

***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 pianeta¹. 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 Francia².

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 sociale³. 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 applicazioni⁴.

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.

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 health 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.

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 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 circolazione⁶. 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 derivarne⁷.

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 www.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*

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 impiego⁸.

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 personale⁹, qualora venisse correlata alla positività al virus del

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), 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

soggetto, la tutela ad essa apprestata sarebbe rinforzata dal rilievo di quel dato, in quanto relativo allo stato di salute e, pertanto, particolare¹⁰.

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 distanza¹¹. Di recente, inoltre, l'attenzione – non solo delle Autorità pubbliche ma anche dei *mass media* – si sta incentrando sull'eventuale uso per il contrasto

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 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.

dell'epidemia in corso di sistemi di sorveglianza attiva – specificamente, la geolocalizzazione – e, tra essi, le App.

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 proposte¹⁵.

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

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 applicazioni¹⁶. 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 tracciare¹⁷. 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 sincronizzati¹⁸.

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.

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, *Coronavirus, scelta l'app per il tracciamento dei contagi: 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_s_i_chiamera_immuni-254235342/).

¹⁶ Sul punto, C. MELZI D'ERIL – G. E. VIGEVANI, *Tre le ipotesi in campo: monitorare i flussi di persone 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.

Muovendo da tale assunto, indagheremo preliminarmente se al lume della disciplina vigente sia lecito e, pertanto, in astratto, prospettabile l'eventuale tracciamento degli individui.

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 emergenziale²⁰, 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 informativa²¹. 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 pubblico²², i soggetti che operano nel Servizio nazionale di protezione civile e nell'ambito del Servizio sanitario nazionale, quelli deputati a monitorare e a

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).

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 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 emergenza²⁴. 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 bisogna improvvisare"*, in *Il corriere della Sera*, 18 marzo 2020, 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 personali²⁵».

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 regione²⁶.

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 Umbria²⁷. 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 malattia²⁹.

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>.

contatti³⁰. 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 altri³¹.

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 mobile³². 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 diversi³³.

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 pubblico³⁴; 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 infettive³⁵. 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 ambito³⁶.

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 assunto a paradigma per l’individuazione della strategia più adeguata per sconfiggere il virus³⁷.

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=a3040200000&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 esse³⁸ 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’utente che al funzionario governativo nel caso di violazione dell’obbligo di autoisolamento³⁹. 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 paziente⁴⁰.

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’utente dello *smartphone*, di un soggetto positivo al virus⁴². Senonché, 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+UtY0JOIXJytnXoyYNHR.no de40?bbsId=BBSMSTR_00000000205&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 evitare⁴³. 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 riferiscono⁴⁴.

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 particolare⁴⁵. 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 quarantena⁴⁶.

Misure che hanno sollevato da subito dibattito e – condivisibili – critiche⁴⁷, in un Paese che oltre alla epidemia in corso deve fare i conti anche con non semplici equilibri di politica interna⁴⁸. 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 positivo⁴⁹.

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, *Israel 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 salute⁵⁰.

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.it/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 giorni⁵¹.

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 correlazioni⁵².

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 salute⁵³.

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 applicazioni⁵⁵.

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 domestico⁵⁷; 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 personali⁵⁸.

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.