REVISTA MULTIDISCIPLINAR
ISSN 1809-1628
HUMANIDADES E TECNOLOGIAS (FINOM)
FACULDADE DO NOROESTE DE MINAS

CONTACT TRACING ATRAVÉS DO APLICATIVO: A EXPERIÊNCIA ITALIANA E QUESTÃO DE PRIVACIDADE

CONTACT TRACING VIA APP: THE ITALIAN EXPERIENCE AND PRIVACY ISSUE

Michele Ferrazzano[1]

Abstract (PT): O monitoramento da população na época da COVID-19 se tornou um tópico interessante para debate entre especialistas e não especialistas. "Especialistas" significa pessoas com habilidades verticais de vários tipos: do técnico ao jurídico, do social e filosófico à saúde e político. Este artigo examina a abordagem italiana da "fase 2" e o impacto do aplicativo Immuni em questões de privacidade e pessoas frágil, examinando os aspectos técnicos.

Abstract (EN): The monitoring of the population at the time of COVID-19 has become an exciting topic to debate between experts and not. "Experts" means people with vertical skills of various types: from technical to legal, from social and philosophical to health and political ones. This article examines the Italian approach to "phase 2" and the impact of the Immuni app on privacy issues and weak people, by examining the technical aspects.

Abstract (IT): Il tema del monitoraggio della popolazione ai tempi del COVID-19 è divenuto argomento di appassionante dibattito tra esperti e non solo, dove per “esperti” si possono considerare persone con competenze verticali di varia tipologia: da quelle tecniche a quelle giuridiche, da quelle maturate in ambito sociale e filosofico, a quelle più propriamente connesse alla dimensione sanitaria e politica. In questo articolo verrà esaminato l’approccio italiano alla “fase 2” e l’impatto dell’app Immuni rispetto a tematiche di privacy e rispetto dei soggetti deboli attraverso l’esame degli aspetti tecnici.

Keywords: Contact tracing. Immuni. Italy.GDPR. Digital divide.

Premessa

[1] Professore a contratto di Informatica all’Università di Modena e Reggio Emilia. Componente dell’Officina informatica su Diritto, Etica, Tecnologie (DET) del CRID (Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell’Università di Modena e Reggio Emilia. Il presente lavoro rientra nell’ambito di un più ampio confronto sugli impatti delle misure in epoca COVID-19. E-mail: michele@bit4law.it

Recebido em 25/05/2020
Aprovado em 07/07/2020

Il tema del monitoraggio della popolazione ai tempi del COVID-19 è divenuto argomento di appassionante dibattito tra esperti e non solo, dove per "esperti" si possono considerare persone con competenze verticali di varia tipologia: da quelle tecniche a quelle giuridiche, da quelle maturate in ambito sociale e filosofico, a quelle più propriamente connesse alla dimensione sanitaria e politica.

Le contestazioni all'uso di strumenti di monitoraggio si sono basate in un primo momento su questioni di carattere tecnico, poi superate con proposte che verranno in seguito meglio descritte. Superate le questioni tecniche, le contestazioni hanno posto possibili violazioni della normativa sulla privacy, evidenziando la possibilità che soggetti di vario tipo (aziende, privati, malviventi…) avrebbero potuto avere accesso ai dati, rischi di data breach e conseguentemente alle libertà dei cittadini, sino a spingersi a usi impropri da parte dello Stato[2]. Occorre tuttavia focalizzare l'attenzione su quanto esplicitamente riportato al considerando 4 del GDPR, il quale prevede 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*".

Si evidenzia così la *funzione sociale* del trattamento dei dati, a conferma dell'idea che la protezione degli stessi dati sia un presidio irrinunciabile di tutte le libertà e, al contempo, anche un interesse generale della collettività[3].

Uno strumento di monitoraggio non deve avere alcuna altra finalità se non quella di monitorare la popolazione al solo fine di ridurre il contagio e intercettare nel più breve tempo situazioni di soggetti che possono diventare – anche inconsapevolmente – pericolosi dal punto di vista virologico nei confronti degli altri cittadini.

Previo inquadramento giuridico (§1), verranno in questa sede illustrate le componenti tecnologiche alla base di questo genere di monitoraggio e le sue logiche di funzionamento (§

[2]Tra le voci che esprimono riserve, supportate da puntuali argomentazioni a sostegno delle proprie tesi, all'uso di tali strumenti di monitoraggio per incompatibilità con la normativa privacy, si citano PIETROPAOLI, Stefano. La scia dell'untore: privacy, ICT e virus non informatici, 2020, online su https://www.lafionda.org/2020/04/10/la-scia-delluntore-privacy-ict-e-virus-non-informatici/. MINISCALCO, Noemi. "La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?", in Osservatorio costituzionale, n. 3, p. 95-115, 2020. NICOLICCHIA, Fabio. "Sorveglianza di massa e prerogative di riservatezza dell'individuo durante l'emergenza SARS-CoV-2. Scenari attuali e prospettive future", in Diritto Virale, 1 aprile 2020, online su http://www.giuri.unife.it/it/coronavirus/allegati/VIRALE-Nicolicchia.pdf/at_download/file.

[3] SINISI, Martina. Uso dei big data e principio di proporzionalità, in federalismi.it, 8, 2020, p. 358-378, online all'URL https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41623.

2), nonché le modalità di utilizzo in caso di contagio oppure in assenza (§ 3), per giungere infine ad alcune considerazioni a sostegno di un equilibrato utilizzo, che tenga conto di alcuni aspetti problematici, specie con riferimento al divario digitale (§ 4).

Inquadramento giuridico

Già il 23 marzo 2020, il direttore dell'Istituto Superiore della Sanità ha espressamente affermato che la tracciatura dei positivi 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 possono essere facilmente superate[4] in virtù di quanto previsto dall'art. 14 del D.L. 9 marzo 2020[5], nonché dagli artt. 9[6] e 23[7] del GDPR e dal considerando

[4] Cfr. DE FALCO, Domenico, MADDALENA, Maria Laura. 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", 13 marzo 2020, online su https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41629.

[5] Prevista ampia deroga alla disciplina del trattamento dei dati personali e della riservatezza in favore delle autorità sanitarie che sono così autorizzate a effettuare trattamenti di dati (anche scambio) relativi ai nominativi delle persone per finalità connesse al contenimento della diffusione dell'infezione, anche mediante meccanismi di sorveglianza attiva in linea con le raccomandazioni dell'OMS.

[6] Art. 9 GDPR:
1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
[…]
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
i) il trattamento è 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 modelli e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale
[…].

[7] 1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:
[…]
i) la tutela dell'interessato o dei diritti e delle libertà altrui.

73[8], che consentono limitazioni alla privacy per motivi di sanità pubblica[9]. Non si può altresì ritenere che tali misure di sorveglianza 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: secondo la Corte costituzionale[10], solo chi è in vita può esercitare i propri diritti e quindi il diritto alla vita costituisce la priorità su tutti gli altri, giustificando così la compressione di tutti gli altri interessi, limitatamente al perseguimento di tale superiore interesse e per il tempo necessario[11].

Si consideri inoltre che le misure di tracciamento erano già ammesse dal "Piano Nazionale di Preparazione e Risposta ad una Pandemia Influenzale", di cui il nostro Paese è dotato fin dal 2003, che 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[12].

In un contesto giuridico di questo genere, lo stesso Garante Privacy si è dovuto "arrendere" e ha dichiarato che, pur essendo personalmente contrario a ipotesi di sorveglianza generalizzata mediante la geolocalizzazione di tutti i cittadini, non vi sono preclusioni al ricorso alla tecnologia per monitorare i contatti purché si tratti di misure proporzionate e ragionevoli, previste da fonte primaria e destinate a perdere efficacia non appena l'emergenza sia finita[13].

[8] Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana[…].

[9] Tra le voci dello stesso avviso, si segnala POLLICINO, Oreste, RESTA, Federica, Data tracing, no a deleghe in bianco all'algoritmo, 24 marzo 2020, online all'URL https://www.corrierecomunicazioni.it/privacy/data-tracing-no-a-deleghe-in-bianco-allalgoritmo/.

[10] *Cfr*. Corte Costituzionale, ordinanza n. 207/2018 e sentenze n. 242/2019, 35/1997 e 223/1196.

[11] Si veda sul tema BISCONTINI, Guido, COMBA, Mario, DEL PRATO, Enrico, MAZZAROLLI, Ludovico, POGGI, Annamaria, VALDITARA, Giuseppe, VARI, Filippo. Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile, in federalismi.it, 23 marzo 2020, online su https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=41342&dpath=document&dfile=23032020165227.pdf&content=Primo%2Bpiano%2B%2D%2BLe%2Btecnologie%2Bal%2Bservizio%2Bdella%2Btutela%2Bdella%2Bvita%2Be%2Bdella%2Bsalute%2Be%2Bdella%2Bdemocrazia%2E%2BUna%2Bsfida%2Bpossibile%2E%2B%2D%2Bstato%2B%2D%2Bpaper%2B%2D%2B.

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

[13] SORO, Antonello. 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

A livello europeo, a seguito della Raccomandazione dell'UE del 8 aprile 2020[14] che invitava gli stati membri a un approccio paneuropeo con le migliori pratiche[15] al fine di limitare rigorosamente il trattamento dei dati personali al contrasto della crisi Covid-19, garantire che i dati personali non siano utilizzati per alcun altro scopo (dunque né per l'applicazione di norme di legge, nè per fini commerciali), garantire un riesame periodico del persistere della necessità del trattamento dei dati personali per il contrasto della crisi Covid-19, sopprimere il servizio e distruggere i dati quando non più necessario.

Seguivano il 14 aprile 2020 le linee guida dello *European Data Protection Board*[16] che invitano i paesi intenzionati a dotarsi di un simile strumento a rispettare alcune regole: installazione su base volontaria, smantellamento quando non più necessario, non trattamento di dati di localizzazione perché lo scopo non è seguire i movimenti degli individui né il rispetto di prescrizioni.

Monitoraggio: di cosa?

Preliminarmente occorre porsi la domanda "quali sono i dati che effettivamente tornano utili per monitorare lo stato di contagio e prevenire la diffusione del virus?".

La Raccomandazione UE del 8 aprile 2020 sembra aver in larga parte già offerto una risposta a questa domanda.

Si ritiene poi doveroso porre l'enfasi sul fatto che, a fronte del timore che qualcuno (Governi? Aziende private? Malintenzionati?) possano venire in possesso dei tragitti coperti, delle persone che incontriamo quotidianamente o occasionalmente, dello stato di salute, tutti

[14] https://ec.europa.eu/digital-single-market/en/news/coronavirus-recommendation-use-mobile-data-response-pandemic.

[15] Si citano in particolare: 1) misure di salvaguardia che garantiscano il rispetto dei diritti fondamentali e la prevenzione della stigmatizzazione, in particolare le norme applicabili alla protezione dei dati personali e alla riservatezza delle comunicazioni; 2) preferenza per le misure meno intrusive e comunque efficaci, compreso l'uso dei dati di prossimità, ma senza il trattamento dei dati relativi all'ubicazione o agli spostamenti delle persone, e l'uso di dati anonimizzati e aggregati ove possibile; 3) requisiti tecnici riguardanti le tecnologie appropriate (ad esempio Bluetooth a bassa energia) per stabilire la prossimità del dispositivo, la cifratura, la sicurezza dei dati, l'archiviazione dei dati sul dispositivo mobile, il possibile accesso da parte delle autorità sanitarie e la memorizzazione dei dati; 4) requisiti di cibersicurezza efficaci per proteggere la disponibilità, l'integrità, l'autenticità e la riservatezza dei dati; 5) scadenza delle misure adottate e cancellazione dei dati personali ottenuti attraverso tali misure, al più tardi quando la pandemia sarà dichiarata sotto controllo; 6) caricamento di dati di prossimità in caso di infezione confermata e metodi appropriati per allertare le persone che hanno avuto contatti stretti con la persona infettata, che deve rimanere anonima; e 7) prescrizioni relative alla trasparenza per le impostazioni sulla privacy in modo da garantire la fiducia nelle applicazioni.

[16] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

questi dati sono già collezionati quotidianamente da numerose società private, spesso extra-europee.

Alcuni esempi sono indicativi a questo proposito: i nostri spostamenti sono quotidianamente raccolti dai produttori dei nostri smartphone (es. Apple e Google), spesso da sviluppatori di app, ma anche da altri soggetti quali ad esempio le assicurazioni per chi installa scatole nere, dalle società che gestiscono tratti autostradali (si pensi al Telepass), dalle banche e dai negozi per quanto attiene l'uso di strumenti di pagamento elettronici e carte fidelty, dai gestori telefonici per quanto concerne l'aggancio del proprio dispositivo mobile alle antenne BTS sparse sul territorio.

Sui nostri smartphone troviamo quotidianamente il popup che ci informa del tempo per arrivare in ufficio o tornare a casa oppure suggerimento di percorrenze per evitare traffico. E questi dati vengono spesso utilizzati per scopi diversi da quelli per i quali ha avuto origine il trattamento, tra cui le finalità di giustizia (si pensi all'analisi dei tabulati telefonici o all'analisi di smartphone in caso di incidente stradale[17]).

Proprio i grandi colossi del mercato dei dispositivi mobili hanno documentato "aggregando dati anonimi" già collezionati quotidianamente (dietro consenso degli utenti) come in effetti un'ampissima fetta della popolazione italiana abbia rispettato le regole imposte dal Governo, con un drastico calo tra 85% e 90% degli spostamenti, per poi riprendersi con l'inizio della "Fase 2" pur mantenendo ancora significativamente limitati i movimenti, come ad esempio dimostra il seguente grafico.

[17] Sul tema degli accertamenti legati a dati utili ai fini di spostamento e tracciamento, sia concesso il rimando a FERRAZZANO, Michele. Dai veicoli a guida umana alle autonomous car: aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense, Giappichelli, 2018.

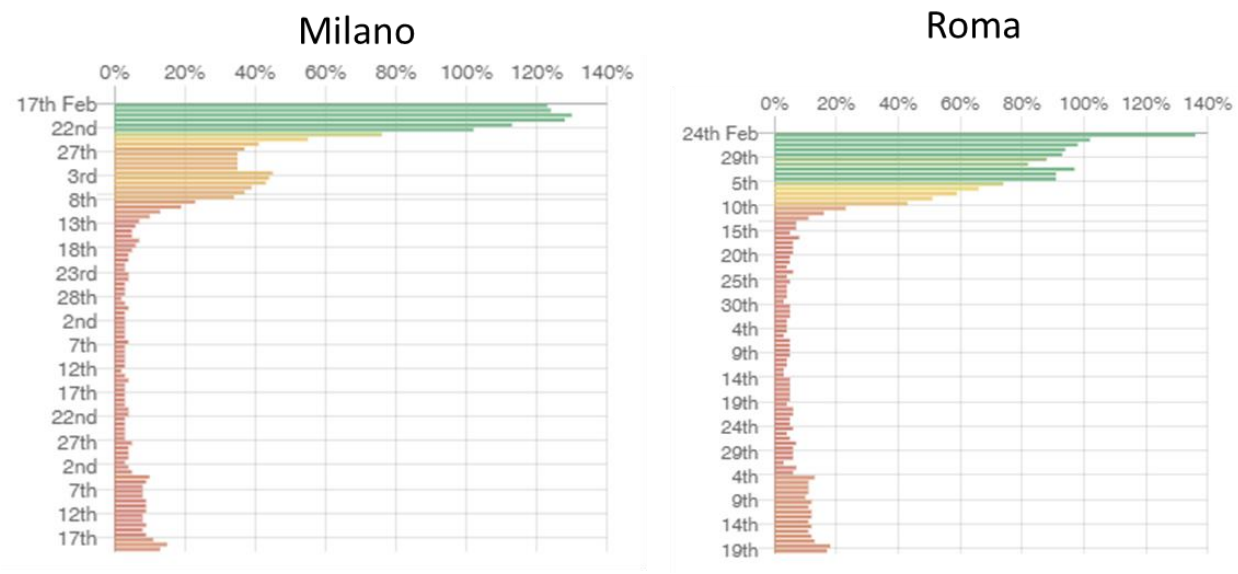

Figura 1 – Percentuale di persone in movimenti a Roma e Milano[18]

Dunque, a fronte delle perplessità poste, ci troviamo nella situazione in cui i buoi (i dati) sono già scappati dal recinto (usciti dai propri dispositivi). E chi volesse farne utilizzo illecito avrebbe già tutti gli elementi per agire in tal senso.

Il monitoraggio mediante *contact tracing*

I dati citati in precedenza rappresentano solo degli esempi di ciò che i cittadini quotidianamente producono e divulgano a terzi. Si tratta di dati anche molto intimi da cui emergono comportamenti illeciti o almeno potenzialmente equivoci, eppure il loro collazionamento è quasi universalmente accettato.

Tutti questi dati sembrerebbero tuttavia poco utili rispetto al tipo di analisi necessaria per le finalità di contenimento della pandemia. Ciò di cui ci sarebbe bisogno è solo il monitoraggio dei contatti: non importa dove il cittadino sia, quanto si allontani, che ora del giorno o della notte sia; cercando di semplificare più possibile, l'unico dato utile è avere una triade di dati relativa a: cittadino1, cittadino2, *timestamp* (data e ora).

Si tratta cioè di informazioni utili a documentare quando due persone hanno avuto un contatto sociale a breve distanza, da cui deriva l'espressione "*contact tracing*".

[18] Fonte: https://citymapper.com.

Occorre quindi chiarire come operativamente sviluppare questa tecnologia, quale sia la competenza tecnica che ogni cittadino deve possedere, e se questa tecnologia effettivamente sia rispettosa della riservatezza o meno.

L'obiettivo del contact tracing

Una tecnologia basata su *contact tracing* intende collezionare i contatti tra persone con una profondità definita dagli esperti del settore di competenza (i virologi), ossia proporzionata ai tempi di incubazione del virus.

Questa tecnologia non ha l'obiettivo di sostituire i tamponi o gli altri strumenti sanitari nella diagnosi della malattia, ma di segnalare i soggetti potenzialmente a rischio contagio.

I soggetti a potenziale rischio contagio sono quelli che entro un certo numero di giorni hanno avuto contatti con un altro soggetto che è risultato contagiato.

Dunque, l'obiettivo del *contact tracing* è di informare tutti i cittadini che hanno avuto contatti con la persona ammalata dell'opportunità di sottoporsi ad accertamenti e/o di porsi in uno stato di quarantena (anche in questo caso, sono i medici che devono indicare le procedure da seguire).

Da ciò consegue che l'assenza di segnalazioni di rischio non garantisce l'immunità ma rappresenta una grande forma di potenziale rassicurazione per il cittadino sulle proprie condizioni di salute.

Come realizzare tecnicamente il contact tracing

La specificità del controllo sfugge dalle tipologie di tracciamento tipicamente utilizzate. Solitamente per queste finalità si fa uso di BTS, che però hanno un raggio di copertura troppo ampio (anche nell'ordine di chilometri), o di vicinanza a reti Wi-Fi 802.11, che pongono lo stesso problema sebbene in un'area di dimensioni inferiori, o il GPS, che però è inefficace nei luoghi chiusi o multipiano. Inoltre, tutte queste tecnologie si basano non sul concetto di vicinanza fisica tra due dispositivi (e dunque due utenti) ma sulla posizione dell'utente monitorato nel mondo, dato del tutto irrilevante rispetto alle finalità del controllo dei contagi.

Il dato di cui c'è bisogno nelle condizioni nelle quali ci troviamo è relativo alla vicinanza tra persone. Al momento, la tecnologia più alla portata, a basso costo e disponibile già per gran

parte della popolazione, è quella Bluetooth: si tratta di un tipo di connessione senza fili a breve raggio (entro 10 metri circa) che consente di tenere traccia quando due dispositivi si vedono tra di loro.

Assumendo che tutti i cittadini escano sempre con il proprio smartphone, sarà sufficiente abilitare un'app che si occupi di verificare quali altri dispositivi sono nel raggio di alcuni metri e vicendevolmente si scambiano l'informazione su chi sono. Ogni smartphone dunque dovrebbe trasmettere a breve distanza un identificatore con validità limitata, autenticato e anonimo che non può essere collegato a un utente. Tale scambio informativo si basa su meccanismi di "pseudonimizzazione" (ad esempio, numeri casuali attribuiti dal sistema che fa coordinamento centralizzato) che quindi non consentono di associare tale identificativo a un nome e cognome.

Quando due dispositivi entrano nel rispettivo raggio d'azione (sono in prossimità "epidemiologicamente sufficiente") per un certo periodo di tempo ("epidemiologicamente sufficiente") come determinato da esperti sanitari, viene reciprocamente registrato l'identificativo anonimo dell'altra parte. Nessuna geolocalizzazione, nessuna informazione personale o altri dati vengono registrati per consentire l'identificazione dell'utente, al punto tale che neppure l'utente è in grado di esaminare la lista del proprio smartphone in quanto i dati verrebbero memorizzati in un'area criptata. Trascorso un certo tempo, gli eventi più vecchi di una soglia "epidemiologicamente non importanti" verrebbero distrutti.

Si può valutare se mantenere i dati localmente (con il rischio di perderli in caso di smarrimento del dispositivo o danneggiamento) o trasmetterli a un sistema centralizzato via rete, presupponendo però il possesso di una connessione a Internet affidabile per lo smartphone. Il dibattito su questo punto è stato acceso anche tra i membri del progetto *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT)[19], che avrebbe dovuto trovare un punto d'accordo sulle caratteristiche tecniche da adottare.

Se un utente non esegue dei test sanitari (esempio, il tampone) o risulta negativo, la cronologia rimane comunque memorizzata. Se invece è confermato che l'utente è positivo, le autorità sanitarie contatteranno il paziente-utente fornendogli un codice che consente di formalizzare il trasferimento, impedendo l'invio di informazioni errate da utenti infedeli. Ad ogni modo, in caso di infezione, sarà possibile trasmettere una notifica ai dispositivi degli utenti

[19] https://www.pepp-pt.org/.

che negli ultimi *n* giorni (da valutare da parte dei medici la durata) sono entrati in contatto per l'effettuazione dei test.

Quali rischi per la privacy nel contact tracing?

Sulla base di quanto descritto (una procedura di estremo dettaglio sarebbe senza dubbio l'invenzione allo stato attuale di grande valore economico, oltre che sociale), si evidenzia che nessun cittadino ha necessità di esplicitare *quali siano i luoghi di incontro* poiché non è un dato rilevante ai fini del contagio, così come *quali siano le ragioni dell'incontro* (si trattano allo stesso modo sia incontri cercati che involontari con sconosciuti come, ad esempio, altre persone al supermercato).

Il vero rischio di tale tecnologia è, dal mio punto di vista, rappresentato dalla possibilità di verificare la reale condotta del sistema, ossia se rispetto alle specifiche funzionali dichiarate sia fatta esattamente quella tipologia di raccolta e trattamento di dati oppure se la "scatola nera" nasconde al proprio interno qualche trattamento di diverso tipo.

Invero, il problema è del tutto analogo ad altro già affrontato da giuristi e politica negli ultimi anni, ossia l'utilizzo dei captatori da parte dell'Autorità Giudiziaria, per i quali di fatto i cittadini non hanno alcun tipo di diritto di difesa, trattandosi di un "atto di fede" nei confronti di chi fa indagini e di chi produce il software di controllo[20].

Per i captatori esiste un problema legato all'impossibilità di rendere il codice pubblicamente disponibile, in quanto gli stessi si basano sullo *sfruttamento di vulnerabilità dei sistemi informatici* che sono ignoti ai produttori[21].

Ciò significa che il produttore del sistema operativo potrebbe correggere l'errore rendendo il captatore non installabile e quindi inutilizzabile.

Nel caso dell'app di contact tracing, non esiste il problema della riservatezza della vulnerabilità poiché la sua installazione è su base volontaria ed esplicita. Questa differenza è cruciale in quanto è possibile seguire la strada dell'app basata su codice sorgente pubblicato per l'esame da parte dei cittadini (c.d. codice *open source*) in modo da consentire a chiunque la verifica del rispetto dei requisiti fissati.

[20] Cfr. TORRE, Marco. Il captatore informatico, Giuffré, 2017.
[21] Sul punto sia consentito rinviare a FERRAZZANO, Michele. "Considerazioni sul captatore informatico", in BRIGHI, Raffaella, PALMIRANI, Monica, SANCHEZ JORDAN, Maria Elena (Org.), Informatica giuridica e informatica forense al servizio della società della conoscenza, Aracne, 2018, p. 283-295.

Inoltre, si può ipotizzare un meccanismo per il quale nessuno possa consultare i dati dei contatti registrati (potenzialmente, vietandolo anche ai professionisti del settore sanitario), potendo procedere unicamente all'invio di una notifica informativa a cura dei sanitari, piuttosto che del paziente stesso attraverso ~~dei~~ meccanismi di verifica incrociati finalizzati ad evitare falsi allarmi.

Infine, superata l'emergenza, sarà sufficiente rimuovere l'app – ancora una volta in maniera esplicita da parte dell'utente – per impedire il proseguimento del controllo.

Considerazioni conclusive e problemi aperti

Permangono perplessità in merito all'efficacia di tale strumento (ma sul punto, gli esperti che possono offrire risposte adeguate sono i virologi) e a tematiche legate al c.d. *digital divide*. Occorre infatti considerare che non tutti i cittadini sono in possesso di un dispositivo smartphone abbastanza aggiornato e con tecnologia Bluetooth[22]. Ampie fette di popolazione non ne fanno uso (si pensi ai bambini o agli anziani) con la conseguenza che occorrerà pensare a tecnologie alternative ad hoc (esempio, dei braccialetti) da distribuire a basso costo (o meglio, nullo) per il singolo cittadino. Dispositivi che poi, a seconda di come dovrà essere implementato lo strumento, dovranno avere disponibilità di connessione a Internet in maniera continuativa per poter inviare e ricevere aggiornamenti.

Queste tematiche si incrociano con concrete riserve sulla sua efficacia. In particolare, risulta altamente improbabile che venga raggiunta una copertura idonea ad un corretto funzionamento e tale circostanza non può non incidere sul bilanciamento complessivo[23].

Altro tema è legato all'obbligo di uscire di casa con tali apparati: può infatti capitare di uscire senza dispositivo perché si dimentica o perché si lascia volontariamente in casa, perdendo informazioni.

[22] Secondo l'ISTAT, circa un quarto delle famiglie italiane non dispone di un accesso a Internet, in particolare tra gli over 65 solo il 34% dispone di una connessione. Fonte: *https://www.istat.it/it/archivio/236920*. In un recentissimo articolo del 2 aprile 2020, Pew Research Center - un *think tank* statunitense con sede a Washington che fornisce informazioni su problemi sociali, opinione pubblica, andamenti demografici sugli Stati Uniti ed il mondo in generale - ha evidenziato che in Italia i possessori di smartphone sono il 77% della popolazione. Fonte: *https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/*.

[23] DELLA MORTE, Gabriele. Giuridicamente "Immuni"? Vantaggi e dubbi sull'efficacia dell'app, online all'URL https://www.cattolicanews.it/giuridicamente-immuni-vantaggi-e-dubbi-sull-efficacia-dell-app.

In tutti i casi dunque il rischio è di perdere informazioni e il rischio coinvolge significativamente i soggetti vulnerabili, con la conseguenza che si rischia di non riuscire a intercettare tempestivamente nuovi focolai.

Infine, elemento critico fortissimo è la frammentazione della proposta da parte dei vari paesi: sarebbe stato auspicabile che almeno a livello di Unione Europea, così come ci sono stati diversi provvedimenti sul tema, ci si orientasse su un'unica soluzione condivisa, soprattutto in funzione della riapertura dei confini interni. E invece, lasciando a ogni paese autonomia di scelta sull'applicazione (se adottarla e quale adottare), è forte il rischio di partorire un topolino, ossia un sistema di tracciamento di fatto inutile in un mondo globalizzato, peraltro in prossimità di una stagione estiva nella quale il numero di cittadini che si sposta da un paese all'altro raggiunge il picco.

Bibliografia

BISCONTINI, Guido, COMBA, Mario, DEL PRATO, Enrico, MAZZAROLLI, Ludovico, POGGI, Annamaria, VALDITARA, Giuseppe, VARI, Filippo. Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile, in federalismi.it, 23 marzo 2020, online su https://www.federalismi.it/ApplOpenFilePDF.cfm?artid=41342&dpath=document&dfile=23032020165227.pdf&content=Primo%2Bpiano%2B%2D%2BLe%2Btecnologie%2Bal%2Bservizio%2Bdella%2Btutela%2Bdella%2Bvita%2Be%2Bdella%2Bsalute%2Be%2Bdella%2Bdemocrazia%2E%2BUna%2Bsfida%2Bpossibile%2E%2B%2D%2Bstato%2B%2D%2Bpaper%2B%2D%2B.

DE FALCO, Domenico, MADDALENA, Maria Laura. 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", 13 marzo 2020, online su https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41629.

DELLA MORTE, Gabriele. Giuridicamente "Immuni"? Vantaggi e dubbi sull'efficacia dell'app, online all'URL https://www.cattolicanews.it/giuridicamente-immuni-vantaggi-e-dubbi-sull-efficacia-dell-app.

FERRAZZANO, Michele. "Considerazioni sul captatore informatico", in BRIGHI, Raffaella, PALMIRANI, Monica, SANCHEZ JORDAN, Maria Elena (Org.), Informatica giuridica e informatica forense al servizio della società della conoscenza, Aracne, 2018, p. 283-295.

FERRAZZANO, Michele. Dai veicoli a guida umana alle autonomous car: aspetti tecnici e giuridici, questioni etiche e prospettive per l'informatica forense, Giappichelli, 2018.

MINISCALCO, Noemi. "La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?", in Osservatorio costituzionale, n. 3, p. 95-115, 2020.

NICOLICCHIA, Fabio. "Sorveglianza di massa e prerogative di riservatezza dell'individuo durante l'emergenza SARS-CoV-2. Scenari attuali e prospettive future", in Diritto Virale, 1 aprile 2020, online su http://www.giuri.unife.it/it/coronavirus/allegati/VIRALE-Nicolicchia.pdf/at_download/file.

PIETROPAOLI, Stefano. La scia dell'untore: privacy, ICT e virus non informatici, 2020, online su https://www.lafionda.org/2020/04/10/la-scia-delluntore-privacy-ict-e-virus-non-informatici/.

POLLICINO, Oreste, RESTA, Federica, Data tracing, no a deleghe in bianco all'algoritmo, 24 marzo 2020, online all'URL https://www.corrierecomunicazioni.it/privacy/data-tracing-no-a-deleghe-in-bianco-allalgoritmo/.

SINISI, Martina. Uso dei big data e principio di proporzionalità, in federalismi.it, 8, 2020, p. 358-378, online all'URL https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=41623.

SORO, Antonello. 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.

TORRE, Marco. Il captatore informatico, Giuffré, 2017.