretabile. Tale pratica, da tempo auspicata anche dal mondo scientifico, dovrebbe essere estesa a tutto il territorio nazionale, al fine di consentire l'effettuazione di un numero almeno doppio di test con le stesse risorse, soprattutto se, come si legge su La Repubblica del 26 marzo 2020, fosse vero che le scorte di reagenti stanno per finire (articolo di Michele Bocci: "*Allarme tamponi. Dobbiamo farne di più ma mancano i test e le scorte di reagenti stanno finendo*").

Va rilevato infine che in data 27 marzo 2020 è stato adottato da un giudice civile del Tribunale di Santa Maria Capua Vetere un provvedimento di urgenza volto ad imporre l'effettuazione di un test per covid 19 ad un soggetto non rientrante nelle linee giuda ministeriali, in applicazione del primario diritto costituzionale alla salute; ciò pare confermare l'opportunità di dare celere attuazione alle misure di sorveglianza attiva indicate dall'OMS, anche al fine di evitare che vi siano decisioni giudiziali assunte caso per caso su questo delicato tema.

[10] http://www.normativasanitaria.it/jsp/dettaglio.jsp?id=73714

4. L'uso di strumenti di data tracing e di intelligenza artificiale per l'individuazione dei contatti dei soggetti positivi e la tutela della privacy.

Interpellato sulla possibilità di applicare i modelli coreano e cinese di sorveglianza attiva nella conferenza stampa del 23 marzo scorso presso la Protezione Civile, il direttore dell'Istituto Superiore della Sanità ha espressamente affermato che la tracciatura dei positivi attraverso sistemi GPS o satellitari potrebbe incontrare difficoltà in Italia, a differenza di altri paesi come Corea e Cina, per problemi di carattere "giuridico" anche connessi alla tutela della privacy.

Tali perplessità, ad avviso di chi scrive, possono essere facilmente superate.

In primo luogo nulla impedirebbe di somministrare un test ad una persona che volontariamente lo richieda per aver avuto contatti stretti (e comprovati) con soggetti positivi, pur non mostrando i sintomi di una infezione respiratoria acuta. Ed infatti, l'art. 14 del DL 9 marzo 2020, n. 14 prevede a questo fine modalità semplificate per la prestazione del consenso.

Tale articolo, inoltre, prevede un'ampia deroga alla disciplina del trattamento dei dati personali e della riservatezza, proprio in favore delle autorità sanitarie, le quali sono dal 9 marzo autorizzate a effettuare trattamenti dei dati riservati e quindi a scambiarsi informazioni relative ai nominativi delle singole persone, per finalità connesse al contenimento della diffusione dell'infezione incluse, deve ritenersi, quelle di attuare meccanismi di sorveglianza attiva in linea con le raccomandazioni dell'OMS.

La deroga in parola appare perfettamente coerente rispetto al quadro costituzionale e alla disciplina nazionale ed europea in materia di privacy vigente da tempo nel nostro ordinamento. Infatti, il nostro Codice della privacy (art. 2 sexies) e il diritto dell'Unione europea, in particolare agli artt. 9, comma 2, e 23 del GDPR, consentono limitazioni alla privacy per motivi di sanità pubblica (v. anche Considerando n. 73 del GDPR).

In tale contesto, anche le misure di tracciamento e isolamento dei focolai di infezione (oggi mediante il ricorso all'intelligenza artificiale) erano già ammesse dal "Piano Nazionale di Preparazione e Risposta ad una Pandemia Influenzale" di cui il nostro Paese è dotato fin dal 2003, ma che non risulta essere stato applicato per l'emergenza Covid-19; tale piano, nel prevedere una dettagliata sequenza di azioni da intraprendere e nell'individuare livelli e di competenze decisionali, include l'adozione di modelli anche mediante l'impiego di algoritmi di contenimento e mappatura del contagio attraverso misure eccezionali e ricorso a controlli generalizzati[11].

Del resto, lo stesso Garante per la privacy ha dichiarato che, pur essendo contrario ad ipotesi di sorveglianza generalizzata mediante la geolocalizzazione di tutti i cittadini 24 ore al giorno, non vi sono

[11] http://www.salute.gov.it/imgs/C_17_pubblicazioni_501_allegato.pdf

preclusioni al ricorso alla tecnologia per il data tracing, purché si tratti di misure proporzionate e ragionevoli, previste da fonte primaria e destinate a perdere efficacia non appena l'emergenza sia finita[12]. Inoltre, lo stesso ministero dell'innovazione ha lanciato una call per il reperimento di specifiche app a ciò destinate.

5. Compatibilità delle misure di sorveglianza attiva con il quadro costituzionale

Non si può ritenere che le predette misure di sorveglianza "attiva" contrastino con i principi fondanti del nostro ordinamento che, invece, pone al vertice della Costituzione il bene della vita, riconoscendogli una posizione di preminenza tra i valori tutelabili: solo chi è in vita può esercitare i propri diritti e quindi il diritto alla vita costituisce, secondo la stessa Corte costituzionale, la priorità logica, oltre che giuridica, su tutti gli altri, con ciò giustificando la compressione di tutti gli altri interessi, limitatamente al perseguimento di tale superiore interesse e per il tempo necessario ([13]).

Sarebbe una contraddizione in termini che un ordinamento giuridico non consentisse un bilanciamento dinamico, dipendente cioè dalle situazioni contingenti che propone la realtà, tra i valori che esso tutela, in quanto una rigidità ed inviolabilità assoluta dei diritti produrrebbe di fatto una paralisi dell'attività e l'impossibilità di governare gli eventi e, nel caso di specie, di proteggere la popolazione e la salute collettiva. Quotidianamente, anche in situazioni non emergenziali, i poteri dello Stato contemperano di continuo interessi protetti dall'ordinamento, sacrificandone alcuni a vantaggio di altri nel perseguimento di un interesse pubblico selezionato come prioritario, nell'osservanza dei basilari principi di proporzionalità e ragionevolezza[14]. Tanto accade per l'attività del Legislatore quanto per gli atti adottati dalle Amministrazioni pubbliche. [15]

In altra prospettiva, è stato efficacemente rilevato, proprio con riferimento alle misure di contenimento dell'epidemia per Covid-19, che "*l'interesse della collettività, di fronte a situazioni di gravissima emergenza sanitaria e alla minaccia per la salute di tutti e di ciascuno, assurge ad un valore superiore, capace di giustificare severe restrizioni alla*

[12] Antonello Soro: emergenza Covid 19, le deroghe sul diritto alla privacy non devono diventare punto di non ritorno,23 marzo 2020, in https://www.federprivacy.org/informazione/primo-piano/item/1339-emergenza-covid-19-le-deroghe-sul-diritto-alla-privacy-non-devono-essere-un-punto-di-non-ritorno

[13] cfr. Corte Costituzionale ordinanza n. 207 del 2018 e sentenze n. 242 del 2019, 35 del 1997 e 223 del 1996. V. inoltre sul tema Guido Biscontini, Mario E. Comba, Enrico Del Prato, Ludovico A. Mazzarolli, Annamaria Poggi, Giuseppe Valditara, Filippo Vari, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in questa Rivista, Osservatorio Covid.

[14] cfr. M. CARTABIA, *I principi di ragionevolezza e di proporzionalità nella giurisprudenza italiana, Relazione predisposta per la Conferenza trilaterale della Corti costituzionali italiana, portoghese e spagnola*, Roma, Palazzo della Consulta 24-26 ottobre 2013

[15] Cfr.. M. NOCCELLI sul tema della prevalenza del principio solidaristico in materia di tutela alla salute rispetto all'esercizio delle proprie libertà: La *lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in questa Rivista.

libertà della persona e agli atti della sua vita quotidiana e di imporre rigorosi limiti ad altri diritti costituzionalmente garantiti, appunto, di tutti e di ciascuno"[16].

6. L'applicazione del principio di proporzionalità nella adozione delle misure di contenimento del virus.

Le misure limitanti i diritti dei cittadini naturalmente devono essere adottate in stretta applicazione del principio di proporzionalità. Tale principio, tuttavia, deve essere correttamente interpretato in relazione alle peculiarità della situazione esistente e dunque declinato in modo dinamico, non dovendosi sovrapporre i concetti di proporzionalità e di gradualità.

Infatti, se è vero che spesso il check di proporzionalità esige che l'adozione di misure via via più incisive (o del caso di specie più limitative della sfera giuridica dei destinatari) sia preceduta dalla prova della inadeguatezza di misure meno restrittive (ed è appunto a tale tipo di valutazione che il Garante della Privacy ha fatto recentemente cenno nella questione della tracciatura dei contatti dei malati di covid-19), talvolta la necessità di adottare il più celermente possibile le misure più idonee, onde evitare effetti più gravi, può legittimare, sempre in base al parametro della proporzionalità, che siano da subito presi gli accorgimenti più rigidi atti a minimizzare nel tempo e nello spazio la loro permanenza.

Dunque, la proporzionalità può giustificare in alcuni casi, in cui il rischio è particolarmente elevato, l'immediata adozione di misure di massimo rigore che, invece, un approccio improntato a gradualità potrebbe pregiudicare, conducendo poi all'adozione obbligata di provvedimenti ben più invasivi dei diritti individuali e della collettività.

Pertanto, alla luce delle precedenti considerazioni, il principio di proporzionalità non sarebbe probabilmente stato ostativo all'adozione di misure ancor più restrittive sin dalla prima manifestazione di diffusione dell'epidemia, posto che ogni ritardo nell'adozione di misure di contenimento in tali situazioni conduce inevitabilmente a provvedimenti successivi ben più incisivi sui diritti individuali e sulla collettività sia dal punto di vista della loro estensione che della loro durata. Non è un caso che l'adozione tempestiva di misure pesantemente incisive è l'approccio indicato nello stesso Piano antipandemico italiano del 2003 già citato.

Inoltre, applicando il principio di proporzionalità così inteso, può dirsi che esso avrebbe giustificato e giustificherebbe anche ora l'adozione di misure di sorveglianza attiva anche tramite tecnologie di geolocalizzazione, *data tracing* ed analisi dei dati mediante il ricorso ad algoritmi, purché autorizzati da una

[16] Così M. NOCCELLI, *La lotta contro il coronavirus*, cit., pag. 3.

fonte primaria unicamente nell'attuale situazione emergenziale, stante le loro strumentalità con gli obiettivi di contenimento dell'epidemia, alla luce delle recenti indicazioni OMS.

Una volta esteso l'isolamento a tutto il territorio nazionale, infine, deve ritenersi che le Autorità pubbliche competenti siano ora tenute, sempre in base al principio di proporzionalità, a compiere tutti gli sforzi necessari a ridurre al minimo la durata del periodo di isolamento e di blocco dell'attività economica, ponendo in essere tutte le attività utili a circoscrivere l'infezione, rendendo quindi ora opportuno, sotto il profilo giuridico, l'adozione di quelle misure di "sorveglianza attiva" che hanno dimostrato il loro successo in altri Paesi e che sono raccomandate a gran voce dall'OMS.

Tale obbligo di attuazione delle misure di sorveglianza attiva discenderebbe anche dal principio di precauzione che "impone al decisore pubblico (legislatore o amministratore), in contesti determinati, di prediligere, tra le plurime ipotizzabili, la soluzione che renda possibile il bilanciamento tra la minimizzazione dei rischi e la massimizzazione dei vantaggi, attraverso l'individuazione, sulla base di un test di proporzionalità, di una soglia di pericolo accettabile; la selezione di tale soglia, tuttavia, può compiersi unicamente sulla base di una conoscenza completa e, soprattutto, accreditata dalla migliore scienza disponibile" che nel caso di specie non può non identificarsi sugli studi e raccomandazioni elaborate sulla scorta delle esperienze finora maturate, tenendo conto che il grado di certezza risulta necessariamente variabile, in un contesto come quello attuale, di un'epidemia le cui connotazioni specifiche sono ancora in corso di studio[17].

Con ciò, sia ben chiaro, non si vuol sostenere che la misura dell'isolamento generalizzato debba essere posta in discussione, anzi l'allarmante grado di diffusione raggiunto dall'infezione di Covid-19 in questo momento la giustifica ampiamente e ne impone la prosecuzione. Ed è anzi a questo proposito opportuna l'introduzione, ad opera del dl 19/2020 di sanzioni ad hoc più severe, stante la blanda efficacia dissuasiva del reato di cui all'art. 650 c.p. su cui inizialmente si era fondato l'apparato repressivo, atteso che i comportamenti scorretti di alcuni potrebbero pregiudicare gli sforzi sostenuti dalla stragrande maggioranza dei cittadini.

Tuttavia, considerazioni di ordine economico collegate alla necessaria ripresa dell'attività produttiva, che si connettono strettamente a quelle sanitarie, rendono ora assolutamente urgente l'attuazione in Italia di tutte le misure che possano rendere più rapido possibile questo processo di ritorno alla normalità.

[17] Così Cons. Stato, Parere, Comm.-Spec. 20 settembre 2017, n. 2065: "*Che questa sia l'interpretazione corretta del principio di precauzione è confermato dalla giurisprudenza amministrativa nazionale che si è occupata del tema (tra i molti precedenti, si richiama la sentenza del Consiglio di giustizia amministrativa della Regione siciliana 3 settembre 2015, n. 581) e, specialmente, dalla comunicazione interpretativa della Commissione europea del 2 febbraio 2000 - COM/2000/01 def. (va ricordato infatti che il principio di precauzione è di origine internazionale e sovranazionale), nella quale si è chiarito che "(l)'attuazione di una strategia basata sul principio di precauzione dovrebbe iniziare con una valutazione scientifica, quanto più possibile completa, identificando, ove possibile, in ciascuna fase il grado d'incertezza scientifica".*

Non vi è dubbio, infatti, che tutte le misure adottate e quelle annunciate, ivi compresi gli acquisti dei materiali necessari a consentire la risposta terapeutica del sistema sanitario, siano fondate necessariamente sul ricorso all'indebitamento pubblico in un momento di blocco quasi totale dell'attività produttiva e del PIL del paese.

Nondimeno, non si può pensare che tale opzione resti praticabile a tempo indefinito, posto che l'aumento prevedibile del deficit nazionale unitamente all'inevitabile recessione che si produrrà nei prossimi mesi (cfr. M. Draghi intervista al Financial Times 26 marzo 2020[18]), potrebbe porre a breve una questione di sostenibilità finanziaria del debito da parte del Paese, ciò che rende ancora più urgente il contenimento del contagio e l'adozione di tutte le misure utili a tal fine, anche attraverso il sacrificio di altri diritti da considerare in questo momento certamente recessivi rispetto alla tutela della salute collettiva.

In questo contesto le considerazioni relative alla tenuta del sistema economico non costituiscono infatti un profilo avulso da quello sanitario, ma devono costituire parte di una strategia unitaria collegata alla finalità primaria della tutela della salute, atteso che la stessa capacità di risposta del sistema sanitario alla pandemia in atto non può non fondarsi sulla disponibilità delle risorse materiali e umane necessarie, che, a loro volta, non possono prescindere dalla conservazione della struttura produttiva del paese e dalla sua credibilità sul piano internazionale[19]. Con ciò, è bene chiarire, non si allude alla tematica dei vincoli di bilancio come legittimo limite alla spesa sanitaria, ma ribaltando la prospettiva, si vuol evidenziare che la tenuta della struttura produttiva e del sistema finanziario costituisce la premessa per la continuità delle prestazioni sanitarie e la copertura del crescente fabbisogno.

[18] https://www.ft.com/content/c6d2de3a-6ec5-11ea-89df-41bea055720b

[19] Sul collegamento e contemperamento tra le esigenze di tutela del diritto alla salute e vincoli finanziari vi è una notevole casistica di decisioni della Corte costituzionale per la quale si rimanda a "*La tutela dei diritti e vincoli finanziari*", Quaderno di giurisprudenza costituzionale, maggio 2013 (pagg. 18 e ss.) in https://www.cortecostituzionale.it/documenti/convegni_seminari/STU247tuteladiritti.pdf

APP PER IL TRACCIAMENTO: OTTO REGOLE DA RISPETTARE

JUAN CARLOS DE MARTIN

Le tecnologie digitali possono svolgere un ruolo importante nel contrasto all'epidemia in corso. Relativamente, però, allo specifico tema dell'uso di una "app" per realizzare il tracciamento dei contatti si registrano sia aspettative d'efficacia molto dibattute, sia preoccupazioni sempre più intense in merito ai rischi connessi alla messa in campo di soluzioni tecniche non adeguate. Preoccupazioni che ora hanno anche raggiunto la sfera della politica: molte forze politiche, infatti, hanno espresso dubbi sia in merito alla specifica "app" "Immuni" selezionata dal commissario Arcuri, sia più in generale in merito ai rischi connessi ad un'adozione troppo frettolosa di soluzioni così potenzialmente delicate.

L'adozione di una "app" telefonica, infatti, può costituire un valido ausilio per la corretta ricostruzione della catena del contagio a condizione che l'adozione di tale tecnologia sia inserita in un'efficace strategia sanitaria complessiva e che sia largamente accettata e utilizzata dalla popolazione. Affinché quest'ultima condizione si realizzi è essenziale che la "app" sia tecnologicamente trasparente, sicura e rispettosa dei diritti fondamentali delle persone. Solo così si potrà conquistare la fiducia dei cittadini e suscitare la volontà di contribuire al contrasto dell'epidemia utilizzando una "app" installata sul loro telefono personale.

Partiamo dalle aspettative. Per i limiti della tecnologia attuale la ricostruzione dei contatti ravvicinati non potrebbe essere puramente automatica. In tal caso, infatti, il numero di falsi positivi sarebbe inevitabilmente considerevole, basta leggere la definizione ufficiale di contatto ravvicinato per comprenderlo. La "app" dovrebbe, quindi, limitarsi ad essere un aiuto a un processo di tracciamento dei contagiati condotto in larga parte da personale specializzato. Sicuramente utile, ma altrettanto sicuramente non una panacea.

Tuttavia, e veniamo ai requisiti, anche solo una "app" di sostegno di questo tipo sarebbe comunque molto delicata, visto che per definizione riguarderebbe i nostri spostamenti e il nostro stato di salute. Se si vuole che molti cittadini la adottino è quindi essenziale che, indipendentemente dalle specifiche funzionalità, venga progettata rispettando alcuni principi di fondo.

In particolare, come messo in evidenza di recente non solo da Commissione europea, Parlamento europeo e Garanti Privacy europei, ma anche da molti studiosi di tutto il mondo, una "app" (o un dispositivo da indossare) dovrebbe avere le seguenti caratteristiche:

- basata su adozione volontaria;
- progettata in stretta collaborazione con chi realizza il tracciamento dei contatti;
- utilizzata solo per uno scopo preciso;
- disponibile solo il tempo strettamente necessario;
- idonea a raccogliere solo i dati strettamente necessari, da cancellare non appena trascorsa la loro utilità;
- liberamente disponibile, con relativi codice sorgente, specifiche tecniche e altri documenti rilevanti;
- basata su una tecnologia distribuita, in modo da evitare i seri rischi associati alla creazione di un database centralizzato;
- gestita e supervisionata da un ente pubblico.

Sono tutti punti tecnicamente fattibili, e anche in tempi rapidi. Che l'Italia li faccia propri senza indugio: così facendo mostrerebbe al mondo come contrastare l'epidemia adottando uno strumento digitale allo stesso tempo efficiente e rispettoso dei principi democratici e dei diritti delle persone. —

© RIPRODUZIONE RISERVATA

Virus e algoritmi. Impariamo da un’esperienza dolorosa

1 Aprile 2020

di **Giovanna De Minico***

In questi giorni il Governo si sta chiedendo se seguire e come il modello coreano che traccia gli spostamenti di chiunque per prevenire l’ulteriore diffondersi del virus. Chiariamo che col termine “prevenire” si vogliono indicare quegli atti che anticipano con prognosi *ex ante* il verificarsi di un evento futuro, ma incerto nell’accadere. Nel nostro caso il rischio è la diffusione del virus e la sua velocità di propagazione da individuo a individuo. A differenza delle prognosi *ex ante* che si fanno rispetto al terrorismo, l’epidemia si caratterizza per la certezza dell’*an*, mentre l’incertezza riguarda solo il tempo della propagazione e la sua ampiezza.

Questa precisazione era necessaria per capire meglio il perimetro entro il quale il legislatore dell’emergenza si deve muovere quando valuta, misura e compensa i due beni a confronto, libertà fondamentali e sanità pubblica, equivalenti costituzionalmente anche in termini di certezza tra costi e benefici. Diversamente, accade col terrorismo, dove al danno sicuro alle libertà corrisponderà un vantaggio probabile alla sicurezza, ignorandosi se accadrà il prossimo attacco.

Al momento questo bilan ciamento è stato fatto comprimendo le nostre libertà: non usciamo, non lavoriamo, non ci incontriamo. Nell’elenco dei beni sacrificati la privacy non figura, era stata mantenuta indenne. Ma questa salvezza potrebbe svanire, se il nostro Governo avviasse un’azione di tracciatura dell’intero suo popolo ricorrendo a sofisticherie che la tecnica con un menu ricco offre al decisore politico.

Da noi, seguendo quanto è già accaduto in Paesi poco sensibili alle libertà individuali, si vorrà diffondere nei nostri telefonini intelligenti un’app, la quale dovrà raccogliere in un unico pool i dati che ci riguardano. E questa sarà la prima fase. Poi i dati di ciascuna confluiranno in un server centrale: il secondo step. E infine un algoritmo li interrogherà, li intreccerà e secondo una logica, a noi oscura, vi dedurrà valutazioni funzionali alla prevenzione. Si pensi a un provvedimento di quarantena vigilata ordinato nei confronti di una lunga catena di persone con cui un individuo, poi risultato infetto, era entrato in contatto.

Quali sono i problemi per un giurista? Di metodo e di fine.

Metodo – Il primo riguarda come e chi deciderà la tracciatura. Il dato positivo è lineare: l’art. 9 del Regolamento UE 2016/679 (da ora GDPR) vieta il trattamento dei dati sensibili, ma nel porre il divieto contempla tra le vie di fuga (art. 9, par.2, lett.i) l’esigenze di pubblica utilità, tipizzate, anche se non in via esclusiva, nella salute pubblica. Queste possono giustificare che il divieto si rovesci nella facoltà di tracciare, proprio come l’eccezione deroga alla regola generale. Spetterà agli Stati membri dell’Unione decidere se attivare o meno questo *ius singulare*.

In questa valutazione il decisore non è solo, ma neppure integralmente supportato dalla tecnica. Quest’ultima potrà confortarlo sulla metodologia più appropriata, la meno invasiva possibile, ma la decisione se ricorrervi o farne a meno rimarrà affidata alla scelta dell’Autore politico. Questi in ultima istanza dovrà rendere il conto di ciò che ha fatto o non fatto a chi lo ha eletto. Quindi, il tentativo già battuto da Macron, che in più occasioni sembra voler proteggere le sue decisioni come ineluttabili conseguenze di quanto sentenziato dal *Comité* di saggi istituito *ad hoc*, non è un esempio da seguire.

In democrazia chi decide, deve rendere il conto in ultima istanza al corpo elettorale e quindi non si può nascondere sotto l'ombrello protettivo dell'indispensabilità tecnica.

Con ciò vogliamo dire che niente è inevitabile, come l'emergenza non è una fonte di per sé legittimante il diritto eccezionale, perché è necessario passare per le fonti *ordinem* dell'ordinamento, così la valutazione tecnica sarà solo il sostengo ragionevole alla politica, superabile se questa lo voglia.

Chiarito il ruolo giocato dalla tecnica nel *rule-making*, una particolare attenzione merita il "come" il legislatore imporrà questa tracciatura.

Se il Governo dovesse porsi l'alternativa tra decreto-legge e dpcm, come ha fatto finora (D.L. 6/2020, art. 3), riterrei che si stia giocando una *chance* che in punto di diritto non ha mai avuto. La Costituzione ha già risolto il dualismo *ex ante* nel momento in cui ha presidiato le libertà con la garanzia della riserva di legge. E anche a voler intendere come relativa la riserva a difesa della nostra privacy, essa comunque significa che il legislatore deve parlare per primo e quindi già dettare una disciplina sufficientemente prescrittiva. Solo in seconda battuta potrà intervenire l'atto normativo secondario del governo, il regolamento. Qui il decreto-legge – ad esempio il D.L. 19/2020 che al momento è l'ultimo di questa lunga serie – se è pur vero che non ha disposto una girata in bianco al Presidente del consiglio, è però innegabile che abbia fatto meno di quanto avrebbe dovuto fare per soddisfare quella assorbente attribuzione di competenza consegnata nella riserva. L'art. 2 dell'ultimo decreto-legge enumera le misure restrittive delle libertà, ma lascia alla valutazione politica del Presidente del consiglio la scelta di quale rendere concretamente operante, senza neanche vincolare il suo libero apprezzamento politico ai parametri della necessità, qui degradata ad adeguatezza, e della precauzionalità, qui diluita nella proporzionalità.

Se si continuasse su questo pentagramma, la privacy sarebbe retrocessa dinanzi alla sicurezza non per volontà di legge, e neppure di un decreto-legge, più che legittimo vista l'urgenza del provvedere, ma in forza di un atto formalmente amministrativo del Presidente del consiglio. La degradazione della fonte, e con essa l'amministrativizzazione delle libertà, non è una *querelle* per i soli addetti ai lavori, toccando fin nelle ossa tutti noi cittadini. Infatti, le prerogative in difesa delle libertà, intangibili dal potere costituito in tempo di emergenza sono state alleggerite fino a evaporare: e allora il dpcm è stato proposto come una risorsa fungibile al decreto-legge. Questa disinvolta sostituzione tra fonti rovescia in un colpo solo troppe regole del nostro stato di diritto: il dpcm ha un'efficacia definitiva, contro la temporaneità e provvisorietà del decreto-legge; il primo si risolve nella volontà incontestabilmente monocratica, contro la subordinazione del decreto-legge alla parola ultima del Parlamento; è esente dall'esame di legittimità preventivo, anche se sommario, del Capo dello Stato, cui non sfugge invece il decreto-legge e, infine, è sindacabile dai giudici comuni, contro il riesame della Corte costituzionale sulla coppia decreto/legge di conversione.

In sintesi, stante l'urgenza la tracciatura potrà essere disposta con decreto-legge, e non con la tecnica combinata di un decreto che si limita ad annunciarla e di un dpcm che in concreto la dispone.

Quest'ordine vincolante di interventi è peraltro imposto anche dal diritto comunitario: il GDPR (*General Data Protection Regulation*) che, se nell'art. 9 apre a tracciature in casi eccezionali, facendo saltare il divieto generalizzato, al tempo stesso impone che a farlo sia la legge, cioè l'atto espressivo massimo della sovranità popolare, non dunque un atto, quale il dpcm, preposto a continuare, non già ad avviare *ex novo* il disegno politico.

La questione sulla fonte legittimata a parlare non ha nulla a che vedere con un giudizio di merito sulle regole poste, facile a esprimersi a fatto compiuto, ma difficile quando i rimedi vengono disegnati in anticipo rispetto all'evento temuto nel tentativo di valutare secondo proporzionalità, necessarietà e

precauzionalità quanto probabilmente accadrà. E in questa riffa di critiche al Governo, la più irragionevole è quella di chi ha ritenuto inutile, se non pericoloso per i sentimenti, lo stare tutti agli "arresti domiciliari" perché sarebbero le prescrizioni del Governo a trasformare ogni individuo in un potenziale autore, non certo il virus, nobilitato da questo pensiero all'ennesima *fake news* in coerenza col tempo di Internet. La conseguenza di questa tesi negatrice dei fatti è l'illegittimità dello stato d'emergenziale dichiarato non per proteggerci, ma come scusa per affermare poteri eccezionali e conservarli a emergenza esaurita. Riteniamo che questo rischio, sempre insito quando si apre una stagione emergenziale, non vada contrastato negando la realtà, cioè con l'equazione il virus=bugia, ma con il rispetto delle garanzie dello stato di diritto, la cui osservanza si impone ai nostri governanti soprattutto in tempo di emergenza. Ed è proprio intorno a queste garanzie – ordine delle fonti del diritto, riserva di legge, intangibilità del nocciolo duro dei diritti – che proviamo a ragionare in questo scritto.

E ora le questioni di fine

Esse sono poste nel GDPR che ripete, come il ritornello di una canzone estiva, che i dati vanno trattati nei limiti dello stretto necessario. Dunque, se la compressione del diritto è altrimenti evitabile, questa sarà la sola via da percorrere.

Tale *leit motiv* si combina bene con le misure precauzionali disseminate nel GDPR, tendenti a prevenire l'inutile sacrificio prima che sia troppo tardi, anche ricorrendo a tecniche di disegno che assicurano in anticipo la compatibilità del mezzo con un'inedita fisionomia della privacy.

E allora tornando alla nostra app, essa andrà strutturata in modo da raccogliere i nostri dati di geolocalizzazione, ad esempio, dove siamo stati e per quanto tempo? Oppure, sarà sufficiente il solo dato del nostro avvicinamento sociale, cioè se abbiamo rispettato la distanza di sicurezza nell'incontrare una persona per strada? In altre parole, l'app raccoglierà anche i dati superflui ai fini della prevenzione o solo quelli strettamente necessari per risalire a ritroso la catena dei contatti? La risposta non è nella tecnica che potrà orientare la macchina indifferentemente verso destra o sinistra, bensì nella volontà del legislatore, il solo legittimato a scegliere la sua direzione.

La *call* lanciata dal governo, che ci invitava a presentare progetti di app, non si è posta né la domanda relativa alla tipologia di dati, né quella sui soggetti da tracciare. Tutti noi o solo gli infetti? La soluzione *omnibus* appare funzionalmente più adatta perché la misura per prevenire il possibile contagio deve poter includere tutti, in quanto potenziali portatori del virus. Una cernita però si potrà, anzi si dovrà, fare in un momento successivo, quando le autorità competenti avranno accesso a dati. In questa fase saranno trasmessi loro solo i dati delle persone che hanno contratto il virus. Esito questo, suggerito dal principio, secondo il quale le liberà possono essere legittimamente compresse nella misura strettamente necessaria al conseguimento di uno specifico scopo, ragione ricorrente nei *case law* del giudice europeo in materia di prevenzione al terrorismo (C.G. 8 aprile 2014, *Digital Rights Ireland c. Ireland*).

Ancora nelle questioni attinenti al fine rientra l'interrogativo se l'esito dell'algoritmo si risolverà in una decisione esclusivamente automatizzata o si limiterà a essere una parte di un processo volitivo umano che assume l'algoritmo, ma al tempo stesso lo supera.

Ebbene, il GDPR, un po' come per la tracciatura, pone un divieto: no automatizzazioni assolute, ma poi al rigo successivo, art. 22, par.2, lett.b., rompe il tessuto della drastica proibizione e apre ai provvedimenti meccanici, sempre che il legislatore lo voglia. A noi preoccupa proprio l'ipotesi che il decisore politico possa decidere di far coincidere l'esito dell'algoritmo con una misura limitativa ad applicazione automatica. Escludiamo che questa sia la via da seguire perché l'algoritmo potrebbe aver commesso errori, che invece la volontà dell'uomo è in grado di correggere. Si pensi a una

localizzazione che porti a individuare una persona che ha visitato uno stabile, dove solo al 1 piano c'è un individuo infetto, non anche nelle abitazioni dislocate ai piani superiori. Se la conseguenza è trattare l'intero palazzo come interamente infetto, il rimedio peccherebbe per difetto. Pertanto, la misura a operatività automatica potrebbe essere la quarantena vigilata per tutti, e quindi in assenza di pericolo per la salute pubblica si spazzerebbero via in un colpo solo più diritti di più individui.

Un'ultima questione di fine, inteso ora come prospettiva ultima di questa *policy* precauzionale: quale sorte avrà la pesca a strascico dei nostri dati?

La voce europea risponderebbe che i dati devono essere cancellati, perché la privacy fa un passo indietro solo dinanzi alla sicurezza, cessato il pericolo tutto dovrà torna nella condizione in cui era prima, secondo quanto affermato dalla Corte di Giustizia prima ricordata.

Bene. Ma allora il server dove confluiscono i dati nostri, deve essere di proprietà del nostro Stato. Qui si chiedono due attributi: pubblicità e nazionalità. Diversamente, in caso di suo affidamento alla mano privata niente ci assicurerebbe che questa tracciatura non fosse utilizzata come merce di scambio contro denaro in una trattativa con i Google di turno, avidi di dati per alimentari i loro affari *data driven*. Se così fosse, avremmo rinunciato alle nostre libertà per assecondare i piani lucrativi dei Giganti della rete.

Quali suggerimenti positivi dal virus

Il primo positivo è la dimostrazione che le soluzioni tecniche non sono mai neutre, perché se procurano vantaggi a tutti o privilegi a pochi, dipende esclusivamente da come la mano pubblica le abbia orientate.

Il secondo positivo è nella spinta verso una generale solidarietà che ha bisogno dell'apporto di ciascuno di noi: sperimentare la solidarietà nel rinunciare quotidianamente a esercitare le nostre libertà per il tempo necessario.

Il terzo positivo si compie con l'apporto dei soggetti pubblici.

I nostri governanti darebbero prova di solidarietà nel conservare intatti alle generazioni future i diritti fondamentali, esposti a minacce più insidiose nella stagione dell'emergenza che non in tempi ordinari.

I governanti dell'Unione sono dinanzi a una sfida decisiva: fare esperienza di un sentire politico comune concependo l'Italia, la Spagna, la Francia e gli altri Paesi come frammenti di uno stesso corpo politico, il quale per continuare a esistere deve funzionare come un unico armonico, responsabile e identitario. Diversamente, qualche sua parte potrebbe cedere al canto ammaliatore e amaro delle Sirene d'oriente.

* Prof. diritto costituzionale – Università Federico II, Napoli

Alcune delle questioni qui solo accennate, tra cui: la *Law of fear*, le valutazioni precauzionali, il bilanciamento tra beni di rilevanza costituzionale in tempo di emergenza, sono state da me affrontate in: G. De Minico, *Costituzione. Emergenza e Terrorismo*, Jovene, 2016, e a quelle riflessioni mi sia consentito rinviare.

SIDIBlog
il blog della Società italiana di Diritto internazionale e di Diritto dell'Unione europea

diritto dell'Unione europeadiritto internazionale pubblicoForum COVID-19

La tempesta perfetta COVID-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa

Gabriele Della Morte · Marzo 30, 2020
0 11 1

Gabriele Della Morte, Università Cattolica, Milano

1. **Avviso ai naviganti**

Una premessa di metodo si impone: di fronte al nuovo tutte le competenze sono vecchie. A causa dell'epidemia da COVID-19 inediti quesiti giuridici si irradiano in ogni direzione. Alcuni di essi, tutt'altro che minori, si pongono sul piano delle possibili deroghe in materia di protezione dei dati personali: è su questi che concentrerò le mie riflessioni.

2. **Acque agitate**

Poco dopo l'ufficializzazione dello stato di pandemia l'opportunità di ricorrere a sistemi di tracciamento al fine di contrastare la diffusione del virus ha presidiato il dibattito mediatico – ne ha discusso la stampa internazionale, quella interna e finanche l'Organizzazione mondiale della sanità. Secondo alcune fonti giornalistiche sarebbero più di dieci gli Stati che, in senso lato, vi fanno ricorso e tra questi si riscontra una grande varietà di situazioni che oscilla dalle ipotesi più blande, quali il controllo di assembramenti grazie ai dati aggregati, sino a quelle più incisive, quali la geo-localizzazione e il tracciamento di spostamenti individuali (si tratta del cd. *contact tracing*, potenzialmente incrementabile anche con i dati GPS di *Facebook*, *Google Maps* ecc.).

Tra le forme più incisive il caso più noto è quello di *Alipay Health Code*, una *App* diffusa in Cina. Si tratta di un software che, una volta installato nello *smartphone*, consente una classificazione degli individui sulla base dei dati relativi allo stato di salute, ai contatti avuti in precedenza ecc. Il fine è quello di contrastare l'epidemia attraverso un monitoraggio costante di movimenti e contatti. A ogni controllo occorre esibire il *QR-code* di riferimento generato dalla *App*. Il colore del codice, assegnato da un algoritmo che calcola un coefficiente di rischio, determina diverse conseguenze: il *QR-Code* rosso obbliga a restare al proprio domicilio; quello giallo garantisce mobilità limitata; quello verde consente libertà di movimento. Se non si è provveduto a installare l'applicazione si è ritenuti *ipso facto* (e … *jure*!) *QR-code* rosso.

3. **I dati in alto mare**

Le questioni che i sistemi di controllo fondati su algoritmi sollevano sul versante dei diritti – dalla privacy alla tutela dei dati personali, passando per la compressione di fondamentali libertà, ad esempio quella di movimento – sono innumerevoli. In un'ottica complessiva gli indubbi benefici di breve termine vanno comparati agli effetti che si potrebbero sedimentare in una prospettiva di più lunga durata.

In un'articolata riflessione ospitata dal *Financial Times*, il filosofo Yuval Noah Harari adotta questa chiave di lettura, insistendo sui rischi del ricorso a tecnologie di sorveglianza di massa. Sino a ieri, toccando il nostro *smartphone* «the government wanted to know what exactly your finger was clicking on», oggi con il coronavirus «the focus of interest shifts. Now the government wants to know the temperature of your finger and the blood-pressure under its skin». L'analisi di Harari è, peraltro, approssimata solo *per difetto*: in molti casi (come quello cinese riportato *supra*) il controllo non viene esercitato direttamente dai governi, ma da compagnie private che agiscono in collaborazione con i primi. È questa la ragione per la quale alcuni esperti che si sbilanciano a favore di simili tecnologie (Benanti: «per potere continuare a vivere dobbiamo donare qualcosa di immateriale […]: i nostri dati») sollevano il problema di quale sia il soggetto incaricato di tale compito («Non di certo soggetti privati […] L'ideale sarebbe una grande azienda pubblica»). Purtroppo una simile azienda al momento non c'è, a meno che non si intenda gravare di tale peso l'Autorità garante per la protezione dei dati personali (il cui Presidente ha comunque testimoniato una discreta apertura rispetto a simili sistemi di controllo purché corredati da adeguate garanzie). Abbiamo però un importante novero di disposizioni internazionali le quali, in coordinamento con le norme statali, offrono un valido riferimento. Sulle regole interne sono già state elaborate diverse osservazioni, tra le quali segnalo le puntuali riflessioni di Oreste Pollicino e Federica Resta. Mi limiterò dunque alle seconde, con speciale riguardo alla normativa europea e internazionale in materia di protezione dei dati personali, in dialogo con gli altri interventi già ospitati in questo Forum.

4. **La bussola di riferimento**

Dopo il distanziamento sociale e il confinamento in dimora, il dibattito sulle strategie di contrasto all'epidemia si sta indirizzando sulle misure di sorveglianza e *contact tracing*, atteso che, come ha sostenuto il Direttore dell'Organizzazione Mondiale della Sanità nel *media briefing* del 16 marzo 2020: «you cannot fight a fire blindfolded. And we cannot stop this pandemic if we don't know who is infected».

Ma in che modo tali misure impattano sul regime di protezione internazionale dei dati personali? Quante e quali deroghe sono da considerarsi ammissibili? (sia consentito rimandare, per un primo inquadramento, a Della Morte).

Innanzitutto, il quadro normativo internazionale è composito e va dedotto, nell'assenza di un trattato universale, da un insieme di disposizioni settoriali e regionali in combinazione con norme di *soft law*. Tralasciando il discorso su queste ultime – che pure contribuiscono in via ermeneutica alla formazione dei principi che regolano la *governance senza governo* delle reti – è possibile osservare che sono diverse le convenzioni regionali e settoriali di cui l'Italia è parte.

Un esempio settoriale è rappresentato dall'**art. 17 del Patto internazionale sui diritti civili e politici**, dedicato al divieto di interferenze arbitrarie o illegittime nella vita privata. Nel ***General Comment* n. 16** del Comitato dei diritti umani si ricorda, al par. 1, come il divieto debba essere inteso a tutela di ogni intromissione illegale o arbitraria proveniente tanto dal potere pubblico quanto dalle persone fisiche o giuridiche; al par. 3 si precisa che l'aggettivo «unlawful» deve essere interpretato nel senso per cui alcuna interferenza è ammissibile fuori dai casi nei quali essa è autorizzata dalla legge, e nel successivo par. 4 si puntualizza che anche qualora l'interferenza sia autorizzata deve essere conforme alle disposizioni, agli scopi e agli obiettivi del Patto medesimo. Giacché, aggiunge il par. 7, «all persons live in society, the protection of privacy is necessarily relative» e considerato che nel quadro dell'art. 17 non è prevista alcuna eccezione, si applica il regime di deroghe generali sancito dall'art. 4 dello stesso Patto. Ai sensi di quest'ultima disposizione (sulla quale v. Tammone): «In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed» gli Stati parte possono derogare agli obblighi sanciti «to the extent strictly required by the exigencies of the situation». Tuttavia anche quest'ultima disposizione deve essere interpretata alla luce del *General Comment* menzionato. Il relativo par. 8 specifica che «relevant legislation *must specify in detail the precise circumstances* in which such interferences may be permitted» (*corsivo* aggiunto), aggiungendo che una simile decisione «must be made only by the authority designated under the law», e ancora che «surveillance, whether electronic or otherwise […] should be prohibited». Ma c'è di più: secondo il Comitato non è solo la sorveglianza a dovere essere regolata dalla legge, quanto anche la raccolta e la conservazione di «data banks and other devices, whether by public authorities or private individuals or bodies» (par. 10).

Quanto alle disposizioni aventi portata regionale, un primo gruppo di norme è riscontrabile in seno al Consiglio d'Europa. È il caso dell'**art. 8 della Convenzione europea dei diritti dell'uomo** dedicato al rispetto della vita privata e familiare. L'art. 8, par. 2, diversamente dal Patto, specifica le condizioni al verificarsi delle quali le interferenze delle autorità pubbliche sono da considerarsi ammissibili: che siano previste dalla legge; che siano necessarie nel quadro di una società democratica; che corrispondano agli scopi tutelati, quali la sicurezza nazionale, la protezione della salute ecc. Va da sé che con il corso del tempo l'ambito d'applicazione dell'art. 8 ha registrato una notevole estensione grazie all'opera di interpretazione euristica dei giudici. Non è questo il contesto per una ricostruzione sistemica, ma ci riserviamo la possibilità di ritornarvi qualora le circostanze lo rendano opportuno.

Sempre a livello regionale e sempre *ex multis*, merita un breve richiamo la **Convenzione 108** sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale. Il relativo art. 6 è dedicato alla protezione delle categorie 'speciali' di dati, tra i quali rientrano a pieno titolo quelli relativi alla salute che richiedono una tutela rafforzata.

Un discorso a parte merita **l'Unione europea**, in quanto la protezione dei dati prevista in tale contesto configura un sistema eccezionale e senza precedenti, alla cui formazione hanno contribuito tanto ragioni di ordine economico (i dati dei consumatori europei sono particolarmente attraenti nel mercato globale), quanto di ordine storico-politico (non bisogna dimenticare che l'Unione poggia le propria fondamenta sulle ceneri dell'Olocausto realizzato attraverso discriminazioni fondate su dati personali).

Il sistema di regole in seno all'Unione orbita, oggi, intorno al *corpus iuris* del **Regolamento generale per la protezione dei dati personali (GDPR)**.

Innanzitutto, **l'art. 23**, disciplinando le limitazioni che uno Stato membro può apportare a diversi principi e regole, richiede che essa rispetti «l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica» per salvaguardare [*inter alia*] la sanità pubblica. Dette limitazioni devono essere previste «mediante misure legislative» (par. 1), che

contengano indicazioni relative a : *a*) le finalità di trattamento; *b*) le categorie di dati personali; *c*) la portata delle limitazioni introdotte; *d*) le garanzie per prevenire abusi o illeciti; *e*) l'indicazione del titolare del trattamento; *f*) i periodi di conservazione e le garanzie applicabili; *g*) i rischi per i diritti e le libertà degli interessati; e *h*) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità medesima (par. 2).

A ciò va aggiunto che le tecniche di sorveglianza in questione **non concernono i semplici «dati personali»** (e cioè, «qualsiasi informazione riguardante una persona fisica identificata o identificabile», *ex* **art. 4 GDPR, n. 1**), ma quella particolare categoria che, ai sensi **dell'art. 4, n. 15, è rappresentata dai dati *attinenti alla salute*** «*compresa la prestazione di servizi di assistenza sanitaria*». Tali dati, che secondo il **considerando n. 35** ricomprendono «un numero, un simbolo o un elemento specifico attribuito a una persona fisica» (o ancora «qualsiasi informazione, [ad esempio il «rischio di malattie»] indipendentemente dalla fonte») rientrano nel novero dei cd. **dati soggetti a trattamento speciale**.

Questi, ricorda il **considerando n. 51**, sono informazioni «che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali». Per tale ragione meritano una tutela rafforzata, prontamente specificata all'**art. 9, par. 2**, dove si enunciano le dieci ipotesi in cui non si applica il divieto di trattamento di tali dati speciali. Nel novero di tali eccezioni a noi pare che assumano particolare rilievo la lettera *h*), che fa riferimento ai trattamenti necessari a scopi di «diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei servizi o sistemi sanitari»; e la lettera *i*), che richiama «l'interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici […] ». La disposizione di cui alla lettera *h*) rinvia al **considerando n. 53** ai sensi del quale nel trattamento di dati sensibili per finalità sanitarie, da un lato, «[i]l diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali» e, dall'altro, «gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati […] relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione […]». Diversamente, la disposizione di cui alla lettera *i*) richiama il **considerando n. 54** ai sensi del quale in simili casi il trattamento potrebbe avere luogo «senza il consenso dell'interessato» purché nel rispetto di «misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche».

Il tema è ripreso in seguito dall'**art. 9, par. 4**, che attribuisce agli Stati membri il potere di introdurre «ulteriori condizioni, comprese limitazioni, con riguardo al trattamento dei dati […] relativi alla salute». Tale ultima disposizione menziona ben cinque considerando (n. 8, n. 10, n. 41, n. 45 e n. 53) dei quali almeno uno merita attenzione. Mi riferisco al **considerando n. 41** che, facendo riferimento ai casi in cui il Regolamento richiama «una base giuridica o a una misura legislativa», specifica che questa non deve essere necessariamente intesa come un «atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale», purché risulti «chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo».

Il concetto d'altra parte è ribadito anche dall'**art. 52** della **Carta dei diritti fondamentali dell'Unione europea** – il primo strumento che distingue tra privacy (art. 7) e tutela dei dati personali (art. 8) – laddove si prevede che eventuali «limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà», aggiungendo che dette limitazioni devono essere adottate «nel rispetto del principio di proporzionalità [e] solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

Da ultimo merita un cenno la **Direttiva *ePrivacy* del 2002,** il cui **art. 15** garantisce agli Stati membri la possibilità di limitare – attraverso il ricorso a «disposizioni legislative» – gli obblighi in materia di riservatezza dei dati sul traffico per finalità determinate e purché in «una misura necessaria, opportuna e proporzionata all'interno di una società democratica». Sebbene il coordinamento tra il GDPR e la Direttiva *ePrivacy* contempli più di una questione aperta, l'opinione dell'***European Data Protection Board*** sul punto è orientata verso il riconoscimento di un valore di *lex specialis* in favore della Direttiva (del Comitato europeo per la protezione dei dati personali v. anche lo *Statement*, alquanto scarno in verità, proprio sulla gestione in tempo di COVID -19).

5. Come segnare il nord

In attesa di un più articolato quadro normativo sul punto (al momento il richiamo legislativo interno è principalmente quello, del tutto inadeguato, dell'**art. 14 del decreto legge 9 marzo 2020, n. 14**), mi sembra di potere concludere che, nel ricorso a un trattamento per così dire 'rafforzato' di dati personali e sanitari, occorrerà innanzitutto accertarsi che siano rispettati quanto meno i seguenti requisiti:

- **Formalità**: le interferenze devono essere previste da una base giuridica variamente intesa;
- **Indispensabilità**: le interferenze devono essere necessarie nel quadro di una società democratica;
- **Finalità**: le interferenze devono corrispondere allo scopo di protezione della salute;
- **Tassatività**: le interferenze devono essere specificate nel modo più dettagliato;
- **Temporalità**: le interferenze devono indicare il periodo di vigenza;
- **Impugnabilità**: le interferenze devono essere contestabili in qualche forma;
- **Proporzionalità**: le interferenze non devono mai essere eccessive rispetto allo scopo perseguito.

Chiaramente alcuni di questi principi possono sovrapporsi o articolarsi in una relazione di *genus* a *species*, oltre a modularsi diversamente a seconda del tipo di interferenza: *contact tracing* più o meno invasivo; trattamento di soli dati personali o anche di dati anonimi e/o pseudo-anonimi; trattamento subordinato al consenso di tutte le persone potenzialmente interessate ecc. Si è comunque deciso di stilare un primo elenco per costituire le basi per una più meditata riflessione successiva (*work in progress*).

6. Quale approdo?

In conclusione c'è certamente qualcosa di contro-intuitivo nel fatto che le democrazie occidentali ricorrano a strumenti propri del *Capitalismo della sorveglianza* (mi riferisco qui al significativo studio di Shoshana Zuboff) per difendere se stesse. Ma questo paradosso è solo apparente, perché frutto di un espediente retorico – piuttosto in voga, purtroppo – che pone la questione nei termini di *trade-off* tra salute e privacy, mentre a un più attento esame appare evidente che la questione non può essere articolata in termini alternativi/oppositivi.

Come salvaguardare *sia* la tutela dei dati personali *sia* la salute, a fronte di una minaccia pandemica? Certamente un approccio ispirato al criterio di gradualità – come quello evocato da Pollicino e Resta nel già menzionato scritto – fornisce una strategia ragionevole per ogni situazione inedita: occorre innanzitutto testare l'efficacia delle misure meno invasive e quindi incrementarle in caso di bisogno.

Al contempo bisogna contemplare limiti invalicabili perché se è vero che talvolta gli Stati fanno ricorso a legislazioni d'urgenza per ristabilire in un secondo momento un adeguato sistema di garanzie (è accaduto anche in Italia: si consideri la stagione del terrorismo), oggi è il matrimonio tra regolamentazione d'urgenza e innovazione tecnologia che richiede particolare attenzione: dalla prima si può tornare indietro, dall'innovazione tecnologica, *historia magistra*, no.

In definitiva, in attesa che passi la 'tempesta perfetta' si possono anche ammainare le vele. Ma occorre prestare molta attenzione alla bussola per ritrovare, in seguito, la rotta.

CoVid-19

Nel ginepraio delle app di tracciabilità

Samuele Dominioni

24 aprile 2020

Nei giorni scorsi il governo italiano, attraverso un'ordinanza firmata dal commissario per l'emergenza sanitaria Domenico Arcuri, ha scelto quale sarà la **app per il tracciamento dei contagi in Italia**. Si tratta di Immuni, una app sviluppata da Bending Spoon s.p.a., una società milanese di sviluppo informatico, prima in Europa in termini di produttività. La scelta è stata fatta tra oltre 300 proposte arrivate al Ministero dell'Innovazione e Digitalizzazione a seguito di una fast call lanciata il 24 marzo. Nel frattempo si è sviluppato un ampio dibattito, spesso confusionario e contraddittorio, riguardo all'utilizzo di tecnologie di tracciamento dei contagi anche alla luce delle esperienze di altri paesi che hanno adottato soluzioni simili, come accaduto in Corea del Sud o Singapore. Cerchiamo di fare ordine.

È importante sottolineare che, benché il fine sia sempre la tracciabilità, le modalità e i risultati che si possono ottenere sono molto diversi. Per semplicità si possono categorizzare **tre grandi tipologie di utilizzo di tecnologia per la tracciabilità**, in alcuni casi combinati tra di loro: **il numero telefonico**, **il GPS**, **il Bluetooth**.

Il primo è il meno accurato, tant'è che si parla di tracciabilità collettiva, e allo stesso tempo meno rispettoso della privacy dell'utente. È stato adottato ad esempio in Lombardia per verificare la mobilità degli abitanti nonostante il lockdown. Le compagnie telefoniche hanno messo a disposizione i dati del traffico dei ripetitori alle autorità regionali. Il secondo tipo utilizza la raccolta di informazioni attraverso la geo-localizzazione GPS. Questa tecnologia è alla base della piattaforma sviluppata dal Massachusset Institute of Technology (MIT) con il progetto Safe Paths, attualmente al vaglio in diversi paesi al mondo e scelta da Cipro. Infine, le soluzioni che sfruttano solo la tecnologia Bluetooth, come quella sviluppata da Immuni o usata a Singapore. In questo caso, il tracciamento avviene raccogliendo i dati unidirezionali (*beacon*) tra due dispositivi a distanza ravvicinata.

Una delle priorità, rispetto al fiorire di soluzioni alternative, **è che i diversi sistemi di tracciamento siano interoperabili tra di loro**. Gli ambiti sono molteplici e l'Unione europea ha pubblicato recentemente delle regole che gli sviluppatori di queste piattaforme e le autorità sanitarie di ciascun paese devono rispettare. Inoltre, il Parlamento europeo ha auspicato che si utilizzi un modello decentralizzato per il tracciamento, ovvero che i dati rimangano nel dispositivo di ciascun cittadino il quale genera anche il codice identificativo personale anonimo. Il governo italiano ha comunicato che seguirà questo modello. Viceversa, il modello centralizzato, come quello adottato in Francia e in Germania, prevede che i dati non rimangano sul cellulare ma vengano raccolti da un server centrale, il quale genera anche i codici identificativi anonimi per ciascun utente. Ad ogni modo, è molto probabile che il modello decentralizzato **diventi quello seguito dalla maggior parte dei paesi**, non solo perché tutela di più la privacy del cittadino, ma perché quello centralizzato potrebbe non essere compatibile con i dispositivi Apple (iOS) e Google (Android). I due colossi americani sono in prima linea per evitare che i governi centrali possano raccogliere dati sistematicamente dai loro utenti. Infatti, se rendessero questa eventualità disponibile in un paese, lo sarebbe per tutti, **inclusi i regimi autoritari**. Il coordinamento e la compatibilità tra le diverse soluzioni sviluppate e i diversi sistemi operativi è fondamentale per ottenere interoperabilità e quindi universalità tecnica. Inoltre, Apple e

Google hanno annunciato di voler sviluppare loro stessi dei sistemi di tracciabilità integrati ai loro dispositivi, anche se si prevede che non saranno pronti prima dell'anno prossimo.

Rimangono tuttavia altre criticità, come quella concernente **il *digital divide***, e la **cybersecurity** dei dispositivi e dei dati. Uno dei maggiori punti critici sul quale occorre lavorare è la necessaria universalità di questi sistemi di tracciamento. Tuttavia, secondo uno studio del Financial Times in realtà essi escluderebbero diversi segmenti della popolazione come chi non possiede uno smartphone (spesso anziani, meno abbienti) o chi ha cellulari vecchi anche solo di cinque anni con sistemi operativi non aggiornabili. Perciò, non vi è solo il rischio di aumentare il ***digital divide*** tra regioni, paesi o fasce della popolazione, ma anche di **non avere una copertura minima necessaria** affinché la tracciabilità abbia effetto. Pensiamo al caso italiano: si stima che per essere efficace Immuni dovrebbe essere scaricata ed utilizzata almeno dal 60% della popolazione. Considerato che il 71% degli italiani possiede uno smartphone (e non entriamo nel merito di che modello sia), significa che almeno l'85% di questi debba scaricare l'app.

Infine, è necessario un accenno agli aspetti di **cybersecurity**. Sebbene la tecnologia Bluetooth sia più sicura rispetto ad altre, le criticità si riscontrano nel momento di **raccolta e stoccaggio dei dati sanitari**. Domenico Arcuri ha dichiarato che le informazioni relative al tracciamento saranno conservate in un server o *cloud* italiano e pubblico (alla luce della scelta di un modello decentralizzato, resta da capire quali dati saranno raccolti). Infine, in molti hanno sottolineato che il codice sorgente delle app debba essere *open source* per permettere a chiunque di controllare la corretta scrittura e funzionamento del software. La ministra Paola Pisano ha annunciato che presto sarà rilasciato con licena *open source* MPL 2.0 il codice sorgente di Immuni. Ciò avrebbe effetti positivi anche rispetto **all'economia del dato**. La licenza, infatti, permetterebbe di creare spillover di sviluppo di ulteriori piattaforme in perfetta sinergia con quanto già presente sul mercato.

LA *DATA PROTECTION* AI TEMPI DEL CORONAVIRUS TRA PREVENZIONE DEI REATI E REPRESSIONE DEL CONTAGIO

Massimo Farina[*]

**** 20 marzo 2020 ****

1. La recente e virulenta epidemia che ha gradualmente conquistato lo scenario nazionale, europeo ed internazionale rivela tutta la delicatezza degli interessi individuali e collettivi posti in gioco. Riecheggiano prepotentemente, nelle difficoltà interne tese ad apprestare idonee garanzie ai contrapposti interessi, l'insegnamento dell'Alexy sul bilanciamento tra principi costituzionali e sulla teoria dei diritti fondamentali (*Teoria dell'argomentazione giuridica. La teoria del discorso razionale come teoria della motivazione giuridica*, Milano, 1998). Tali insegnamenti, tuttavia, risultano di più ardua e critica applicazione alla luce del dinamismo ordinamentale e delle fonti del diritto multilivello, implicando necessariamente un confronto dialogico con le fonti del diritto sovranazionale e con le più recenti generazioni di diritti fondamentali. Nel corso degli ultimi anni, invero, è stata riposta a livello europeo un'attenzione crescente alla protezione dei dati personali relativi alle persone fisiche: in effetti, tanto l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, quanto l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Ciononostante, il riconoscimento giuridico non impedisce la verificazione di nuove sfide per la protezione dei dati personali, provocate dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione: in tali casi, è posto nelle mani delle istituzioni pubbliche il delicato compito del contemperamento, attraverso il sugello impresso da atti politici a contenuto variamente normativo.

Tale scenario si riespande nell'attuale momento storico, ove la tecnologia si dimostra idoneo strumento per il controllo della popolazione (C. Faralli, *Diritti e nuove tecnologie*, in *Rivista di scienze della comunicazione e di argomentazione giuridica* n. 2/2019, 43 ss). Si tratta di una prassi già a lungo invalsa in Cina, tesa a garantire l'ordine pubblico e la sicurezza. In

[*]Ricercatore presso l'Università degli Studi di Cagliari, DIEE, docente di Diritto dell'Informatica e delle Nuove Tecnologie e di Informatica Forense. Mail: m.farina@unica.it. Il contributo è stato accettato per la pubblicazione nell'ambito della call *Diritto, diritti ed emergenza ai tempi del Coronavirus*, su BioLaw Journal – Rivista di BioDiritto.

particolare, la peculiare forma di stato cinese ha da sempre trovato un valido supporto nell'impiego dei sistemi di videosorveglianza (ad esempio, attraverso l'impiego dei droni), nel riconoscimento biometrico e nella geolocalizzazione. Di conseguenza, si è assistito in questo periodo di emergenza sanitaria al riadattamento degli strumenti tecnologici di controllo: si pensi, ad esempio, all'impiego dei sistemi di videosorveglianza per intercettare le persone che non indossavano una mascherina, ovvero per effettuare una scansione termica contactless, così da individuare eventuali stati di alterazione febbrile. Al contempo, tuttavia, lo smartphone rappresenta lo strumento tecnologico privilegiato per l'implementazione delle politiche pubbliche: sono state infatti create, d'intesa con il governo cinese, apposite applicazioni per il monitoraggio e l'attuazione delle politiche per il contenimento dell'epidemia. Tali app, in particolare, utilizzando i big data in possesso della sanità cinese, procedeva attraverso strumenti di Intelligenza artificiale all'identificazione dei potenziali portatori di virus, che venivano così assoggettati all'obbligo di quarantena forzata e coatta.

Il ricorso a simili misure, ed in particolare quelle relative alla geolocalizzazione, per quanto riscontratesi efficaci per la riduzione dei contagi, è attualmente oggetto di acceso dibattito a livello europeo. Nonostante la recente posizione adottata dall'*European Data Protection Board* (*Statement on the processing of personal data in the context of the COVID-19 outbreak*) sembrerebbe sopire l'acredine, si scorgono ulteriori criticità se il trattamento dei dati personali raccolti venga effettuato per finalità di prevenzione del crimine. La prospettiva non risulta invero utopica: come è noto, a seguito delle recenti misure normative sull'obbligo di quarantena, si è affermato che il mancato rispetto di tali prescrizioni possa configurare i delitti di epidemia (di cui agli artt.438 e 452 c.p., a seconda che il reato sia stato compiuto, rispettivamente, con dolo o colpa) e del più mite reato contravvenzionale di cui all'art. 650 c.p.

Lo scarso rispetto di tali misure, inoltre, sta progressivamente inducendo i vari Stati membri dell'Unione al ricorso a strumenti di controllo e monitoraggio degli spostamenti dei propri cittadini. Tale opzione, tuttavia, non si traduce esclusivamente nel trattamento di dati personali per la tutela di interessi vitali degli interessati, considerato lecito ai sensi dell'articolo 6, paragrafo 1, del Regolamento 2016/679/Ue: piuttosto, tali attività di trattamento potrebbero essere sorrette da ragioni di ordine pubblico, da finalità di prevenzione, indagine, accertamento e perseguimento dei reati sopra citati. Simili finalità, in altri termini, legittimerebbero l'attività di monitoraggio delle competenti autorità di controllo, ai sensi della Direttiva 2016/680/Ue. Tale Direttiva, che compone assieme al coevo Regolamento n. 679 (il cd. GDPR) e alla

Direttiva n. 681 (sul trattamento dei dati del codice di prenotazione delle prenotazioni aeree) le misure predisposte dal legislatore dell'Unione per assicurare una completa protezione dei dati personali, potrebbe trovare in questo particolare momento storico piena applicazione, sollevando molteplici criticità ed osservazioni, che si tenterà qui di sintetizzare.

2. La Direttiva 2016/680/Ue inaugura un nuovo versante per l'applicazione della *data protection* nel settore della cooperazione giudiziaria e di polizia in materia penale. In passato, invero, la disciplina era affidata alla competenza del Consiglio ed era sprovvista di uno strumento giuridico di portata generale nel settore in esame: per tali ragioni, a seguito delle esigenze già evidenziate nel 2005 dalla Commissione, il Consiglio emanò la Decisione quadro 2008/977/GAI: ciononostante, la Decisione quadro non ha registrato alcun significativo progresso nella realizzazione di standard e regole comuni in materia di *data protection*, rivolgendosi agli Stati membri con un approccio minimalista, escludente dal proprio ambito di applicazione il trattamento dei dati svolti all'interno dei confini nazionali. Alla luce del flebile contesto normativo, pertanto, la Direttiva 2016/680/Ue apporta un notevole miglioramento, dimostrando tutto l'intento del legislatore dell'Unione di armonizzare un settore così delicato. Con essa, infatti, si è proceduto all'abrogazione della Decisione quadro 2008/977/ AI e all'obbligo di recepimento, per tutti gli Stati membri, entro il 6 maggio 2018. L'Italia ha provveduto al recepimento della Direttiva attraverso il d.lgs. del 18 maggio 2018, n. 51, limitandosi ad una mera riproduzione del testo normativo di rango europeo. In ogni caso, tale scelta non esautora l'efficacia della Direttiva ed il contenuto delle sue disposizioni, che, alla luce del contesto attuale, assumono nuova colorazione.
Preliminarmente, si osserva che la Direttiva n. 680 consente il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali. Sul punto, l'art. 3, lett.g), specifica che per "autorità competente" debba intendersi (*i*) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ovvero (ii) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica. Ne discende, pertanto, che il trattamento possa esser svolto dalle autorità di

pubblica sicurezza (come ad esempio dalla Polizia di Stato, ovvero dalla Polizia Postale), oltre che dalla magistratura inquirente.

Procedendo con la disamina della Direttiva, inoltre, si scorgono molteplici similitudini con le disposizioni contenute nel Regolamento n. 679, per quanto concerne i principi sul trattamento dei dati personali, sul rapporto tra titolare del trattamento e soggetto interessato, nonché dei diritti che quest'ultimo può far valere nei confronti del titolare per garantire la piena protezione dei propri dati. In effetti, l'articolo 12 della Direttiva corrisponde, specularmente, all'articolo 12 del Regolamento, che imprime regole di condotta per il trattamento dei dati personali, basato su canoni di trasparenza, liceità e correttezza: il titolare del trattamento, pertanto, dovrebbe comunicare al soggetto interessato tutte le informazioni relative al trattamento, in forma concisa, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Sul punto, tuttavia, la Direttiva introduce un regime derogatorio rispetto agli oneri informativi che il Regolamento attribuisce categoricamente in capo al titolare del trattamento. Viene in rilievo, in particolare, l'articolo 13, paragrafo 3, della Direttiva: tale disposizione, infatti, stabilisce che gli Stati membri possano adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato, ogniqualvolta ciò comprometta le indagini, la prevenzione o il perseguimento dei reati, ovvero la sicurezza pubblica e, nondimeno, i diritti e le libertà fondamentali altrui. La norma, pertanto, non solo consente il differimento, ma legittima qualsiasi forma di manifestazione preventiva di comunicazione. Ciò si traduce, nell'attuale contesto empirico di riferimento, nella possibilità, per le autorità di pubblica sicurezza, di geolocalizzare i soggetti sottoposti a quarantena obbligatoria, per monitorare gli eventuali spostamenti non concessi, condotta che potrebbe assumere rilevanza ai sensi dell'art. 438 c.p.; in tal senso, l'attività di trattamento potrebbe risultare preordinata a prevenire il reato di epidemia, garantendo al contempo la sicurezza pubblica e la tutela dei diritti fondamentali altrui alla salute e, alla luce del particolare fenomeno pandemico, alla vita stessa. Le attività di trattamento condotte *inaudita altera parte*, inoltre, potrebbero essere volte a verificare la veridicità delle dichiarazioni contenute all'interno delle autodichiarazioni che ogni cittadino deve compilare per legittimare i propri spostamenti: si ricorda, al riguardo, che l'art. 483 c.p. punisce chiunque attesti falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità. In tal caso, l'autorità pubblica potrebbe monitorare gli spostamenti del soggetto, al fine di constatarne la corrispondenza rispetto ai tragitti dichiarati nell'autodichiarazione; inoltre – e questo potrebbe costituire un punto molto critico –, attraverso

l'incrocio dei dati relativi alla dislocazione dei contagiati presenti in un predeterminato raggio d'azione, si potrebbe verificare se l'interessato sia entrato più o meno volontariamente in contatto con un altro soggetto positivo al virus.

Infine, il regime derogatorio introdotto all'articolo 13, paragrafo 3, riduce le tutele che sono invece predisposte dal Regolamento n. 679: più precisamente, ai sensi della Direttiva, l'autorità pubblica potrà omettere ogni comunicazione all'interessato avente ad oggetto il periodo di conservazione dei dati personali, la base giuridica per il trattamento, le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali, ma soprattutto ulteriori informazioni, in particolare nel caso in cui i dati personali siano raccolti all'insaputa dell'interessato. Il riferimento a "ulteriori informazioni" risulta alquanto vago e ambiguo, potendo costituire un parametro di incertezza definitoria che potrà essere colmato, in misura eterogenea e variabile, da ciascun Stato membro.

In conclusione, alla luce delle molteplici criticità sommariamente evidenziate, è evidente che l'impiego della tecnologia possa apportare significativi benefici per la tutela della salute. Al contempo, occorre riflettere sul rapporto tra utilitarismo e tutela della collettività, al fine di scorgere il grado massimo di compressione dei diritti del singolo, per apportare benefici generalizzati all'intera collettività.

Tale riflessione è tanto più necessaria alla luce delle disposizioni contenute nella Direttiva 2016/680/Ue, confinata fino ad ora nel dimenticatoio, all'ombra del Regolamento 2016/679/Ue (il cd. GDPR), che fino ad ora ha ricevuto maggiore clamore mediatico. I tempi particolari, tuttavia, potrebbero in realtà costituire la prima vera e utile occasione per rivitalizzare la valenza applicativa della Direttiva, che costituisce fino ad ora un obliato fondamento giuridico che giustificherebbe il ricorso alla tecnologia per il contrasto al contagio.

01 Apr Per governare l'epidemia (e non uccidere il paese) serve il digitale

in Quaderno 6 - 2020 by Vittorio Ferla 0 Commenti

di Vittorio Ferla

Per quanto durerà il tempo del contenimento contro il Coronavirus? Inutile girarci intorno: durerà a lungo. Secondo le previsioni, la curva dei contagiati non potrà decrescere seriamente prima della fine di aprile. Ovviamente, ciò non esclude che molti positivi al virus saranno ancora presenti sul territorio nazionale, con il rischio di riattivare focolai di contagio. Senza contare il passaggio possibile, salvo chiusura delle frontiere, di nuovi infetti provenienti da altri paesi europei, dove il virus comincia a circolare con qualche settimana di ritardo rispetto all'Italia. Non sappiamo se il caldo della bella stagione sarà in grado di sospendere la circolazione del virus. Che, in ogni caso, tornerà in circolazione con l'arrivo del freddo, riprendendo vigore in autunno e in inverno. Anche i tempi per l'individuazione e uso del vaccino – studio, sperimentazione, produzione, distribuzione – saranno lunghi (si parla di almeno un anno, più probabilmente 18 mesi). Se è vero tutto ciò che abbiamo qui elencato, significa che le misure di contenimento e di isolamento, non si sa con quale grado di intensità, non potranno essere completamente superate per diversi mesi.

Ci vuole tempo. Ma servono soluzioni

Che cosa succederà nel frattempo? Difficile immaginare di tenere impegnati gli italiani a cantare da finestre e balconi l'inno d'Italia o Azzurro o Poo-poroppo-popo-poo, a un'ora indicata, ogni giorno per molte settimane. Così come sembra improbabile tenere chiuse tanto a lungo le attività economiche senza impedire la distruzione di lavoro e l'impoverimento generalizzato fino al tracollo totale del paese. Senza dimenticare l'impatto psicosociale della restrizione in casa con la possibile esplosione di conflitti, depressione, attacchi di panico, abuso di sostanze, omidici e suicidi.

C'è da chiedersi se non sia questo il momento di cercare altre soluzioni, ispirandosi non tanto o non soltanto alle misure costrittive cinesi – impedire la libertà di movimento e la libertà d'impresa, certamente più 'facili' in un regime autoritario – quanto, piuttosto, alle misure 'tecnologiche' – basate sull'intelligenza artificiale e sui big data – applicate in Corea del Sud, Singapore, Taiwan. La risposta a questa domanda è certamente: "sì".

Come ha risposto l'Italia

Ma prima di capire quali sono queste misure tecnologiche, ricordiamo quali sono i capisaldi della nostra reazione all'arrivo dell'epidemia. Com'è normale che sia, l'Italia ha messo in campo le attitudini che meglio la caratterizzano. La risposta medico-sanitaria, fondata sul Servizio sanitario nazionale, considerato uno dei migliori nel mondo (è così almeno al Nord, dove si trova l'epicentro della crisi). L'attenzione ai più vulnerabili, anziani, portatori di patologie e malati cronici, che, purtroppo, in molti casi, non riescono a sopravvivere al contagio. La vocazione all'emergenza nata e gestita dalla Protezione civile nella gestione dei terremoti e fondata sull'apporto dei volontari. La

capacità di sacrificio morale e di partecipazione civica dei cittadini che, dopo una breve fase di sorpresa, sembrano rispondere bene alle misure contribuendo attivamente alla realizzazione di una politica pubblica nazionale. Infine, la promessa di intervento statale, forzando definitivamente i vincoli europei, per fornire aiuto a quei lavoratori e a quelle imprese che subiranno tutto il peso della chiusura forzata delle attività.

Tuttavia, ognuna di queste positive attitudini nazionali ha dei risvolti preoccupanti. Il Ssn non è così forte come si pensa: il numero di posti di terapia intensiva al Nord non è adeguato alla quantità di contagiati che necessitano di cure e molte regioni del Sud rischiano il collasso se i numeri degli infetti fossero gli stessi della Lombardia. La stessa Protezione civile non sembra più la stessa di qualche anno fa e non è ancora stata utilizzata per realizzare quelle zone di assistenza intermedia tra l'isolamento in casa e l'acuzie in ospedale che la Cina ha messo in piedi nelle palestre e nei capannoni. In più, essere bravi ad agire in stato di emergenza potrebbe significare che non lo siamo nel governo ordinario dei processi. Dei cittadini abbiamo già detto che potranno sopportare restrizioni pesanti soltanto per un tempo definito oltre il quale le cose, soprattutto sul piano economico, potrebbero diventare disastrose. Non parliamo poi dello stato del debito pubblico italiano, la cui situazione è nota, e che non potrà che peggiorare quando bisognerà ulteriormente indebitarsi – al quel punto sarà giusto farlo, ovvio – per affrontare la recessione da virus.

-

Che significa "governare" nel corso di un'epidemia?

Tutto questo può bastare? Al netto della enorme riconoscenza per tutti coloro i quali, ogni giorno, fanno il massimo per salvare le vite dei cittadini, la risposta probabilmente è: "no".

L'Italia non può limitarsi all'approccio clinico-sanitario suggerito da medici e scienziati benemeriti. Né consegnarsi alle strategie repressive di un regime totalitario come la Cina. Il governo del paese non può ridursi alla resistenza al virus. La tutela della salute e della vita ha la precedenza, ma non può ammalare l'Italia di povertà. Stiamo salvando i più vulnerabili ma rischiamo alla fine di ritrovarci in un paese di zombi. La prudenza – splendida virtù cardinale – che ci ha fatto chiudere l'Italia a marzo dovrebbe dirci che l'harakiri non può essere lo strumento ideale per fronteggiare Covid-19. Insomma, il problema del governo è un po' più complesso dell'impedire il sovraccarico degli ospedali. La scelta fatta dal nostro governo, dopo tanti tentennamenti, è radicalmente diversa rispetto a quella – a dir poco temeraria – che farà il Regno Unito, ma potrebbe rivelarsi comunque un azzardo. Sempre che l'azione emergenziale contro l'epidemia non si trasformi presto in una strategia di governo capace di convivere con una epidemia ancora presente (con il rischio che i contagi possano comunque riprendere), di prevenirne le possibili conseguenze future e garantire l'esercizio di una normale vita lavorativa ed economica.

Quali sono gli altri strumenti di governo? Certamente gli investimenti specializzati in sanità per aumentare il personale medico-sanitario e creare strutture sanitarie ad hoc. La realizzazione di strutture di assistenza intermedia o di quarantena utilizzando quartieri fieristici, palestre e fabbricati. La trasformazione (o l'ampliamento) delle catene produttive (per esempio, al fine di fabbricare la quantità necessaria di mascherine o di tamponi). Potrebbe essere necessario perfino un controllo ferreo delle frontiere per impedire il contagio "di ritorno". Ma soprattutto bisogna fare una cosa: usare la tecnologia. Come è successo in Corea del Sud, a Singapore, a Hong Kong e a Taiwan (dove il numero di decessi e di contagi è proporzionalmente inferiore rispetto a quello del nostro paese).

Buone pratiche dai paesi asiatici (no, non parliamo della Cina)

"Ciascuno a suo modo, Singapore, Taiwan e Hong Kong – tre posti con caratteristiche socioeconomiche e politiche notevolmente diverse – sono stati in grado di interrompere la catena della trasmissione della malattia. E lo hanno fatto senza abbracciare le misure drastiche e altamente dirompenti adottate dalla Cina. Il loro successo suggerisce che anche altri governi possono fare progressi". Così scrive sul New York Times Benjamin J. Cowling, professore di epidemiologia delle malattie infettive all'Università di Hong Kong.

A **Hong Kong**, per esempio, città che condivide un confine con la Cina continentale ed è formalmente parte della Cina, spiega Cowling, "subito dopo il primo caso dichiarato a Wuhan, sono state ampliate le stazioni di screening della temperatura esistenti nei luoghi di ingresso e ai medici locali è stato chiesto di segnalare alle autorità sanitarie della città qualsiasi paziente con febbre o sintomi respiratori acuti risalendo alla 'storia' del recente viaggio a Wuhan". Dopo i primi cinque giorni di controlli, prosegue Cowling, "chiunque attraversava il confine – specie se proveniente dalla Cina continentale – doveva sottoporsi a un periodo obbligatorio di auto-quarantena di 14 giorni. Allo stesso modo sono stati rintracciati e messi in quarantena quanti hanno avuto stretti contatti con i positivi registrati. E siccome la trasmissione poteva verificarsi prima che una persona infetta mostrasse i sintomi, la tracciatura ha incluso tutte le persone che erano entrate in contatto con il paziente a partire da due giorni prima dell'inizio della sua malattia".

Tra le buone pratiche segnalate dalla Technology Review del MIT di Boston c'è il monitoraggio che la **Corea del Sud** sta realizzando sui cittadini in quarantena tramite una app per smartphone – sia Android che iPhone – sviluppata dal Ministero degli Interni e della Sicurezza. In sostanza, come ricorda Max S. Kim nell'articolo, "migliaia di persone nel lockdown del coronavirus saranno monitorate per rilevare i sintomi, per assicurarsi che restino a casa e che non diventino dei 'super-diffusori' del virus; per tenere traccia della loro posizione e per assicurarsi che non stiano rompendo la quarantena sarà utilizzato anche il GPS". L'adozione di queste misure di monitoraggio tecnologico ha considerevolmente limitato l'esplosione dei contagi e, di conseguenza, dei decessi.

"C'è un limite alle risorse umane disponibili per i governi locali per monitorare le persone in quarantena", afferma Jung Chang-hyun, funzionario del ministero che ha supervisionato lo sviluppo dell'app. "L'app è un servizio di supporto volto a rendere più efficiente l'attività di osservazione".

Aggiunge Jung: "Le persone possono uscire dalle aree di quarantena sia intenzionalmente che per errore: ma poiché esiste il rischio di infezione secondaria in entrambi i casi, speriamo che l'app, con una maggiore organizzazione, possa aiutare a bloccare questi incidenti". L'app si unisce a un elenco di altre misure lanciate per combattere l'ondata di nuovi casi in Corea del Sud, tra cui: le stazioni di test "drive-through" per verificare la positività al coronavirus (circa 15 mila al giorno in più), una serie di servizi cartografici sviluppati da privati che monitorano gli spostamenti dei positivi, gli avvisi di emergenza che i governi municipali e distrettuali inviano regolarmente ai telefoni delle persone per informarli di nuovi casi di coronavirus. Ricordiamo che in Corea del Sud, dopo l'esplosione iniziale la curva dei contagi ha già iniziato a flettere: mentre scriviamo, sono morti circa 70 pazienti su circa 8 mila contagi (numeri assai modesti rispetto al caso dell'Italia). Importante la disponibilità del governo sudcoreano a condividere la sua tecnologia con altre nazioni: "Non abbiamo ancora avuto richieste da altri paesi, ma se arrivassero, saremmo pronti a condividere assolutamente queste esperienze", assicura Jung.

Qualcosa del genere è accaduto a **Singapore**. "Colpita in anticipo, per il fatto di essere uno dei principali partner commerciali della Cina, ma forte dell'esperienza con il virus SARS del 2002-3, Singapore ha iniziato a monitorare attentamente i casi per trovare i punti in comune che li

collegavano. Nel giro di un giorno o due, successivi alla scoperta di un nuovo caso, le autorità sono state in grado di mettere insieme la complessa catena di trasmissione da una persona all'altra, come un moderno Sherlock Holmes in possesso di un database. A partire da febbraio, tutti coloro che sono entrati in un edificio governativo o aziendale a Singapore hanno dovuto fornire i dettagli di contatto per accelerare il processo". A raccontare la vicenda di Singapore, ancora una volta sulla Technology Review del Mit, è Spencer Wells, genetista, antropologo, già collaboratore della National Geographic Society. Secondo Walls, "non è semplicemente la capacità di rilevare i casi e spiegare perché sono successi che rendono Singapore un modello di riferimento in questa epidemia: kit di test per acido nucleico sono stati rapidamente sviluppati e distribuiti nei luoghi di entrata al paese. Entro tre ore, mentre gli individui vengono messi in quarantena sul posto, i funzionari possono confermare se sono stati infettati o meno dal virus prima di consentire loro di entrare".

Il caso di **Taiwan** – a un passo dall'epicentro dell'epidemia, quasi 24 milioni di abitanti, più del doppio della Lombardia, concentrati in poco più di 36 mila km quadrati – lo racconta bene sul suo profilo Twitter Fabio Sabatini, docente di politica economica dell'Università La Sapienza. "Data la frequenza dei voli dalla Cina, si prevedeva che Covid-19 avrebbe travolto l'isola, invece ha registrato soltanto 50 contagi e 1 decesso: come hanno fatto?", si chiede l'economista. Ecco la sua ricostruzione: "Grazie all'esperienza della SARS, Taiwan ha riconosciuto subito l'emergenza. Il 31 dicembre 2019, tutti i passeggeri provenienti da Wuhan sono stati sottoposti a screening a bordo, prima di scendere dall'aereo. I passeggeri sbarcati da Wuhan nei 14 giorni precedenti sono stati rintracciati e visitati. Quelli con sintomi sospetti sono stati messi in quarantena e accuratamente monitorati. Pochi giorni dopo, le autorità hanno integrato il database delle informazioni sanitarie di tutti i cittadini con i dati dell'agenzia dell'immigrazione. Sono state rintracciate tutte le persone a rischio, che avevano recentemente manifestato sintomi e avevano storie di viaggio sospette. Inoltre, il sistema integrato genera un allarme ogni volta che un paziente a rischio chiede assistenza medica, consentendo ai sanitari di identificare immediatamente i potenziali casi di Coronavirus". Ovviamente non è mancata la fase del contenimento anche a Taiwan. Ma anche questo è stato realizzato con strumenti digitali. "I pazienti a rischio – perché con sintomi, per aver transitato in aree a rischio nei 14 giorni precedenti o per eventuali contatti con dei contagiati – sono messi in quarantena e testati. Inoltre – avverte Sabatini – devono installare sullo smartphone una app per il monitoraggio di sintomi e spostamenti. Grazie al sistema di tracciamento mediante lo smartphone, è possibile ricostruire la rete di contatti di tutti i contagiati, al fine di testarli, curarli in isolamento e interrompere la catena di contagio". Come si legge nell'editoriale di Jason Wang, della Stanford University, pubblicato sul Journal of The American Medical Association, il governo ha informato i cittadini con conferenze stampa e comunicati estremamente dettagliati: "un po' diversi dai bollettini della nostra Protezione Civile, purtroppo", chiosa Sabatini. È stato spiegato pubblicamente che, a causa dell'emergenza, gli ospedali e le farmacie avrebbero temporaneamente avuto accesso alle informazioni sui viaggi dei pazienti. Secondo i sondaggi il pubblico ha reagito molto bene. Nel frattempo scuole, università, palestre e ristoranti sono rimasti aperti. Se e quando il virus si diffonderà, le autorità potranno così contare su un sistema di contrasto già ben rodato.

Tracce digitali per impedire il contagio (e salvare l'economia)

Ovviamente, ricorda Sabatini, "per noi è tardi e il lockdown è necessario. Tuttavia, c'è il rischio che, se non si tracciano i contagiati e la loro rete di contatti al fine di isolarli e curarli, al primo allentamento del lockdown l'epidemia riprenderà a galoppare".

Una deduzione confermata dal paper appena pubblicato su Lancet per il quale bastano pochi casi isolati in circolazione per rilanciare il contagio. In conclusione, avverte Sabatini, "in Italia abbiamo bisogno di un sistema di tracciamento simile a quelli dei paesi orientali che stanno riuscendo, per ora, a contenere l'epidemia. Che cosa aspettiamo?".

Nelle scorse settimane due studiosi come Alfonso Fuggetta, professore di Informatica del Politecnico di Milano, e Carlo Alberto Carnevale Maffè, docente di Strategia dell'Università Bocconi, hanno proposto alle istituzioni italiane un progetto per l'uso di big data per il governo strategico dell'epidemia. Ma sono rimasti inascoltati. "La Corea del Sud sta sconfiggendo l'epidemia anche grazie a semplici tecnologie di *contact tracing* del contagio su smartphone. In Italia, è stato proposto alle autorità l'uso delle stesse tecnologie, settimane fa, ma hanno preferito il modulo cartaceo con l'autodichiarazione", ha scritto Carnevale Maffè su Twitter. "In Corea del Sud – aggiunge Carnevale Maffè in un altro tweet – il fattore di riproduzione (R0) è già stimato sotto 1, grazie alla georeferenziazione dei casi di contagio e alla identificazione dei singoli focolai su mappe molto precise. Le tecnologie salvano la vita, nel rispetto della privacy". Questo perché la proposta si basa su un processo di raccolta dei dati in forma anonima e quindi nel pieno rispetto della privacy delle persone. Verrebbe da dire che, di fronte ai limiti della libertà di movimento e di impresa, alla distruzione del lavoro, all'impoverimento generalizzato e al suicidio dell'economia di un intero paese, una piccola rinuncia alla privacy non sarebbe poi così grave. Qualcuno potrebbe pure obiettare che non ci sono risorse sufficienti per un'operazione del genere. Ma ne servirebbero infinitamente di meno rispetto a quelle che saranno necessarie per resuscitare l'economia.

(Pubblicato su Linkiesta il 16 marzo 2020)

Il contact tracing via app: quale strategia usare

Dopo la scelta della app italiana per il tracciamento via telefono, sono arrivate anche Apple e Google a dare man forte per limitare i contagi. Ecco pregi e difetti delle diverse strategie

(illustrazione: Getty Images)

di Giuseppe Attardi, università di Pisa
ed Enrico Santus Aversano, Bayer

Il commissario straordinario all'**Emergenza Covid-19**, **Domenico Arcuri**, ha deciso di adottare la soluzione **Immuni**, proposta dalla società **Bending Spoons** e indicata dalla task force del ministero dell'Innovazione e digitalizzazione, guidato da **Paola Pisano**, tra le più di 300 raccolte in risposta alla fast call dello stesso ministero.

Proviamo a riflettere su questa scelta e su cosa si dovrà fare perché possa risultare efficace, nell'interesse di tutti. Nel seguito analizzeremo la versione in cui la app **Immuni** utilizza solo **Bluetooth** per rilevare i contatti tra persone e memorizzi i dati localmente sui dispositivi.

Questa è la soluzione seguita a **livello internazionale** dal progetto **Covid Watch**, dal consorzio **Pepp-Pt**, e adottato nel framework proposto congiuntamente da **Apple** e **Google**.

Tecnologia Bluetooth

La soluzione **Immuni** può utilizzare la tecnologia **Bluetooth** per tracciare per raccogliere segnali unidirezionali (*beacon*) di presenza ravvicinata tra i dispositivi mobili (smartphone) che due persone portano con sé.

Bluetooth ha diversi vantaggi: la versione **Bluetooth Low Energy** consuma **poca energia** e quindi il segnale può restare sempre attivo senza scaricare troppo la batteria; il segnale si propaga fino a **pochi metri** e la sua intensità permette di calcolare la **distanza** tra i dispositivi, evitando quindi di raccogliere troppi falsi positivi. Al contrario, i rilevamenti tramite Gps non consentono di distinguere per esempio se due persone si trovano in stanze diverse o in piani diversi di uno **stesso edificio**, e peggio ancora la localizzazione all'interno di celle telefoniche rischia di considerare decine di persone come presenti tutte **nello stesso luogo**. Tralasciamo poi i riflessi sulla **privacy** del dover raccogliere la posizione e i movimenti di tutti i cittadini per lungo tempo.

Un altro vantaggio della soluzione Bluetooth è che può operare anche **in assenza di connessione internet**, scambiando segnali direttamente tra i dispositivi e senza intermediari.

Quindi la scelta della soluzione Immuni può essere considerata condivisibile

Le altre iniziative

Nei mesi scorsi diversi gruppi in tutto il mondo hanno studiato e proposto soluzioni basate su **Bluetooth**, con varianti rispetto ai dati raccolti e alle garanzie di riservatezza.

Alcune di queste soluzioni combinano Bluetooth con la raccolta di informazioni di geolocalizzazione tramite Gps: per esempio **SafePaths del Mit Medialab**, che utilizza una tecnica di cifratura dei percorsi (Path) per assicurare la privacy degli utenti. La app messa per prima in uso effettivo è stata **TraceTogether** a **Singapore**, che oltre a tracciare le posizioni degli utenti, raccoglie anche il loro **numero telefonico** per poterli contattare per segnalare un rischio di contagio. Gli sviluppatori di **TraceTogether** si sono anche impegnati a un'analisi dettagliata di misura dei segnali emessi da dispositivi di marche diverse, per poter stimare con maggiore accuratezza la distanza effettiva. Con il rilascio del codice sorgente open source di **TraceTogether**, queste informazioni potranno essere utili anche in altre app simili.

Covid Watch è invece una soluzione sviluppata in collaborazione con l'università di Stanford, che per prima ha proposto e rilasciato il **17 marzo 2020** una soluzione Bluetooth originale che non richiede l'uso di **localizzazione**.

L'idea originale della soluzione è che ai fini del tracciamento epidemiologico dei contagi, non è necessario sapere **dove** sia avvenuto un possibile contagio, ma basta sapere **quando** è avvenuto e fare in modo che i diretti interessati, e solo loro, lo possano venire a sapere.

La app si limita a raccogliere solo dei **codici anonimi** durante un contatto ravvicinato, che cambiano ogni pochi minuti, in modo da non poter essere **né identificati né tracciati**. Spiegheremo più avanti il meccanismo, perché è simile a quello successivamente proposto da Apple e Google.

Un altro vantaggio della soluzione è che lo spazio necessario per memorizzare i dati raccolti è minimo (poche decine di KB al giorno) e quindi sarebbe possibile utilizzarla anche su **dispositivi più piccoli**, come i braccialetti di fitness. In tal caso si potrebbe accoppiare il tracciamento con la raccolta di **dati sanitari**, che possono essere utili per la diagnosi, quando c'è un sospetto di contagio.

Tutte queste soluzioni citate sono state rilasciate con codice open source e sono disponibili su repository di codice pubblici.

La stessa tecnica di scambio di identificativi anonimi attraverso Bluetooth è adottata anche da Pan-European Privacy-Preserving Proximity Tracing, un'organizzazione svizzera a cui partecipano ricercatori da 8 paesi europei.

Nella versione Bluetooth, Immuni pare segua lo schema di riservatezza basato sullo scambio di codici casuali

Tutte le soluzioni Bluetooth si sono però dovute scontrare con un problema riguardante l'**attivazione del segnale** sugli iPhone o altri **dispositivi iOs** di Apple. Quando la app viene messa in background, su iOs il segnale si spegne, diversamente da quanto avviene su **Android**. Pertanto la soluzione Bluetooth non è pienamente utilizzabile su iPhone, ed esclude dalle possibilità di partecipare al tracciamento circa il **25%** dei possessori di smartphone in Italia.

Vari gruppi di sviluppatori si sono pertanto rivolti ad **Apple**, chiedendo di rimuovere questa limitazione, con una lettera aperta: "*Apprezzeremmo molto se poteste rivedere questa restrizione su iOs e considerare di abbandonarla. Molte altre app di contact tracing devono affrontare questo stesso problema*".

La collaborazione tra Apple e Google

Il 10 aprile Apple e Google hanno annunciato un accordo di collaborazione per aiutare le agenzie sanitarie pubbliche a ridurre la diffusione del **coronavirus**, facilitando l'uso della tecnologia **Bluetooth** su un'ampia gamma di dispositivi mobili (smartphone, smartwatch, bracciali di fitness). A tal fine hanno pubblicato le specifiche di un framework di Api che sarà disponibile a metà maggio su tutti i dispositivi iOs e Android. Le autorità sanitarie di ciascun paese potranno sviluppare le proprie app per tracciare i contatti a distanza ravvicinata con persone infette dal virus. Il meccanismo di tracciamento è concepito in modo da consentire la **massima riservatezza** nei confronti di chi lo utilizza, che è comunque libero di scegliere se partecipare al tracciamento.

Oltre al framework che verrà rilasciato a breve, **Apple** e **Google** dichiarano l'intenzione di apportare delle modifiche ai rispettivi sistemi operativi e includere una **loro app di tracciamento** nelle versioni rilasciate a partire dall'anno prossimo.

Che fine faranno a quel punto le app sviluppate dalle **singole autorità sanitarie**? Rimarranno disponibili in alternativa e gli utenti potranno scegliere quale usare? Le app di Apple e Google continueranno a comunicare coi server delle rispettive autorità sanitarie? Chi garantisce in questi casi la **riservatezza dei dati**?

A causa della **guerra commerciale** tra Stati Uniti e Cina, **Huawei**, che è uno dei principali produttori di smartphone, non ha più accesso agli aggiornamenti di Google per Android e ha annunciato una propria variante. Sarebbe auspicabile che anche Huawei adotti il framework di Apple e Google, lasciando da parte i conflitti in nome dell'interesse comune alla **salute**. Ricordiamo che il codice di Android è Open Source e casi come questi dimostrano la libertà che questo principio concede agli sviluppatori.

L'intervento di Apple e Google è utile per agevolare l'utilizzo di Bluetooth, ma lascia adito ad alcuni dubbi che esamineremo più avanti

Riservatezza

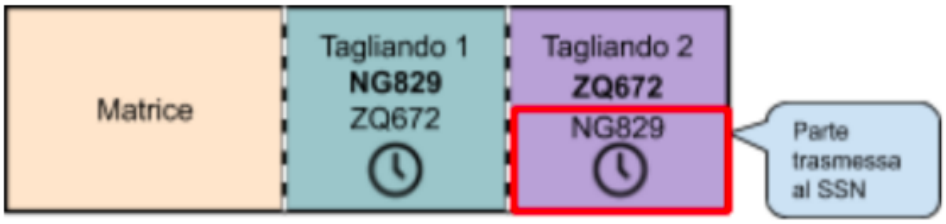
La soluzione di contact tracing proposta da Apple e Google, denominata **Privacy-Preserving Contact Tracing**, sfrutta la tecnologia Bluetooth per raccogliere segnali di presenza (*beacon*) inviati da un'analoga **app di tracciamento**, da una distanza ravvicinata. Di seguito descriviamo in che modo questa soluzione preserva la privacy degli utenti, analizzando cosa traccia e cosa **non** traccia.

Cosa traccia

Se due persone rimangono a distanza ravvicinata per alcuni minuti, il loro contatto viene considerato a **rischio di contagio**. Da un punto di vista epidemiologico, non è cruciale sapere il **luogo fisico** in cui il contatto è avvenuto: è sufficiente ricordare l'**ora**. Il sistema aiuta le persone coinvolte nel contatto a memorizzare sul proprio dispositivo dei dati riguardanti il contatto, ma **nessun dato identificativo dei partecipanti**. La app di tracciamento registra il minimo indispensabile per ricostruire il contatto avvenuto e permettere ai partecipanti di verificare la loro eventuale presenza a uno di essi.

Per garantire l'anonimato la soluzione si basa sull'utilizzo di **numeri casuali**, un po' come nelle estrazioni dei biglietti di una lotteria. Nelle lotterie ogni biglietto è formato da una **matrice** e un **tagliando**. Chi acquista un biglietto stacca il tagliando e lo conserva per sé, privatamente. Dal numero di serie sulla matrice non si può risalire a chi ha comprato il biglietto.

La app di tracciamento dei contatti usa un **meccanismo simile a quello di una lotteria**. Ogni contatto è rappresentato da un biglietto composto da **due tagliandi**, come nella figura seguente, assegnati uno a ciascuno dei due partecipanti: nessuna delle due persone può risalire all'identità dell'altra tramite ciò che è riportato sul tagliando; nessun ente esterno al contatto potrebbe risalire tramite i tagliandi alle identità dei due partecipanti.



In una **lotteria**, dopo che è avvenuta l'estrazione, gli acquirenti dei biglietti vanno a verificare se i loro **tagliandi** appaiono nella lista di quelli vincenti. Nel caso delle **app di tracciamento dei contatti** succede qualcosa di simile: tramite la app fanno una **verifica** del proprio tagliando.

Come avviene però l'**individuazione dei tagliandi da controllare?** Quando i medici diagnosticano una persona infetta dal virus, le chiedono di trasmettere a un **server**, gestito dal servizio sanitario pubblico, una parte dei dati conservati dalla loro app. Bastano le **date** dei contatti e le **chiavi** giornaliere usate dal generatore per produrre numeri casuali, detti **Rolling Proximity Identifier**, la parte cerchiata in rosso nella figura, durante gli ultimi 14 giorni. Nelle specifiche del protocollo questo sottoinsieme di dati viene denominato **Diagnosis Keys**. Anche questi dati vengono conservati in **forma anonima**, senza che nessuno sappia a chi appartengono. Solo l'utente stesso può andare a verificare, attraverso la sua app, se uno dei tagliandi conservati nel proprio dispositivo, coincida con uno di quelli elencati dal servizio sanitario pubblico. In tal caso la app invita la persona a **rivolgersi a un medico**, perché potrebbe essere lo sfortunato *vincitore* della lotteria del contagio.

I numeri dei tagliandi sono **numeri generati casualmente** e quindi non sono riconducibili ad alcuna informazione personale né tracciabili nel tempo perché cambiano **ogni decina di minuti**. Qualcuno teme che venga usato il **Mac address**, il numero univoco dell'interfaccia Bluetooth, il quale potrebbe fare risalire al **dispositivo**. Ma non è così: ciò che viene trasmesso è un numero casuale, che nel protocollo è denominato **Rolling Proximity Identifier**, che solo la app può riconoscere.

Quando due persone si trovano a distanza ravvicinata, si scambiano i **rispettivi numeri casuali**, e ciascuno li conserva sul proprio dispositivo, insieme con l'orario del contatto e l'indicazione della distanza tra i dispositivi, ricavata dalla forza del segnale Bluetooth. Queste informazioni non lasciano il dispositivo fintanto ché la persona **rimane sana**.

Cosa non traccia

Con la tecnica degli identificativi casuali la soluzione **Bluetooth** garantisce la **massima riservatezza** in quanto non tiene traccia gli spostamenti delle persone, non raccoglie informazioni sulla loro posizione, diversamente dalla versione Gps che effettua la geolocalizzazione degli smartphone e consente di "*vedere i suoi spostamenti nello spazio*".

La soluzione opera anche **senza connettività telefonica** e **senza connettività Internet**: opera semplicemente attraverso la segnalazione di un beacon Bluetooth direttamente tra i dispositivi. Perciò non ci sono terzi coinvolti nella raccolta di dati degli utenti.

In conclusione la soluzione basata solo su Bluetooth offrirebbe adeguate garanzie di riservatezza dei dati

***Immuni* e il Framework di Apple e Google**

La soluzione di **Immuni** è stata concepita prima della pubblicazione delle specifiche del Framework di Apple e Google.

Dovrà Immuni adeguarsi e adottare questo framework? A quanto è dato sapere, i principi di base di **Immuni** sono **compatibili col framework**. D'altra parte Apple e Google dichiarano la disponibilità di discutere il protocollo con le autorità sanitarie nazionali.

La libreria di Apple e Google e gli aggiornamenti previsti ai sistemi operativi mobili delle due aziende sono necessari per la piena funzionalità di app come Immuni.

Quindi è auspicabile che Bending Spoons adegui la sua implementazione al framework e si presenti qualificandosi insieme con rappresentanti del Team Digitale a incontri con le due aziende per concordare i passi per l'utilizzo del framework

Criticità

Analizziamo alcuni i problemi di implementazione e di funzionamento della app che potrebbero inficiarne l'efficacia.

Efficacia: tempo di individuazione e diffusione dell'app

Il tracciamento dei contatti può essere efficace se aiuta a individuare i soggetti infetti **prima che abbiano iniziato a infettare altri**. Se A viene individuato come positivo, occorre rintracciare ogni

persona B con cui è entrato in contatto prima che B termini il periodo di incubazione della malattia, stimato in un massimo di 14 giorni.

Uno studio di Hellewell et al, conclude che il tracciamento è efficace per ottenere il contenimento dell'epidemia, se il tempo medio di individuazione del contagio è di 3,8 giorni dopo l'emergere dei sintomi della malattia e l'**accuratezza del tracciamento** è intorno all'**80%**.

I due aspetti sono **correlati**, in quanto tanto più agevole sarà l'individuazione dei sospetti contagiati, quanto diffusa sarà la app e quanto più ci si potrà concentrare su soggetti a rischio piuttosto che su analisi a tappeto, che rischiano di impegnare eccessivamente le strutture sanitarie.

Occorre quindi sia un impegno delle strutture sanitarie nello svolgimento rapido di test, che una ampia partecipazione della popolazione al tracciamento attivo dei contagi

Per l'efficacia del tracciamento è necessario che **almeno il 60% della popolazione vi aderisca**, un livello molto elevato, ben superiore da quello raggiunto anche in altri paesi: a Singapore solo i 16% della popolazione ha scaricato TraceTogether e di questi il 50% l'ha attivata. Tenendo conto che i posessori di smartphone in **Italia** sono circa il **63% della popolazione**, significa che praticamente **tutti** dovrebbero adottare la app.

Siccome in Italia è prevista l'adozione volontaria della app, occorre che la popolazione sia convinta della sua **utilità** e non abbia riserve sul suo funzionamento e sull'intrusione nella sua **privacy**.

Bending Spoons è qualificata nello sviluppo di app di vasto utilizzo, quindi non ci sono riserve sulla sua capacità di produrre una app di uso agevole

Per incoraggiare l'**adesione volontaria** al tracciamento, occorre coinvolgere la **pubblica opinione** e i **media** in una campagna trasparente che chiarisca i vantaggi e l'interesse comune.

Ognuno di noi dovrebbe essere interessato a sapere se è sano e, qualora avesse il sospetto di essere stato **contagiato**, di poterlo verificare il prima possibile, così da potersi rivolgere tempestivamente ai medici. Per far ciò servirebbero o **test a tappeto**, che però sono impraticabili per i costi e la mancanza delle materie prime, oppure usando una **app di tracing** che permette la collaborazione e la condivisione di informazioni utili a individuare i possibili contagi. La parola definitiva riguardo a un contagio spetta ai medici e agli esami di laboratorio, ma tutti possono aiutare a restringere i **casi sospetti**, su cui i sanitari possono concentrare l'attenzione ed evitando soluzioni di contenimento indiscriminato, che impongono restrizioni a tutta la popolazione.

L'interesse personale in questo caso si tramuta in **interesse collettivo**, perché restringere i casi di contagio riduce il rischio per ciascuno di ammalarsi.

Come per l'immunità di gregge, che diventa efficace quando un'alta percentuale della di popolazione è immunizzata, così il tracciamento degli infetti sarà efficace quando almeno il 60% della popolazione ci partecipa.

Premi per gli utilizzatori

Per incentivare maggiormente la partecipazione al tracing da parte dei cittadini, si potrebbe associare una **lotteria all'uso della app**, sorteggiando dei **premi settimanali** tra chi la usa.

Licenza d'uso oppure open source

Il decreto del commissario Arcuri ritiene "*opportuno procedere all'acquisizione del diritto di autore sul codice sorgente del sistema di contact tracing digitale sviluppato dall'azienda Bending Spoons Spa*", ma dispone la "*stipula di un contratto di concessione gratuita di una licenza d'uso del software di contact tracing e di appalto di servizio gratuito*" con **Bending Spoons**. Oltre che opportuno acquisire il codice sorgente, sarebbe necessario che il software fosse reso disponibile con **licenza open source**. La condivisione del sorgente aperto permette infatti non solo di analizzare il codice, ma consente anche a terzi di **contribuire allo sviluppo**, fornendo estensioni ed adattamenti, che potrebbero tornare utili alla comunità.

È superfluo ricordare che una licenza d'uso gratuita è diversa da una licenza open source: nel primo caso l'azienda conserva la **proprietà del software** e la possibilità di modificarlo. Ogni intervento sul software andrebbe necessariamente richiesto al proprietario, creando un rischio di lock-in.

Riteniamo necessario insistere che il codice del servizio di tracing sia disponibile con licenza Open Source, altrimenti si rischia di gettare ombre sulla trasparenza del servizio e di non essere in grado di collaborare con altri gruppi internazionali attivi sul problema

Conservazione dei dati

Quanto alle riserve sulla privacy, abbiamo illustrato che la tecnica di rilevamento dà alte **garanzie di anonimato**. Tuttavia i dati raccolti dovrebbero essere conservati sotto il diretto controllo del Servizio Sanitario Nazionale, come per tutti i dati sanitari dei cittadini, a garanzia della loro riservatezza.

Il decreto del Commissario Arcuri lascia incertezza sulla conservazione dei dati e sull'erogazione del servizio, indicando che viene appaltato alla stessa ditta che fornisce la app

Autorità sanitaria e decentralizzazione

Nel documento di Apple e Google si fa riferimento all'autorità sanitaria, senza però ben specificare chi siano o quante siano queste **autorità**: una per nazione, più di una per nazione, chi stabilisce quale sia l'autorità in un certo territorio?

In Italia, sarebbe preferibile che l'autorità sia unica a livello **nazionale**, rappresentata dal **ministero della Salute**, anziché averne una per regione.

Tuttavia nella descrizione dell'utilizzo previsto del framework di **Apple** e **Google**, si suggerisce un **sistema decentralizzato** di raccolta dei dati, ossia le Diagnosis Key di un contagiato andrebbero raccolte sul server di una autorità sanitaria di una determinata ***region***. I dati raccolti vengono poi inviati a ciascun utente di quella *region* perché possa verificare se risulti a rischio di contagio. Quale sia l'ambito di queste *region* non è chiaro, né tantomeno cosa succede se persone si trovano a viaggiare da una regione all'altra. Anche supponendo che le regioni siano definite a **livello nazionale**, e che quindi i dati vengano salvati in maniera centralizzata per l'intera nazione, una persona che rientrasse dal Brasile, per esempio, e venisse trovata infetta da un **medico in Italia**, dovrebbe trasmettere i dati dei suoi contatti al **Sistema sanitario nazionale italiano**. Ma il Ssn brasiliano rimarrebbe all'oscuro dei contatti che il paziente avrebbe avuto in Brasile. Pertanto sarebbe necessario un **coordinamento** tra le autorità sanitarie di diverse regioni. Inoltre, poiché la app non tiene traccia dei luoghi dei contatti, rimane affidato alla persona infetta di indicare se si trovava in un'altra regione e occorre fidarsi dei suoi ricordi.

Consideriamo questo ultimo punto particolarmente rilevante anche a livello europeo. Quando i confini verranno riaperti, sarà necessario un coordinamento sulle attività di tracciamento tra le autorità sanitarie di tutti i paesi

Memoria e Traffico

I dati dei contatti vengono memorizzati sullo **smartphone dell'utente**. Fortunatamente, la registrazione di un contatto richiede poche decine di byte. Una persona con un lavoro non particolarmente a contatto col pubblico, potrebbe avere tra 200-500 contatti al giorno. Poiché è previsto si conservino solo i contatti degli **ultimi 14 giorni**, pari alla durata media di incubazione della malattia, lo spazio necessario è stimabile intorno ai 200 KB in tutto.

Quando una persona risulta **contagiata**, col suo consenso e con l'autorizzazione del medico curante, le sue **Diagnosis Keys** vengono trasmesse al server del servizio sanitario. Sul server vengono conservate solo le Diagnosis Keys relative agli ultimi 14 giorni. Anche questa non è una quantità eccessiva: considerando una quantità di 4000 contagi al giorno, 20 B per contagio al giorno, lo spazio totale richiesto sarebbe intorno a **1 GB**.

Più rilevante sarebbe invece il **traffico di rete** per andare a consultare gli elenchi delle chiavi dei contagiati.

Ciascun cittadino che utilizza la app dovrebbe scaricarsi ogni giorno l'elenco dei nuovi contagi, di circa 80 KB. Se il 60% degli italiani utilizzasse la app, il traffico complessivo che il server del servizio sanitario dovrebbe erogare sarebbe circa 3 TB. Con una connessione di rete da 10 Gbps, si potrebbero gestire oltre **10mila richieste al secondo**, per i quali un piccolo numero di server ridondati sarebbe sufficiente. In sostanza, l'infrastruttura necessaria per erogare il servizio non sarebbe particolarmente complessa o costosa.

Se l'app si limita a raccogliere i dati dei contatti ravvicinati, il carico di memoria è molto limitato. Se le regioni sono molto ampie e ci sono milioni di utenti, il traffico di rete potrebbe essere molto elevato

Funzionalità avanzate

Il framework di **Apple** e **Google** lascia spazio per estensioni. Per esempio, quando la app riceve un contatto, è prevista l'invocazione, tramite callback, di un algoritmo che ha il compito di stabilire il rischio del contatto, distinguendo se si tratta di un contatto prolungato o di un nuovo contatto, e valutando altri fattori, quali la distanza temporale e spaziale delle due segnalazioni, o l'abitudine dell'utente a usare mascherine.

La app potrebbe svolgere questo compito adottando anche tecniche di apprendimento automatico (Machine Learning) per adattarsi ai comportamenti di singole persone.

Per quanto riguarda il caso di Immuni, rimane rilevante in questo rispetto il problema della licenza d'uso, che renderebbe più trasparente l'utilizzo di sistemi di intelligenza artificiale sui dati degli utenti

Spoofing e altri attacchi

Oltre agli **attacchi informatici** possibili contro qualunque servizio di rete, ci potrebbero essere atti malevoli specifici. Per esempio un attaccante potrebbe produrre una lista di **Rsi fasulli**, allo scopo per mandare in **confusione** il sistema di tracciamento. Il caricamento dei dati viene però eseguito su

richiesta dei medici, che abilitano al trasferimento fornendo una **chiave di accesso riservata**. La persona che compisse tale atto sarebbe pertanto rintracciabile e soggetta a **sanzioni**.

Altre forme di possibili attacchi sono analizzate nell'articolo Decentralized Privacy-Preserving Proximity Tracing (DP3T) di **Carmela Troncoso et al**, concludendo che i rischi sono **inferiori** a quelli di approcci centralizzati. Al contrario, la pandemia può essere un'occasione per mettere in esercizio e conservare un'infrastruttura di tracciamento pubblica a disposizione e secondo le direttive dei cittadini.

Serge Vaudenay ha analizzato lo schema di funzionamento di DP3T, indicando possibili **attacchi malevoli** al servizio e suggerendo come mitigare questi rischi.

La pubblicazione dell'architettura e del codice aperto di Immuni possono facilitare lo scrutinio degli aspetti di sicurezza della sua implementazione

Tempistica

Apple e **Google** hanno promesso di rilasciare la libreria comune per l'utilizzo nel contact tracing a **metà maggio**. Le specifiche delle Api sono già state **pubblicate**, quindi gli sviluppatori di Immuni possono già predisporre la **prossima versione** in modo da farne uso. Pertanto a metà maggio potrebbe essere già disponibile e sottoposta a un periodo di **beta-testing** per verificarne il corretto funzionamento sul campo.

Nel frattempo dovrà essere messo in esercizio il **server** dove raccogliere e distribuire le Diagnosis Key delle persone infette.

Contemporaneamente si dovrebbe predisporre il materiale per istruire i **medici** all'uso dell'app di Immuni, per la **diagnostica** e **profilazione dei contagiati**, e su come comportarsi nei confronti dei contagiati, come ottenere e inviare loro il codice per effettuare l'upload delle loro Diagnostic Keys.

Conclusioni

Da quanto è stato reso noto finora, pare che la tecnologia adottata da **Immuni** sia in linea con il framework proposto da Apple e Google, ed è presumibile che l'implementazione lo sfrutti **appena sarà disponibile**. Non è chiaro cosa succederà quando Apple e Google rilasceranno le proprie app di tracciamento all'interno dei rispettivi sistemi operativi.

Abbiamo segnalato alcune **criticità** da esaminare per assicurare la massima efficacia dell'applicazione di uno strumento che, come alcuni studi dimostrano, può essere di fondamentale importanza per il contenimento della **diffusione del coronavirus** e per consentire indagini più mirate sui rischi di contagio, riducendo l'impatto sulle strutture sanitarie.

LE TECNOLOGIE, LA PROTEZIONE DEI DATI E L'EMERGENZA CORONAVIRUS: RAPPORTO TRA IL POSSIBILE E IL LEGALMENTE CONSENTITO

Francesco Paolo Micozzi[*]

**** 15 marzo 2020 ****

Nel periodo a cavallo tra il 2019 e il 2020 ha iniziato a diffondersi, a livello mondiale, la pandemia di COVID-19 (causata dal virus SARS-CoV-2). La pandemia in questione, la cui diffusione avrebbe avuto origine nella città cinese di Wuhan, arriva in Italia verso la fine del mese di gennaio 2020 con una tale viralità da imporre al Governo l'adozione una serie di misure emergenziali (racchiuse nei provvedimenti D.L. nn. 6, 9 e 14 del 2020 e DPCM del 1, 4, 8, 9 e 11 marzo 2020, reperibili nel *Dossier Coronavirus Italia* su *biordiritto.org*). Non sono mancati, col moltiplicarsi delle notizie sull'incremento esponenziale dell'epidemia, episodi di minacce, lesioni e atti discriminatori ai danni di persone dai tratti asiatici che, per gli aggressori, erano sicuro indizio di veicolo d'infezione e per ciò solo sufficienti a certificarne la qualità di moderni untori, giustificandone, infine, la persecuzione.

Episodi tragicamente simili a quelli descritti dal Manzoni ne *I promessi sposi* (cap. XXXII), in cui ai tempi della peste a Milano (1630) le persone si convincevano dell'esistenza stessa degli untori e delle loro "unzioni" di "*muraglie, porte d'edifizi pubblici e usci di case*"; credenza rapidamente diffusa attraverso il chiacchiericcio. E il chiacchiericcio popolare, intriso d'isteria collettiva determinata dalla paura, si trasformava quasi inevitabilmente in conferma delle unzioni ("*il sentire faceva l'effetto del vedere*") e nella conseguente caccia all'untore, ossia a coloro che "*gli animi, sempre più amareggiati da' mali*" riconoscevano come la causa del diffondersi della peste e contro i quali la gente potesse "*far valere le sue vendette*" ("*ogni atto poteva dar gelosia; e la gelosia diveniva facilmente certezza, la certezza furore*"). Analoghi episodi di violenza, (forse meno cruenti) si sono registrati nella cronaca di quasi quattro secoli dopo, a seguito della diffusione del COVID-19.

Certo, durante la pandemia descritta dal Manzoni non si disponeva delle conoscenze della medicina moderna (e al più si faceva ricorso a soluzioni pseudoscientifiche commiste a riti

[*]*Avvocato e Professore a contratto di Informatica Giuridica, Università degli Studi di Perugia*. Mail: *francescopaolo.micozzi@unipg.it*. Il contributo è stato accettato per la pubblicazione nell'ambito della call *Diritto, diritti ed emergenza ai tempi del Coronavirus*, sul n. 2/2020 di BioLaw Journal – Rivista di BioDiritto.

religiosi o, nelle migliori ipotesi, alle decameroniane "quarantene"), né ci si interrogava sul bilanciamento degli interessi nella tutela dei dati personali. Occorreranno, infatti, quasi tre secoli perché Samuel Warren e Louis Brandeis, dalle pagine della Harward Law Review, presentino al mondo "*The right to privacy*" (1890).

Tuttavia, ai giorni nostri, benché il concetto di privacy e la rilevanza fondamentale della protezione dei dati personali siano largamente riconosciuti, è comunque possibile costatare come la stessa disciplina di tutela sia percepita e abbia un impatto differenziato in ragione del contesto democratico, culturale e giuridico raggiunto nelle differenti aree del pianeta. La diffusione di una pandemia – che è di per sé situazione eccezionale – può, pertanto, incidere nel bilanciamento tra i valori da tutelare, fino a lasciar insinuare la suggestione che la diffusione di informazioni personali degli "untori", nel supremo interesse alla salute pubblica, sia qualcosa di ragionevole. Difficilmente ci si interroga, con altrettanta determinazione, sulla mancanza di evidenze circa la prevalenza dei benefici offerti dalla diffusione dei dati personali dei contagiati, in termini di contenimento della diffusione virale, né sulle conseguenze negative che i soggetti i cui dati personali venissero diffusi andrebbero a scontare.

Secondo quanto riportato dalla BBC, ad esempio, la Corea del Sud, al fine di monitorare la diffusione del COVID-19 avrebbe messo in atto per la prima volta le misure straordinarie già varate nel 2015, in occasione della diffusione di un'altra epidemia di coronavirus simile alla SARS (MERS-CoV – Middle East Respiratory Syndrome). Con i "messaggi di orientamento sulla sicurezza", realizzati con un invio massivo di SMS da parte del Governo sudcoreano, si è voluto informare la popolazione sulle misure igieniche raccomandate, comprendendo anche l'indicazione dei luoghi frequentati dalle persone risultate infette. A ciò si aggiunge la possibilità di tracciare le persone contagiate attraverso i dati GPS, le informazioni di riconoscimento facciale provenienti dalle telecamere di sorveglianza o le informazioni bancarie circa le transazioni con carte di credito. Si ottiene così un monitoraggio costante, in tempo reale, estremamente parcellizzato e su larga scala dell'intera popolazione, che viene giustificato con l'interesse "supremo" della salvaguardia della salute collettiva. Il contenuto degli SMS inviati ai cittadini, inoltre, è arricchito da dettagli del seguente tenore "*Un quarantatreenne residente nel distretto di X è risultato positivo al Coronavirus. Egli si trovava nel distretto di Y, dove lavora, e frequentava un corso sulle molestie sessuali. Ha contratto il virus dal suo istruttore*". Nel corpo dell'SMS non sono dunque indicate le generalità della persona asseritamente contagiata, ma ne sono diffusi il genere, l'età e un codice di riferimento della segnalazione, insieme a un

link attraverso cui seguire gli spostamenti del soggetto segnalato. Tuttavia, attraverso una ricerca online sul codice della segnalazione si possono recuperare ulteriori dettagli della persona contagiata, tra i quali, "volto", "fotografie", "familiari" o, anche, elementi relativi a eventuali ipotesi di "adulterio" (ad esempio per essersi recati, in determinate ore del giorno, in ambienti nei quali, notoriamente, si pratica la prostituzione).

Tale attività, definita di "contact tracing", ossia di tracciamento dei soggetti incontrati e dei luoghi frequentati dalle persone contagiate mira, in sostanza, ad osservare la propagazione del virus sul territorio, e, allo stato attuale della tecnica, potrebbe astrattamente essere attuato tramite dati GPS, installazione di applicazioni da parte delle autorità sui dispositivi dei cittadini, analisi delle transazioni con carte di credito o altri mezzi di pagamento, analisi dei dati di geolocalizzazione a disposizione dei gestori di telefonia mobile, o attraverso l'uso dei Big Data (dati provenienti, ad esempio, da società produttrici di *device* "smart", dati delle tessere fedeltà dei market, dati di rilevamento delle targhe, dati provenienti da telecamere con riconoscimento facciale…). Dal *mashup* di questa enorme mole di informazioni personali provenienti da diverse fonti, è possibile disegnare un quadro assai dettagliato circa gli spostamenti di un'intera popolazione e dei singoli soggetti contagiati, oltre a quelli entrati con loro in contatto.

Un sistema come quello descritto è certamente più efficiente di quello demandato alle autodichiarazioni degli individui (previsto invece dai provvedimenti d'urgenza emanati dal Governo italiano): l'analisi automatizzata dei dati incrociati consentirebbe, anche grazie all'ausilio di algoritmi di Intelligenza Artificiale, di intervenire con azioni di prevenzione e contenimento più rapide e mirate. Ma l'interrogativo è un altro: per quale ragione si propone di utilizzare le nuove tecnologie per contrastare l'epidemia? Perché i mezzi a disposizione – sia quelli di prevenzione (come i dispositivi personali di protezione) che quelli di diagnosi (come i tamponi) e cura (tra cui i respiratori artificiali) – sono limitati e un quadro più chiaro e dettagliato della situazione potrebbe consentire agli operatori di non agire alla cieca e ottimizzare gli interventi.

Occorre, a questo punto, comprendere se e come nel nostro Paese possano essere predisposte misure tecniche analoghe.

Il presupposto è il necessario bilanciamento tra diritti di pari rilevanza: da una parte la libertà personale e il diritto alla protezione dei dati personali, dall'altra la protezione della salute individuale e pubblica.

L'Europa conosce, ormai da qualche anno, un Regolamento sulla protezione dei dati personali

(Regolamento UE 2016/679, comunemente indicato con l'acronimo GDPR) che definisce la tutela dei dati personali come contributo «alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche» (considerando 2). Al contempo, pur riconoscendo (cons. 1) la tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale come diritto fondamentale ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8, par. 1) e del Trattato sul funzionamento dell'Unione europea (art. 16, par. 1), esclude che si tratti di una "prerogativa assoluta" (cons. 4) e afferma, anzi, che tale tutela vada considerata alla luce della sua funzione sociale e contemperata con altri diritti fondamentali.

La protezione dei dati personali, in situazioni emergenziali come quelle attuali, caratterizzate anche dal diffuso timore del contagio di un male inarrestabile, viene messa a dura prova. E ciò in considerazione del crescente (come si vedrà, falso) convincimento, che la riduzione delle tutele garantite (anche) agli "untori" sia un male necessario, ma minore rispetto a quello cui è esposta la salute pubblica.

Come contemperare, allora, la protezione dei dati personali con l'interesse pubblico a che il virus non si propaghi oltre la soglia di reazione del sistema sanitario?

L'art. 6 del GDPR contempla, tra le diverse basi giuridiche di legittimità del trattamento, sia la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica, sia la necessità di realizzare un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito il titolare (bisogna focalizzare l'attenzione sul fatto che tale trattamento debba essere "necessario" agli scopi menzionati). Il considerando 46 del GDPR, oltretutto, prevede la possibilità che alcune finalità, quale quella di tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, possano trovare il giusto inquadramento in entrambe le basi giuridiche appena menzionate.

Ogni informazione relativa allo stato di salute di una persona fisica rappresenta un dato appartenente alle "categorie particolari" di cui all'art. 9 del GDPR, che detta il divieto generale di trattare tale categoria di dati personali salvo che non ricorrano alcune specifiche eccezioni. Tra queste ultime è ricompreso il trattamento di dati relativi a una persona fisica (e specificamente al suo stato di salute) necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero", sempreché siano predisposte (dalle norme dell'UE o dello Stato) delle "misure appropriate e

specifiche per tutelare i diritti e le libertà dell'interessato (quale, ad esempio, il segreto professionale). Ciò significa, ad esempio, che – come esplicitato dal considerando 54 – il trattamento di categorie particolari di dati, in presenza di tali basi giuridiche, può prescindere dal consenso dell'interessato (che rappresenta un'altra delle basi giuridiche previste dall'art. 6 GDPR).

Con riferimento alla situazione della pandemia COVID-19, inoltre, è rilevante l'art. 14 del D.L. 9 marzo 2020, n. 14 (disposizioni sul trattamento dei dati personali nel contesto emergenziale), che prevede misure specifiche in tema di trattamento dei dati personali (efficaci fino al termine dell'attuale stato d'emergenza). In specie, nel rispetto degli artt. 9, par. 2, lett. g), h) e i), e 10 del GDPR, determinati soggetti impegnati nel contrasto all'emergenza COVID-19 (tra i quali il Servizio nazionale di protezione civile, gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale) possono trattare anche dati personali di cui agli artt. 9 e 10 del GDPR, che risultino necessari all'espletamento delle funzioni loro attribuite nella gestione dell'emergenza. Non si realizza pertanto, né si poteva realizzare, una deroga alle disposizioni del GDPR (fonte gerarchicamente sovraordinata), ma si definiscono i ruoli e i compiti nel trattamento dei dati (in particolare quelli relativi allo stato di salute) per finalità di tutela della salute pubblica. Si prevede inoltre (al secondo comma dell'art. 14) la possibilità che tali dati personali vengano "comunicati" anche a soggetti diversi e, ancora, che vengano "diffusi" dati personali diversi da quelli previsti negli artt. 9 e 10 GDPR, ma unicamente nelle ipotesi in cui la comunicazione o la diffusione risultino indispensabili alla gestione dell'emergenza in atto. Rilevante è, infine, l'ultimo comma, a mente del quale una volta cessato lo stato d'emergenza devono essere adottate misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali.

Nello stesso senso si dirige il comunicato del Garante privacy (del 2 marzo 2020) nel ricordare ai soggetti pubblici e privati che le attività di accertamento e la raccolta di informazioni relative ai sintomi tipici del Coronavirus e alle informazioni sui recenti spostamenti di ogni individuo spettano agli operatori sanitari e al sistema attivato dalla protezione civile, che sono gli organi deputati a garantire il rispetto delle regole di sanità pubblica recentemente adottate. Ad ulteriore conferma, si segnala il Comunicato del Comitato europeo per la protezione dei dati personali del 16 marzo 2020 (http://bit.ly/2UcFfDh).

I termini "necessario" e "indispensabile", contemplati dalle norme europee e nazionali appena menzionate, sono un chiaro richiamo ai principi regolatori di ogni trattamento dei dati personali e, in particolare, al principio di "minimizzazione", in base al quale possono essere trattati unicamente i dati personali adeguati, pertinenti e limitati a quanto necessario a soddisfare le finalità per le quali sono trattati.

Nella vigenza di tale quadro normativo, è agevole comprendere che uno scenario come quello descritto dalla Corea del Sud (in cui si è assistito a una diffusione di dati relativi allo stato di salute, sebbene pseudonimizzati) non sarebbe giustificato nemmeno dalla normativa d'emergenza contenuta nel DL 14/2020, proprio perché nel "modello" sudcoreano non sarebbe rispettato il principio di minimizzazione, che non potrebbe essere "silenziato" da una fonte gerarchicamente subordinata al GDPR. Inoltre, il DL 14/2020 nulla prevede in relazione al trattamento dei dati relativi all'ubicazione di utenti o abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico. In assenza di una specifica previsione, il trattamento dei dati di ubicazione è soggetto alla disciplina di cui all'art. 126 D.Lgs. 196/03 (in conformità a quanto previsto dall'art. 9 della c.d. Direttiva e-privacy, 2002/58/CE). Le eventuali disposizioni interne, derogatorie alle limitazioni a tali trattamenti, possono essere introdotte – ai sensi dell'art. 15 della Direttiva e-Privacy – qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica.

Potrebbero piuttosto utilmente essere adottate modalità di informazione del pubblico in modo da evitare la diffusione di dati personali identificativi, relativi allo stato di salute, ma comunque "allertando" le persone potenzialmente contagiate, e permettere loro di acquisire informazioni più dettagliate da parte delle autorità preposte.

Non si ravvisano – quantomeno nella vigenza del DL 14/2020 – ostacoli particolari a che i già menzionati soggetti, deputati alla gestione dell'emergenza, possano trattare i dati personali dei contagiati (anche provenienti da terze parti) al fine di effettuare attività di *contact tracing* utile a delineare i contorni del fenomeno virale. Ovviamente, una volta cessata l'emergenza (e raggiunta, quindi, la finalità del trattamento), la mole di informazioni raccolte non potrà – in assenza di ulteriore base giuridica che ne giustifichi il trattamento – essere "convertita" al soddisfacimento di finalità ulteriori. Al contrario, una volta anonimizzate, le informazioni potrebbero essere riutilizzate a fini di ricerca e per qualsiasi finalità lecita, e senza limiti temporali. È fuori di dubbio, infatti, che il dato informativo, una volta reso anonimo – ossia quel

dato che, passando attraverso un procedimento di anonimizzazione, non possa essere in alcun modo ricondotto a una singola persona fisica – non rientrerebbe nell'ambito applicativo del GDPR e il suo riuso non creerebbe problemi di sorta.

Occorre evitare, però, di confondere il concetto di dato anonimo sia con quello di dato pseudonimo (che, in quanto dato personale, resta disciplinato dal GDPR) che con quello di Open Data (o "dato aperto", così come definito dall'art. 1, co. 1, lett. l-ter del D.Lgs. 82/2005 e che potrebbe anche racchiudere anche dati personali), che, infine, con quello di Big Data (con il quale si indica, solitamente, la raccolta di una mole enorme di dati informativi eterogenei per fonte, formato e contenuti).

Una delle soluzioni proposte nel 2015, proprio dal Garante europeo per la protezione dei dati personali (con riferimento al caso del virus Ebola), allo scopo di prevedere la diffusione del contagio sul territorio e di informare tempestivamente i gruppi di persone eventualmente e direttamente coinvolte, è rappresentata proprio dall'uso dei Big Data (o "megadati"). Con questo termine ci "*si riferisce alla crescita esponenziale sia della disponibilità sia dell'utilizzo automatizzato di informazioni, indicando enormi serie di dati digitali detenuti da società, governi e altre organizzazioni di grandi dimensioni, successivamente analizzati in modo estensivo attraverso algoritmi informatici*" (parere 3/2013, Article 29 WP). Al contemperamento degli interessi del singolo con quelli della collettività si dirige la strategia dell'UE di promozione della progettazione e dello sviluppo di "*algoritmi che mascherano l'identità e aggregano i dati al fine di proteggere le persone, sfruttando al contempo il potere predittivo degli stessi dati*" (EDPS, Parere 4/2015, "*Verso una nuova etica digitale*").

In conclusione, la disciplina sulla protezione dei dati personali non rappresenta un ostacolo all'efficientamento della prevenzione e contrasto dell'epidemia ma, al contempo, non ammette un'abdicazione alla tutela dei diritti fondamentali. Pertanto, nel perseguimento delle finalità preventive e di contenimento dell'epidemia dovranno, anzitutto, preferirsi le soluzioni tecnologiche che impieghino dati anonimi. L'uso, invece, di dati personali sarà ammissibile – in una situazione di emergenza che, comunque, come può determinare la compressione di altre libertà fondamentali (quale quella alla libera circolazione delle persone) potrà determinare anche la compressione del diritto alla protezione dei dati personali – purché le misure predisposte siano proporzionate alle esigenze di contrasto e siano circoscritte al tempo dell'emergenza. La questione, quindi, non può ridursi all'alternativa dell'utilizzo o meno delle tecnologie disponibili, ma va sapientemente condotta, con l'utilizzo delle tecnologie e dei dati

personali, nel rispetto dei principi generali in materia di protezione dei dati personali.

AIC
ASSOCIAZIONE ITALIANA
DEI COSTITUZIONALISTI

OSSERVATORIO COSTITUZIONALE
Codice ISSN: 2283-7515
Fasc. 3/2020
Data: 21 aprile 2020

La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?·

di **Noemi Miniscalco** – *Assegnista di ricerca in Istituzioni di Diritto pubblico nell'Università degli studi di Modena e Reggio Emilia*

ABSTRACT: In addition to the social distancing measures, almost all the countries affected by the Covid-19 pandemic – and, among these, Italy – are using technology to implement tracking systems, including applications. Indeed, Apps could be additional tools to combat the spread of the virus and to protect health. The use of them, however, could compress other rights, as the right to the protection of personal data. Starting from the regulatory framework, the article highlights the processing of personal data carried out by some applications that have been launched in Italy to contrast the spread of Covid-19. After illustrating some possible solutions, also comparing to the experiences of the other countries, the paper identifies the requirements that a tracking system through the App should respect, searching for a balance between the constitutional interests at stake.

SOMMARIO: 1. Premessa. – 2. La sorveglianza attiva in Italia nel contesto emergenziale. – 2.1. Le modalità della sorveglianza. – 2.2. Le App per il contrasto alla diffusione del Covid-19 in Italia. – 3. Il *panopticon* (sud) coreano. – 4. La scelta tecnologica israeliana. – 4.1. Hamagen (The Shield). – 5. La localizzazione: da (possibile) strumento di controllo a strumento di garanzia per i cittadini.

· Lavoro sottoposto a referaggio secondo le linee guida della Rivista. Il contributo si colloca nell'ambito del forum sull'emergenza CoViD-19.

1. Premessa

Scoppiata in Cina a novembre 2019, la pandemia di Covid-19 si è rapidamente diffusa in tutto il pianeta[1]. Secondo l'Organizzazione mondiale della sanità, l'Europa è il nuovo epicentro della pandemia, con un aumento esponenziale del numero di casi di contagi in Italia, Spagna e Francia[2].

Per contrastare il propagarsi del virus, la quasi totalità dei Paesi colpiti – e, tra questi, l'Italia – ha adottato, sin da subito, una strategia di distanziamento sociale[3]. In aggiunta ad essa, in molti luoghi del pianeta i Governi stanno ricorrendo alla tecnologia, implementando sistemi di tracciamento e di sorveglianza attiva, anche tramite applicazioni[4].

Invero, proprio le App potrebbero essere uno strumento ulteriore contro la diffusione del virus, sì da far ritenere che il beneficio ottenibile – la riduzione dei contagi e la tutela della salute (e, prima ancora, della vita stessa) – non possa che far propendere per il loro massiccio utilizzo. Tale, pur condivisibile, prospettiva andrebbe però meglio indagata, in considerazione del diverso livello di limitazione che altri diritti potrebbero subire dall'implementazione di tali tecnologie.

Il ricorso ad esse, invero, pur finalizzato alla tutela della salute, porta ad emersione un interesse diverso e potenzialmente confliggente: la protezione delle informazioni a carattere personale

---

[1] Informazioni dettagliate sull'origine e lo sviluppo della pandemia, allo stato attuale delle conoscenze, sono reperibili al link www.salute.gov.it/nuovocoronavirus. I dati della diffusione sono consultabili al link http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioContenutiNuovoCoronavirus.jsp?lingua=italiano&id=5338&area=nuovoCoronavirus&menu=vuoto.

[2] A titolo indicativo, si vedano L'ANSA, *Oms, Europa nuovo epicentro pandemia*, 13 marzo 2020, http://www.ansa.it/sito/notizie/mondo/europa/2020/03/13/oms-europa-nuovo-epicentro-pandemia_b36c844e-923f-49aa-a639-758649890ade.html; RAI NEWS, *Oms: Europa ormai epicentro della pandemia di Coronavirus*, 13 marzo 2020, http://www.rainews.it/dl/rainews/articoli/oms-coronavirus-Ue-epicentro-pandemia-faa78146-c73d-4123-8526-76eb28bbc751.html?refresh_ce; P. G. DAFORN, *Coronavirus: comment l'Europe est devenue l'«épicentre» de la pandémie»*, in *Le Monde*, 19 marzo 2020, https://www.lemonde.fr/les-decodeurs/article/2020/03/18/en-graphiques-comment-l-europe-est-devenue-l-epicentre-de-la-pandemie-de-covid-19_6033558_4355770.html; P. LINDE, *Europa se ha convertido en el epicentro de la pandemia del coronavirus*, in *El País*, 13 marzo 2020, https://elpais.com/sociedad/2020-03-13/europa-se-ha-convertido-en-el-epicentro-de-la-pandemia-del-coronavirus.html.

[3] L'elenco di tutti i provvedimenti vigenti, approvati dal Governo italiano in seguito all'emergenza sanitaria, è rinvenibile al link http://www.governo.it/it/approfondimento/coronavirus/13968. Per un approfondimento sulle misure per il contrasto alla diffusione dell'epidemie, v. EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL, *Guide to public healt measures to reduce the impact of influenza pandemics in Europe – 'The ECDC Menu'*, settembre 2009,https://www.ecdc.europa.eu/sites/default/files/media/en/publications/Publications/0906_TER_Public_Health_Measures_for_Influenza_Pandemics.pdf.

[4] Nel prosieguo anche, semplicemente, "App". Per un approfondimento sulle politiche di "sorveglianza attiva" nel contenimento dell'epidemia del Covid-19 sia a livello internazionale che nazionale si veda il contributo di D. DE FALCO, M. L. MADDALENA, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *federalismi.it*, 28 marzo 2020.

indispensabili per il loro funzionamento, nonché di quelle che, a loro volta, i programmi potrebbero generare.

Ebbene, anche se, ovviamente, «le norme in materia di protezione dei dati […] non ostacolano l'adozione di misure per il contrasto della pandemia di coronavirus»[5], resta però ferma la necessità di ricercare un ragionevole bilanciamento tra gli interessi in rilievo. Del resto, per fronteggiare l'epidemia in corso, anche l'Italia, come altri Paesi, sta adottando misure che – in gradazione diversa – incidono sui diritti e libertà riconosciuti dalla Costituzione, basti qui pensare a quella di circolazione[6]. Sicché, tra di essi, anche la protezione dei dati personali potrebbe, in ottica di bilanciamento, arretrare, ma giammai *in toto* o comunque in misura irragionevole rispetto al beneficio che all'interesse prevalente, ossia al diritto alla salute, potrebbe derivarne[7].

---

[5] Testualmente, EUROPEAN DATA PROTECTION BOARD, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, adottata il 19 marzo 2020, reperibile sul sito www.garanteprivacy.it, doc. web. 9295504, che specifica che «occorre pertanto tenere conto di una serie di considerazioni per garantire la liceità del trattamento di dati personali e, in ogni caso, si deve ricordare che qualsiasi misura adottata in questo contesto deve rispettare i principi generali del diritto e non può essere irrevocabile. L'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza». Considerazioni – queste ultime – che si rinvengono, peraltro, anche nella giurisprudenza della Corte costituzionale, a partire dalla storica sentenza n. 15 del 1982, in *Giur. cost.*, 1982, pp. 87 ss.

[6] Come è stato evidenziato, è «di scontata evidenza come, in una graduazione delle emergenze, la garanzia della salute – e della vita – dei cittadini prevalga su qualsiasi altro diritto. Tuttavia è doveroso, soprattutto di fronte ad una crisi di così vasta portata e destinata a durare nel tempo, interrogarsi sulle modalità e sui limiti degli interventi emergenziali, sempre alla ricerca della proporzionalità e del bilanciamento tra i diversi interessi in gioco. Se è chiaro a tutti che il tempo dell'emergenza può distorcere e comprimere il ventaglio di libertà cui le nostre generazioni sono state abituate, è pur sempre desiderabile che, passato il virus, resti lo stato costituzionale di diritto» (testualmente, L. CUOCOLO, *I diritti costituzionali di fronte all'emergenza Covid-19: una prospettiva comparata*, in ID. *I diritti costituzionali di fronte all'emergenza COvid-19. Una prospettiva comparata*, in *federalismi.it*, p. 8). Pone l'accento sulla valenza del diritto alla salute – non solo come diritto della persona ma anche – come interesse della collettività, M. NOCCELLI, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in *federalismi.it*, che ricorda come «la Corte costituzionale nella sentenza n. 218 del 2 giugno 1994, [ha osservato che] la tutela della salute implica anche il dovere dell'individuo di non ledere né porre a rischio con il proprio comportamento la salute altrui, in osservanza del principio generale che vede il diritto di ciascuno trovare un limite nel reciproco riconoscimento e nell'eguale protezione del coesistente diritto degli altri (spec. p. 8). Specificamente, sulla compatibilità delle misure di sorveglianza attiva con il quadro costituzionale, D. DE FALCO, M. L. MADDALENA, *La politica del tracciamento dei contatti*, cit., pp. 9 ss.

[7] Nello stesso senso, Antonello Soro, Presidente del Garante per la protezione dei dati personali, in una recente intervista di A. MAJOLI, *Soro, la sfida privacy in era coronavirus. Garante, sì misure straordinarie, ma proporzionate e temporanee*, doc. web. 9292565, reperibile sul sito ww.garanteprivacy.it, ha affermato: «La sfida posta da questa emergenza di tipo sanitario è coniugare efficacia dell'azione di prevenzione e contrasto del contagio, con le garanzie essenziali di tutela dei diritti fondamentali, quali appunto la privacy, che sono soggetti a bilanciamento con altri beni giuridici quali, in primo luogo, la salute pubblica». Si veda anche il contributo di G. BISCONTINI, A. POGGI, M. E. COMBA, G. VALDITARA, E. DEL PRATO, F. VARI, L. A. MAZZAROLLI, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *federalismi.it*, 23 marzo 2020. Più in generale, sulla valenza costituzionale del diritto alla protezione dei dati personali, sulla quale sarebbe qui ultroneo soffermarsi, ricordiamo, soltanto, che la Corte costituzionale, nella sentenza n. 20 del 2019, ha affermato che «il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata (sentenza n. 366 del 1991),

Il diritto alla protezione dei dati personali può subire, invero, una compressione allorché si ricorra all'uso di droni, di sistemi GPS, di videosorveglianza, di tracciamento tramite celle telefoniche o applicazioni, di monitoraggio attraverso la ricostruzione dei pagamenti effettuati con carte di credito. Tra essi, nel presente contributo, focalizzeremo l'attenzione sulle App, poiché, proprio queste ultime, stanno trovando una sempre maggiore diffusione e nuove forme di impiego[8].

Volendo provare a fornirne una classificazione, le applicazioni per contrastare la diffusione del Covid-19 possono essere bipartite in "informative" e "identificative": rientrano nella prima categoria tutti quei *tools* atti ad informare – appunto – le persone in merito ai comportamenti da adottare, alle misure predisposte dal Governo, ai numeri cui rivolgersi, nonché sulle principali notizie ed aggiornamenti relativi alla pandemia in corso; nella seconda, invece, quelli finalizzati alla geolocalizzazione dei soggetti positivi oppure al contenimento del virus tramite la correlazione dei "diari di viaggio" dell'utente rispetto ai dati dei percorsi effettuati dai contagiati.

Laddove – è evidente – il diritto alla protezione dei dati personali assume peculiare rilievo rispetto alla seconda delle *species* individuate, poiché, se è fuor di dubbio che la posizione di una persona fisica sia *ex se* un dato personale[9], qualora venisse correlata alla positività al virus del

---

che attiene alla tutela della vita degli individui nei suoi molteplici aspetti» è «un diritto che trova riferimenti nella Costituzione italiana (artt. 2, 14, 15 Cost.), già riconosciuto, in relazione a molteplici ambiti di disciplina, nella giurisprudenza» costituzionale (cfr. sentenze n. 173 del 2009, n. 372 del 2006, n. 135 del 2002, n. 81 del 1993 e n. 366 del 1991) «e che incontra specifica protezione nelle varie norme europee e convenzionali […]. Nell'epoca attuale, esso si caratterizza particolarmente quale diritto a controllare la circolazione delle informazioni riferite alla propria persona, e si giova, a sua protezione, dei canoni elaborati in sede europea per valutare la legittimità della raccolta, del trattamento e della diffusione dei dati personali. Si tratta dei già ricordati principi di proporzionalità, pertinenza e non eccedenza, in virtù dei quali deroghe e limitazioni alla tutela della riservatezza di quei dati devono operare nei limiti dello stretto necessario, essendo indispensabile identificare le misure che incidano nella minor misura possibile sul diritto fondamentale, pur contribuendo al raggiungimento dei legittimi obiettivi sottesi alla raccolta e al trattamento dei dati». Si veda, sul punto, altresì, la relazione di N. ZANON, Privacy *e trasparenza in conflitto: il caso della pubblicazione* on line *dei dati reddituali e patrimoniali dei dirigenti della pubblica amministrazione*, 10-12 ottobre 2019, reperibile nella sezione "relazioni internazionali" del sito www.cortecostituzionale.it.

[8] Solo di recente, invero, si è pensato di ricorrere all'implementazione di applicazioni per il tracciamento degli utenti al fine del controllo (e contenimento) della diffusione delle malattie. Uno dei primi studi in materia è "The fluPhone project", condotto nel 2011 dai ricercatori dell'Università di Cambridge, di Liverpool e della London School of Hygiene and Tropical Medicine, che hanno programmato e utilizzato una applicazione per indagare con quale frequenza le persone entrano in contatto tra loro (e, tramite tale informazione, ricostruire l'evoluzione della trasmissione di una malattia). Per un approfondimento su tale progetto si veda il link https://www.cl.cam.ac.uk/research/srg/netos/projects/archive/fluphone2/.

[9] Ai sensi dell'art. 4 del Regolamento UE 679/2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito anche, semplicemente, "GDPR") è un "dato personale" «qualsiasi informazione riguardante una persona fisica identificata o identificabile» ossia che «direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale». Sul concetto di dati personali, *ex multis*, si veda F. DI RESTA, *La nuova "privacy europea". I principali adempimenti del*

soggetto, la tutela ad essa apprestata sarebbe rinforzata dal rilievo di quel dato, in quanto relativo allo stato di salute e, pertanto, particolare[10].

Muovendo da tali premesse, nelle pagine che seguiranno, dopo avere ricostruito il quadro normativo di riferimento, individueremo alcune delle applicazioni che sono state lanciate in Italia per il contrasto alla diffusione del Covid-19, analizzando il processo di trattamento dei dati personali che, tramite esse, viene effettuato. L'analisi dei programmi già sviluppati permetterà, in seguito, di individuare – anche guardando ad altre esperienze – le soluzioni possibili e di formulare una proposta, in chiave conclusiva, circa le condizioni da rispettare affinché, nell'introduzione di un sistema di tracciamento tramite App, sia svolto un equilibrato bilanciamento tra gli interessi costituzionali in gioco.

2. La sorveglianza attiva in Italia nel contesto emergenziale

Come noto, il 31 gennaio 2020 il Governo italiano ha proclamato lo stato di emergenza e attuato una strategia per il contenimento e la gestione della diffusione dei contagi da Covid-19, prevalentemente basata sul distanziamento sociale. La tecnologia ha giocato un ruolo importante, specie rispetto all'utilizzo di modalità di lavoro agile per le attività che possono essere svolte al proprio domicilio o in modalità a distanza[11]. Di recente, inoltre, l'attenzione – non solo delle Autorità pubbliche ma anche dei *mass media* – si sta incentrando sull'eventuale uso per il contrasto dell'epidemia in corso di sistemi di sorveglianza attiva – specificamente, la geolocalizzazione – e, tra essi, le App.

---

regolamento UE 2016/679 e profili risarcitori, Giappichelli, Torino, 2018, p. 8. Per un approfondimento sui diversi modelli di classificazione dei dati personali, v. ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 4/2007 on the concept of personal data*, 20 giugno 2007.

[10] Come noto, il GDPR appresta una tutela rafforzata per talune categorie di dati, vietandone il trattamento se non al ricorrere di determinate condizioni. Nello specifico, l'art. 9 GDPR qualifica come "particolari" i «dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché […] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

[11] Si vedano, in particolare, il d.p.c.m., 1° marzo 2020, "Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da CO-VID-19" confermate dal d.p.c.m. 4 marzo 2020 e dal d.p.c.m. 11 marzo 2020. V. anche le "disposizioni in materia di lavoro agile" di cui all'art. 39 del d.l. 17 marzo 2020, n. 18.

Si ipotizza, in altri termini, di ricorrere al tracciamento (*recte* alla storicizzazione) delle posizioni dei soggetti, sia per elaborare dei "diari di viaggio" e, tramite correlazioni, individuare tanto i contagiati quanto i sospetti tali in ragione dei percorsi effettuati, sia a garanzia del rispetto delle prescrizioni dell'isolamento domiciliare.

In tale ottica, con il d. l. 17 marzo 2020, n. 18, c.d. cura Italia, è stata prevista «al fine di dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus COVID-19» la nomina di «un contingente di esperti, in possesso di specifica ed elevata competenza nello studio, supporto, sviluppo e gestione di processi di trasformazione tecnologica»[12].

A seguire, il 24 marzo 2020, nell'ambito del progetto "Innova per l'Italia"[13], sono poi state pubblicate due *fast call* specificamente finalizzate al reperimento: a) «di App e soluzioni tecniche di teleassistenza per pazienti domestici»; b) di «soluzioni per il tracciamento continuo, l'*alerting* e il controllo tempestivo del livello di esposizione al rischio delle persone e dell'evoluzione dell'epidemia sul territorio»[14], attraverso le quali sono state raccolte, solo per la seconda delle categorie *de quibus* (ossia per l'individuazione di tecnologie che aiutino a contenere l'epidemia in corso, tramite il tracciamento degli utenti) 319 proposte[15].

---

[12] Cfr. art. 76 d. l. 17 marzo 2020, n. 18, recante "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19".

[13] Il progetto "Innova per l'Italia" è nato su iniziativa del Ministro per l'innovazione tecnologica e la digitalizzazione, del Ministro dello Sviluppo Economico e del Ministro dell'Università e Ricerca, con Invitalia e il supporto tecnico di Agid, a sostegno dei soggetti individuati per la gestione dell'emergenza da Coronavirus.

[14] Per ulteriori informazioni, si veda MINISTERO PER L'INNOVAZIONE TECNOLOGICA E LA DIGITALIZZAZIONE, *Telemedicina e sistemi di monitoraggio, una call per tecnologie per il contrasto alla diffusione del Covid-19*, 23 marzo 2020, https://innovazione.gov.it/telemedicina-e-sistemi-di-monitoraggio-una-call-per-tecnologie-per-il-contrasto-alla-diffusione-del-covid-19/. Risultano essere 319 le proposte arrivate al Ministero per l'innovazione tecnologica e la digitalizzazione relative alla seconda delle *call* indicate come documenta, ANSA, *Coronavirus e app, 319 proposte in attesa task force.*, 27 marzo 2020, https://www.ansa.it/sito/notizie/tecnologia/software_app/2020/03/26/coronavirus-e-app-319-proposte-in-attesa-task-force_e05ac652-8894-48f8-a1fb-9231340a92fe.html.

[15] Il Ministero per l'innovazione tecnologica e la digitalizzazione, in data 31 marzo 2020, ha nominato un "Gruppo di lavoro *data-driven* per l'emergenza di Covid-19" con il compito di effettuare attività di analisi e studio degli impatti dell'epidemia in corso e di procedere alla valutazione delle soluzioni pervenute dai partecipanti alla *fast call*. Nelle more della pubblicazione del presente contributo, il Gruppo di lavoro ha valutato le proposte presentate ed ha selezionato l'App denominata "Immuni", della società Bending Spoons S.p.A. A seguire, il 16 aprile 2020, con l'ordinanza n. 10 del 2020, il Commissario per l'emergenza Domenico Arcuri ha disposto di procedere alla stipula, con tale società, di un contratto di concessione gratuita della licenza d'uso sul *software* di *contact tracing* e di appalto di servizio gratuito. Ad oggi, non sono ancora state rese pubbliche tutte le informazioni relative al funzionamento dell'App – ragion per cui non ci è possibile esprimere una valutazione su tale soluzione – ma soltanto che essa sarà funzionale: al tracciamento dei contagiati e di coloro che, per i percorsi effettuati, potrebbero avere contratto il virus; all'elaborazione di un diario clinico contenente le informazioni rilevanti dell'utente e, tra queste, il sesso, l'età, le malattie pregresse, i sintomi e i cambiamenti dello stato di salute. L'applicazione, attraverso il Bluetooth, rileverà la vicinanza tra due *smartphone* entro un metro, conservando sul dispositivo dell'utente una lista di codici identificativi anonimi, così da permettere di ripercorrere a ritroso tutti gli incontri di una persona risultata positiva al Covid-19 (cfr. G. VITALE,

Le soluzioni generalmente prospettate per l'implementazione di tali misure sono: il monitoraggio tramite dati anonimi; la localizzazione dei soli soggetti risultati positivi al tampone; oppure il tracciamento di tutti, tramite l'uso delle celle telefoniche o delle applicazioni[16]. In un crescendo che incide con intensità sempre maggiore sul diritto alla protezione dei dati personali e che quindi richiede un attento scrutinio, nell'ottica del necessario bilanciamento tra interessi.

Tali misure, naturalmente, per risultare adeguate rispetto al fine della tutela della salute, richiederebbero di essere correlate ad altri strumenti o strategie. Così, ad esempio, il monitoraggio dei soli positivi potrebbe ridurre i contagi, ma solo se e nella misura in cui venisse aumentato il numero di tamponi effettuati, poiché solo in tal caso si avrebbe l'esatta conoscenza di tutti i soggetti da tracciare[17]. Nella stessa ottica, la sorveglianza generalizzata richiederebbe previamente una capacità di gestione efficiente e trasparente della mole di dati che verrebbero raccolti, anche in termini di garanzia di sicurezza dei dati stessi, nonché di uso di essi per test diagnostici generalizzati e sincronizzati[18].

Eccezion fatta per la prima delle soluzioni prospettate (ossia quella basata sull'elaborazione di informazioni anonime), l'attuazione della sorveglianza attiva tramite sistemi di geolocalizzazione implica, come si è anticipato, un trattamento di dati personali.

Muovendo da tale assunto, indagheremo preliminarmente se al lume della disciplina vigente sia lecito e, pertanto, in astratto, prospettabile l'eventuale tracciamento degli individui.

Coronavirus, scelta l'app per il tracciamento dei contati: si chiamerà Immuni, in *La Repubblica*, 16 aprile 2020,https://www.repubblica.it/politica/2020/04/16/news/coronavirus_scelta_l_app_per_il_tracciamento_dei_contagi_si_chiamera_immuni-254235342/).

[16] Sul punto, C. MELZI D'ERIL – G. E. VIGEVANI, *Tre le ipotesi in campo: monitorare i flussi di perosne tramite dati anonimi; monitorare tutti gli utenti, per sapere chi, quando e dove si muove; monitorare soltanto gli utenti contagiati*, in *Ilsole24ore*, 22 marzo 2020, https://www.ilsole24ore.com/art/coronavirus-tracciare-spostamenti-si-ma-maniera-anonima-ADvAC8E.

[17] Della stessa opinione è Antonello Soro, Presidente del Garante per la protezione dei dati personali, che, in una recente intervista ha affermato: «Sento parlare molto di modello coreano. Se significa definizione di un protocollo di tracciamento precoce dei positivi e delle persone che sono venute a contatto con loro, oltre che un controllo sul rispetto della quarantena, non avrei obiezioni. Purché a questo seguano poi test mirati, ma diffusi su tutti coloro che sono stati esposti a rischio di contagio e si garantiscano al contempo le adeguate protezioni al personale sanitario» (P. RUSSO, *Un'app per la salute grazie a precise deroghe alla privacy. Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali*, in *La Stampa*, 25 marzo 2020, doc. web. 9298389, reperibile sul sito www.garanteprivacy.it).

[18] Nello stesso senso, Antonello Soro, Presidente del Garante per la protezione dei dati personali, in una recente intervista di A. MAJOLI, *Soro, la sfida privacy in era coronavirus. Garante, sì misure straordinarie, ma proporzionate e temporanee*, doc. web. 9292565, reperibile sul sito www.garanteprivacy.it.

Anzitutto, «in linea di principio, i dati relativi all'ubicazione possono essere utilizzati dall'operatore solo se resi anonimi o con il consenso dei singoli. Tuttavia l'art. 15 della direttiva e-privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica», fermo restando che «tale legislazione eccezionale è possibile solo se costituisce una misura necessaria, adeguata e proporzionata all'interno di una società democratica»[19].

Il legislatore italiano, con il disposto di cui all'art. 14 del d. l. n. 14 del 2020, recante disposizioni sul trattamento delle informazioni relative alle persone fisiche nel contesto emergenziale[20], pur rinviando alle regole di cui al Regolamento UE 2016/679 ed ai principi di cui all'art. 5 di tale atto, ha innestato nel sistema talune temporanee eccezioni, prevedendo la possibilità, per i soggetti direttamente coinvolti nella gestione dell'emergenza, di conferire le autorizzazioni di cui all'art. 2-*quaterdecies* del d.lgs. 196 del 2003 con modalità semplificate (ed anche oralmente), nonché sospendendo l'obbligo della informativa[21]. Al contempo, con il medesimo intervento, sono stati previsti due regimi differenziati e specifici, in materia di trattamento dei dati personali, per i soggetti direttamente coinvolti nella gestione dell'emergenza e per quelli interessati da attività ad essa connesse.

Quanto al primo gruppo, sono state espressamente individuate le condizioni di liceità dei trattamenti effettuati per la gestione dell'epidemia in corso, disponendo che, fino al termine dello stato di emergenza, per motivi di interesse pubblico[22], i soggetti che operano nel Servizio nazionale di protezione civile e nell'ambito del Servizio sanitario nazionale, quelli deputati a monitorare e a garantire l'esecuzione delle misure disposte, gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, «anche allo scopo di assicurare la più efficace gestione dei flussi e

[19] Così, EUROPEAN DATA PROTECTION BOARD, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, cit., secondo cui «le autorità pubbliche dovrebbero innanzitutto cercare di trattare i dati relativi all'ubicazione in modo anonimo (ossia, trattare dati in forma aggregata e tale da non consentire la successiva re-identificazione delle persone), il che potrebbe permettere di generare analisi sulla concentrazione di dispositivi mobili in un determinato luogo ("cartografia")».

[20] Decreto legge 9 marzo 2020, n. 14, recante "Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19", in Gazzetta Ufficiale Serie Generale n. 62 del 9 marzo 2020.

[21] Regime temporaneo ed eccezionale previsto entro il termine dello stato di emergenza di cui alla delibera del Consiglio dei ministri del 31 gennaio 2020. Invero, «al termine dello stato di emergenza di cui alla delibera» *de qua* tutti i soggetti dovranno adottare «misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali» (cfr. art. 14, comma 6, d. l. 9 marzo 2020, n. 14).

[22] Sono, in particolare, motivi di interesse pubblico: «garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19 mediante adeguate misure di profilassi», nonché «assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale» (così, art. 14, comma 1, d. l. 9 marzo 2020, n. 14).

dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19»[23].

Quanto al secondo gruppo, invece, ossia ai soggetti pubblici e privati diversi da quelli poc'anzi menzionati, essi, sulla base di quel presupposto di liceità, possono essere destinatari dei dati personali ovvero possono diffondere dati, purché non particolari, «nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto».

Ebbene, in forza di tali previsioni normative, la sorveglianza attiva tramite geolocalizzazione potrebbe, già ora, stante il contesto emergenziale, essere giustificata sulla base di motivi di interesse pubblico e, tra essi, quello della protezione dalla diffusione dall'emergenza sanitaria, se posta in essere da una o più delle Autorità pubbliche cui sono stati attribuiti compiti di gestione dell'emergenza stessa.

Ciò nondimeno, sarebbe comunque auspicabile uno specifico intervento *ad hoc* del legislatore che, stante la possibile pervasività della misura, ne dettagliasse maggiormente le condizioni di ammissibilità, fermo restando il limite temporale già individuato nella scadenza dello stato di emergenza[24]. Limite temporale dal quale – giova sottolinearlo – non si può prescindere e che andrebbe attentamente presidiato, per evitare il rischio che dalla temporanea introduzione di tali misure, giustificata dall'emergenza, si strabordi in un monitoraggio anche in situazioni non eccezionali.

[23] Cfr. art. 14, comma 2, d. l. 9 marzo 2020, n. 14.

[24] Nello stesso senso, Antonello Soro, Presidente del Garante per la protezione dei dati personali, in due recenti interviste di M. PENNISI, *Coronavirus, come funzionano il controllo delle celle e il tracciamento dei contagi. Il Garante: "Non bisona improvvisare"*, in *Il corriere della Sera*, 18 marzo 2019, doc. web. 9294705 e A. IANNUZZI, *Soro: "Sì al tracciamento dei contatti ma con un decreto temporaneo". Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali*, in *La Repubblica*, 26 marzo 2020, doc. web. 9299193, reperibili sul sito web www.garanteprivacy.it.

2.1. Le modalità della sorveglianza

Riconosciuta l'ammissibilità, in astratto, della misura, il discorso non può che spostarsi sulle modalità, in concreto, attraverso le quali essa potrebbe essere correttamente implementata e sugli auspicabili limiti (di necessità, adeguatezza e proporzionalità) che al trattamento dei dati personali con finalità di sorveglianza attiva andrebbero posti.

Invero, seppure non possa escludersi che il trattamento di dati storici di localizzazione in forma non anonimizzata possa risultare proporzionato in circostanze eccezionali e in relazione alle modalità concrete tramite cui viene posto in essere, in ogni caso le misure prescelte «dovrebbero essere soggette a un controllo rafforzato e a garanzie più stringenti per assicurare il rispetto dei principi in materia di protezione dei dati personali[25]».

Un presidio di garanzie rinforzate che andrebbe vagliato rispetto: alla durata e portata della misura, alla durata di conservazione dei dati, al rispetto del principio di limitazione della finalità e di trasparenza, nonché di sicurezza del trattamento.

Sicché, volendo vagliare le strategie prospettate alla luce delle contingenze di questo momento storico, ci pare possa già pervenirsi ad una prima conclusione: il monitoraggio di tutti gli utenti, al netto delle valutazioni tecniche che pur potrebbero portare ad escludere un'adeguata capacità di gestione di una simile mole di dati, sarebbe certamente irragionevole, non foss'altro per il perdurante divieto di spostamenti, che renderebbe priva di utilità siffatta misura.

Invero, un'App con funzione 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. Sproporzione che può, peraltro, cogliersi anche alla luce della sussistenza di altre – e meno invasive – misure, quali il tracciamento dei soli positivi, se correlato, come si diceva, ad un incremento del numero di tamponi effettuati, oppure il monitoraggio su dati anonimi.

Se così è, il campo delle scelte "possibili" andrebbe ristretto alle altre due strategie prospettate; semmai, ricercando tra esse soluzioni intermedie, come meglio si dirà nel prosieguo.

---

[25] Così, EUROPEAN DATA PROTECTION BOARD, *Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19*, cit.

Ma preliminarmente, muovendo da tali premesse, dobbiamo chiederci quali sono le caratteristiche che un'App per la salute, che rispetti anche la privacy degli utilizzatori, dovrebbe avere; a tal fine, nel prossimo paragrafo, individueremo alcune delle App sviluppate in Italia, ricostruendone il funzionamento per poi vagliarne la conformità al quadro normativo prospettato.

2.2. Le App per il contrasto alla diffusione del Covid-19 in Italia

Le App che si sono diffuse sull'intero territorio nazionale sono – ad oggi, solo – a carattere informativo e, tra esse, la più nota è COVID News – Italia, un *tool* attraverso il quale è possibile reperire tutte le notizie pubblicate dalle principali testate giornalistiche, nonché i consigli sulla prevenzione e i numeri utili, regione per regione[26].

Invece, non ha ancora trovato concreta attuazione l'eventuale potenziamento delle misure in atto tramite il ricorso a sistemi di localizzazione (il c.d. *contact tracing* digitale), così come nessuna applicazione di tracciamento ha, fino ad ora, avuto una diffusione sull'intero territorio nazionale.

Tutto all'opposto, alcune Regioni italiane hanno lanciato (o sperimentato) diverse applicazioni, non solo di carattere informativo, ma anche specificamente dirette al tracciamento degli utenti.

Rientrano nella prima categoria, ad esempio, AllerLOM della Regione Lombardia e TreCovid19 della Provincia autonoma di Trento, utilizzate per informare i cittadini sulle ultime notizie relative all'epidemia in corso.

A queste si aggiungono le App dirette al contrasto della diffusione del Covid-19 e a ridurre pertanto il rischio di contagi, tramite sistemi di tracciamento degli utenti.

La più rilevante è STOPcovid19, un'applicazione ideata e realizzata da Webtek S.p.A, che è stata sperimentata dalla Regione Umbria[27]. Di quest'ultima è opportuno ricostruire il funzionamento, ponendo mente al processo di trattamento dei dati che essa effettua.

---

[26] Cfr. A. GRAZIANO, *Tenersi aggiornati sul coronavirus con un clic, grazie all'App COVID News – Italia. Sviluppatori originari di Torremaggiore*, 7 marzo 2020, in *quotidiano.net*, https://www.immediato.net/2020/03/07/tenersi-aggiornati-sul-coronavirus-con-un-clic-grazie-allapp-covid-news-italia-sviluppatori-originari-di-torremaggiore/. Il link per scaricare l'APP per Android è:https://play.google.com/store/apps/details?id=biquadro.covid19italia.

[27] Abbiamo nel testo attribuito rilievo a tale App proprio in considerazione della sperimentazione che essa ha avuto su un intero territorio regionale. Tra gli articoli delle principali testate giornalistiche sul tema, si vedano S. BENNEWITZ, *Coronavirus, ecco l'app per individuare i contatti e limitare il contagio*, in *La Repubblica*, 17 marzo 2020,

L'applicazione, in particolare, raccoglie e memorizza i seguenti dati: il numero di cellulare dell'utente e alternativamente il numero seriale e il Comune di rilascio della carta d'identità, del passaporto, oppure il nome, cognome e l'indirizzo. In aggiunta, nel momento in cui «e solo se viene premuto il tasto "*Avvio*", ogni 10-15 minuti [essa] raccoglie e memorizza la posizione geografica in cui si trova il cellulare fornito dall'utente»[28]. Dato – quest'ultimo – che viene conservato per un periodo di trenta giorni e non è conoscibile da Webtek, ma soltanto dalla Regione Umbria. Pertanto, se un utilizzatore, che abbia installato l'App, dovesse risultare positivo al virus solo il soggetto pubblico ricostruirà «a ritroso i contatti georeferenziati dell'utente e dunque i dati personali anche dei soggetti potenzialmente contagiati che hanno a loro volta installato l'App e avviato la geolocalizzazione». Tramite tali informazioni, inoltre, le autorità sanitarie potranno contattare l'utente, inviando un avviso in caso di possibile contagio.

Ebbene, alla luce di tale funzionamento, seppure l'applicazione ci paia complessivamente conforme ai principi in materia di protezione dei dati personali, da un lato, potrebbe risultare preferibile una esclusiva titolarità "pubblica" dei trattamenti dei dati personali, non limitata al dato relativo alla posizione; dall'altro lato, andrebbe scrutinato maggiormente il periodo di conservazione previsto, in relazione al tempo di incubazione della malattia[29].

Ad ogni modo, come si diceva, STOPCovid19 è stata sperimentata dalla Regione Umbria e pertanto rimane certamente l'App attualmente più rilevante; ma, ovviamente, non è l'unico *tool* esistente.

SoftMining S.r.l., ad esempio, ha sviluppato l'applicazione SM_Covid19, in grado di valutare il rischio di trasmissione del virus attraverso il monitoraggio del numero, della durata e del tipo di

---

https://www.repubblica.it/economia/2020/03/17/news/app_coronavirus-251422094/ e V. UGOLINI, *L'Umbria come la Corea: «Una app per tracciare gli spostamenti e scoprire i contagi»*, in *Il Messaggero*, 22 marzo 2020, https://www.ilmessaggero.it/umbria/coronavirus_umbria_app_contagi_spostamenti_22_marzo_2020-5126703.html.

[28] Testualmente, *Privacy policy* dell'applicazione STOPcovid-19, consultabile al link https://www.stopcovid19.it/it/privacy-policy/. Le informazioni raccolte dall'applicazione – previo consenso dell'interessato ed esclusivamente per fronteggiare l'emergenza sanitaria relativa al diffondersi del virus – sono gestite sia dalla Regione che dalla società sviluppatrice, soggetto di natura privatistica, sulla base di uno specifico accordo di contitolarità (cfr. art. 26 del Regolamento UE 2016/679).

[29] Considerato, invero, il periodo di incubazione del virus – che si stima vari da 2 e 11 giorni, fino ad un massimo di 14 giorni – in ossequio ai principi di minimizzazione e di limitazione della conservazione sarebbe preferibile prevedere un termine di trattamento di 14 giorni. Sul periodo di incubazione della malattia, v. MINISTERO DELLA SALUTE, *Faq – Covid-19, domande e risposte*, aggiornate, da ultimo, il 31 marzo 2020, http://www.salute.gov.it/portale/malattieInfettive/dettaglioFaqMalattieInfettive.jsp?lingua=italiano&id=228.

contatti[30]. Tale applicazione, una volta installata, acquisisce, in particolare, le informazioni sul numero e sulla durata degli incontri, dati dai quali determina, sulla base di un algoritmo, il "rischio probabile" di contagio. Più nel dettaglio, l'App monitora i contatti, attraverso l'acquisizione, da parte del dispositivo, di un ID univoco di tutti gli *smartphone* che rileva dai 2 ai 30 metri di distanza, in base ai sensori disponibili, e raccoglie i dati suddetti ogni 60 secondi, salvandoli su un *database*, condiviso con le autorità sanitarie. In tal modo, i dati vengono comunicati alle autorità sanitarie, mentre ogni utente può conoscere soltanto il proprio livello di rischio e non invece quello degli altri[31].

Da ultimo, comunque connessa al tema che ci occupa, è la misura adottata dalla Regione Lombardia che, per contenere il contagio da Coronavirus, ha fatto ricorso – non ad una App, ma – al *contact tracing* digitale, analizzando i flussi di dati aggregati (*rectius* anonimi), ottenuti dai principali operatori di telefonia mobile[32]. Trattandosi, pertanto, di un trattamento avente ad oggetto dati anonimi, esso non rientra nell'ambito di applicazione della disciplina di protezione, dimostrando la possibilità di ricorrere ad un'altra strategia, basata anch'essa sulla geolocalizzazione, pur se attuata con strumenti diversi[33].

Ebbene, se queste sono le applicazioni lanciate in Italia, il quadro comparato offre un più vasto ventaglio di soluzioni, alcune delle quali vale qui la pena di ripercorrere. Volgendo, dunque, lo sguardo ad altre esperienze, individueremo dapprima le principali App attualmente in uso nella Repubblica di Corea, il cui modello è stato più volte evocato nel dibattito pubblico[34]; a seguire,

---

[30] Cfr. M. GABANELLI – F. SAVELLI, *Covid-19: l'arma tecnologica per arginare il virus e gestire il dopo crisi. Come funziona*, in *Corriere della sera*, 22 marzo 2020, https://www.corriere.it/dataroom-milena-gabanelli/covid-19-arma-tecnologica-arginare-virus-contagio-gestire-dopo-crisi-come-funziona/b5f459e2-6c6b-11ea-8403-94d97cb6fb9f-va.shtml.

[31] La *privacy policy* dell'applicazione "SM_COvid19" è consultabile al link https://www.softmining.it/index.php/sm-covid19-app/.

[32] In sostanza, i dati delle posizioni, rilevati dai dispositivi mobili dei cittadini, sono stati utilizzati per la mappatura e il tracciamento degli spostamenti al fine di verificare il rispetto delle prescrizioni e misurare le distanze percorse dagli utilizzatori. Invero, i nostri *smartphone* utilizzano il segnale che viene diffuso dai ripetitori più vicini, ognuno dei quali copre una "cella". Ed il cellulare si aggancia da una cella all'altra, informazione che può essere elaborata per calcolare la durata e la distanza dello spostamento.

[33] Monitoraggio che, se e nella misura in cui venisse effettuato su dati anonimi o aggregati, potrebbe risultare preferibile ad ogni altro strumento, in ottica di riduzione dei rischi per il diritto alla protezione dei dati personali e di minimizzazione dei dati stessi, ma che pur andrebbe maggiormente scrutinato per vagliarne l'adeguatezza (o meno) rispetto al fine perseguito.

[34] Tra gli altri, C. DE CESARE, *Coronavirus, il modello Corea del Sud raccontato dagli italiani di Seul*, in *Corriere della Sera*, 19 marzo 2020, https://www.corriere.it/economia/consumi/20_marzo_19/coronavirus-modello-corea-sud-raccontato-italiani-seul-cfcef72a-69c1-11ea-a8a1-df48c20e9d2e.shtml; C. GRISANTI, *La lezione della Corea del Sud nella lotta al Covid-19*, in *Internazionale*, 18 marzo 2020, https://www.internazionale.it/notizie/claudia-

richiameremo, seppure in sintesi, la "scelta tecnologica" israeliana per il contrasto dell'epidemia, focalizzando l'attenzione sull'App "Hamagen", da quel Governo implementata. E proprio sulla falsariga di quel modello formuleremo, in conclusione, la nostra proposta in relazione all'ordinamento nazionale.

3. Il *panopticon* (sud) coreano

Al pari di molti Paesi, la Repubblica di Corea pone in essere, in generale ed anche in tempi non caratterizzati da epidemie, una sorveglianza sanitaria per la prevenzione delle malattie infettive[35]. Ciò che, tuttavia, sta richiamando attualmente l'attenzione – non solo del mondo scientifico ma anche dell'opinione pubblica – è il modello utilizzato per il contrasto alla diffusione del Covid-19 e, per quanto di nostro interesse, l'uso che, in aggiunta alle misure di isolamento e distanziamento sociale, il Governo sudcoreano sta facendo della tecnologia in questo ambito[36].

I dati raccolti dalle reti dei cellulari, dai GPS, dalle transazioni effettuate con carta di credito e dalle telecamere di videosorveglianza, combinati tra loro, permettono di monitorare (le persone e) i contagi, sì che il modello è assurto a paradigma per l'individuazione della strategia più adeguata per sconfiggere il virus[37].

---

grisanti/2020/03/18/lezione-corea-sud-covid-19; K. RICCARDI, *Coronavirus, gli sms della Corea del Sud sulle tracce dei contagiati. Un grande fratello che spaventa più del virus*, in *La Repubblica*, 6 marzo 2020, https://www.repubblica.it/esteri/2020/03/06/news/coronavirus_dignita_privacy_corea_del_sud_chat_sms_messaggi_contagi-250414120/.

[35] Cfr. WORLD HEALTH ORGANIZATION, *Communicable disease surveillance and response systems. Guide to monitoring and evaluating,* 2006, https://www.who.int/csr/resources/publications/surveillance/WHO_CDS_EPR_LYO_2006_1.pdf.

Per uno studio specifico sulla tempestività del sistema nazionale coreano di sorveglianza delle malattie dal 2001 al 2006 si veda, H. YOO, O. PARK, H. PARK ET AL., *Timeliness of national notifiable diseases surveillance system in Korea: a cross-sectional study*, BMC Public Health 9, 93, 2009, https://doi.org/10.1186/1471-2458-9-93.

[36] Quanto alle misure adottate per l'isolamento dei soggetti infetti v. DIVISION OF RISK ASSESSMENT AND INTERNATIONAL COOPERATION, *Enhanced the 2019-nCoV quarantine guideline in Republic of Korea*, 3 febbraio 2020, https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030&act=view&list_no=365953&tag=&nPage=1. Invece, sull'uso della tecnologia in ottica ricostruttiva delle principali misure implementate in Cina, Corea e Singapore v. G. ZUNINO, *Coronavirus, app e sistemi per tracciare i positivi: come funzionano*, in *agendadigitale.eu*, 20 marzo 2020, https://www.agendadigitale.eu/sicurezza/privacy/coronavirus-i-sistemi-per-tracciare-i-positivi-come-funzionano/.

[37] Cfr. S. WRAY, *South Korea to step-up online coronavirus tracking*, in *SmartCitiesWorld.net*, 12 marzo 2020, https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109; YONHAP, *S. Korea to run system to better detect virus patients' routes*, in *The Korea Herald*, 11 marzo 2020, http://www.koreaherald.com/view.php?ud=20200311000132. Ma sul tema, si veda anche KOREA CENTERS FOR

In questo contesto, anche in Corea del sud le App stanno giocando un ruolo fondamentale nella lotta alla diffusione del Covid-19 e tra esse[38] anzitutto "self-quarantine safety protection", che utilizza il GPS del telefono per tracciare la posizione dei soggetti in quarantena ed invia un avviso sia all'utilizzatore che al funzionario governativo nel caso di violazione dell'obbligo di autoisolamento[39]. L'applicazione, il cui *download* è facoltativo, permette al Governo di ricostruire gli spostamenti effettuati da un soggetto positivo nei giorni precedenti alla scoperta del contagio e, per conseguenza, porre in essere le misure ritenute adeguate, sia per avvisare i soggetti esposti, che per monitorare il paziente[40].

In aggiunta, stanno trovando diffusione ulteriori applicazioni, tra cui, anzitutto, "Corona 100m"[41], lanciata l'11 febbraio 2020, che, utilizzando i dati del Governo, avvisa gli utenti quando arrivano a 100 metri da un luogo visitato da una persona infetta.

Tale applicazione consente, in particolare, alle persone di conoscere la data in cui un soggetto sia risultato positivo, la nazionalità dell'interessato, il sesso, l'età e i luoghi frequentati. Attraverso essa è altresì possibile visualizzare la vicinanza, rispetto all'utilizzatore dello *smartphone*, di un soggetto positivo al virus[42]. Sennonché, il dettaglio su orari e luoghi rende possibile l'identificazione delle singole persone, almeno ai loro conoscenti più stretti, e solleva conseguentemente preoccupazioni per la tutela del diritto alla protezione dei dati personali, senza considerare, peraltro, situazioni di emarginazione sociale che potrebbero derivarne.

DISEASE CONTROL AND PREVENTION, Osong Public Health and Research Perspectives 2020, 11(1), 60-63, https://doi.org/10.24171/j.phrp.2020.11.1.09.

[38] Daremo conto, nel prosieguo, soltanto delle più note applicazioni utilizzate. Ulteriori *tools*, dei quali non ci occuperemo, sono, ad esempio, "Corona Doctor" e "KMA corona fact".

[39] Per ulteriori informazioni sul funzionamento dell'applicazione si veda il link https://www.mois.go.kr/frt/bbs/type002/commonSelectBoardArticle.do;jsessionid=7bA+UtY0JOIXJytznXoyYNHR.node40?bbsId=BBSMSTR_000000000205&nttId=76155. Informano dell'implementazione del sistema di tracciamento tramite l'applicazione "self-quarantine safety protection", C. WALSH, *South Korea plans to use a GPS-based app to monitor people quarantined at home*, in *cnn.com*, 4 marzo 2020, https://edition.cnn.com/asia/live-news/coronavirus-outbreak-03-04-20-intl-hnk/h_878ccdcbf1c36b0a299cbf9b784a36e5; M. S. KIM, *South Korea is watching quarantined citizens with a smartphone app*, in *MIT Technology Review*, 6 marzo 2020, https://www.technologyreview.com/s/615329/coronavirus-south-korea-smartphone-app-quarantine/.

[40] N. KIM, *'More scary than coronavirus': South Korea's health alerts expose private lives*, in *The Guardian*, 6 marzo 2020, https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives, pone l'accento sulle violazioni della privacy dei soggetti risultati positivi perpetrate tramite il sistema di monitoraggio e diffusione degli spostamenti da essi effettuati.

[41] Cfr. S. CARRER, *Corea: ecco come le infezioni rallentano*, in *Il sole 24 ore,* 9 marzo 2020, reperibile al link https://www.ilsole24ore.com/art/corea-eco-come-infezioni-rallentano-ADBnfyB.

[42] Cfr. I. WATSON – S. JEONG, *Coronavirus mobile apps are surging in popularity in South Korea*, in *Cnn business*, 28 febbraio 2020, https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html.

Allo scopo di facilitare l'individuazione delle aree maggiormente colpite dal coronavirus rispondono, invece, Corona Map e Coronaita che, localizzando su mappa i soggetti risultati positivi, indicano le aree da evitare[43]. In particolare, l'elaborazione dei dati (*id est* delle localizzazioni) degli utenti contagiati – o presunti tali – avviene attraverso l'indicazione del genere e dell'età, senza indicazione del nome, ma attraverso l'assegnazione di un numero di caso; informazioni che vengono poi utilizzate nei messaggi di *alert* inviati a chi può avere incrociato un soggetto positivo. Anche in tale ipotesi il sistema, che dovrebbe funzionare attraverso l'inserimento di dati anonimi, come da taluni rilevato, pare reggersi, tutto all'opposto, sulla diffusione di messaggi che potrebbero permettere di identificare la singola persona cui essi si riferiscono[44].

Ebbene, poiché non può escludersi il rischio di re-identificazione del soggetto cui le informazioni si riferiscono, deve pervenirsi alla conclusione che il trattamento abbia ad oggetto dati personali. Senza considerare, peraltro, che l'indicazione del luogo e dell'orario non solo potrebbero essere sufficienti per correlare un percorso ad una persona specifica, ma rendere manifeste anche ulteriori informazioni a carattere particolare[45]. Sicché – in tesi – il tracciamento dei soli positivi, così gestito, potrebbe portare a una forte incisione del diritto alla privacy di quei soggetti, che mal si attanaglierebbe al nostro sistema di valori e diritti costituzionali che, semmai, richiede altre e maggiori garanzie, nell'ottica della tutela della persona.

---

[43] Si vedano rispettivamente i siti internet https://coronamap.site/ e https://coronaita.com/#/.

[44] Descrivono la diffusione dei messaggi di *alert* nella Repubblica di Corea in termini di "virus patient travel log" M. JOO KIM e S. DENYER, *A 'travel log' of the times in South Korea: Mapping the movements of coronavirus carriers*, in *The Washington Post*, 13 marzo 2020, https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html. L'articolo riporta alcuni dei messaggi che vengono inviati dal sistema: «In central city of Daejeon, more than 1 million phones received an alert saying a virus carrier visited "Magic Coin Karaoke in Jayang-dong at midnight on Feb. 20." In Cheonan, a text alert to residents showed that an infected person visited "Imperial Foot Massage at 13:46 on Feb. 24." The digital diaries of infected people grew to cover all kinds of places: bars, karaoke clubs and short-stay "love hotels"». Secondo il Professore in sociologia della Korea University in Seoul, Yoon In-jin, - riportano i giornalisti - «a month into this nationwide experiment, we have yet to gauge its epidemiological effectiveness, but already saw too many virus patients getting ridiculed and judged for places they visited».

[45] Basti qui ipotizzare l'eventuale localizzazione di un soggetto presso uno studio medico specialistico (ad esempio, oncologico).

4. La scelta tecnologica israeliana

Anche il Governo israeliano, superati i 1000 casi di tamponi positivi, ha ritenuto di utilizzare la geolocalizzazione, in aggiunta alla strategia del distanziamento sociale.

Dapprima approvando misure di emergenza per rintracciare, attraverso il monitoraggio dei cellulari, le persone sospette o per le quali vi sia certezza di contagio, ricorrendo alla tecnologia sviluppata per il contrasto al terrorismo. E, a tal fine, sono stati riconosciuti pieni poteri all'agenzia di sicurezza Shin Bet, per il tracciamento degli *smartphone* al duplice scopo di inviare messaggi di avviso a coloro che sono stati esposti, avvicinandosi ad un paziente Covid-19, e garantire il rispetto degli ordini di quarantena[46].

Misure che hanno sollevato da subito dibattito e – condivisibili – critiche[47], in un Paese che oltre alla epidemia in corso deve fare i conti anche con non semplici equilibri di politica interna[48]. Ad esse ne è poi seguita un'altra, che pur mirando allo stesso fine – il tracciamento – assicura maggiori tutele per i diritti, e tra questi la protezione dei dati personali: il 22 marzo 2020 il Ministero della salute israeliano ha, infatti, lanciato una nuova App, finalizzata al contrasto della diffusione del coronavirus, attraverso un sistema di tracciamento che permette agli utenti di sapere se hanno avuto contatti con un paziente positivo[49].

Per vero, già prima del ricorso alla geolocalizzazione tramite App il Ministero pubblicava, in forma anonima, la storia epidemiologica dei pazienti con COVID-19, elencando i luoghi che questi avevano frequentato e invitando tutti coloro che vi si erano recati a mettersi in quarantena per 14

---

[46] Tali misure sono state annunciate dal Primo Ministro israeliano Benjamin Netanyahu nella serata di lunedì 16 marzo 2020. Si veda, tra i vari articoli di informazione, O. HOLMES, *Istrael to track mobile phones of suspected coronavirus cases*, in *The Guardian*, 17 marzo 2020, https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases; della stampa italiana D. FRATTINI, *Israele, i servizi segreti arruolati per pedinare gli infettati dal Coronavirus: «E' una guerra»*, in *Corriere della sera*, 15 marzo 2020, https://www.corriere.it/esteri/20_marzo_15/israele-servizi-segreti-arruolati-pedinare-infettati-coronavirus-guerra-4fdf7d9c-66af-11ea-a26c-9a66211caeee.shtml.

[47] Tra i rilievi che vengono mossi vi è, non a caso, quello della compressione del diritto alla privacy. In particolare, «the Association for Civil Rights in Israel said providing the country's internal security agency, the Shin Bet, with new secretive powers was a "dangerous precedent and a slippery slope that must be approached and resolved after much debate and not after a brief discussion"» (così O. HOLMES, *Israel to track mobile phones*, cit.).

[48] Sul punto v., ad esempio, O. HOLMES, *Netanyahu key ally resigns as speaker of Israeli parliament*, in *The Guardian*, 25 marzo 2020, https://www.theguardian.com/world/2020/mar/25/netanyahu-ally-yuli-edelstein-resigns-speaker-israel-parliament.

[49] S. WINER, *Health Ministry launches phone app to help prevent spread of coronavirus*, in *The Times of Israel* , 23 marzo 2020, https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus/.

giorni. Ciò che muta, pertanto, è la possibilità per le persone di utilizzare uno strumento tecnologico che, sovrapponendo i percorsi effettuati dai pazienti positivi a quello rilevato dallo *smartphone* dell'utente, calcola automaticamente il rischio di contatto, e conseguente contagio. A tale applicazione dedicheremo specifica attenzione perché suscettibile di offrire un valido modello implementabile anche nel nostro Paese.

4.1. Hamagen (The Shield)

Hamagen (The Shield) – così è stata chiamata l'applicazione israeliana – permette di rilevare se un utente nei 14 giorni precedenti è stato vicino ad un soggetto risultato positivo, ed opera, come testé accennato, attraverso l'intersezione della cronologia delle posizioni del dispositivo sulla quale viene scaricata con i dati aggiornati sulla localizzazione sanitaria del Ministero della salute[50].

In particolare, le tracce vengono confrontate con i pazienti positivi solo sul telefono e i dati relativi alla posizione non vengono inviati a terzi, né trasmessi al Ministero o ad altra Autorità.

Misura, questa, che ci pare essere particolarmente rispettosa del diritto alla privacy degli utenti e sulla quale intendiamo richiamare l'attenzione. Infatti, poiché soltanto i dati aggiornati del Ministero della salute vengono trasmessi unilateralmente al dispositivo per il confronto, il trattamento viene posto in essere dall'utente e rimane a carattere personale.

Ma scendiamo più nel dettaglio. L'app scarica un file dal *cloud* del Ministero della Salute con un elenco anonimo di localizzazioni (incluse date e orari) dei pazienti positivi ed incrocia le posizioni memorizzate dal dispositivo con gli spostamenti dei soggetti infetti. Tali informazioni – ed è questo un aspetto importante – sono intersecate soltanto nel dispositivo e non, invece, nel *cloud*, sicché esse rimangono nella disponibilità (e sotto il controllo) del solo utilizzatore.

Dei dati oggetto di trattamento viene tenuta traccia per due settimane, decorrenti dal momento in cui l'applicazione viene scaricata sul dispositivo; termine di conservazione che risulta conforme

[50] Ulteriori informazioni sull'applicazione Hamagen (The Shield) sono disponibili al *link*: https://govextra.gov.il/ministry-of-health/hamagen-app/download-he/.

rispetto alla finalità per la quale il trattamento viene posto in essere, considerato che il tempo massimo di incubazione della malattia è di 14 giorni[51].

La veridicità ed esattezza delle informazioni relative ai pazienti positivi vengono garantite a monte, poiché il file viene implementato esclusivamente dal Ministero della salute israeliano e contiene le informazioni verificate provenienti da laboratori e indagini epidemiologiche.

Quanto, invece, alle misure di sicurezza predisposte, anzitutto l'applicazione è stata sviluppata per il Ministero della salute e si basa sui valori dell'*open source*: chiunque, pertanto, può implementare funzionalità aggiuntive, essendo il codice sorgente stato pubblicato su GitHub.

Inoltre, il file contenente i dati dei pazienti positivi viene firmato digitalmente dal Ministero della salute ed inviato, su linee di comunicazione dedicate, al *cloud*, ove viene archiviato. Nel momento della ricezione, poi, l'applicazione verifica la firma a garanzia dell'esattezza del mittente e procede con le correlazioni[52].

Qualora l'applicazione dovesse individuare delle corrispondenze – e rilevare pertanto che l'interessato si trovava in un dato momento nello stesso luogo di un paziente risultato positivo – essa non trasmette i dati ad alcuno, ma collega l'utente al sito del Ministero della salute[53].

L'uso dell'applicazione è facoltativo e quando essa viene disattivata le informazioni sul dispositivo vengono eliminate.

Ebbene, con il lancio della nuova applicazione, il Governo israeliano conferma la volontà di ricorrere alla tecnologia per contrastare la diffusione del virus, ma con modalità che (almeno per ora) segnano un deciso cambiamento di rotta.

Così programmata, l'applicazione risulta essere attualmente uno strumento "per i cittadini" e non "di controllo dei cittadini". Tuttavia, non è detto che essa rimanga tale in futuro e taluni dubbi emergono se si legge tra le righe dei termini d'uso. In esse, invero, sembra potersi intuire che questa modalità di trattamento dei dati sia soltanto il primo *step* di un processo più ampio, i cui possibili sviluppi potrebbero prevedere la trasmissione delle informazioni al Ministero della salute, seppure a

[51] Si veda la nota n. 28.

[52] Sul funzionamento dell'App si possono consultare i termini d'uso reperibili al link https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/.

[53] Da tale sito, in particolare, l'utente, a seconda della specifica situazione, potrà inviare una dichiarazione di isolamento; un *report* nell'ipotesi in cui sia stato messo in isolamento a casa dopo uno stretto contatto con un paziente confermato, oppure un "report a violation of the home isolation duty". Il link attraverso il quale è possibile compilare i moduli *de quibus* è https://govextra.gov.il/ministry-of-health/corona/corona-virus-en/, consultato in data 25 marzo 2020.

fronte della garanzia che, se tale fase verrà raggiunta, si provvederà ad acquisire il consenso degli interessati.

5. La localizzazione: da (possibile) strumento di controllo a strumento di garanzia per i cittadini

Tornando dallo sguardo comparato al discorso da cui siamo partiti circa il bilanciamento tra gli interessi in gioco nell'uso di soluzioni tecnologiche per la sorveglianza attiva nel corso dell'emergenza da Covid-19, ferma restando la possibile prevalenza della tutela della salute, quale *prius* logico di ogni altro diritto, e la conseguente recessività della protezione dei dati personali, possiamo tuttavia osservare come, tra le varie soluzioni che permettano di raggiungere un determinato fine, dovrà individuarsi quella che comporti il minor sacrificio possibile dell'interesse conculcato.

In particolare, nella selezione della strategia preferibile, occorrerà «orientarsi secondo un criterio di gradualità», ricercando un ragionevole punto di equilibrio tra gli interessi in gioco, «e dunque valutare se le misure meno invasive possano essere sufficienti a fini di prevenzione»[54].

Come si è visto, tre sono, in astratto, le soluzioni prospettabili: il monitoraggio tramite dati anonimi; la localizzazione dei soli soggetti risultati positivi al tampone; oppure il tracciamento di tutti, tramite l'uso delle celle telefoniche o le applicazioni[55].

L'analisi di alcune esperienze straniere ci consente di proporre una quarta strategia: quella della "localizzazione responsabile"[56].

La localizzazione responsabile potrebbe essere attuata attraverso la programmazione di un'App che rispetti le seguenti condizioni: 1) che sia implementata da parte di un'Autorità pubblica; 2) che

[54] Tali parole di Antonello Soro, Presidente del Garante per la protezione dei dati personali, sono state raccolte in una recente intervista da C. FUSANI, *In uno stato di eccezione è lecito rinunciare a qualche libertà. Ma il nostro modello non potrà mai essere la Cina*, in *Tiscali News*, 19 marzo 2020, doc. web. 9294061, reperibile sul sito www.garanteprivacy.it.

[55] Si veda il paragrafo 2 del presente contributo.

[56] Una quarta soluzione o, se si preferisce, una strategia intermedia tra le due che abbiamo detto essere le uniche percorribili attualmente (ossia, il monitoraggio tramite dati anonimi e il tracciamento dei soli positivi). Sul punto si veda il paragrafo 2.1. La proposta prende ampiamente spunto dall'applicazione israeliana, per come risulta ora in uso, ma prevede un diverso meccanismo di comunicazione dei dati elaborati (si veda, in particolare, la condizione n. 5 enunciata nel testo), nell'ottica di una maggior tutela degli interessati.

indichi in modo intellegibile le modalità di funzionamento; 3) che utilizzi i soli dati verificati dalle autorità sanitarie; 4) che sia programmata in modo tale per cui soltanto i dati aggiornati delle autorità sanitarie vengano inviati unilateralmente al dispositivo per il confronto, sicché, lasciando ai singoli utenti la possibilità di correlare le proprie posizioni con quelle risultanti dal tracciamento dei pazienti positivi, quel trattamento di dati resti a carattere esclusivamente personale o domestico[57]; 5) che, in caso di riscontro di un contatto con un soggetto positivo, non renda conoscibili la posizione e l'orario in cui esso è avvenuto, ma comunichi soltanto, tramite *alert*, il rischio di contagio, sì da rendere non identificabile la persona infetta; 6) il cui funzionamento sia basato sui valori dell'*open source*; 7) della quale sia pubblicato il codice sorgente; 8) che dia garanzia dell'adeguatezza delle misure di sicurezza adottate; 9) che preveda un periodo di conservazione dei dati limitato al tempo strettamente necessario per il raggiungimento della finalità (ossia, la protezione dall'emergenza sanitaria al fine del contenimento e contrasto della diffusione del virus); 10) il cui funzionamento sia condizionato alla perduranza dello stato di emergenza.

Un'applicazione che lasci agli utenti – e solo a questi – il pieno controllo delle proprie informazioni, garantendo la tutela della salute senza compromettere (eccessivamente) la protezione dei dati personali[58].

In tal modo, in conclusione, potrebbe darsi concretezza al bilanciamento di interessi: «senza cedere alla tentazione della scorciatoia tecnologica solo perché apparentemente più comoda, ma valutando attentamente benefici attesi e "costi", anche in termini di sacrifici imposti alle nostre libertà»[59].

---

[57] Il trattamento *de quo*, invero, sarebbe riconducibile all'eccezione di cui all'art. 2, par. 2, lett. c) del Regolamento UE 679/2016, essendo esso effettuato «da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico».

[58] Ciò, peraltro, già a monte, ossia prevedendo l'uso della applicazione come facoltativo, nella convinzione che la collettività, a fronte di uno strumento a tutela della salute che assicuri anche la protezione dei dati personali, responsabilmente, sceglierà di utilizzarlo. Del resto, non sarebbe prospettabile la doverosità dell'utilizzo di una simile tecnologia, senza, al contempo, la previsione non solo dell'obbligo che ogni individuo abbia uno *smartphone*, ma anche il trasporto di esso in ogni attività quotidiana; misure che, di tutta evidenza, finirebbero per incidere – in maniera sproporzionata – su altri diritti costituzionali e, per conseguenza, sarebbero illegittime.

[59] In tal senso, Antonello Soro, Presidente del Garante per la protezione dei dati personali, in una recente intervista di A. MAJOLI, *Soro, la sfida privacy in era coronavirus*, doc. web. 9292565, cit.

Avvenire.it

Coronavirus. Mirabelli: l'app per legge e a tempo

Angelo Picariello venerdì 24 aprile 2020
Il presidente emerito della Corte costituzionale: occorreva più cautela negli annunci. Non basta un Dpcm, serve una legge E i dati poi vanno distrutti

«Intervenire si può, a patto che sia una misura di carattere temporaneo», avverte Cesare Mirabelli. Come «temporaneo deve essere anche l'utilizzo dei dati», sul modello di quanto previsto per le intercettazioni. Per il presidente emerito della Consulta sull'introduzione della app 'Immuni' occorreva maggiore cautela, «evitando effetti-annuncio». Ma se emergerà ora una pubblica utilità «facendone un uso proporzionato potrebbe diventare anche una misura obbligatoria».

Ma sarebbe stato meglio porsi prima questi problemi.

Sarebbe opportuno, in questi casi, essere meno precipitosi nella comunicazione. Si rischia di creare contraccolpi da cui poi è difficile uscire. Certo, non può essere esclusa una misura del genere di fronte all'esigenza di fronteggiare una grave epidemia. Ma va adottata con cautela, sia nei principi che nelle procedure.

Partiamo dai princìpi.

Un controllo degli spostamenti è ammesso dalla Costituzione per motivi sanitari. Ma serve allora un provvedimento con forza di legge: un Dpcm o il decreto di un'autorità indipendente o di un commissario non basta. L'altra limitazione che si pone, in ordine al diritto alla riservatezza, è la proporzionalità dell'intervento, la sua ragionevolezza rispetto all'obiettivo da perseguire. La tutela della salute è fra i principi inviolabili previsti dall'articolo 2, lo esplicita poi l'articolo 32, che la definisce un «fondamentale diritto dell'individuo». Ma c'è un dovere di solidarietà previsto dallo stesso articolo. E fra questi due principi (diritto alla salute, dovere di solidarietà) va operato il concreto il bilanciamento di interessi individuali e collettivi.

In presenza, però, di un concreto rischio pandemia.

Certo, debbono essere misure strettamente funzionali all'obiettivo. In concreto, si ipotizza di tracciare gli spostamenti delle persone e di conoscere il loro stato di salute. Ma questo deve riguardare solo gli

elementi finalizzati alla prevenzione dell'epidemia, esaminando in concreto il funzionamento degli strumenti tecnologici.

E qui si aggiunge il problema della volontarietà.

Attenzione: la misura, anche se volontaria, non può aggirare le garanzie costituzionali: il problema della riservatezza e della gestione dei dati resta. C'è l'esigenza di una temporaneità delle gestione di questi dati sensibili che va disciplinata dall'Autorità garante della privacy. Il problema che si pone, similmente a quanto accade per le intercettazioni, è l'incrocio fra i dati di chi ha fornito la sua disponibilità con quello di altri che non la hanno fornita.

La misura, anche se volontaria, non può aggirare le garanzie costituzionali. Ma se è una misura necessaria, anziché fingere che sia volontaria è meglio imporla, entro i limiti in cui può essere imposta. Se il sacrificio richiesto è proporzionale, se può funzionare solo con un'ampia adesione, a quel punto, forse, sarebbe meglio renderlo obbligatorio

Quindi?

Per questo serve una legge: non può essere la porta d'ingresso per introdurre il controllo degli spostamenti e dello stato di salute delle persone. Ma, vista la delicatezza del tema, è necessaria anche una periodica informativa al Parlamento che deve poter esercitare in concreto i suoi poteri di indirizzo e controllo.

Si ipotizza di subordinare lo spostamento da Regioni ancora sotto contagio all'accettazione di questa app.

Ma i confini regionali potrebbero essere un riferimento artificioso, forse servirebbe un criterio più flessibile, per comprensori, spesso a cavallo di più Regioni. In ogni caso, la politica non può pensare che sia la tecnica a vigilare sulla concreta attuazione.

Chi dovrà vigilare?

Più che comitati, che spesso complicano le cose, debbono vigilare da un lato l'Autorità garante della Privacy, e dall'altro una commissione parlamentare che vigili sull'adeguatezza, sulla proporzionalità e sulla ragionevolezza dei provvedimenti. Ma questo sarà possibile solo con l'adozione di una legge, che consente anche al Quirinale e alla Consulta di esercitare il loro potere di controllo. In questo modo potrà essere valutata un'interruzione della misura (con tutte le esigenze connesse di auto-distruzione dei dati) o se necessario, in seguito, una sua reintroduzione.

Serve una commissione ad hoc?

Potrebbe essere opportuna una commissione speciale per valutare tutti gli effetti relativi alla pandemia.

Ma condizionare la fruizione di alcuni diritti a questa app non può costituire un'obbligatorietà mascherata?

Non mi sembra una modalità percorribile. Perché metterebbe in relazioni soggetti che hanno effettuato opzioni diverse, e questo creerebbe sicuramente dei problemi. Se si tratta di un servizio che viene offerto è un conto. Ma se è una misura necessaria, anziché fingere è meglio imporla, entro i

limiti in cui può essere imposta. Se il sacrificio richiesto è proporzionale, con tutte le garanzie, può funzionare solo con un'ampia adesione. E a quel punto, forse, sarebbe meglio renderlo obbligatorio.

“Immuni”, l’app del governo per il tracciamento del contagio da Covid-19

“Immuni” è l’app selezionata, tra le oltre 300 soluzioni proposte da privati, società ed enti, per il tracciamento dei positivi al coronavirus tramite tecnologia bluetooth, totalmente anonima e su base volontaria, fornita dalla società Bending Spoons S.p.a. in partnership con il Centro Diagnostico Santagostino. Solo chi avrà scaricato “spontaneamente” l’applicazione potrà fare a meno dell’autodichiarazione cartacea e, quindi, muoversi con meno restrizioni nella agognata Fase 2.

Con l’ordinanza n. 10/2020, del 16 aprile scorso, il Commissario straordinario per l’attuazione e il coordinamento delle misure di contenimento e contrasto dell’emergenza epidemiologica Covid-19 ha disposto di procedere alla stipula del contratto di concessione gratuita della licenza d’uso sul *software* di *contact tracing* e di appalto di servizio gratuito con la società Bending Spoons S.p.a in relazione all’app “Immuni”.

Immuni è stata scelta, **con una procedura atipica**,

anche perché dovrebbe garantire la tutela della privacy degli utenti in modo nuovo, consentendo di mantenere il **controllo dei propri dati**, senza che questi vengano condivisi con le istituzioni.

Attraverso il ***bluetooth*** la app rileva la vicinanza tra due *smartphone* entro un metro e ripercorre a ritroso tutti gli incontri di una persona risultata positiva al Covid-19, così da poter rintracciare e isolare i potenziali contagiati. Una volta scaricata, infatti, “Immuni” memorizza e conserva in locale, sul dispositivo di ciascun cittadino, una lista di codici identificativi anonimi (tutti i **codici *bluetooth***) degli altri dispositivi ai quali è stata vicino, dotati della stessa app (siano questi ***smartphone***, ***smart watch*** o ***device stand alone*** come braccialetti). I contatti avuti con altre persone vengono tracciati attraverso il *bluetooth* che “aggancia” gli altri *smartphone* nel raggio di pochi metri con la stessa app installata senza definirne la posizione geografica. **Sistemi di crittografia** e **pseudoanonimizzazione** impediscono di associare il codice all’identità del proprietario di quel dispositivo.

Tali informazioni sono archiviate all'interno della memoria del dispositivo su cui è installata l'app e lì vengono conservate fino a quanto le autorità sanitarie non hanno la certezza che il proprietario di quello *smartphone* sia risultato positivo al tampone da Coronavirus.

L'operatore sanitario, prima di compilare il **questionario analogico**, chiede al paziente se ha installato l'app Immuni e se intende prestare il proprio **consenso al trattamento dei dati conservati sul cellulare**, permettendo – solo in quel caso – di ricostruire la sua rete di contatti nei giorni precedenti e, quindi, i suoi spostamenti; l'operatore genera, con una diversa app, un codice con cui il cittadino può caricare su un *server* i dati raccolti dalla sua app, ovvero una **lista dei codici *bluetooth*** con cui il soggetto è entrato in contatto.

Il *server* calcola per ognuno di questi codici il rischio che ci sia stato un contagio (vicinanza, tempo di contatto) e, quindi, invia una notifica ai dispositivi di persone potenzialmente a rischio, sempre tramite l'app.

La notifica contiene un messaggio predisposto dalle autorità sanitarie con il protocollo al quale il destinatario deve adeguarsi (isolamento, contattare numeri di emergenza per tamponi).

Da quanto è dato sapere fino a questo momento, l'app Immuni, **ancora in fase di scrittura definitiva**, si comporrà di due parti distinte:

1. un **diario clinico**, anonimo e volontario, dove gli utenti possono scrivere informazioni rilevanti dal punto di vista medico (oltre a età, sesso anche malattie pregresse e farmaci assunti) e che dovrebbe essere aggiornato tutti i giorni con eventuali sintomi e cambiamenti sullo stato di salute; informazioni che potranno essere utilizzate dagli operatori sanitarie qualora il cittadino si rivolga al servizio sanitario;
2. i **dati gps** di **geolocalizzazione** per tenere traccia dei contatti e spostamenti, che possono essere utilizzati solo in forma aggregata, per tracciare nuovi possibili focolai: lo permette la tecnologia dell'app di Bending Spoon, ma al momento non è chiaro se il Governo vorrà usare anche questa funzione.

In ogni caso, prima di essere avviato definitivamente, il *software* verrà testato in alcune regioni pilota a partire dal mese di maggio.

Immuni sembrerebbe differenziarsi, dunque, dalle app utilizzate in altri paesi colpiti dalla pandemia, dove i governi hanno fatto ricorso a forme di sorveglianza informatica intrusiva, attraverso l'utilizzo del *bluetooth* e altri sensori e dovrebbe garantire l'anonimato degli utenti, attraverso un ID (codice identificazione utente) anonimo e temporaneo, basandosi – in ogni caso – su un utilizzo volontario da parte dei cittadini.

La tecnologia *bluetooth*, del resto, è stata giudicata dall'Unione europea come la più idonea per le app di tracciamento che hanno la missione di "*stimare con sufficiente precisione*" (circa 1 metro) "*la vicinanza*" tra le persone per rendere efficace l'avvertimento se si è venuti a contatto con una persona positiva al Covid-19 e non quella di seguire i movimenti delle persone o far rispettare le regole, perché questo "*creerebbe rilevanti problemi di sicurezza e privacy*" (si v. la raccomandazione della Commissione europea dell'8 aprile 2020 contenente una serie di misure e azioni che mirano a sviluppare un approccio comune dell'Ue per l'utilizzo di applicazioni e dati mobili in risposta alla pandemia di coronavirus: una *toolbox* contente regole per il sistema di tracciamento).

La **tutela della privacy viene in** rilievo, così, quale **criterio fondamentale per la scelta dell'app governativa** per il controllo tempestivo del livello di esposizione al rischio delle persone e

conseguentemente dell'evoluzione dell'epidemia Covid-19 sul territorio. Il governo, dunque, nel **bilanciamento tra il diritto alla riservatezza e la lotta alla diffusione dell'epidemia sembrerebbe aver scelto, laddove sia confermato che i dati inseriti non possano essere riutilizzati dalla società, la soluzione meno invasiva per i cittadini**, garantendo la tutela piena della privacy.

"Le app degli spostamenti solo su base volontaria" - Intervista ad Antonello Soro

"Le app degli spostamenti solo su base volontaria"

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali
(Di Valentino Di Giacomo, Il Mattino, 17 aprile 2020)

"Bisognerebbe adottare - e presto - una disciplina uniforme a livello nazionale che impedisca disparità di trattamento tra cittadini su base territoriale e assicuri garanzie equivalenti per tutti. C'è stata, invece, una proliferazione di iniziative". Antonello Soro guida da otto anni l'autorità per la protezione dei dati personali. Il Garante della privacy ha letto l'inchiesta pubblicata ieri dal Mattino sui meccanismi adottati in Campania per tracciare i possibili spostamenti di chi ha contratto il Covid-19, ma teme che di questo passo non si riuscirà a tenere il conto delle tante iniziative regionali, con seri rischi sul profilo della sicurezza dei nostri dati. Fughe in avanti che potrebbero pregiudicare gli obiettivi comuni.

Attualmente la mappatura attiva in Campania avviene in forma anonima, senza associare i dati degli spostamenti a un nominativo. Lo ritiene un buon metodo?

"Il sistema cui fa riferimento l'articolo del vostro giornale sembra diverso dal "contact tracing" vero e proprio, in quanto funzionale alla localizzazione di coloro ai quali siano imposte misure di permanenza domiciliare e non, invece, alla ricostruzione della catena dei contagi. Anche tale soluzione deve però mantenersi entro il perimetro normativo, garantendo la proporzionalità e non eccedenza del trattamento dei dati".

Resta il problema che una guida univoca a livello nazionale per affrontare questo tema non esista ancora. Teme che, come in Campania, possa svilupparsi un fai-da-te regionale che possa creare ancor più confusione?

"Ad ora ci sono tante iniziative. A ciascuna di esse, mi chiedo, è seguita effettivamente un'autonoma valutazione d'impatto privacy, l'individuazione di server sicuri nei quali allocare i dati in maniera protetta, impedirne usi a fini diversi e cancellarli non appena ne cessi l'utilità? Di fronte a una pandemia che esige un coordinamento almeno in ambito europeo, sarebbe contraddittorio differenziare - addirittura a livello regionale - le modalità di azione".

Il Governo, su impulso del ministero dell'Innovazione, ha istituito una Commissione straordinaria denominata "Data Drive" al fine di sviluppare un'app che possa servire a tracciare gli spostamenti. Quali spunti ha dato il Garante?

"L'Autorità partecipa ai lavori della Commissione, in una posizione del tutto distinta da quella degli esperti di nomina ministe riale, per esprimere le esigenze di protezione dati sin dalla fase di scelta della soluzione da adottare. In quella sede, abbiamo in particolare indicato come preferibili le misure basate sulla volontaria adesione del singolo, sulla conservazione "in locale" del diario dei contatti, sui dati blue tooth (pseudonimizzati), in quanto maggiormente selettivi e, dunque, di minore impatto sulla privacy".

Il cittadino può quindi rifiutare di essere mappato pur avendo contratto il virus e rappresentando un potenziale pericolo

per la collettività? Non ritiene debba essere obbligatorio pur pregiudicando alcune libertà individuali?

"L'indicazione fornita alla Commissione è che siano preferibili soluzioni fondate sulla volontaria adesione del singolo, anche perché misure basate sui dati raccolti dai dispositivi mobili (che presuppongono dunque la costante presenza del telefono accanto a noi) sono difficilmente coercibili. Il contact tracing necessita dell'adesione di circa il 60% della popolazione: se si riesce a sensibilizzare tale quota di cittadini, il risultato potrebbe essere a un tempo rispettoso della privacy e proficuo per il contenimento dei contagi".

L'Ue sta provando anche a creare un'unica app per l'intera Unione Europea. Avremmo uguali garanzie a quelle che abbiamo in Italia circa la tutela della privacy? Sarebbe una buona soluzione?

"L'ipotesi di un'app paneuropea non comporterebbe in alcun modo una riduzione delle garanzie di protezione dati. La disciplina della materia è, infatti, ormai di fonte direttamente europea e dunque gli Stati mèmbri applicano tutti la stessa disciplina, salvo limitati margini di dif ferenziazione. Peraltro, con riferimento al contact tracing, il Comitato europeo per la protezione dati ha condiviso un approccio assolutamente conforme a quello da noi indicato".

Diritto alla salute e diritto alla privacy: saremo costretti a scegliere o esiste una terza via?

"La potenziale contrapposizione tra privacy e salute pubblica è il riflesso della più generale tensione tra libertà individuali e interessi collettivi, che solo la democrazia può rendere equilibrio, se non addirittura in sinergia. La sfida di oggi è nel garantire che i diritti individuali siano limitati nella (sola) misura necessaria a salvaguardare quante più vite umane possibili. La disciplina di protezione dati già comprende al suo interno le limitazioni necessarie a garantire istanze solidaristiche quali quelle espresse dalle esigenze di salute pubblica, secondo i criteri della proporzionalità, precauzione e temporaneità".

Soro: "Sì al tracciamento dei contatti ma con un decreto temporaneo" - Intervista ad Antonello Soro

Soro: "Sì al tracciamento dei contatti ma con un decreto temporaneo"

Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali
(di Andrea Iannuzzi, "La Repubblica" - 26 marzo 2020)

Tra le strategie messe in campo dal governo per contenere il contagio da coronavirus c'è il cosiddetto contact tracing digitale, cioè l'uso dei dispositivi mobili dei cittadini per la mappatura e il tracciamento dei soggetti entrati in contatto con persone infette: il modello coreano. Ma come si assicura la tutela della privacy e dei dati personali? Il Garante della privacy Antonello Soro, con il suo team di esperti, è al lavoro per conciliare tutte le esigenze: "*Non si tratta* - dice a Repubblica - *di sospendere la privacy, ma di adottare strumenti efficaci di contenimento del contagio, pur sempre nel rispetto dei diritti dei cittadini".*

C'è bisogno di uno strumento legislativo ad hoc per attuare questo protocollo? Quale?

"La disciplina di protezione dei dati coniuga esigenze di sanità pubblica e libertà individuale, con garanzie di correttezza e proporzionalità del trattamento. Ma una misura quale il contact tracing, che incide su un numero elevatissimo di persone, ha bisogno di una previsione normativa conforme a questi principi. Un decreto-legge potrebbe coniugare tempestività della misura e partecipazione parlamentare. Va da sé che la durata deve essere strettamente collegata al perdurare dell'emergenza".

Come si evitano gli abusi nel trattamento dei dati? Come ci si difende da intrusioni malevole?

"La nostra disciplina offre gli strumenti per minimizzare il pericolo di abusi, secondo i principi di precauzione e prevenzione, che impongono misure di sicurezza e garanzie di protezione dati già nella fase di progettazione e impostazione della struttura tecnologica. Rispettando questi criteri, si può valorizzare al massimo grado l'innovazione".

Si può immaginare uno scambio di dati criptato o anonimizzato?

"Lo scambio e, prima ancora, la raccolta dei dati devono avvenire nel modo meno invasivo possibile per gli interessati, privilegiando l'uso di dati pseudonimizzati (ove non addirittura anonimi), ricorrendo alla reidentificazione laddove vi sia tale necessità, ad esempio per contattare i soggetti potenzialmente contagiati. Nella complessa filiera in cui si articolerebbe il contact tracing, soggetti privati - a partire dalle grandi piattaforme - dovrebbero porre il patrimonio informativo di cui dispongono a disposizione dell'autorità pubblica, alla quale dovrebbe invece essere riservata la fase dell'analisi dei dati, che necessita delle garanzie e della responsabilità degli organi dello Stato. In ogni caso, le società coinvolte in questo progetto dovrebbero possedere requisiti di affidabilità e trasparenza di azione. Nella valutazione è fondamentale il vaglio di conformità ai requisiti di protezione dati, per la garanzia dei diritti degli interessati, per l'attendibilità dell'analisi dei dati e anche per la sicurezza nazionale. Non sottovaluterei l'odierno richiamo in proposito da parte del Copasir".

Come si potrà poi tornare alla "normalità" una volta finita emergenza?

"La chiave è nella proporzionalità, lungimiranza e ragionevolezza degli interventi, oltre che nella loro temporaneità. Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando per efficienza la rinuncia a ogni libertà e la delega cieca all'algoritmo per la soluzione salvifica".

Impact of contact tracing on SARS-CoV-2 transmission

Flickr · Jay Sterling Austin

Lancet Infect Dis 2020

Published Online
April 27, 2020
https://doi.org/10.1016/S1473-3099(20)30357-1

See Online/Articles
https://doi.org/10.1016/S1473-3099(20)30287-5

As the far-reaching impacts of the coronavirus disease 2019 (COVID-19) pandemic expand to more and more countries, key questions about transmission dynamics and optimal intervention strategies remain unanswered. In particular, the age profile of susceptibility and infectivity, the frequency of super-spreading events, the amount of transmission in the household, and the contribution of asymptomatic individuals to transmission remain debated. The study by Qifang Bi and colleagues[1] in *The Lancet Infectious Diseases* explores some of these questions by analysing detailed contact tracing data from Shenzhen, a large and affluent city in southern China at the border with Hong Kong. To dissect the drivers of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) transmission, the authors modelled PCR-confirmed infections in 391 cases and 1286 of their close contacts from Jan 14 to Feb 12, 2020.[1]

Shenzhen is an interesting location to study the dynamics of SARS-CoV-2 because it was affected early in the pandemic and reacted quickly.[2] Strict case isolation, contact tracing, and social distancing measures kept the transmission rate near the epidemic threshold throughout the study period.[2] Bi and colleagues report that most secondary infections occurred in the household (77 of 81), with a secondary attack rate estimated at 11·2% (95% CI 9·1–13·8) among household contacts.[1] This figure should be considered an underestimate of the unmitigated household attack rate of SARS-CoV-2, since transmission chains were cut short in Shenzhen because of strict control measures. Index cases detected by symptom-based surveillance were isolated outside of the home on average 4·6 days (95% CI 4·1–5·0) after symptom onset. Furthermore, individuals identified via contact tracing were isolated or quarantined outside of the home on average 2·7 days (95% CI 2·1–3·3) after symptom onset.[1] Consequently, the serial interval of SARS-CoV-2 in Shenzhen (mean estimate 6·3 days; 95% CI 5·2–7·6) should be considered a lower bound and would probably increase in less successfully controlled outbreaks.

The age profile of PCR-confirmed infections in Shenzhen indicates that children are as susceptible to SARS-CoV-2 infection as adults, although they are less likely to display symptoms.[1] The distinctive age profile of COVID-19 severity has been noted very early on in the pandemic,[3] although the biological mechanisms at play remain unclear. In the Shenzhen data, the authors noted no difference in the transmission potential of SARS-CoV-2 from children or adults.[1] This is in contrast to pandemic influenza virus, which is more easily transmitted by children. It will be useful to confirm the age profile of SARS-CoV-2 transmissibility with data from other locations and serological surveys, which capture more infections than PCR. Age-specific susceptibility, infectivity, and severity are important factors to get right to project the impact of school closures on SARS-CoV-2 dynamics and disease burden. School closures exert a substantial economic toll on societies and maintaining these interventions for long periods of time requires robust supportive evidence.

As would be expected from a well controlled outbreak, the mean *R* in Shenzhen was very low, at 0·4,[1] substantially reduced from a baseline non-intervention value of 2·0–4·0.[4] This aligns with the strict interventions implemented in this city. However, the mean *R* does not tell the full story. There is evidence of transmission heterogeneity with SARS-CoV-2, with 10% of cases accounting for 90% of transmission.[1] Such a high level of heterogeneity is consistent with, if a little more extreme than, that of SARS-coronavirus (SARS-CoV), and more pronounced than for other directly transmitted respiratory viruses such as measles or influenza.[5] Beyond the intensity of contacts, there is no clear factor in the Shenzhen data that could explain the high transmission potential of some infections. Further research into the biological (eg, shedding and symptoms) and social factors (eg, type of contacts and environment) that drive transmission heterogeneity is warranted to guide more targeted interventions against SARS-CoV-2.

Armed with their descriptive findings, Bi and colleagues go on to simulate the impact of case isolation and contact tracing on SARS-CoV-2 dynamics.[1] They consider a range of possible durations for the infectious period of SARS-CoV-2, which is reasonable given the scarcity of data on this figure. They show that for a given *R*, the longer the infectious period, the more easily the epidemic can be brought under control with case-based interventions. This is because case isolation reduces the full transmission potential of each case, particularly if

the infectious period is long and cases can be isolated 2–5 days after symptom onset. Furthermore, Bi and colleagues show that contact-based interventions are more efficient than case-based interventions to reduce transmission, since infected contacts are typically isolated earlier in their infection history than index cases. This worthwhile modelling exercise highlights the urgent need for more information about the infectious period of SARS-CoV-2.

However, there is an important caveat in this modelling work: the potential for pre-symptomatic and asymptomatic transmission is not considered. As a result, the conclusion that case-based or contact-based interventions alone could bring the epidemic under control for longer durations of the infectious period is optimistic, and contrasts with previous simulation studies.[6] Viral shedding studies and epidemiological investigations suggest that in the household, around 40% of transmission occurs before symptom onset, the live virus is shed for at least 1 week after symptom onset, and there is high shedding in asymptomatic individuals.[7–9] Crucially, the effectiveness of case isolation and contact tracing will depend on the fraction of transmission originating from asymptomatic and pre-symptomatic individuals.[9]

As we look towards post-lockdown strategies, we should examine the experience of countries that have successfully controlled SARS-CoV2 transmission or have low mortality (eg, China, Singapore, Taiwan, South Korea, Germany, and Iceland). Successful strategies include ample testing and contact tracing, supplemented by moderate forms of social distancing.[10] Contact tracing on the scale that is needed for the SARS-CoV-2 response is labour intensive, and imperfect if done manually. Hence new technology-based approaches are greatly needed to assist in identification of contacts, especially if case detection is aggressive.[9] Building on the SARS-CoV-2 experience in Shenzhen and other settings, we contend that enhanced case finding and contact tracing should be part of the long-term response to this pandemic—this can get us most of the way towards control.[9]

We declare no competing interests. The conclusions expressed by the authors do not necessarily reflect the official position of the US National Institutes of Health.

*Kaiyuan Sun, *Cécile Viboud*
viboudc@mail.nih.gov

Division of International Epidemiology and Population Studies, Fogarty International Center, National Institutes of Health, Bethesda, MD 20892, USA

1 Bi Q, Wu Y, Mei S, et al. Epidemiology and transmission of COVID-19 in 391 cases and 1286 of their close contacts in Shenzhen, China: a retrospective cohort study. *Lancet Infect Dis*. 2020; published April 27. https://doi.org/10.1016/S1473-3099(20)30287-5.

2 Zhang J, Litvinova M, Wang W, et al. Evolving epidemiology and transmission dynamics of coronavirus disease 2019 outside Hubei province, China: a descriptive and modelling study. *Lancet Infect Dis* 2020; published online April 2. https://doi.org/10.1016/S1473-3099(20)30230-9.

3 Sun K, Chen J, Viboud C. Early epidemiological analysis of the coronavirus disease 2019 outbreak based on crowdsourced data: a population-level observational study. *Lancet Digital Health* 2020; **2:** e201–08.

4 Majumder MS, Mandl KD. Early in the epidemic: impact of preprints on global discourse about COVID-19 transmissibility. *Lancet Digital Health* 2020; published online March 24. https://doi.org/10.1016/S2214-109X(20)30113-3.

5 Lloyd-Smith J, Schreiber SJ, Kopp PE, Getz WM. Superspreading and the effect of individual variation on disease emergence. *Nature* 2005; **438:** 355–59.

6 Ferguson NM, Laydon D, Nedjati-Gilani G, et al. Report 9 - Impact of non-pharmaceutical interventions (NPIs) to reduce COVID-19 mortality and healthcare demand. March 16, 2020. https://www.imperial.ac.uk/mrc-global-infectious-disease-analysis/covid-19/report-9-impact-of-npis-on-covid-19/ (accessed April 17, 2020).

7 Wölfel R, Corman, VM, Guggemos W, et al. Virological assessment of hospitalized patients with COVID-2019. *Nature* 2020; published online April 1. DOI:10.1038/s41586-020-2196-x.

8 He X, Lau EHY, Wu P, et al. Temporal dynamics in viral shedding and transmissibility of COVID-19. *Nat Med* 2020; published April 15. DOI:10.1038/s41591-020-0869-5.

9 Ferretti L, Wymant C, Kendall M. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 2020; published online March 31. DOI:10.1126/science.abb6936.

10 Park SW, Sun K, Viboud C, Grenfell BT, Dushoff J. Potential roles of social distancing in mitigating the spread of coronavirus disease 2019 (COVID-19) in South Korea. *medRxiv* 2020; published online March 30. https://doi.org/10.1101/2020.03.27.20045815 (preprint).

Il contact tracing digitale e l'epidemia: sindrome cinese?

9 Aprile 2020

Print PDF

di **Giuseppe Tropea**

Nel capitolo intitolato "La sindrome cinese" del già ben noto ampio saggio su *Il capitalismo della sorveglianza* di Shoshana Zuboff, si osserva come il governo cinese stia sviluppando un sistema di "credito sociale" destinato ad essere il "nucleo" del suo approccio ad internet. L'idea è di fare leva sull'esplosione dei dati personali per "migliorare" il comportamento dei cittadini.

Non si può non pensare al sistema capillare di tracciamento dei dati messo in capo dal governo cinese, e poi sud-coreano, nella vicenda Covid-19.

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

I quotidiani di questi ultimi giorni, quando il "picco" dell'epidemia pare superato, pubblicano infatti editoriali, interviste e dichiarazioni di politici (e non solo) in cui si prospetta, anche come modalità di uscita *soft* (cd. *mitigation*) dalle durissime regole imposte dall'emergenza epidemiologica, il tracciamento informatico dei "positivi" (ancorché asintomatici) utilizzando una o più delle centinaia di sistemi e di app proposti da società private al governo. In questa settimana, dopo l'istruttoria della task force del ministero dell'Innovazione, sarà pronta probabilmente una short list da sottoporre al Governo per la scelta dell'app da utilizzare.

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

A livello di normativa interna, al momento l'unica fonte di rango primario sul punto risulta essere l'art. 14 del d.l. 9 marzo 2020, n. 14 (Disposizioni sul trattamento dei dati personali nel contesto emergenziale) che prevede: "fino al termine dello stato di emergenza […] le strutture deputate pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati monitorare e a garantire l'esecuzione delle misure disposte ai sensi del decreto legge 23 febbraio 2020 n. 6 anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli art. 9 e 10 del regolamento UE 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19".

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

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

Cookie preferences

Il richiamato regolamento UE 2016/679 (cd. GDPR) interpreta il trattamento delle informazioni personali (in rapporto al diritto alla riservatezza) anche alla luce della sua funzione sociale, affermando, al considerando n. 4 che: "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (…)". Inoltre, al considerando 46, prevede in effetti che "alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana".

Si comprende, in tal senso, come la posizione del nostro garante della *privacy* sia tendenzialmente conforme a quella registrata in sede europea, dove il Comitato europeo per la protezione dei dati personali (EDPB) sostiene, con statement del 16 marzo 2020, che "l'emergenza è una condizione giuridica che può legittimare limitazioni delle libertà, a condizione che tali limitazioni siano proporzionate e confinate al periodo di emergenza". L'EDPB sottolinea, inoltre, che
quando non è possibile elaborare solamente dati anonimi, la direttiva europea sulla privacy consente agli Stati membri di introdurre misure legislative per salvaguardare la sicurezza pubblica.

Questo passaggio è molto rilevante.

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

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

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

Non è detto che, stanti i presupposti emergenziali inediti nei quali ci si trova ad operare, questi requisiti vengano oggi rispettati.

Mi soffermerò su quattro questioni, che mi sembrano particolarmente pressanti.

i) Quanto alla fonte, il rischio non mi pare che possa tanto configurarsi nell'alternativa fra una legislazione organica che preveda il procedimento da adottare e l'autorità giudiziaria cui eventualmente il cittadino possa rivolgersi, ovvero di un intervento governativo con decreto-legge, posto che nel nostro caso proporzionalità implica il carattere assolutamente temporaneo del trattamento. È vero, infatti, che il fine non può che essere quello dell'uscita dall'emergenza: occorre dunque che gli strumenti messi in campo abbiano solo ed esclusivamente questa finalità ed abbiano una durata limitata nel tempo, tale da garantire che, una volta terminata l'emergenza, i dati vengano distrutti e non siano più utilizzabili se non, eventualmente, in forma aggregata ed anonima, al solo fine di ricerca. D'altra parte queste due prospettive appaiono conciliabili, nella misura in cui la decretazione d'urgenza possa poi essere eventualmente corretta, migliorata e "messa a regime" attraverso l'ineludibile passaggio parlamentare, che deve evidentemente costituire la sede per realizzare la accountability politico-governativa fondamentale in questo settore.

I veri problemi sono piuttosto altri due: la cd. *soft law* e il rapporto con la legislazione regionale.

Come si è detto, le iniziative *de facto* o di livello normativo comunque non primario tendono a moltiplicarsi, evidentemente ponendosi fuori dal sistema tracciato dal combinarsi fra fonte europea e fonte nazionale. Si pensi, ad esempio, alla recente nota ENAC del 23 marzo 2020, prot. 32363, relativa all'uso dei droni per il monitoraggio dello spostamento dei cittadini sul territorio comunale, con la quale si autorizzano tutti gli "Enti di Stato di cui all'art. 744 del Codice della Navigazione e delle Polizie Locali dei Comuni italiani" ad operare in deroga a svariati requisiti di registrazione e di identificazione nonché anche su aree urbane, senza la necessità di alcuna autorizzazione da parte di ENAC. Questa vicenda dovrebbe allarmare tutti, come cittadini. Non si dimentichi, peraltro, che dopo un primo intervento il 16 luglio 2015, l'ENAC ha pensato bene di emendare il proprio regolamento cinque mesi dopo, vale a dire il 21 dicembre di quello stesso anno. Alla luce di queste e altre analoghe esperienze nazionali degli stati membri, la Commissione europea ha dovuto correre ai ripari, presentando una proposta di revisione del regolamento UE 216/2008, al fine di riappropriarsi dei poteri normativi in materia di droni fin qui delegati, tra gli altri, appunto all'ENAC.

Cookie preferences

Quanto alla legislazione, come è noto il vice presidente della Regione Lombardia, ha dichiarato, ad esempio, che questa ha chiesto e ottenuto da gestori telefonici un numero imprecisato ma rilevante di dati di traffico telefonico di cittadini lombardi o persone viventi nel territorio della Regione e li ha incrociati con dati di altri interessati, prevalentemente risultati positivi a test sul coronavirus, al fine dichiarato di verificare se e in che misura le ordinanze del Governo e della Regione impattavano sui comportamenti dei cittadini. Non mi pare che le regioni possano intervenire in materia. Sul punto può essere utile notare che quando il giudice amministrativo ha affrontato sinora *ex professo* la questione della compatibilità del potere di ordinanza con la privacy (nel caso dell'ordinanza del sindaco di Messina che, fra l'altro, imponeva la registrazione on-line dei dati personali di coloro che intendessero attraversare lo stretto) ha perentoriamente data un parere nel senso dell'illegittimità – anche su questo fronte – del provvedimento, per violazione della potestà legislativa statale (Cons. St., sez. I, 7 aprile 2020, n. 735).

La fonte primaria, quindi, dovrà essere statale e non vi saranno margini per interventi regionali in materia.

ii) Quanto alla proporzionalità bisogna intendersi. È da condividere l'impostazione di chi ritiene che in questa materia proporzionalità implichi: soluzioni pseudo-anonimizzate che evitino trattamenti che esulino da compiti e responsabilità di tipo epidemiologico; carattere assolutamente temporaneo del trattamento; suo legame con strategie di "vigilanza attiva" (tamponi sui soggetti potenziali positivi non sintomatici).

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

Più discutibile mi pare invece l'approccio di chi ritiene che in questi casi la proporzionalità deve attuarsi tramite l'immediata adozione di misure di massimo rigore che, se fondate invece su approccio improntato a gradualità potrebbero poi implicare, data la presumibile inefficacia, successivi provvedimenti beni più invasivi dei diritti individuali e della collettività. Sembra evocarsi qui la nota immagine della "rana bollita". Senonché una cosa è la valutazione giurisdizione che in sede cautelare viene effettuata in questi convulsi e tristi giorni, rispetto alla quale può essere assolutamente comprensibile una particolare attenzione del giudice per la prevalenza l'interesse pubblico alla salute (sul diritto al lavoro, es. Cons. St., sez. III, decreto presidenziale 30 marzo 2020, n. 1553; sulla tutela preventiva delle interdittive antimafia, es. Tar Calabria, Reggio Calabria, decreto presidenziale 16 marzo 2020, n. 55) altra è la proporzionalità e adeguatezza delle misure legislative che determineranno presumibilmente il trattamento digitale dei dati, che deve essere adottata nel rispetto dei principi d'una società democratica, ai sensi dell'art. 15 della direttiva 58/2002 CE. In effetti quando si tratta di privacy il diritto alla salute deve essere ponderato con più attenzione, attenendo la prima al nucleo fondamentale della dignità umana.

iii) un altro aspetto problematico ha a che fare con il tema delle decisioni amministrative automatizzate tramite algoritmi, molto dibattuto nella giurisprudenza amministrativa (si v. il caso della distribuzione dei posti dei docenti delle scuole secondarie nell'ambito della cd. "buona scuola"). È corretto ritenere che, seppure vi siano spiragli in tal senso nel GDPR, il decisore politico non possa far coincidere l'esito dell'algoritmo con una misura limitativa ad applicazione automatica; l'uomo deve poter correggere eventuali errori commessi dall'algoritmo (v. De Minico sulle pagine di questa *Rivista*). Sul punto è doveroso aggiungere che il giudice amministrativo sembra avere un approccio ancora non univoco: da una parte si registrano sentenze che contestano radicalmente un processo decisionale gestito unicamente da un algoritmo preimpostato e predefinito onde tener conto in automatico di posizioni personali (v. Tar Lazio, sez. III-bis, 27 maggio 2019, n. 6606), dall'altra vi sono decisioni più possibiliste, che pretendono però il rispetto dell'obbligo di motivazione, di trasparenza e di correttezza, oltre all'ampiezza del sindacato giurisdizionale (v. Cons. St., sez. VI, 8 aprile 2019, n. 2270).

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

Condividi!

Attualità
dati personali, privacy, virus
‹ Le asimmetrie dell'Unità di monitoraggio per il contrasto alle fake news sul COVID-19
› Le conclusioni dell'Eurogruppo: anatomia di una capitolazione

Cookie preferences

COVID-19

App Immuni, tra sicurezza e privacy: i presupposti per una reale efficacia del tracciamento

Nell'attuale emergenza pandemica è utile domandarsi cosa dovrebbe fare il Governo per gestire con credibilità ed efficacia la fase 2 dell'emergenza Covid-19 con la mobile app Immuni. Ecco alcune best practice per le attività di monitoraggio e controllo del progetto

23 Apr 2020
Ioannis Tsiouras Consulente, Assessor/Auditor e Formatore - Information Security e Privacy, Risk Management, Business Continuity e Sistemi di Gestione per la Qualità

L'adozione di **un'app per contenere e contrastare l'emergenza epidemiologica** in un determinato contesto altamente complesso, com'è quello italiano, è **una sfida senza precedenti**: questo perché il download dell'app **Immuni** che il Governo ha deciso di adottare, per dare risultati attendibili e considerare efficace lo strumento di tracciamento, deve essere installata su 60% degli smartphone della popolazione, e inoltre perché si tratta di un sistema complesso che vede coinvolte competenze interdisciplinari.

Per raggiungere questo risultato il Governo deve essere convincente e per esserlo deve **garantire una certa trasparenza verso i cittadini**, mettendo a disposizione la metodologia seguita dall'organizzazione che progetta e sviluppa l'applicazione, l'applicazione stessa e le caratteristiche dell'organizzazione che gestirà il servizio.

È evidente che il progresso e l'ottimizzazione dell'app non consiste nell'accumulo di certezze che si basano sull'oscurità, ma nella progressiva eliminazione degli errori che si scoprono attraverso il confronto e il contributo degli esperti.

Perciò **tutto deve essere messo a disposizione dei cittadini**, visto che sono essi stessi che devono essere tracciati e devono fornire i propri dati.

App Immuni: alcune domande al Governo italiano

Le domande da fare al Governo relativamente alla privacy sono quelle che la signora Elizabeth Denham (UK Information Commissioner) ha formulato e ha riportato nel blog dell'ICO e noi le proponiamo in modo personalizzato per il contesto in esame:

- **Hai dimostrato come la privacy è integrata nella tecnologia del responsabile del trattamento?** I principi di protezione dei dati "by design e by default" (art. 25 del GDPR) sono fondamentali. La collaborazione di Google ed Apple, per utilizzare la tecnologia di tracciamento dei contatti nel loro lavoro congiunto, chiarisce bene come questi si stanno allineando a questi principi. Le organizzazioni che creano apps devono adottare un approccio simile. È ovvio che le organizzazioni devono muoversi rapidamente, ma lo sviluppo iniziale di una DPIA sulla privacy dovrebbe essere eseguita in quanto costituisce un requisito minimo.

Il Governo italiano è in grado di dimostrare come la privacy è integrata nella tecnologia di Bending Spoons S.p.A. e che è stata eseguita la DPIA?

- **La raccolta e l'uso dei dati personali sono necessari e proporzionati?** I dati personali che vengono raccolti devono essere solo quelli necessari (art. 25 del GDPR) e proporzionati alla specifica finalità del trattamento. L'utilizzo dell'innovazione digitale per affrontare le sfide poste da questa emergenza sanitaria pubblica, è accettata nel momento in cui il pubblico è informato sul fatto che il governo sta pensando di trovare le soluzioni meno invadenti per la privacy e che eventuali restrizioni alla libertà sono necessari per proteggere la salute pubblica. **Il Governo italiano ha effettuato un'analisi sulla necessità e proporzionalità nella raccolta e utilizzo dei dati personali?**
- **Quale controllo hanno gli utenti sui propri dati?** Come possono gli interessati a esercitare i loro diritti? Il Titolare del trattamento dovrebbe fornire agli interessati informative chiare sull'utilizzo dei propri dati personali e indicazioni chiare per impedire i trattamenti non autorizzati e non desiderati. Se, per esempio, il tracciamento dei contatti venisse incorporato in un trattamento più ampio, queste informazioni aggiuntive dovrebbero essere chiare. **Il Governo italiano metterà a disposizione informative chiare sui dispositivi personali mobile degli utenti?**
- **Quanti dati devono essere raccolti e trattati centralmente?** Il punto di partenza per il tracciamento dei contatti dovrebbe basarsi su un'architettura distribuita che mira a trattare i dati, in primis, ove possibile, sui dispositivi degli utenti. Devono essere pertanto applicate misure di sicurezza adeguate a tali trattamenti locali e per eventuali trasferimenti di dati verso il database centrale. Naturalmente stiamo parlando di Smart Object con tecnologia IoT. **Il Governo italiano ha stabilito i dati che devono essere raccolti dai dispositivi mobile degli utenti e quali dati devono essere trasmessi e per quanto tempo devono essere conservati nel database centrale?**
- **Esistono policies per garantire la riservatezza, l'integrità e la disponibilità dei dati durante l'esercizio?** Durante l'esercizio, i processi di governance e di responsabilità relativa alla capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento sono stati definiti (art. 32 del GDPR)? **Il Governo italiano ha stabilito le policies per garantire la riservatezza, l'integrità e la disponibilità dei dati durante l'esercizio?**
- **Cosa succede quando il trattamento non è più necessario?** Questo caso è particolarmente critico: quello che è appropriato e proporzionato in risposta a un'emergenza internazionale in materia di salute pubblica, appare piuttosto diverso al termine di tale emergenza. Quale considerazione è stata presa su come termina la raccolta dei dati e cosa succede ai dati raccolti? Naturalmente la risposta a tale domanda potrebbe non essere data durante la DPIA iniziale. Questo è il motivo per il quale la DPIA dovrebbe essere riesaminata e aggiornata anche in tempi successivi dopo la prima esecuzione. Il database centralizzato, sebbene i dati siano pseudonimizzati o cifrati, è una raccolta di lingotti d'oro, appetibile a diverse entità e diventa un bersaglio senza precedenti. **Il Governo italiano ha predisposto una policy per il decommissioning del sistema Immuni e del database e le notifiche a ciascun destinatario (come il sistema sanitario nazionale) cui sono trasmessi i dati personali?**

App Immuni: analisi del contesto

Nell'Ordinanza n. 10/2020 del Commissario Straordinario per l'Attuazione e il Coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, firmata dal dott. Arcuri, si legge che "*è stata selezionata la soluzione "Immuni", proposta dalla società Bending Spoons S.p.A., ritenuta 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* (Pan-

European Privacy Preserving Proximity Tracing) *e per le garanzie che offre per il rispetto della privacy*".

A tale proposito si ricorda che anche se il Governo ha stipulato il contratto di concessione gratuita della licenza d'uso sul software di *contact tracing* e di appalto per il servizio con la società Bending Spoons S.p.A., il Governo rimane l'unico titolare del trattamento dei dati personali dei cittadini, trattamento che avviene attraverso l'app e il sistema in questione.

L'analisi della situazione porta a dedurre che non si tratta solo dell'app Immuni da installare sul dispositivo mobile individuale, ma di un sistema complesso composto da diversi sottosistemi ICT e sistemi convenzionali, che formano una catena per erogare il servizio.

A titolo di esempio si possono citare alcuni sottosistemi che possono comporre il sistema Immuni: l'app Immuni, il Bluetooth LE, l'algoritmo per la creazione del codice riconducibile allo smartphone e la crittografia, l'algoritmo per l'elaborazione locale e, in funzione del modello, l'autorità sanitaria, il Wi-Fi o GPS per la connessione al server con il database di memorizzazione del codice fornito dall'autorità sanitaria, le reti pubbliche di trasmissione dei dati, il datacenter o cloud eccetera.

Sicurezza delle informazioni e privacy

Allo scopo di rendere quanto segue comprensibile vorrei chiarire alcuni concetti.

Occorre tenere presente che in alcuni articoli e in alcuni Considerando del GDPR viene richiamato, in modo non proprio evidente, un concetto che pochi hanno colto. Questo concetto è la "information security" trattato dalla norma ISO/IEC 27001[1]. La norma ISO/IEC 29100[2] invece utilizza il concetto di "Privacy", mentre la norma ISO/IEC 27701[3] ha introdotto il concetto di "information security e privacy". Quest'ultima è stata emessa per agevolare la situazione in quanto integra i requisiti del GDPR con i requisiti della ISO/IEC 27001 (supportata dalle linee guida ISO/IEC 27002[4] e ISO/IEC 27018[5]).

La "sicurezza delle informazioni" è quella attività volta a definire, conseguire e mantenere la *riservatezza*, *l'integrità* e la *disponibilità* delle informazioni e dei dati nell'ambito dei processi di trattamento.

D'altro canto, l'art. 32, par. 1 b) del GDPR specifica che il titolare del trattamento e il responsabile del trattamento mettono in atto, tra le altre misure, anche "*la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*".

Risulta evidente, quindi, che entrambi i concetti hanno lo stesso obiettivo.

La "sicurezza delle informazioni" di un'organizzazione rappresenta la base per la protezione della "privacy". Si può dire che la sicurezza delle informazioni è un'impostazione più estesa rispetto alla privacy, in quanto ingloba tutte le informazioni e i dati dell'organizzazione: dati di business e dati personali delle persone fisiche.

Pertanto, si sottolinea che la parola "privacy" non è citata dal GDPR, ma solo dalla norma ISO/IEC 29100. Il suo significato corrente è relativo al diritto della persona fisica di pretendere che le informazioni che la riguardano vengano trattate da altri solo in caso di necessità. In questo contesto il GDPR ha come oggetto "*la protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

La “sicurezza delle informazioni e privacy” rappresenta la base per creare un rapporto di fiducia verso tutti gli stakeholder (clienti, fornitori, dipendenti, persone interessate che forniscono i propri dati personali ecc.). Una “sicurezza delle informazioni” solida è la base della protezione della “privacy”. La privacy richiede una sicurezza effettiva, ma quest’ultima da sola non garantisce una privacy effettiva.

Quale modello per l’app Immuni?

Nell’Ordinanza n. 10/2020 si legge che “*è stata selezionata la soluzione “Immuni”, proposta dalla società Bending Spoons S.p.A., ritenuta 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*“.

Diverse organizzazioni hanno intrapreso l’iniziativa per sviluppare sistemi di tracciamento dei contatti con architetture che vanno da quella centralizzata a quella decentralizzata o mista. Alcuni progetti sono in fase di sviluppo, altri sono già implementate. L’architettura con le maggiori possibilità di essere effettivamente efficace potrebbe essere quella con una spina dorsale tecnologica comune che consente di comunicare con efficacia e che apre un’ampia partecipazione tra i dispositivi mobili più popolari attualmente in uso.

Su questo versante si muove la collaborazione di Google ed Apple, per utilizzare la tecnologia di tracciamento dei contatti nel lavoro congiunto, utilizzando anche il nome non più “contact tracing”, ma si chiama “notifica di esposizione” per evitare ambiguità di interpretazioni relative alla privacy.

Ad oggi non si conosce con certezza la strada che il nostro governo intraprenderà per garantire la privacy e la sicurezza nelle soluzioni informatiche.

Considerando che gli attori coinvolti (politici e tecnologici) nelle decisioni sono diversi, si è deciso di non descrivere nessuna architettura e tecnologia al riguardo.

Non possiamo dimenticare però la linea guida del Comitato dei Garanti Europei (European Data Protection Bpoard, EDPB) “*Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak”* del 21 aprile 2020 che cerca di fare chiarezza sui requisiti che un’app di *contact tracing* deve rispettare, sottolineando che l’introduzione di uno strumento di questo tipo dovrà far parte di un approccio sistemico applicato alla contrazione del virus e facente parte di una strategia di sanità pubblica nella quale devono essere presenti altri strumenti, come i test diagnostici e la tracciabilità manuale dei contatti per eliminare i casi dubbi (come ha dichiarato Jason Bay, responsabile del progetto del governo TraceTogether di Singapore).

Le linee guida di EDPB chiariscono le condizioni e i principi per l’uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, per due scopi specifici:

- *utilizzare i dati di localizzazione per supportare la risposta alla pandemia modellando la diffusione del virus in modo da valutare l’efficacia complessiva delle misure di confinamento;*
- *tracciamento dei contatti, che ha lo scopo di informare gli individui del fatto che si sono trovati nelle immediate vicinanze di qualcuno che alla fine si è confermato portatore del virus, al fine di rompere le catene di contaminazione il prima possibile.*

Tutto questo rispettando i requisiti del GDPR e della “Privacy Directive” e, l’uso delle applicazioni di tracciamento dei contatti, dovrebbe essere su base volontaria e non deve basarsi sui movimenti dei singoli, ma piuttosto sulle informazioni di prossimità riguardanti gli utenti.

Una cosa è certa che, nel momento in cui il Governo decide il modello dell'app, egli dovrà informare i cittadini e renderla *open source,* allo scopo di dare la possibilità ai cittadini esperti e alla stampa di analizzare e vagliare in che misura la privacy e la sicurezza delle informazioni sono assicurate. Questo sembra che sia la condizione necessaria per convincere almeno il 60% dei cittadini a installare l'App sui propri devices (si precisa che circa il 70%-75% dei cittadini sono in possesso di uno smartphone).

Le linee guida di EDPB (art. 24) sottolineano l'aspetto che "*Il monitoraggio sistematico e su larga scala della localizzazione e/o dei contatti tra persone fisiche è una grave intrusione nella loro privacy. Questo può essere legittimato solo basandosi su una adozione volontaria da parte degli utenti per ciascuna delle rispettive finalità. Ciò implicherebbe, in particolare, che le persone che decidono di non utilizzare o non possono utilizzare tali applicazioni non dovrebbero subire alcuno svantaggio*".

L'app Immuni, perciò, non può che rispettare tutti i requisiti della linea guida EDPB.

Il modello del sistema Immuni adottato dal Governo

Nell'Ordinanza n. 10/2020 si legge che "*è stata selezionata la soluzione "Immuni", proposta dalla società Bending Spoons S.p.A., ritenuta 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*".

Si sta scoprendo invece che non è proprio così. Il modello suggerito da PEPP-PET sembra essere un modello che utilizza l'architettura distribuita, nel senso che non esiste un database centralizzato e che probabilmente è poco efficace per la tracciabilità e la gestione di un individuo potenzialmente positivo al coronavirus da parte delle strutture sanitarie.

Risulta, pertanto, che finora il Consorzio PEPP-PET non abbia messo a disposizione le specifiche del suo modello. Questa mancanza non ispira fiducia e ha portato a qualche operatore esperto del settore (come per es. l'epidemiologo svizzero Marcel Salathé) a dissociarsi dalle iniziative di PEPP-PET.

Dalle informazioni che girano su web si apprende che Immuni non segue il modello PEPP-PET, cioè non è un sistema che si basa su un database centralizzato.

Sembrerebbe (il condizionale è d'obbligo) che il nostro Governo sia orientato a utilizzare l'architettura mista: sistema distribuito con l'installazione dell'app sui dispositivi mobile individuali con la capacità di comunicare tra loro con la tecnologia Bluetooth, la tecnologia GPS e internet e l'applicazione web server con il database centralizzato ubicato in un datacenter o in cloud per raccogliere i dati necessari e per gestire gli utenti potenzialmente positivi.

Visto che il modello del sistema che sta per adottare il Governo non è proprio quello di PEPP-PET, allora la dichiarazione dell'Ordinanza n. 10/2020 non è più valida, in quanto i riferimenti e i requisiti variano completamente.

Non si parla, quindi, di un sistema decentralizzato, ma di un sistema misto con un'infrastruttura che coinvolge il terminale portatile smart dell'utente con la tecnologia Bluetooth, il sistema GPS, la tecnologia internet su reti pubbliche, il Web server e il database centralizzato.

A questo proposito si ricorda che non si tratta di soddisfare i requisiti relativi alla privacy del GDPR, ma anche i requisiti di information security e di cyber security. Se l'Ordinanza non sarà corretta il

Governo rischia di ricevere un sistema che non soddisfa né l'Ordinanza stessa e nemmeno le regole del modello PEPP-PT.

Ci si aspetta, quindi, un aggiornamento dell'Ordinanza n. 10/2020, ma anche la predisposizione delle specifiche tecniche che costituiscono il riferimento per il sistema Immuni a fronte delle quali avverrà la validazione e l'accettazione del sistema stesso da parte del Committente.

App Immuni: alcune preoccupazioni

Le preoccupazioni e i problemi che possono nascere sono diverse e di vario genere.

La lettera "Tracciamento dei contatti e democrazia: lettera aperta ai decisori", preparata, pubblicata sul sito di Nexa Center for Internet & Society e che vede l'adesione di diversi cittadini, esprime preoccupazioni diffuse. Siamo convinti che tutto dovrebbe essere fatto dando priorità alla tutela dei diritti fondamentali dei cittadini, prendendo da subito provvedimenti per evitare che possano insinuarsi interessi con finalità diverse.

Le preoccupazioni aumentano qualora il Governo optasse per una soluzione completamente centralizzata (che al momento sembra essere scongiurata) o con architettura mista con la quale le vulnerabilità e le minacce aumentano, con app sul dispositivo mobile non proprio smart.

Si può citare a titolo d'esempio il fatto che con il Bluetooth è possibile tracciare un contatto e incrociare i dati a prescindere da dove questo sia intercettato. Se l'algoritmo non è proprio intelligente un dato grezzo rilevato viene trattato come tutti gli altri; quindi, per questo tipo di algoritmo logico, un passante incrociato per strada o un vicino di casa che sta al di là del muro che divide i due appartamenti, come anche un collega di lavoro con cui si condivide l'ufficio non fanno differenza.

Non possiamo dimenticare che la tecnologia GPS e internet potrebbero tracciare non solo il contatto, ma anche la sua localizzazione a scapito della privacy. Inoltre, le vulnerabilità della tecnologia GPS e la sicurezza dei servizi applicativi su reti pubbliche sono debolezze critiche che devono essere rimosse fin dalla progettazione del sistema.

È recente la notizia della falla nell'app adottata dal Governo olandese per tracciare i contagi. Stando a quanto scrive il quotidiano DeStandard, circa 100-200 nomi e credenziali di utenti sono stati rese pubblici. Questo potrebbe succedere quando gli sviluppatori non seguono policies per lo sviluppo sicuro del codice. Un errore banale, ma proprio banale, è quando mancano le regole da seguire per sviluppare il codice in modo sicuro. Spesso si inseriscono, non si sa per quale motivo, credenziali in chiaro nel codice. Comunque questo dimostra che per sviluppare un codice sicuro occorre seguire le policies restrittive.

È da non sottovalutare, inoltre, la minaccia del social engineering usata da truffatori e da malintenzionati al fine di spingere gli utenti a scaricare versioni fasulle delle app ufficiali di tracciamento che contengono funzioni nascoste di raccolta di dati, o anche funzioni che falsificano l'identità con la conseguenza di prendere il controllo remoto del dispositivo mobile individuale (smartphone) di chi le scarica e le installa.

Il problema che potrebbe creare veramente molti danni ai cittadini con conseguenze sulla vita e sulla morte degli stessi è quello relativo alle indicazioni non affidabili, cioè risultati di falsi positivi e negativi.

Per far fronte a questo problema è necessario valutare l'affidabilità del sistema e quantificare l'**errore standard** considerato accettabile.

Pianificazione e controllo del progetto

Alla luce di quanto detto finora, ci chiediamo cosa dovrebbe fare il Governo per la buona riuscita del progetto.

Per garantire la trasparenza e conquistare la fiducia dei cittadini allo scopo di convincerli a installare l'applicazione sul proprio smartphone e ottenere il consenso[6], è necessario che il Governo metta a disposizione degli stessi le specifiche tecniche dell'app (specifiche dei requisiti funzionali, requisiti prestazionali, requisiti di qualità (come affidabilità, portabilità, usabilità, efficienza), infine requisiti per la privacy e information security), che costituiscono il riferimento a fronte delle quali occorre effettuare la validazione e l'accettazione del sistema **Immuni**.

La pianificazione e il controllo da parte del Governo non dovrebbe limitarsi a un semplice monitoraggio dello stato di avanzamento delle attività, ma dovrebbe esercitare una gestione rigorosa se veramente sta cercando di evitare sorprese e insuccessi.

Come in tutte le organizzazioni di successo anche il Governo, prima di affidarsi totalmente ai fornitori, avrebbe dovuto preparare un Business Plan del sistema Immuni. Da quello che si legge nell'Ordinanza n. 10/2020, visto che fa riferimento in modo astratto al modello *PEPP-PT* e richiama in modo altrettanto astratto la privacy, si evince che tale documento non esiste.

A questo punto, è auspicabile che la società Bending Spoons S.p.A. proceda con la preparazione di uno studio di fattibilità del sistema Immuni e delle specifiche dei requisiti funzionali e non funzionali del sistema stesso.

Come è stato detto il sistema non è composto solo dal software dell'app, ma anche da una serie di sistemi hardware e software. Perciò il progetto vede coinvolti anche altre risorse, come fornitori di hardware, installatori, fornitori di erogazione di servizi hosting o cloud.

Vista la complessità del sistema e della rapidità con la quale occorre operare per gestire l'emergenza, è auspicabile l'assegnazione di un Project Manager con responsabilità e autorità stabilite per la conduzione e gestione del progetto nella sua integrità e con l'obiettivo di completare il progetto nei tempi e nei budget previsti per la qualità desiderata, economicamente efficace e per la soddisfazione degli stakeholder.

Attività di monitoraggio e di controllo

Non volendo entrare più in dettaglio nelle attività di competenza del fornitore ci limiteremo quindi alle attività di controllo che il Governo dovrebbe esercitare allo scopo di aumentare la consapevolezza dei cittadini e convincerli a installare e utilizzare l'applicazione.

A questo proposito il Governo dovrebbe eseguire le seguenti attività di controllo:

- **audit di valutazione della metodologia di progettazione e sviluppo.** L'audit ha lo scopo di valutare se la metodologia del processo di progettazione e sviluppo della società Bending Spoons S.p.A. segue le norme e le guide internazionali di ingegneria dei sistemi ICT (per esempio ITIL, metodologia AGILE supportata da tools tecnologici avanzati). L'audit, inoltre,

dovrebbe valutare le policies per la sicurezza delle informazioni e privacy con riferimento alla ISO/IEC 27002 e ISO/IEC 27018 (a titolo di esempio si citano le policies per il dimensionamento della capability dei sistemi, per il controllo degli accessi, per lo sviluppo sicuro del software e dei sistemi, per il change management, per la gestione degli errori e anomalie, per la separazione degli ambienti di sviluppo-test-produzione, per i livelli di test prestazionali e di sicurezza, per il trasferimento dei dati, per i controlli crittografici, per il delivery del sistema, per la gestione della configurazione (versioning), per il data breach ecc.);

- **audit di conformità al GDPR.** L'audit ha lo scopo di valutare in che misura sono stati soddisfatti i requisiti del GDPR. In particolare, la soddisfazione dell'art. 35-*Valutazione d'impatto sulla protezione dei dati* (DPIA e valutazione dei rischi che incombono sugli interessati/cittadini) seguendo approcci per il *risk assessment* adeguati alla sicurezza delle informazioni e privacy di sistemi complessi che devono trattare "dati particolari" e dati di soggetti vulnerabili, su "larga scala" e con l'uso di tecnologie innovative. In tal caso il *risk assessment* dovrebbe essere eseguito secondo metodologie consolidate come quella della line guida ISO 31000[7] che, per l'information security, è personalizzata nella linea guida ISO/IEC 27005[8]). Questa metodologia va oltre gli approcci delle linee guida ENISA (queste ultime possono andare bene alle organizzazioni e per sistemi di bassa complessità). Inoltre, questo audit dovrebbe valutare il livello di conformità dell'app Immuni all'art. 32-*Sicurezza dei dati del trattamento*. Il piano di trattamento dei rischi dovrebbe adottare misure che vanno oltre i semplici esempi dell'art. 32 (la pseudonimizzazione e la cifratura) e deve basarsi sui controlli della norma ISO/IEC 27002 e ISO/IEC 27018.
- **test di accettazione del sistema.** Il Governo, prima di installare il sistema in produzione ed effettuare il deployment dell'applicazione ai cittadini, dovrebbe eseguire il test di accettazione su un campione pilota e conosciuto. Lo scopo del test di accettazione è quello di valutare la conformità del sistema ai requisiti delle specifiche funzionali, prestazionali e di sicurezza, di caratterizzare l'affidabilità del sistema e quantificare l'intervallo di confidenza (dimensione dell'**errore standard considerato accettabile**) relativo ai rischi di falsi positivi e negativi (problema che può comportare anche conseguenze sulla vita e sulla morte stessa degli utenti).
- **Vulnerability Assessment.** Un inventario degli asset del sistema completo e aggiornato è un prerequisito per un'efficace gestione delle vulnerabilità tecniche. Sarebbe pertanto necessario eseguire valutazioni per identificare le potenziali vulnerabilità tecniche. Possono essere utilizzati strumenti automatici per l'analisi del codice dell'applicazione Immuni (Code Review), test di sicurezza alla valutazione dell'efficacia delle misure di sicurezza, test di valutazione delle vulnerabilità dell'intero sistema con strumenti automatici (automated vulnernability scanning tool), penetration test, test per la sicurezza dei servizi applicativi su reti pubbliche, per la protezione delle transazioni dei servizi applicativi eccetera.

Conclusioni

Il Commissario Straordinario per l'emergenza coronavirus, dott. Arcuri, nelle varie conferenze stampa, ha dichiarato che l'app Immuni garantirà il rispetto della privacy, il rispetto dei requisiti di sicurezza e l'installazione sarà su base volontaria.

Si spera che dietro le sue parole ci sia un lavoro serio e responsabile, sia da parte del Governo sia da parte del fornitore Bending Spoons S.p.A, per garantire il deployment di queste caratteristiche verso i processi operativi e verso tutte le entità coinvolte.

È giusto che vengano adottate tecnologie innovative. I cittadini, però, come per qualsiasi nuova tecnologia, devono avere fiducia nel fatto che venga utilizzata in modo equo e proporzionato. Il GDPR non ostacola un uso innovativo dei dati personali in un'emergenza di sanità pubblica,

utilizzando applicazioni di tracciamento dei contatti, purché vengano applicati i principi di trasparenza, equità e proporzionalità.

Il sistema di tracciamento dei contatti e il monitoraggio della posizione potrebbero aiutare a combattere la pandemia. Tutti portiamo dentro di noi la speranza che tale tecnologia possa aiutare a combattere questo male e a capire meglio come la società stia rispondendo alle misure di isolamento e per avvisare le persone che potrebbero essere state in contatto con il virus.

Il presente lavoro, dunque, vuole fornire suggerimenti utili al Governo, allo scopo di operare in modo sistemico e con responsabilità per gestire al meglio il progetto Immuni e per evitare inefficienze che potrebbero andare alla fine a discapito dei cittadini.

RIFERIMENTI

Ioannis Tsiouras, GDPR-Privacy Risk Management, Edizioni Youcanprint.

NOTE

1. ISO/IEC 27001 *Information technology — Security techniques — Information security management systems — Requirements*. ↑
2. ISO/IEC 29100: 2018 *Information technology – Security techniques – Privacy framework*. ↑
3. ISO/IEC 27701:2019 – *Security techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information Management – Requirements and guidelines.* ↑
4. ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.* ↑
5. ISO/IEC 27018:2019, *Information technology – Security techniques –Code of practices for protection of personally identifiable information (PII) in public clouds acting as PII processors*. ↑
6. Si ricorda che il limite dichiarato da parte degli esponenti istituzionali (?) per avere risultati attendibili e considerare efficace lo strumento di tracciamento è necessario che ci sia una diffusione del 60% dell'applicazione ↑
7. ISO 31000: 2018 *Risk Management – Guidelines* ↑
8. ISO/IEC 27005: 2018 *Information technology – Security techniques – Information security risk management.* ↑

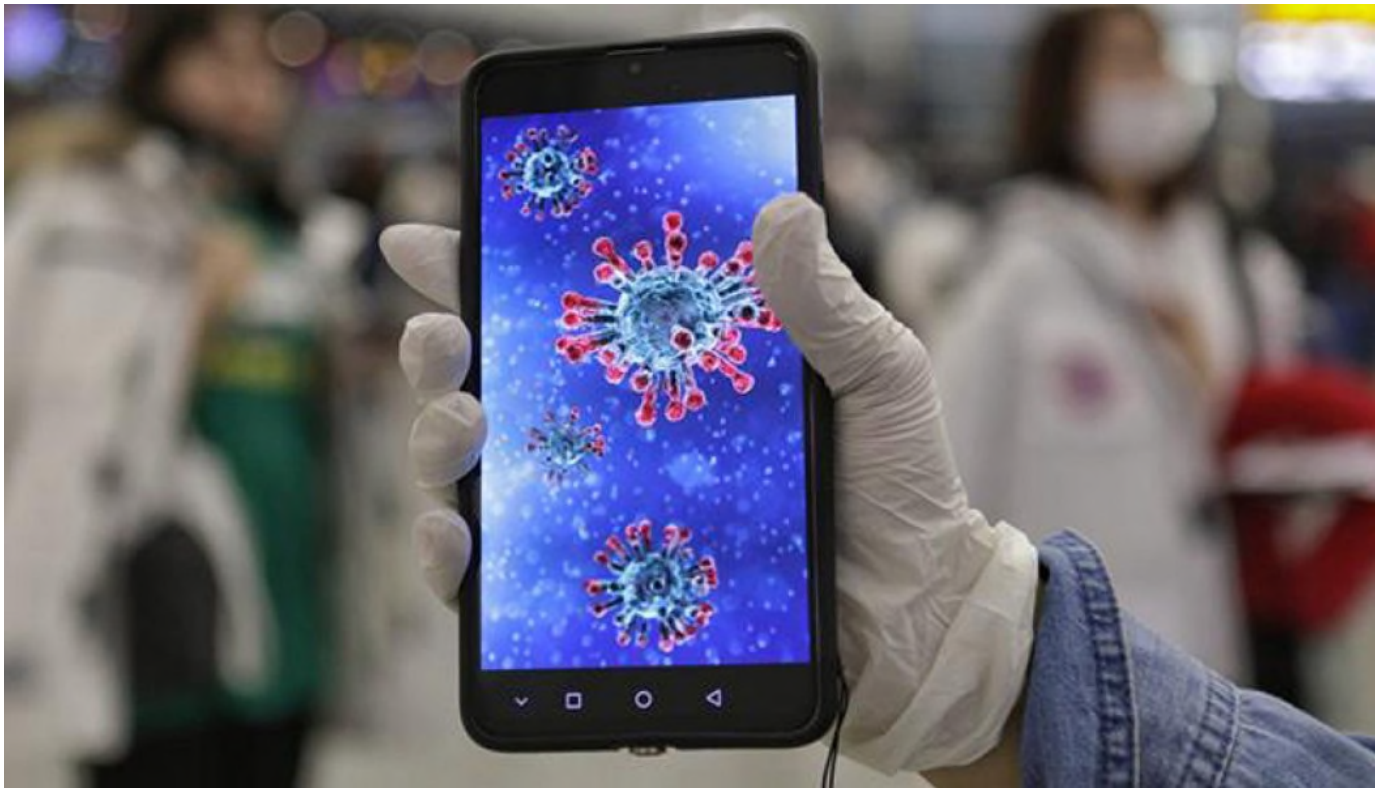
CONTACT TRACING

Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia)

Ecco il funzionamento pratico delle app e dei sistemi tecnologici (e non) con cui Cina, Corea del Sud e Singapore stanno vincendo l'epidemia. E il confronto con la soluzione scelta in Italia

23 Apr 2020

Giorgia Zunino
Project manager ASL Roma 1 e Futurista



Non solo **app** per il tracciamento dei positivi al coronavirus o *fencing* a garanzia del confinamento: si stanno facendo strada nel mondo varie metodologie e tecnologie combinate con mezzi analogici, attuate dai diversi paesi colpiti dalla pandemia CoviD-19.

L'Italia ha già confermato la scelta di **un'app, Immuni di Bending Spoon, il 16 aprile** e vari Paesi europei e gli Stati Uniti stanno facendo scelte analoghe, diverse da quelle dei Paesi orientali.

Analizziamo le differenze

GEOLOCALIZZAZIONE

Coronavirus, anche l'Italia verso il "contact tracing"? Ecco lo spiraglio normativo

CONTINUA A LEGGERE

LO SCENARIO

Dati sanitari, ecco come proteggerli con la blockchain

CONTINUA A LEGGERE

Coronavirus, app e sistemi per tracciare i positivi: come funzionano (nel mondo, in Italia)

Ecco il funzionamento pratico delle app e dei sistemi tecnologici (e non) con cui Cina, Corea del Sud e Singapore stanno vincendo l'epidemia. E il confronto con la soluzione scelta in Italia

23 Apr 2020 Giorgia Zunino

Project manager ASL Roma 1 e Futurista

Non solo **app** per il tracciamento dei positivi al coronavirus o *fencing* a garanzia del confinamento: si stanno facendo strada nel mondo varie metodologie e tecnologie combinate con mezzi analogici, attuate dai diversi paesi colpiti dalla pandemia CoviD-19.

L'Italia ha già confermato la scelta di **un'app, Immuni di Bending Spoon, il 16 aprile** e vari Paesi europei e gli Stati Uniti stanno facendo scelte analoghe, diverse da quelle dei Paesi orientali.

Analizziamo le differenze.

L'app dell'Italia contro i coronavirus: Immuni di Bending Spoon

Immuni, l'app di Bending Spoon (uno dei principali sviluppatori mobile al mondo) e del Centro Medico Santagostino è stata preferita dal ministero dell'Innovazione tra diverse app candidate per il tracking dei contagiati e ha ricevuto la conferma ufficiale dal commissario all'emergenza Domenico Arcuri.

Immuni, come tutte le app vagliate negli Usa e nei principali Paesi europei:

- rispetta la privacy in modo nuovo rispetto alle app orientali, sfruttando il **bluetooth** e altri sensori;
- il suo utilizzo è volontario;

L'identità delle persone resta protetta dall'anonimato; l'app avvisa gli utenti se sono stati vicini a un contagiato – a un metro, per un tempo sufficiente – e quindi potenzialmente a rischio.

Al momento l'app è in sperimentazione in alcune regioni e dovrebbe partire per tutti a inizi maggio.

Come funziona Immuni

L'app segue in parte il modello europeo delineato dal Consorzio **PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing).** Quello di Immuni infatti un modello ibrido che sfrutta in parte centralizzazione dei dati su un server e decentralizzazione sul dispositivo. Adesso sta virando verso un modello più decentralizzato (secondo il modello DP-3T e sposato da Google-Apple), che sarà quello usato quando l'app sarà effettivamente **disponibile, a fine maggio.**

1. L'app memorizza in locale, sul dispositivo, tutti i codici bluetooth degli altri dispositivi, dotati della stessa app (siano questi smartphone, smart watch o device stand alone come braccialetti).

Sistemi di crittografia e pseudoanonimizzazione impediscono di associare il codice all'identità del proprietario di quel dispositivo (nel modello centralizzato puro di Pepp-PT, invece, questi codici sono sul server).

2. Le funzioni scattano quando un cittadino è rilevato positivo dopo un test test per il coronavirus. L'operatore sanitario, prima di fare il questionario analogico, gli chiede se ha installato l'app Immuni.
3. Se la risposta è sì, l'operatore genera, con una diversa app, un codice con cui il cittadino può caricare su un **server** i dati raccolti dalla sua app. Qui c'è la lista dei codici bluetooth, anonimizzati, con cui è entrato in contatto.
   Il server calcola per ognuno di questi codici il rischio che ci sia stato un contagio (vicinanza, tempo di contatto) e quindi fa in modo che arrivi una notifica ai dispositivi di persone potenzialmente a rischio, sempre tramite l'app (nel modello Pepp-PT è il server a fare la crittografia dei dati; in quello DP-3T sono invece i dispositivi stessi, che quindi creano un codice anonimo e se lo scambiano quando entrano in contatto. L'app manda la notifica se riconosce il proprio codice tra quelli della lista di contatti arrivata dal server).
4. La notifica ha un messaggio deciso dalle autorità sanitarie e chiede di seguire un protocollo (isolamento, contattare numeri di emergenza per tamponi).

Si calcola che serve l'app sia usata da almeno il 60-70 per cento della popolazione perché il sistema funzioni bene.

Il diario clinico di Immuni

Immuni ha anche un diario clinico, dove gli utenti possono scrivere informazioni rilevanti dal punto di vista medico (oltre a età, sesso anche malattie pregresse e farmaci assunti). Il cittadino aggiorna il diario ogni giorno, aggiungendo sintomi ed evoluzione dello stato di salute.

Il diario è anonimo e volontario. Ma gli operatori possono utilizzarlo quando il cittadino si rivolge a loro per analizzare meglio la situazione e prendere decisioni più informate.

E il gps?

I dati gps di geolocalizzazione potrebbero usati solo in forma aggregata, per tracciare nuovi possibili focolai: lo permette la tecnologia dell'app di Bending Spoon, ma al momento sembra improbabile che il Governo vorrà usare anche questa funzione (non raccomandato dalla Commissione europea, perché i rischi di sorveglianza, nonostante le tutele, potrebbero essere superiori ai vantaggi).

I principi alla base dell'app italiana per tracciamento Coronavirus

La ministra all'innovazione Paola Pisano l'8 aprile, in audizione alla Camera, ha spiegato che l'app sarà **volontaria, a gestione pubblica, open source.**

Di seguito quanto è riportato nell'audizione. La ministra pone questi punti fermi:

(1) che sia prevista la **volontarietà** della partecipazione. In primo luogo perché, l'efficacia dello strumento richiede la collaborazione attiva del singolo, il quale va reso consapevole che l'uso dell' applicazione qualora venisse adottata può contenere il contagio (proprio e altrui).

(2) È indispensabile, a tal fine, che il singolo possa confidare nella trasparenza e nella correttezza delle caratteristiche del servizio nonché nell'assenza del perseguimento di scopi ulteriori e incompatibili con la finalità di prevenzione sanitaria.

(3) che l'intero sistema integrato di contact tracing sia **gestito da uno o più soggetti pubblici** e che il suo codice sia aperto (ossia in modalità open) e suscettibile di revisione da qualunque soggetto indipendente voglia studiarlo;

(4) che i dati trattati ai fini dell'esercizio del sistema siano "resi sufficientemente anonimi da impedire l'identificazione dell'interessato"

(5) che raggiunta la finalità perseguita, tutti i dati ovunque e in qualunque forma conservati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, siano cancellati con conseguente garanzia assoluta per tutti i cittadini di ritrovarsi, dinanzi a soggetti pubblici e privati, nella medesima condizione nella quale si trovavano in epoca anteriore all'utilizzo della app di contact tracing;

(6) che la soluzione adottata – nelle sue componenti tecnologiche e non tecnologiche – possa essere considerata, almeno in una dimensione prognostica, effettivamente efficace sul piano epidemiologico perché, qualora non lo fosse, diverrebbe difficile giustificare qualsivoglia, pur modesta e eventuale, compressione di diritti e libertà fondamentali equiparabile a quella imposta dalle limitazioni nei movimenti di cittadini in queste settimane.

(7) che la soluzione adotti misure tecniche ed organizzative che minimizzino i rischi di reidentificazione in ogni fase di vita del sistema (a titolo esemplificativo con variazione periodica e casuale dell'ID anonimo dell'applicazione).

Perché usare questi sistemi: Occidente vs Oriente

Sappiamo che l'Italia, come altri Paesi in Europa e Stati Uniti, hanno scelto finora una strada meno tecnologica: con il lockdown delle attività, per appiattire la curva della pandemia .

Nei paesi orientali invece misure coercitive e restrittive di controllo tramite applicazioni, piattaforme e sistemi informativi hanno dato i loro frutti per raggiungere questo scopo:

- **Cina;**
- **Singapore;**
- **Corea del Sud**

In sintesi i sistemi sono usati a tre scopi

1. Controllo sulla popolazione: per obbligare i positivi a restare a casa (con geolocalizzazione via app) e impedire agli altri di violare le misure (con droni ad esempio, che cominciano a essere sperimentati anche in Italia)
2. Tracciamento degli spostamenti dei positivi (con app ad hoc, dati di rete cellulare…) in modo da identificare le persone con cui sono entrati in contatto e isolarle a loro volta. In modo automatico, dato che i metodi di tracciamento analogici, basati su questionari al contagiato, sono molto lenti, costosi e imprecisi (gli Stati Uniti hanno stimato che richiederebbero 300 miliardi di dollari in quel Paese).
3. Fare una mappa dei positivi utile alla popolazione e alla protezione civile

Questi sistemi se applicati nei modi, ovvero nel rispetto e anticipazione dei patterns di comportamento sociale in ambienti critici (fuga dalle città, panico, accaparramenti, rivolte nelle carceri, negazione ecc..), con le infrastrutture coerenti con la scalabilità del sistema applicato a grandi numeri, e con la partecipazione più o meno volontaria dei cittadini ha consentito di rallentare la diffusione del virus.

Ognuno di questi tre paesi hanno applicato un loro approccio coerente con la propria storia, cultura ed infrastruttura e in cui il tempo ha una valenza strategica anche nella scelta delle giuste tecnologie di controllo da applicare.

Singapore: la capacità di agire velocemente

Per Singapore, la storia avrebbe potuto facilmente essere una catastrofe. Singapore la Città stato di 23 milioni di abitanti, dove convivono tre culture diverse occidentale, cinese ed indiana, è considerata la svizzera di oriente. Il territorio dell'isola è strettamente interconnessi con la Cina continentale, con voli diretti per Wuhan, epicentro dell'epidemia .

La chiave del loro successo finora è stata la decisione di rispondere in modo aggressivo sin dall'inizio e la forza del ricordo ancora molto forte delle recenti epidemie dell'Aviaria e di H1N1. L'esperienza delle precedenti pandemie, che hanno colpito Singapore, ha dato luogo alla creazione del National Centre for Infectious Diseases NCID: un'istituzione che negli anni non ha perso forza e capacità ma ha saputo fare tesoro dell'esperienza utilizzando le più avanzate tecnologie e mantenere vigile il controllo ed i sistemi di allerta.

Il controllo dei contagi è potuto avvenire a Singapore direttamente alla fonte e immediatamente dal primo segnale di possibile crisi epidemica.

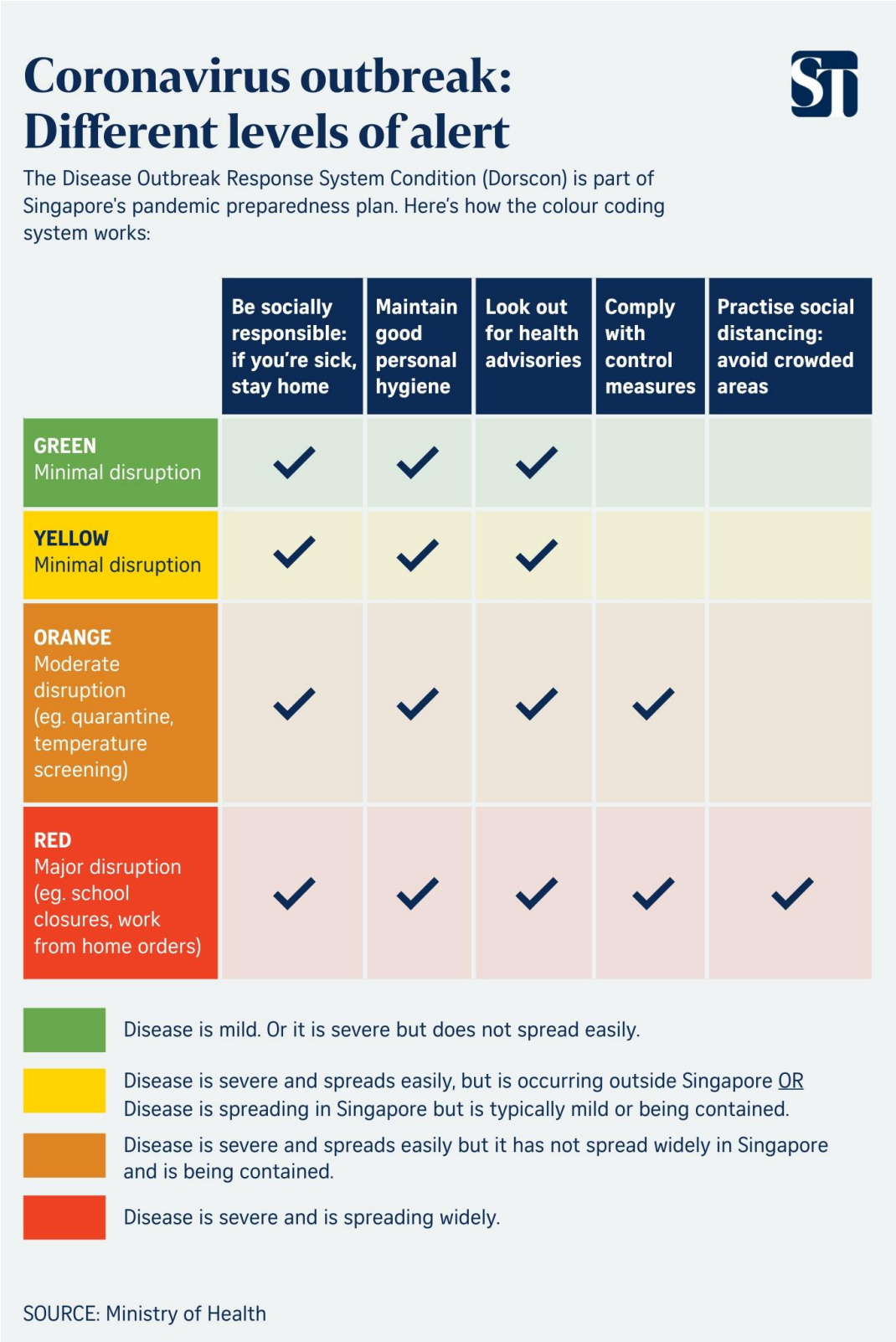
Negli aeroporti gli arrivi da Wuhan sono stati sottoposti a controlli sanitari prima che la trasmissione del virus da uomo a uomo fosse confermata il 20 gennaio, già dal 1 ° febbraio, Taiwan, Hong Kong e Singapore avevano implementato in modo proattivo le restrizioni di viaggio sui passeggeri provenienti dalla terraferma, contravvenendo all'insistenza di organizzazioni e altri paesi.

Le precauzioni anche se hanno comportato un costo economico significativo per questi hub internazionali, che fanno tutti affidamento sulla Cina continentale come principale partner commerciale e fonte di turisti , hanno consentito di applicare il controllo coercitivo ad una ristretta cerchia della popolazione.

Mentre la restante parte doveva attenersi alle disposizioni di crisi del Ministero della Salute (MOH). Ci scrive Raimondo Guerra da Singapore che da ormai oltre 30 giorni tutto il paese è in DEFCON Orange (MOH).

Dall'inizio dell'epidemia migliaia di persone a Singapore si sono isolate.

Nelle prime fasi dell'epidemia Singapore è stata particolarmente colpita. A metà febbraio aveva registrato 58 infezioni , uno dei numeri più alti confermati da qualsiasi paese al di fuori della Cina.



Rilevamento rigoroso e quarantena rigorosa

Singapore sta rilevando quasi tre volte più casi rispetto alla media globale grazie alla sua forte sorveglianza delle malattie e all'accurata tracciabilità dei contatti.

FORUM PA 6- 11 luglio
Innovazione e trasformazione digitale per la resilienza. Scopri il nuovo FORUM PA digitale

Big Data
CIO
Scopri FORUM PA 2020

Sposando il sistema tecnologico di tracciamento delle persone e cose all'interno dell'edificio del National Centre for Infectious Diseases NCID, le autorità sanitarie di Singapore hanno deciso presto di testare tutti i casi di influenza e polmonite, metterle in quarantena e monitorarle da remoto tramite un'applicazione e in presenza.

Non hanno inoltre risparmiato alcun timore nel dare la caccia a ogni possibile contatto delle persone infette un processo che opera 24 ore su 24, 7 giorni su 7, è avviato con interviste ai pazienti e ha coinvolto anche la polizia, volantini sparsi sulla città (come nei tempi di guerra) e un test sviluppato localmente per gli anticorpi, che persistono anche dopo la scomparsa di un'infezione.

Perché questo sistema di quarantena sia efficace, i funzionari devono rintracciare le persone colpite il più rapidamente possibile.

I contatti vengono rintracciati dalle forze di polizia di Singapore, che usano le telecamere di videosorveglianza, interviste con i pazienti per redigere elenchi di persone che potrebbero essere state esposte.

La App predisposta dal governo è relativamente semplice e funzionale, viene utilizzata solo a chi è stata confermata la notifica e quindi limitata ad un numero limitato di persone sottoposte a regime di quarantena, sia per sospetto contagio a causa di prossimità con soggetti positivi o per confermata positività.

Chiunque sia tenuto a farlo può essere chiamato più volte al giorno e può fare clic su un collegamento online che condivide la posizione del proprio telefono.

I funzionari effettuano inoltre controlli a campione di persona per garantire la conformità.

Coloro che non restano a casa possono aspettarsi una multa fino a 10mila dollari o fino a sei mesi di reclusione e la perdita della cittadinanza cosa ancor più grave.

WHAT HAPPENS WHEN YOU GET A STAY-HOME NOTICE?

Each person who gets a Stay-Home Notice (SHN) must stay at home at all times for **14** days

If it applies to you, you will be issued an official hard-copy notice upon arrival at Singapore's checkpoints

How will authorities make sure you stick to this?

- Text messages will be sent to you at various times of the day

- You will have to give an update on your location with GPS on your mobile phone

- You might get random phone calls and house visits from authorities

- If you get a phone call, you must take photos of your surroundings to verify your whereabouts

A partire dal 13 marzo, la città-stato ha avuto 178 casi e zero morti.

I test completi, la rapida quarantena e l'isolamento dei casi sospetti e le misure premiali dei buoni comportamenti con azioni serie sulle politiche di sostegno :

- il test è gratuito e il governo paga le fatture dell'ospedale per i residenti di Singapore che hanno sospettato o confermato casi.
- il governo offre ai lavoratori autonomi $ 100 dollari di Singapore ($ 73) al giorno, mentre ai datori di lavoro è vietato detrarre i giorni di quarantena dalle ferie annuali dei dipendenti.
- una comunicazione efficace del governo, onesta e trasparente capace di contenere il panico e dare segnali fermi e coerenti.
- Un controllo da remoto che fornisce informazioni, volte a rassicurare e contestualmente a controllare le persone in quarantena.

La strategia applicata non è solo in se l'App di controllo, che si ha garantito il contenimento dei casi positivi sopra descritta ma è un mix di "carote e piccole bastonate" che finora ha veramente aiutato soprattutto nei primi duri 20 giorni della crisi.

Corea del Sud: l'importanza di avere fortuna

La rapida mobilitazione di Singapore è in netto contrasto con la Corea del Sud e il Giappone, anch'essi vicini alla Cina e dotati di sistemi sanitari avanzati.

Nonostante la popolazione civile abbia una cultura storica di guerra che alla NATO definirebbero *preparedness* a causa del mai sopito conflitto con la confinante Corea del Nord, nelle metropolitane coreane è normale trovare armadi con presidi di contenimento nucleare dove noi troviamo solo quelli antincendio, e nonostante una collocazione geopolitica che la rende a tutti gli effetti un'isola non isola, la Corea del Sud non è stata in grado per debolezza politica e comunicazioni ambigue di agire velocemente come Singapore (il presidente Moon Jae-in ha dichiarato che il peggio è passato poco prima che i casi si manifestassero, provocando un contraccolpo politico).

E' accaduto che la Shadowy Church nel distretto di Daegu è stata il centro dell'epidemia di Coronavirus in Corea del Sud.

Questo culto religioso praticava la segretezza delle persone infettate e eseguiva cerimoniali per auto contagiarsi e con il volere di Dio guarire oggi più di 1.250 altri membri della chiesa hanno sintomi e oltre 400 risultano positivi.

Questo particolare avvenimento ha circoscritto specificatamente il cluster del contagio, ottenendo quel vantaggio competitivo del paziente zero, ovvero avere quasi la perfetta piena di diffusione tracciando chi aveva avuto contati con gli appartenenti al culto.

Il governo della Corea del Sud ha optato per blocchi localizzati, concentrandosi invece sul test di un gran numero di persone nel tentativo di identificare gli "hotspot" delle infezioni, oltre a incoraggiare il distanziamento sociale tra cui il distretto di Daegu focolare del contagio.

Il paese sta conducendo circa 15.000 test al giorno, gratuitamente, e finora ha effettuato quasi 200.000 proiezioni. Ha inoltre istituito circa 50 centri di test drive-through: ovvero di test attraverso le auto senza far scendere dalla vettura il conducente e all'aria aperta. E distribuito avvisi per smartphone sui movimenti delle persone che sono risultati positivi.

Corea, l'uso della tecnologia digitale e la vergogna

L'applicazione governativa "Corona100" incrocia i dati di geolocalizzazione dell'utente con quelli forniti dal governo, ed è stata lanciata l'11 febbraio.

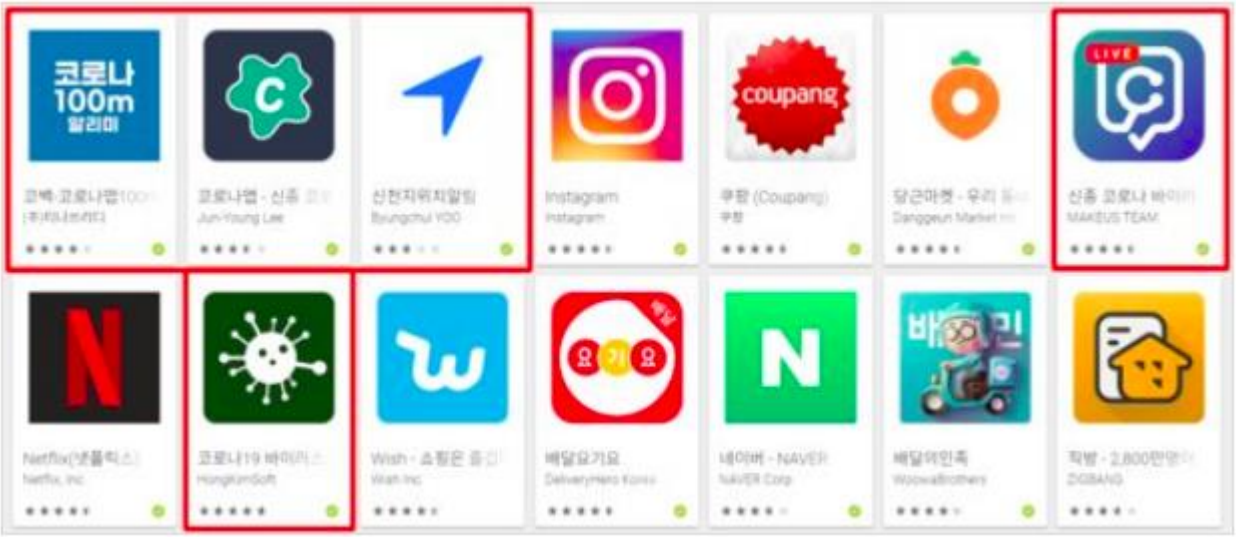
Ma ve sono molte altre messe a disposizione che lavorano con Google Maps che con "Corona 100m", "Corona Map" e "Shincheonji Location Notification" risultano le più scaricate da GooglePay.

Quindi non solo il Governo ma anche il privato, i cittadini coreani sono un popolo giovane e altamente digitalizzato e opera costantemente nel campo nell'innovazione dei prodotti, si è mosso per informare la popolazione sulla prossimità o il rischio di frequentare luoghi da chi risulta positivo o sospetto.

L'App avvia una notifica quando ci si avvicina entro 100 m dalla visita del sospetto o contagiato: sia sul territorio nazionale che internazionale. Tutto quello che devi fare è verificare l'area e si riceve una notifica quando a 100mt. Da te vi è un potenziale rischio, o come per altre app che usano il sistema collaborativo segnalare tu stesso qualcuno.

Da quando il numero di pazienti confermati è aumentato esponenzialmente la App ha guadagnato popolarità. Con un milione di download a partire dal dal 25 febbraio l'app e collassata a a causa della congestione del server. Lo sviluppatore TinaThree sta lavorando alla stabilizzazione del server.

Questo è uno dei pericoli più frequenti nella creazione di queste App: la sua scalabilità.



25 classifiche di app popolari del Google Play Store. Ci sono 5 app correlate a Corona nella top 10. [Foto Google Play Store Capture]

Azioni di leva "culturale"

La Corea del Sud, nonostante la cultura digitale e con le tecnologie avanzate è un paese di forti contraddizioni: la famiglia, l'approvazione della comunità sono al contempo un limite e in questo caso l'utilizzo più o meno volontario del governo ha dato una spinta all'osservanza del confinamento, scrive Ogan Gurel, medico e scienziato.

Il governo sta inoltre utilizzando un'app per smartphone per garantire che le persone restino a casa quando gli è stato ordinato di mettere in quarantena.

Le autorità hanno attivato una serie di messaggi che descrivono dettagliatamente i movimenti di persone infettate da Covid-19, suscitando vergogna pubblica e "chiacchiericcio".

I testi – sebbene intesi come un servizio sanitario pubblico – stanno alimentando lo stigma sociale e in alcuni casi, portando alla speculazione sugli affari extraconiugali.

Chi infrange questo confinamento viene messo nelle condizioni di vergogna davanti alle proprie famiglie e ai datori di lavoro molto severi sull'onorabilità dei propri componenti e dipendenti.

Non vengono diffusi nomi o altro, ma brevi messaggi di testo dove viene descritto l'affaire (una scappatella o un comportamento anomalo) in così minuziosi dettagli che le persone si riconoscono, o si vedono nella stesa situazione che per la paura riducono o si autolimitano sentendosi "osservati".

Una gigantesca telenovela che sta inorridendo e appassionando il popolo coreano che non può fare a meno di questi messaggi sul comportamento dei loro concittadini: la vergogna e sdegno sapranno produrre più risultati del controllo coercitivo?

Cina: il modello pervasivo ubiquitario

La risposta della Cina al virus ha incluso un rigoroso allontanamento sociale, oltre un mese di blocchi in tutta la città di Wuhan e delle aree circostanti, un ampio monitoraggio pubblico dei cittadini , nonché vari metodi di punizione e premi per incoraggiare l'adesione a tali misure.

Gli esperti affermano che il principale fattore che ha contribuito al contenimento del virus in Cina è stato l'uso aggressivo delle quarantene.

Nel caso specifico della Cina i funzionari non si sono mossi per contenere il virus fino alla fine di gennaio, settimane dopo che era stato rilevato per la prima volta.

Quindi l'applicazione di misure restrittive era più che necessario: il contenimento è l'unica soluzione ed il governo cinese ha optato per ampliare o far emergere un sistema di controllo già pronto e solo i suoi effetti e conseguenza non visibili alla popolazione sono emersi alla luce del sole.

"Quando usciamo o restiamo in un hotel, possiamo sentire un paio di occhi che ci guardano in qualsiasi momento. Siamo completamente esposti al monitoraggio del governo"

Maya Wang-China for human Rights Watch

Surveillance di Massa

Il virus è divenuto catalizzatore per un'ulteriore espansione del regime di sorveglianza, che si perfeziona ad ogni evento particolare alzando ancor più l'asticella: a partire dalle Olimpiadi del 2008 tenutesi a Pechino o all'Expo di Shanghai nel 2010.

La Cina insomma, per contenere il contagio, ha sfruttato e al tempo stesso perfezionato un sistema di sorveglianza di massa, già fortemente basato su tecnologia, big data, intelligenza artificiale. Questa in pratica la grande differenza con le altre realtà asiatiche.

La Piattaforme di WeChat e Alipay

WeChat in cina è largamente utilizzata per fare qualunque cosa offrendo innumerevoli funzioni adatte all'uso quotidiano: telefonare, inviare messaggi (vocali), pubblicare foto, noleggiare una bicicletta, prenotare viaggi, acquistare un biglietto del cinema, prenotare un tavolo nel tuo ristorante preferito, cercare le ultime offerte, organizzare un appuntamento dal medico e molto altro ancora, il tutto in un'unica app.

AliPay è invece il sistema di pagamenti di Alibaba: una piattaforma di pagamento online che insieme a Wechat ha conquistato le abitudini della popolazione non solo per la facilità dei pagamenti ma anche per il sistema creditizio vantaggioso rispetto al credito tradizionale.

Nessuna App è nativa ma viene incorporata embedded all'interno di WeChat in cui è possibile aggiungere e incorporare funzioni di fornitori di servizi esterni.

Il tool o la nuova funzione, creata appositamente dal Governo cinese per il controllo del contagio è il sistema chiamato **Health Code**, che all'interno delle applicazione delle citate Alipay o WeChat, ha assegnato automaticamente alle persone uno dei tre codici colore in base alla loro cronologia di viaggio, il tempo trascorso negli hotspot dell'epidemia e l'esposizione a potenziali portatori del virus. Questo per determinare se devono mettersi in quarantena o le persone possano spostarsi liberamente.

E' questo il software, utilizzato in oltre 100 città, che ha consentito alle persone di controllare i colori degli altri residenti quando vengono immessi i loro numeri ID.

L' organismo IT è così "interoperabile" con tutto il sistema sia delle App WeChat e Alipay e con le facilities di smart cities che le informazioni vengono direttamente integrate nelle App di uso comune ad esempio per il web mapping Gaode Maps (il nostro Google Maps). I dati sono aggiornati costantemente tramite REST API anche con dati ufficiali forniti dal governo.

La strategia del governo è stata quindi quella di non creare un'ulteriore App, con il rischio che non solo non venga usata né scaricata o imposta, di usare App ampiamente utilizzate dalla popolazione, Wechat (sistema di messaggistica e di pagamento con Wechat Pay), o di Alipay (sistema di pagamento) e 高德地图 (Gaode ditu o gaode maps), nelle attività di vita quotidiana: muoversi, pagare/comprare, chattare.

Fornendo così dati che confluiscono in data base o un sistemi integrati di CDE (common Data Enviroment). Questo insieme a quelle applicazioni tipicamente istituzionali: videosorveglianza/telecamere, facilities della smart city, dragnet ecc…

Una enorme mole di dati, provenienti dal data mining delle chat, dagli acquisti eseguiti con la app di pagamenti, che non solo evidenzia la perfetta scalabilità di questi sistemi capaci di gestire da pochi a moltissimi dati senza mettere in crisi l'infrastruttura IT, ma ne rivela il disegno già alla sua base di controllo sistematico.

22:16
返回 实时更新：你的定制防疫地图
Confirmed cases around you
信息输入后选择
珠江国际
周边疫情
你所在的 重庆市南岸区 目前已有 15 起新型冠状病毒肺炎确诊病例。离你最近的在 重庆市渝中区菜园坝街道民新花园，距离你 2.32 公里。确诊病例已收入定点医院救治，只要做好自身防护，无需过分担心哦！
支付宝|答答星球温馨提示：
请戴好口罩、勤洗手、不聚会，
一起健康共度疫情期！
统计截至 2020-03-16 11:14:52
滨江路
南开(融侨)中学
金山路
万象城
东原·亲亲里
回龙湾
黄桷坪
重庆南站
防疫答题
城市观察
最新辟谣
(黄桷坪校区)
成渝线
高德地图

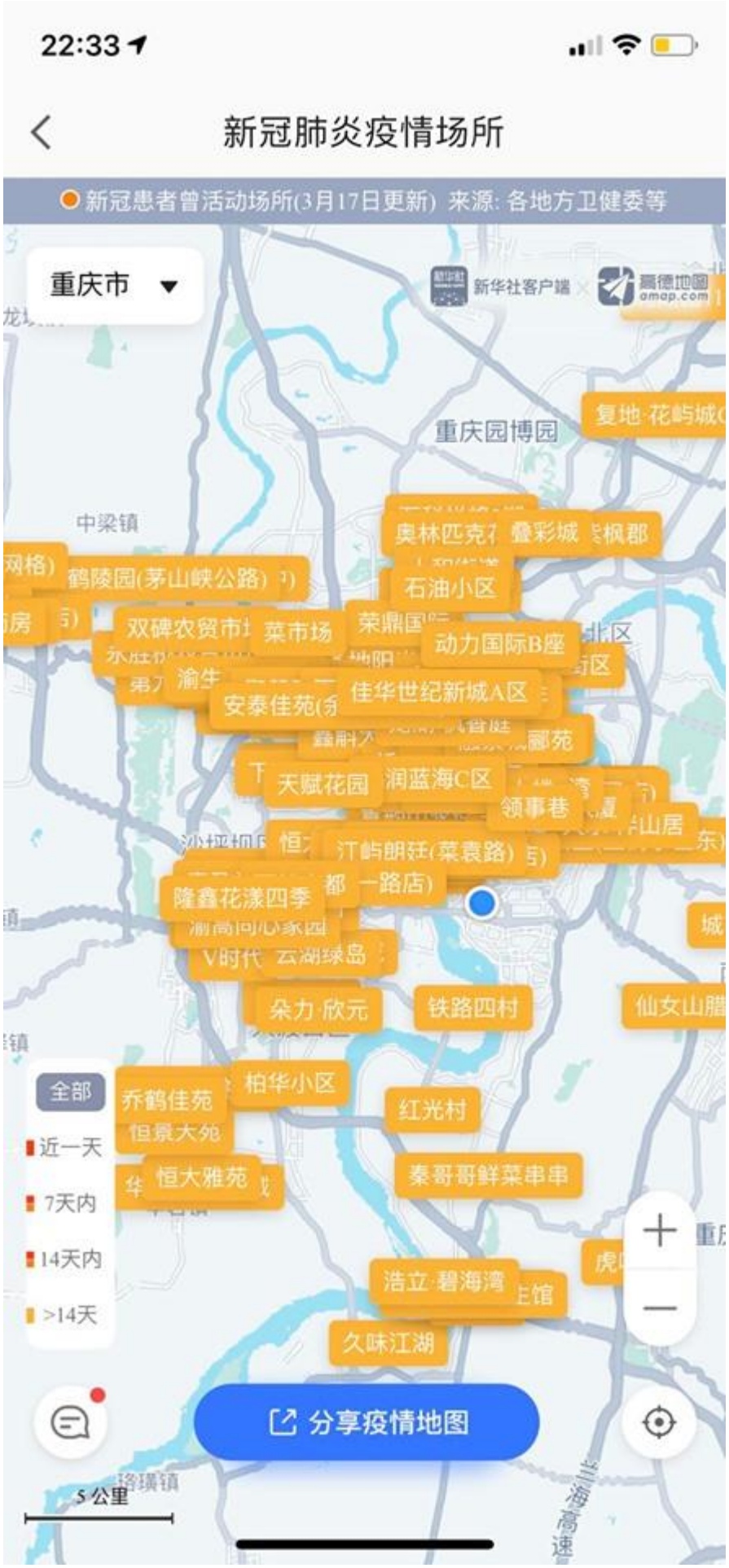

22:33
新冠肺炎疫情场所
新冠患者曾活动场所(3月17日更新) 来源: 各地方卫健委等
重庆市
新华社客户端
高德地图
amap.com
重庆园博园
复地·花屿城
中梁镇
奥林匹克
叠彩城
枫郡
鹤陵园(茅山峡公路)
石油小区
双碑农贸市
菜市场
荣鼎国
动力国际B座
渝生
佳华世纪新城A区
安泰佳苑
天赋花园
润蓝海C区
领事巷
汀屿朗廷(菜袁路)
隆鑫花漾四季
一路店)
V时代
云湖绿岛
朵力·欣元
铁路四村
仙女山
全部
近一天
7天内
14天内
>14天
乔鹤佳苑
柏华小区
红光村
恒大雅苑
秦哥哥鲜菜串串
浩立·碧海湾
久味江湖
分享疫情地图
5公里

Foto credits: Screenshot Zhu Qing 高德地图 Gaode ditu o gaode maps (simile al nostro Google Maps) rivela posti sicuri e la presenza di contagia

ti

Foto credits: Screenshot Zhu Qing: alcuni esempi dei dati forniti dall'app WeChat con allert durante le prenotazioni del public transportation

22:15
返回
新冠肺炎确诊同行程查询
For checking if you have been with any confirmed cases on public transportations
查询地区
Your city
交通方式
Types of transportations
航班号/车次
Flight/train/bus number/subway line
选择日期区间
Time period
输入任意一项即可查询，数据来源于各官方媒体发布
查询
为您找到以下数据
地铁：郑州市地铁1号线转5号线 2020-03-09
出发：医学院站 到达：康宁街站
描述：7时31分，乘坐地铁1号线0144车换乘5号线0532车（医学院站－郑州东站－康宁街站）
来源：郑州发布
地铁：郑州市地铁5号线转1号线 2020-03-09
出发：康宁街站 到达：医学院站
描述：18时45分，乘坐地铁5号线0506车换

Foto credits: Screenshot Zhu Qing: *alcuni esempi dei dati forniti dall'app di Alipay. Mostrano su una mappa i casi confermati nelle vicinanze. E' possibile anche inserire il numero del treno o del bus per sapere se si è viaggiato con persone con covid-19*

Come funziona?

Nell'app wechat c'è una sezione dove si può cliccare per inserire il numero del treno o del bus, analogamente su Alipay, per verificare se si è viaggiato insieme a casi confermati di covid-19.

I pagamenti in Cina, sono quasi al 90% elettronici, e quando si prende il pullman, la metro o il taxi spesso si paga facendo "tap" con una tessera magnetica o scannerizzando un qr-code con Alipay o WeChat pay che hanno i tuoi dati della ID card.

Il governo può sapere in tempo reale con chi hai viaggiato e dove, se invece si paga in cash si deve compilare un foglio che ha l'autista nel quale si registra nome, cognome e numero ID della carta d'identità.

In farmacia se si comprano antibiotici o altri farmaci per sindromi influenzali si viene registrati automaticamente, e si può accendere un allert del tuo score colori alle autorità e potresti essere chiamato o visitato a casa per verifiche.

Oppure se si invia un sms al proprio operatore telefonico (ad esempio 10086 per China Mobile) si riceve un sms con le città nelle quali sono stati durante gli ultimi 14 giorni e questo può essere esibito anche ai datori di lavoro.

Per uscire di casa poi esiste una tessera cartacea tipo “exit card” che serve per uscire ogni 2/3 giorni per andare al supermercato, ma una una sola persona per famiglia, e sopra la scheda, diversa per ogni comunità, appongono uno stamp ogni volta sulla data nella quale sono andati al supermercato.

Foto credits: Zhu Qing. Exit Card utilizzata per poter uscire di casa

Per entrare nel proprio appartamento o sul posto di lavoro è necessario scansionare un codice QR, scrivere il proprio nome e numero ID, temperatura e cronologia di viaggio recente.

Le aziende cinesi stanno nel frattempo implementando la tecnologia di riconoscimento facciale in grado di rilevare temperature elevate in una folla o di bandiera che i cittadini non indossano una maschera facciale. Una serie di app utilizza le informazioni personali sulla salute dei cittadini per avvisare gli altri della loro vicinanza ai pazienti infetti o se sono stati in stretto contatto.

Quale è la situazione oggi in Cina?

Soprassedendo dalle comunicazioni ufficiali, Fabio Baroni web-designer e sviluppatore che ha vissuto in Cina ed in contatto con la sua fidanza Zhu che da Chongqing nel sudovest e ci ha fornito le immagini per l’articolo, mi scrive che nella sua zona, stanno riaprendo i negozi e i centri commerciali, si accede sempre indossando la mascherina chirurgica, viene effettuato il controllo della temperatura all’ingresso e si può fare all’application su Alipay e WeChat per una sorta di autodichiarazione che non si è infetti. Da questa iscrizione si ottiene un qr-code che viene scannerizzato all’ingresso di locali pubblici e ti consente di entrare.

Le maglie si stanno allargando e l'attenzione ed il controllo comincia ad allentarsi anche per comunicare un certo sollievo di quanto fatto a beneficio delle misure restrittive e a volte frustranti.

Le falle del sistema digitale

I problemi ci sono appoggiandosi alla sola spinta automazione, falle che possono farci intravedere uno scenario alla Brazil. Può accadere, ed è accaduto, che se transiti in auto senza fermarti attraverso Hubei, una zona rossa, con Weibo attivo (l'equivalente cinese di Instagram) il tuo codice colore diventa da verde a giallo e quindi sei messo in quarantena.

Oppure in un paese dove la domotica, negli appartamenti e nei megacondomini è tanto effiente da non consentirti di aprire la porta di casa tua, tramite il tuo telefonino o card, se il tuo codice diviene improvvisamente giallo o rosso.

Un panorama di un Grande Fratello e piuttosto capriccioso, forse il maggior punto debole del sistema cinese.

Behavioural Insights

L'OMS ha affermato che le misure più efficaci della Cina sono state la "sorveglianza estremamente proattiva" per rilevare casi, test approfonditi e isolamento immediato dei pazienti, monitoraggio rigoroso e quarantena di contatti stretti e un "livello eccezionalmente elevato di comprensione e accettazione della popolazione" di tali misure.

La leva psicologica di collaborazione ha fornito al paese del Dragone un'arma in più e con l'aggiunta di sistemi tecnologici la mutua sorveglianza tra i cittadini ha collaborato alla grande inflessione della curva dei contagi.

Come detto le applicazioni e la surveillance non può avere effetti seri se non accompagnate da misure di sicurezza a bassa tecnologia ed alta componente umana.

In Cina sono state impiegate tanto quanto quelle ad alta tecnologia, utilizzando le scienze comportamentali per l'orientamento massivo delle abitudini. La "rieducazione" cinese ha sposato appieno le tecnologie digitali con il nudgetting.

Il progetto pilota di un'applicazione che funziona attraverso la piattaforma WeChat, per identificare la presenza di debitori in un raggio di 500m dall'utente la segnalazione e denuncia di comportamenti sospetti dei debitori: acquisti impropri. Sino ad impedire che il debitore possa spendere in viaggi o futuli oggetti il suo denaro: è la sperimentazione applicata del c.d. punteggio sociale, un credito base che va ad assottigliarsi e di conseguenza riducendo le tue libertà personali e creditizie.

Tutto era quindi già pronto: WeChat e Weibo hanno "hotline" per le persone per segnalare altri che potrebbero essere malati e che possono segnalare eventuali infrazioni. Le città offrono ricompense alle persone per informazioni sui vicini malati hanno compiuto il passo successivo con il "rewarding" la ricompensa premio alla base della scienza dei comportamenti e del rafforzamento del ciclo delle abitudini.

Il Limite ed il Diritto

L'uso di queste piattaforme, in particolare WeChat, ha anche un grosso problema: la protezione dei dati: non è un segreto che Tencent collabora con il governo cinese e condivide le informazioni

personali dei propri utenti ed è anche al contempo il valore aggiunto che ha fornito il carburante di dati per alimentare il sistema di apprendimento automatico, riconoscimento facciale ecc…

La sorveglianza intrusiva è già quindi la nuova normalità per il popolo cinese anche se i difetti o bachi della tecnologia sono quelli oggi che frustrano maggiormente il popolo cinese che comunque, per comodità digitale o pigrizia, ha regalato sempre più spazi al sistema di sorveglianza e controllo su tutta la loro vita.

Dagli alti funzionari ai lavoratori della comunità locale, quelli che applicano le regole ripetono lo stesso ritornello: questo è un "tempo straordinario" feichang shiqi, che richiede misure straordinarie. Ma quale è il livello o l'equilibrio di contropartita (privacy-diritto all'informazione) che un cittadino, cinese o no, è in grado di tollerare?

Israele

In Israele, un popolo da oltre 45 anni in guerra, ha fatto quello che è egregiamente capace di fare: attivato e applicato lo stato di straordinario di guerra ove il nemico non sta più oltre la **striscia** di Gaza ma all'interno del suo stesso territorio. Nei giorni scorsi ha approvato una legge di emergenza per tracciare i dati dei cellulari dei cittadini senza bisogno dell'ordine di un magistrato. Il primo ministro Benjamin Netanyahu ha scritto: "aumenteremo drasticamente la capacità di localizzare e mettere in quarantena coloro che sono stati infettati. Oggi abbiamo iniziato a utilizzare la tecnologia digitale per individuare le persone che sono state in contatto con le persone colpite dalla Corona. Informeremo queste persone che devono andare in quarantena per 14 giorni. Si prevede che saranno numeri grandi, anche molto grandi, e lo annunceremo nei prossimi giorni. Entrare in quarantena non sarà una raccomandazione ma un requisito e lo applicheremo senza compromessi. Questo è un passo fondamentale nel rallentare la diffusione dell'epidemia".

I dettagli pratici sono scarsi: le autorità sono molto riservate, in merito. Israele, avviando il monitoraggio informatico dei casi di coronavirus, utilizzerà largamente tecnologie militari di monitoraggio e controllo bypassando la necessaria approvazione da parte della Knesset.

Questo monitoraggio avverrà direttamente da parte del servizio di sicurezza Shin Bet al fine di informare le persone che involontariamente sono venute in contatto con pazienti confermati coronavirus. La polizia pedinerà le persone che circolano per strada e che gli individui verranno scelti sulla base di campioni randomizzati.

La polizia, considerati i comportamenti irresponsabili della popolazione, imporrà violazioni della quarantena utilizzando la tecnologia cellulare di **geolocalizzazione**: la APP Waze di ideazione israeliana potrebbe essere uno dei potenziali veicoli ed interfacce di penetrazione e sostegno collaborativo, di questa tecnologia ma come da copione vige la massima riservatezza.

Hanno collaborato con informazioni ***Raimondo Guerra*** *a Singapore,* ***Fabio Baroni e Zhu Qi***