EJPLT

Un framework per il *contact tracing* in italia tra esigenze scientifiche, possibilità tecnologiche e rispetto di diritti e liberà individuali in termini di data protection

SERGIO GUIDA
Independent Researcher
Sr.Data/Information Governance Mgr.



Abstract

On March 11 the WHO declared COVID-19 a pandemic. Among quarantines and disruptions to public events, this also kick-started the expedited development of therapeutics and vaccines, but in the short time contact tracing, followed by treatment or isolation, is a key control measure.

A simple relationship was found between the efficiency necessary for eradication and the basic reproductive ratio of the disease, but being it a matter of controlling people and their movements, the extent and the ways in which controls can be implemented can also prove to be very invasive. So, various approaches and technological configurations have been developed as long as, depending on the use of geo-location and the methods and times of data storage, solutions that respect human rights and "privacy-preserving" have been identified, as indicated by the European Authorities, too.

Any solution should take care of its ethical implications, and be flexible enough to be improved rapidly, to rectify potential shortcomings and to avoid 'surveillance creep'. Last but not least, it must be designed to support full interoperability within the EU.

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Keywords: Pandemic - multipronged approach - spatial epidemiology - contact tracing - scope creep - cartography - public monitoring - geo-location - data protection by design - proportionality - electronic patient diary - privacy-preserving proximity tracing - function creep - surveillance creep.

Summary: Introduction – 1. Le prescrizioni del Garante Privacy e delle Autorità europee. 2. Razionale scientifico e richiami tecnici. – 3. Centralizzazione vs. decentralizzazione di dati e informazioni: differenze e conseguenze su data protection e privacy. – Conclusions.

Introduction.

Covid-19[1] è una malattia infettiva causata dal nuovo coronavirus SARS-COV-2[2], un beta coronavirus[3], che ha causato una pandemia globale con enormi perdite di vite umane: a livello globale, al 10 luglio 2020, ci sono stati 12.102.328 casi confermati, inclusi 551.046 decessi, segnalati all'OMS[4].

Attualmente, non esistono vaccini o trattamenti antivirali ufficialmente approvati per la prevenzione o la gestione della malattia[5], purtroppo.

Intanto, le misure necessarie per combatterlo hanno capovolto il nostro mondo, influenzando miliardi di persone e bloccando le economie.

Come ha detto Kristalina Georgieva, IMF *Managing Director*[6], questa è una crisi come nessun altra: "prevediamo la peggiore recessione economica dopo la Grande Depressione. Sebbene ci sia un'enorme incertezza sulla previsione, quest'anno prevediamo che la crescita globale scenderà del 3%. E prevediamo una ripresa parziale nel 2021, con una crescita prevista del 5,8 per cento"[7].

Ecco perché dopo la sospensione del Patto di stabilità "e la conseguente 'riscrittura' di alcune delle regole base della disciplina di bilancio europea (debito, deficit strutturale)" [8], "la

---

[1] Cfr. "Dal 2 gennaio 2020, i tre livelli dell'OMS (Ufficio nazionale cinese, Ufficio regionale per il Pacifico occidentale e quartier generale) collaborano per rispondere allo scoppio di COVID-19. Il 30 gennaio l'OMS ha dichiarato l'epidemia un'emergenza sanitaria pubblica di interesse internazionale (PHEIC). L'11 marzo, il Direttore Generale dell'OMS ha definito COVID-19 una pandemia" in https://www.who.int/westernpacific/emergencies/covid-19.

[2] Cfr. "L'11 febbraio 2020 il Comitato internazionale per la tassonomia dei virus (ICTV) ha annunciato la" sindrome respiratoria acuta grave coronavirus 2 (SARS-CoV-2) *severe acute respiratory syndrome–related coronavirus-2* "come nome del nuovo virus. Questo nome è stato scelto perché il virus è geneticamente correlato al coronavirus responsabile dell'epidemia di SARS del 2003. Sebbene correlati, i due virus sono diversi. (...) L'OMS ha annunciato "COVID-19" come nome di questa nuova malattia l'11 febbraio 2020" in https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it.

[3] Cfr. ad es. S. Dong, J. Sun, Z. Mao et Al., 'A guideline for homology modeling of the proteins from newly discovered betacoronavirus, 2019 novel coronavirus (2019-nCoV)', Journal of Medical Virology, 17 March 2020, https://doi.org/10.1002/jmv.25768.

[4] Fonte: WHO Coronavirus Disease (COVID-19) Dashboard , Data last updated: 2020/7/10, 3:54pm CEST.

[5] Cfr. N.L. Bragazzi, Y. Xiao, J. Wu et Al., 'An updated estimation of the risk of transmission of the novel coronavirus (2019-nCov)', Infectious Disease Modelling 5 (2020) 248-255, https://doi.org/10.1016/j.idm.2020.02.001, p. 249.

[6] Cfr. K. Georgieva, IMF Managing Director, 'Exceptional Times, Exceptional Action: Opening Remarks for Spring Meetings Press Conference', Washington, DC April 15, 2020 in https://www.imf.org/en/News/Articles/2020/04/15/ sp041520-exceptional-times-exceptional-action.

[7] Ibidem.

[8] Cfr. "Il 19 marzo 2020 la Commissione ha adottato un nuovo "Quadro Temporaneo" di aiuti di Stato a sostegno dell'economia nel contesto dell'epidemia di coronavirus, basato sull'articolo 107, paragrafo 3, lettera b), del Trattato sul funzionamento dell'Unione europea. Il quadro temporaneo riconosce che l'intera economia

pandemia che ha investito con la forza d'urto di uno tsunami l'economia europea e mondiale sta sostanzialmente ribaltando anche il rituale 'calendario' di finanza pubblica"[9].

"La conseguenza è che da noi il Governo, dall'esplodere del coronavirus, e al netto dei vari Dpcm che hanno scandito il *lockdown* dell'intero Paese, di fatto ha attuato misure urgenti sul piano economico che si configurano come una e più manovre economiche necessariamente anticipate rispetto alla rituale scadenza autunnale"[10].

Il Covid-19 ha travolto l'industria italiana[11]. La produzione industriale è crollata del 29,3%, una "caduta senza precedenti", anzi secondo ISTAT "in termini tendenziali l'indice corretto per gli effetti di calendario mostra una diminuzione che è la maggiore della serie storica disponibile (che parte dal 1990), superando i valori registrati nel corso della crisi del 2008-2009. Senza precedenti anche la caduta in termini mensili dell'indice destagionalizzato. Tutti i principali settori di attività economica registrano flessioni tendenziali e congiunturali, in molti casi di intensità inedite: nella fabbricazione di mezzi di trasporto e nelle industrie tessili, abbigliamento, pelli e accessori la caduta congiunturale e tendenziale supera ampiamente il 50%"[12].

In realtà, "l'area dell'euro sta affrontando una contrazione economica che per entità e rapidità non ha precedenti in tempi di pace. Le misure adottate per il contenimento della diffusione del coronavirus (COVID-19) hanno provocato un arresto di gran parte dell'attività economica in tutti paesi dell'area dell'euro e su scala mondiale"[13]

Di fronte alle gravissime emergenze da tutti i punti di vista, i governi di tutto il mondo si trovano a fronteggiare quello che molto argutamente è stato chiamato "il trilemma Covid-19"[14], schematizzato nella figura seguente:

dell'UE sta vivendo un grave turbamento. Consente agli Stati membri di utilizzare la piena flessibilità prevista dalle norme sugli aiuti di Stato per sostenere l'economia, limitando al contempo le conseguenze negative alla parità di condizioni nel Mercato Unico.".. "La Commissione europea ha adottato un primo emendamento il 3 aprile 2020 e un secondo oggi per estendere il campo di applicazione del Quadro Temporaneo sugli aiuti di Stato e consentire agli Stati membri di sostenere l'economia nel contesto dell'epidemia di coronavirus", recita la *Press Release* 8 May 2020 in https://ec.europa.eu/ commission/presscorner/detail/en/ip_20_838.

[9] Cfr. D. Pesole, 'Manovra da 80 miliardi tra marzo e maggio: come il Covid ha capovolto il calendario dei conti pubblici', 8 maggio 2020 in https://www.ilsole24ore.com/art/manovra-80-miliardi-marzo-e-maggio-come-covid-ha-capovolto-calendario-conti-pubblici-ADkePDP.

[10] Ibidem.

[11] Cfr. F. Gerosa, 'Il Covid-19 travolge l'industria italiana, tracollo record a marzo', Milano Finanza, 11/05/2020 in https://www.milanofinanza.it/news/il-covid-19-travolge-l-industria-italiana-tracollo-record-a-marzo-202005111052428 228.

[12] Cfr. Istat, 'Produzione industriale periodo di riferimento marzo 2020', Comunicato stampa 11/05/2020 in https://www.istat.it/it/files//2020/05/Produzione-industriale.pdf.

[13] Cfr. Banca d'Italia, 'Bollettino economico BCE, n. 3 – 2020' in https://www.bancaditalia.it/pubblicazioni/bollettino-eco-bce/2020/bol-eco-3-2020/index.html?com.dotmarketing.htmlpage.language=102&pk_campaign=EmailAlertBdi&_pk_kwd=it.

[14] Cfr. R. Bamford, H.Dace et al., 'A Price Worth Paying: Tech, Privacy and the Fight Against Covid-19', Institute for Global Change, 24 April 2020 in https://institute.global/policy/price-worth-paying-tech-privacy-and-fight-against-covid-19.

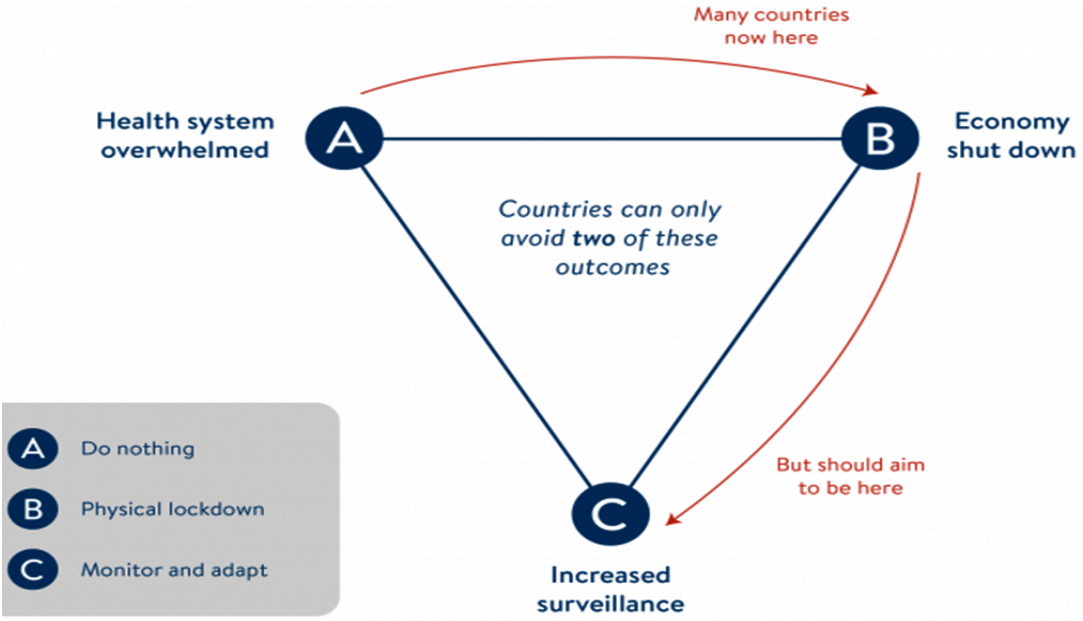


Figura 1: il "Trilemma Covid-19".

Una delle soluzioni più frequentemente proposte – ma, come vedremo con modalità che possono assumere varie connotazioni - è l'utilizzo di App di tracciamento dei contatti (*contact tracing*) per contenere e invertire la diffusione di COVID-19.

Molti sviluppatori "stanno lavorando su iniziative in parallelo e le autorità sanitarie pubbliche in un gran numero di paesi UE/SEE stanno esplorando diverse opzioni. È fondamentale che le autorità sanitarie pubbliche, gli epidemiologi e il personale coinvolti nelle operazioni quotidiane di tracciamento dei contatti siano strettamente coinvolti nel processo di sviluppo per garantire che le app funzionino secondo le migliori conoscenze disponibili sull'epidemiologia di COVID-19, e che le app mobili siano progettate per integrare gli sforzi di tracciamento dei contatti convenzionali"[15].

In effetti, il tracciamento dei contatti (*contact tracing*) è un mezzo[16] consolidato[17] per combattere la diffusione dell'infezione nelle popolazioni se integrata in una strategia di risposta alla salute più ampia e olistica[18]. Tradizionalmente un processo manuale per identificare con chi una persona infetta potrebbe essere entrata in contatto mentre era contagiosa è lungo e difficilmente scalabile per coprire popolazioni più grandi. Pertanto, per accelerare e dimensionare la risposta all'attuale pandemia di COVID-19, vengono progettate e sviluppate nuove soluzioni tecnologiche[19], che consentano di anticipare il momento in cui

[15] Cfr. European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020 in https://www.ecdc.europa.eu/en/publications-data/covid-19-mobile-applications-support-contact-tracing, pag.1.

[16] Cfr. M. Sampathkumar, 'What is contact tracing and can it help in the fight against coronavirus?' | Digital Trends, April 14, 2020 in https://www.digitaltrends.com/news/what-is-contact-tracing-and-how-can-it-help/.

[17] Ad es., "Contact tracing is one of the interventions that have been used to effectively control Ebola virus disease (EVD) outbreaks in Africa" in https://www.who.int/csr/disease/ebola/training/contact-tracing/en/.

[18] Cfr. B. Staehelin, C. Aptel, 'COVID-19 and contact tracing: a call for digital diligence', May 13, 2020 in https://media.ifrc.org/ifrc/2020/05/15/covid-19-contact-tracing-call-digital-diligence/.

[19] Cfr. Centers for Disease Control and Prevention (CDC), 'Contact Tracing : Part of a Multipronged Approach to Fight the COVID-19 Pandemic' in https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.

la persona che *potrebbe* essere contagiosa può innanzitutto esserne messa a conoscenza, come nel seguente schema:

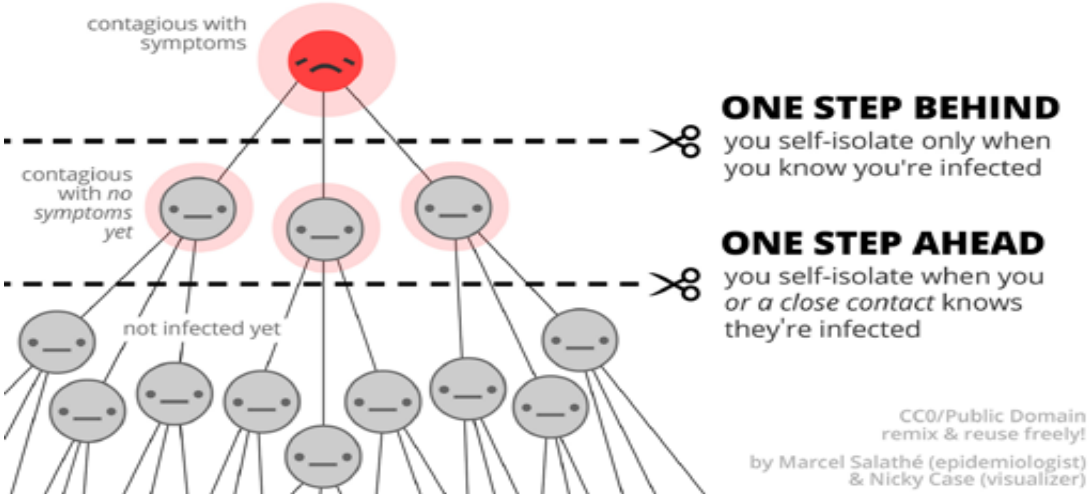


Figura 2: utilizzo del tracciamento dei contatti per limitare la diffusione di un virus.

La maggior parte delle implementazioni si concentra sulla notifica dell'esposizione: notificare a un utente che è stato vicino a un altro utente a cui è stata diagnosticata una diagnosi positiva e metterlo in contatto con le autorità sanitarie pubbliche. Questo tipo di App, che tendono a utilizzare il tracciamento della posizione o il monitoraggio della prossimità, può essere efficace nell'aiutare la lotta contro COVID-19 se esistono anche test diffusi e tracciabilità dei contatti basata su interviste.

In estrema sintesi, per il tracciamento dei contatti si rileva una *summa divisio* a seconda se avvenga:

A) **utilizzando la geo-localizzazione:** alcune App propongono di determinare quali coppie di persone sono state in contatto tra loro raccogliendo dati sulla posizione (compresi i dati GPS) per tutti gli utenti e cercando persone che si trovavano nello stesso posto contemporaneamente. Ma il rilevamento della posizione non è adatto alla ricerca dei contatti dei casi COVID-19, poiché i dati provenienti dal GPS di un telefono cellulare o dalle torri cellulari non sono semplicemente abbastanza precisi da indicare se due persone hanno avuto uno stretto contatto fisico (ovvero entro un raggio di circa 1,80 metri). Ma è abbastanza accurato per esporre informazioni sensibili e identificabili individualmente sulla casa, sul posto di lavoro e sulle abitudini di una persona.

B) **utilizzando il 'monitoraggio di prossimità':** le App di monitoraggio della prossimità utilizzano *Bluetooth Low Energy* (BLE)[20] per determinare se due *smartphone* sono abbastanza vicini da consentire ai loro utenti di trasmettere il virus. BLE misura la prossimità, non la posizione, e quindi è più adatto per la traccia dei contatti dei casi

[20] Cfr. "Ci sono due principali tecnologie nelle specifiche *Bluetooth: Bluetooth classic* e *Bluetooth Smart (Bluetooth Low Energy)*. La principale differenza sta nel consumo di energia in ciascun caso. Tuttavia, ci sono altri fattori per cui *Bluetooth Smart* viene utilizzato per interessanti applicazioni tecnologiche."."2.Applicazioni - Il Bluetooth classico è ideale per le applicazioni che richiedono lo streaming continuo di dati, ad esempio le cuffie. Invece, *Bluetooth LE* è adatto per applicazioni che prevedono un trasferimento periodico di dati e ciò riduce una quantità significativa di utilizzo della batteria. Ciò rende BLE adatto per applicazioni IoT e di marketing di prossimità", M. Adarsh, 'Bluetooth Low Energy (BLE) beacon technology made simple: A complete guide to Bluetooth Low Energy Beacons', April 23, 2020 in https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/.

COVID-19 rispetto alle informazioni sulla posizione del cellulare o GPS. Quando due utenti dell'App si avvicinano, entrambi dispositivi stimano la loro vicinanza utilizzando la potenza del segnale Bluetooth. Se stimano che siano distanti meno di un metro e ottanta per un periodo di tempo sufficiente, ogni dispositivo registra un incontro con il codice dell'altro. Quando un utente dell'App viene a sapere di essere infetto da COVID-19, altri utenti possono essere informati del proprio rischio di infezione.

Tuttavia, l'uso di telefoni cellulari per le App di tracciamento dei contatti ha portato un intenso dibattito al crocevia di sanità pubblica, protezione dei dati e privacy. Anche la fiducia nella tecnologia e i potenziali interessi economici e strategici sono al centro della discussione. Fra le preoccupazioni principali: che la progettazione o l'utilizzo inadeguati di tali App possano portare a stigmatizzazione, aumento della vulnerabilità e fragilità, discriminazione, persecuzione e attacchi all'integrità fisica e psicologica di determinate popolazioni. Ciò tocca la questione più ampia dell'uso responsabile della tecnologia in contesti, come la risposta alle crisi, in cui la fiducia è fondamentale.

Il rischio poi che i dati raccolti allo scopo di tracciare i contatti possano essere utilizzati per altri scopi - o collegati ad altri set di dati per identificare e potenzialmente profilare ulteriori individui - è un aspetto centrale. Questo "*scope creep*" [21] potrebbe portare a sorveglianza intrusiva o uso commerciale non richiesto e indesiderato. Parallelamente, le App di tracciamento dei contatti non sono immuni da attacchi informatici e perdite di dati che potrebbero esporre la privacy e la sicurezza dei loro utenti.

Il tracciamento digitale dei contatti richiede inoltre controlli ed equilibri solidi ed efficaci per controllarne l'efficacia e garantire una gestione trasparente ed equa dell'ecosistema globale; la salute pubblica e i diritti individuali, specialmente in relazione alla privacy, devono poter lavorare di pari passo. Norme scientifiche, etiche e giuridiche aggiornate dovrebbero essere saldamente integrate in questo processo[22] e dovrebbero essere considerate valide solo le soluzioni basate su un approccio di 'protezione dei dati *by design*'.

Come vedremo, in questo contesto la '*data protection by design*' si basa su un'architettura decentralizzata progettata per mantenere il maggior numero possibile di dati particolari sui dispositivi degli utenti. Altre caratteristiche essenziali includono la limitazione dello scopo per mitigare il rischio di '*scope creep*' e un periodo di conservazione dei dati fissato, garantendo che gli strumenti digitali di tracciamento dei contatti vengano prontamente dismessi quando non sono più necessari.

Un esempio notevole di tale protocollo decentralizzato è quello proposto dal consorzio DP-3T [23], successivamente adottato ad es. dalla Croce Rossa austriaca [24] e dalla

[21] Nel *Project Management* con la locuzione '*Scope creep*' (cambiamento di ambito) ci si riferisce alla crescita continua o incontrollata nell'ambito di un progetto in qualsiasi momento dopo l'inizio del progetto stesso.

[22] Come si legge anche in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.1: "La prospettiva della salute pubblica dovrebbe essere al centro della valutazione dell'efficacia e della sicurezza delle app mobili. Inoltre, le app devono essere progettate in modo tale da consentire l'aggiornamento delle impostazioni e dei parametri. Pertanto, il focus di questa guida sono le considerazioni epidemiologiche e operative che le autorità sanitarie pubbliche potrebbero prendere in considerazione quando scelgono una soluzione o lavorano per implementare e valutare una particolare soluzione".

[23] Si veda ad es. in Github, DP-3T consortium e ampiamente *infra.*

[24] Cfr. 'Meet the STOPP CORONA APP' in https://www.roteskreuz.at/site/meet-the-stopp-corona-app/.

Confederazione Svizzera[25] e supportato dall'iniziativa Apple/Google[26].

1. Le prescrizioni del Garante Privacy e delle Autorità europee.

La nostra Autorità Garante è intervenuta in prima battuta il 2 febbraio 2020[27], quando "a seguito della Delibera del Consiglio dei Ministri del 31 gennaio 2020[28] con la quale è stato dichiarato, per sei mesi, lo stato di emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili, il Capo del Dipartimento della protezione civile ha chiesto con urgenza il parere del Garante in ordine a una bozza di ordinanza, contenente i primi interventi urgenti di protezione civile in relazione alla predetta emergenza, da emanarsi ai sensi dell´art. 25 del d.lgs. 2 gennaio 2018, n. 1, Codice della protezione civile"[29].

L'ordinanza, in relazione al trattamento dei dati personali connessi all'attuazione delle attività di protezione civile, allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, ha previsto che

- √ i soggetti operanti nel Servizio nazionale di protezione civile possono "effettuare trattamenti, compresa la comunicazione tra loro, di dati personali anche relativi agli artt. 9 e 10 del Regolamento (UE) 2016/679, che risultino necessari per l'espletamento della funzione di protezione civile fino al 30 giugno 2020"[30] .
- √ la comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli sopra citati, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento (UE) 2016/679, è effettuata, nei casi in cui essa risulti indispensabile, ai fini dello svolgimento delle attività previste dall'ordinanza.
- √ i trattamenti di dati personali devono essere effettuati nel rispetto dei principi di cui all'art. 5 del Regolamento (UE) 2016/679"[31].

Il Garante "osserva che le disposizioni risultano idonee a rispettare le garanzie previste dalla normativa in materia di protezione dei dati personali nel contesto di una situazione di emergenza", evidenziando però come sia necessario "che, alla scadenza del termine dello stato di emergenza, siano adottate da parte di tutte le Amministrazioni coinvolte negli interventi di protezione civile misure idonee a ricondurre i trattamenti di dati personali

---

[25] Cfr. EPFL, 'Switzerland launches DP-3T contact tracing app', 21 April 2020 in https://privacyinternational.org/ examples/3726/switzerland-launches-dp-3t-contact-tracing-app.

[26] Cfr. Apple Newsroom, 'Apple and Google partner on COVID-19 contact tracing technology', April 10, 2020 in https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.

[27] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili – 2 febbraio 2020 [doc. web n. 9265883].

[28] Delibera del Consiglio dei Ministri 31 gennaio 2020, Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili. (20A00737) in GU n.26 del 1-2-2020.

[29] Con il Decreto Legislativo 2 gennaio 2018, n. 224, (Raccolta 2018) (18G00011), GU Serie Generale n.17 del 22-01-2018) è stato approvato il nuovo Codice della Protezione Civile, entrato in vigore il 6 febbraio 2018, e che ha abrogato, tra le altre, la legge 24 febbraio 1992, n. 225. Il Servizio nazionale della protezione civile è definito come il sistema che esercita la funzione di protezione civile costituita dall'insieme delle competenze e delle attività volte a tutelare la vita, l'integrità fisica, i beni, gli insediamenti, gli animali e l'ambiente dai danni o dal pericolo di danni derivanti da eventi calamitosi di origine naturale o derivanti dall'attività dell'uomo. Sono attività di protezione civile quelle volte alla previsione, prevenzione e mitigazione dei rischi, alla gestione delle emergenze e al loro superamento.

[30] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili – 2 febbraio 2020 [doc. web n. 9265883], cit..

[31] Ibidem.

effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali in capo a tali soggetti".

Solo con queste premesse il Garante esprime "parere favorevole sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili"[32].

Il secondo intervento più significativo del Garante è stato quello con cui il 2 marzo ha stabilito che "Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti", dopo numerosi quesiti posti in merito alla possibilità di raccogliere, all'atto della registrazione di visitatori e utenti, informazioni circa la presenza di sintomi da Coronavirus e notizie sugli ultimi spostamenti, come misura di prevenzione dal contagio[33]. Analogamente, datori di lavoro pubblici e privati hanno chiesto al Garante la possibilità di acquisire una "autodichiarazione" da parte dei dipendenti in ordine all'assenza di sintomi influenzali, e vicende relative alla sfera privata.

Da un lato, la raccolta di informazioni relative ai sintomi e ai recenti spostamenti di ogni individuo spettano agli operatori sanitari e al sistema della protezione civile, vale a dire agli organi deputati a garantire il rispetto delle regole di sanità pubblica sancite.

Dall'altro, resta fermo l'obbligo del lavoratore di segnalare al datore di lavoro qualsiasi situazione di pericolo per la salute e la sicurezza sui luoghi di lavoro.

In tale quadro "il datore di lavoro può invitare i propri dipendenti a fare, ove necessario, tali comunicazioni agevolando le modalità di inoltro delle stesse, anche predisponendo canali dedicati; permangono altresì i compiti del datore di lavoro relativi alla necessità di comunicare agli organi preposti l'eventuale variazione del rischio 'biologico' derivante dal Coronavirus per la salute sul posto di lavoro e gli altri adempimenti connessi alla sorveglianza sanitaria sui lavoratori" attraverso l'opera del medico competente, come, ad esempio, la possibilità di sottoporre a una visita straordinaria i lavoratori più esposti.

Le autorità hanno, inoltre, previsto sia a livello nazionale che locale le misure di prevenzione necessarie per assicurare l'accesso dei visitatori a tutti i locali aperti al pubblico.

"Pertanto, il Garante invita tutti i titolari del trattamento ad attenersi scrupolosamente alle indicazioni fornite dal Ministero della salute e dalle istituzioni competenti per la prevenzione della diffusione del Coronavirus, senza effettuare iniziative autonome che prevedano la raccolta di dati anche sulla salute di utenti e lavoratori che non siano normativamente previste o disposte dagli organi competenti"[34].

Un altro intervento fondamentale è stata l'audizione informale del Presidente Soro sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus dinanzi alla Commissione Trasporti, Poste e Telecomunicazioni della Camera dei Deputati l'8 aprile 2020.

"La gravissima emergenza che il Paese sta affrontando ha imposto l'adozione- con norme di vario rango- di misure limitative di molti diritti fondamentali, necessarie per contenere auspicabilmente, il numero dei contagi"[35].

Alcune deroghe al regime ordinario di gestione dei dati sono state previste sin dalle

---

[32] Ibidem.

[33] Cfr. Garante per la Protezione dei Dati Personali, Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti – 2 marzo 2020 [doc. web n. 9282117].

[34] Ibidem.

[35] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Audizione informale, in videoconferenza, del sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus - Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati', 8 aprile 2020, riportato su sito Garante [doc. web n. 9308774].

primissime ordinanze intervenute pochi giorni dopo la deliberazione dello stato di emergenza, ma soprattutto "nuove e più invasive raccolte di dati potrebbero fondarsi su esigenze di sanità pubblica che -al pari del "soccorso di necessità"- costituiscono autonomi presupposti di liceità, in presenza di una previsione normativa conforme ai principi di necessità, proporzionalità, adeguatezza, nonché del rispetto del contenuto essenziale del diritto".

E' questa la cornice entro la quale valutare "l'ipotesi della raccolta dei dati sull'ubicazione o sull'interazione dei dispositivi mobili dei soggetti risultati positivi, con altri dispositivi, al fine di analizzare l'andamento epidemiologico o per ricostruire la catena dei contagi".

Dovendo privilegiare un criterio di gradualità, non pone particolari problemi l'acquisizione di trend, effettivamente anonimi, di mobilità. L'art. 9 della direttiva e-privacy legittima infatti il trattamento, anche in assenza del consenso dell'interessato, dei dati relativi all' ubicazione, purché anonimi.

Tale soluzione consente di realizzare, ad esempio, mappe descrittive dell'andamento dell'epidemia, utilissime a fini prognostici e statistici, meno a scopi diagnostici in senso proprio.

Per altro verso, l'uso di dati identificativi sull'ubicazione o sull'interazione con altri dispositivi può risultare funzionale a diversi scopi, , ma richiede – anche ai sensi dell'art. 15 della direttiva e-privacy – una disposizione normativa sufficientemente dettagliata e contenente adeguate garanzie.

I vari utilizzi possibili di tali dati possono essere finalizzati, in via teorica:

a) o alla verifica della posizione del soggetto sottoposto ad obbligo di permanenza domiciliare perché positivo, utilizzando dunque la geo-localizzazione del telefono (presupponendo segua continuamente il soggetto) per accertare l'effettivo rispetto del divieto di allontanamento dal domicilio, oppure:

b) all'acquisizione, a ritroso, dei dati sull'interazione del soggetto poi risultato positivo con altri soggetti, per verificarne, nel periodo in cui aveva capacità virale, gli eventuali contatti desumibili tramite varie tecniche: celle telefoniche, gps, *bluetooth*.

Le due ipotesi differiscono nella finalità, elemento decisivo per la valutazione della complessiva legittimità del trattamento.

La prima ipotesi infatti, nell'utilizzare la localizzazione del telefono come fosse una sorta di braccialetto elettronico atipico, presuppone la sostituzione, con l'occhio elettronico, dei controlli "umani", dando però per acquisito che chi decida di violare gli obblighi di permanenza domiciliare porti con sé il telefono, il che è evidentemente contro-intuitivo.

Più complessa è la seconda ipotesi, relativa alla mappatura a ritroso dei contatti tenuti, nel periodo d'incubazione, da soggetti risultati contagiati, cioè al *contact tracing*. Tale ricostruzione dei contatti può avvenire, almeno astrattamente, attraverso l'incrocio di tipologie di dati diversi: quelli sulle transazioni commerciali, sulle celle telefoniche, quelli sull'interazione con altri dispositivi mobili desunti dal ricorso a tecnologie *bluetooth*[36].

Va premesso che ciascuna tipologia di questi dati ha, naturalmente, una diversa significatività a fini epidemiologici, tanto maggiore quanto più idonea a selezionare i contatti più rilevanti perché più ravvicinati e, dunque, maggiormente suscettibili di aver determinato, almeno potenzialmente, un contagio, ma incide anche sul complessivo giudizio di proporzionalità, in quanto la maggiore selettività riduce il perimetro di incidenza della misura al solo stretto necessario, con effetti socialmente apprezzabili in termini di tutela della salute, individuale e collettiva.

[36] Per un'ampia disamina tecnica si veda ad es. K. Foy**, '**Bluetooth signals from your smartphone could automate Covid-19 contact tracing while preserving privacy', Lincoln Laboratory**,** MIT NEWS April 8, 2020 in https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409.

In termini generali, comunque, il fine perseguito da tale misura risulta particolarmente apprezzabile perché non repressivo (come invece nel caso della sorveglianza del soggetto in quarantena obbligatoria mediante la sua geo-localizzazione), ma solidaristico.

Anche queste considerazioni inducono a preferire il ricorso a sistemi fondati sulla volontaria adesione dei singoli che consentano il tracciamento della propria posizione. Tuttavia, per garantire la reale libertà (e quindi la validità) del consenso al trattamento dei dati, esso non dovrebbe risultare in alcun modo condizionato[37].

Pertanto, non potrebbe ritenersi effettivamente valido, perché indebitamente e inevitabilmente condizionato, il consenso prestato al trattamento dei dati acquisiti con tali sistemi, se prefigurato come presupposto necessario, ad esempio, per usufruire di determinati servizi o beni (si pensi al sistema cinese).

L'efficacia diagnostica di tale soluzione dipende, in ogni caso, dal grado di adesione che essa incontri tra i cittadini, in quanto la rilevazione potrebbe per definizione avvenire solo limitatamente alla parte della popolazione che consenta di "farsi tracciare": la percentuale minima per l'efficacia è stimata nell'ordine del 60%.

In tal senso, quindi, la volontaria attivazione di un'App funzionale alla raccolta dei dati sull'interazione dei dispositivi, ben potrebbe rappresentare il presupposto di uno schema normativo fondato su esigenze di sanità pubblica, con adeguate garanzie per gli interessati (art. 9, p.2, lett. i) Reg. (Ue) 2016/679).

La seconda fase del trattamento (quella, cioè, successiva alla rilevazione dei dati) consiste essenzialmente nella conservazione degli stessi, in vista del loro eventuale, successivo utilizzo per allertare i potenziali contagiati.

Sotto il profilo dell'impatto sulla riservatezza, determinato dalla conservazione in sé dei dati, in vista del loro successivo utilizzo, è certamente preferibile la soluzione della registrazione del "diario dei contatti" sullo stesso dispositivo individuale nella disponibilità del soggetto. Si eviterebbe così la conservazione di dati personali in banche dati dei gestori, che riproporrebbe le criticità rilevate dalla giurisprudenza della Cgue sulla *data retention*[38].

I criteri di necessità, proporzionalità e minimizzazione rimarcati dalla giurisprudenza europea indicano, comunque, l'esigenza di contenere eventuali limitazioni della privacy nella misura strettamente necessaria a perseguire fini rilevanti, che garantisca cioè il minor ricorso possibile a dati identificativi, sia in fase di raccolta sia in fase di conservazione.

Ecco allora che il *bluetooth*, restituendo dati su interazioni più strette di quelle individuabili in celle telefoniche molto più ampie, si dimostra più efficace nel selezionare i possibili contagiati all'interno di un campione più attendibile proprio perché limitato ai contatti significativi.

In particolare, sarebbero apprezzabili quelle tecnologie che mantengono il diario dei contatti esclusivamente nella disponibilità dell'utente, sul suo dispositivo, ragionevolmente per il solo periodo massimo di potenziale incubazione. Il soggetto che risultasse positivo dovrebbe fornire l'identificativo Imei del proprio dispositivo all'ASL, che sarebbe poi tenuta a trasmetterlo al server centrale per consentirgli così di ricostruire, tramite un calcolo algoritmico, i contatti tenuti con altre persone le quali si siano, parimenti, avvalse dell'App *bluetooth*. Queste ultime riceverebbero poi un *alert* di potenziale contagio, con l'invito a

---

[37] Si veda, tra gli altri, L. Gatt, R. Montanari, I. A.Caggiano, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali', Politica del diritto, 2017, 2, 337 – 353.

[38] Per tutte vedasi O. Pollicino, M. Bassini, 'La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico. Nota a Corte Giustizia UE, sent. 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15', in Diritto Penale Contemporaneo https://archiviodpc.dirittopenaleuomo.org/upload/POLLICINOBASSINI_2017a.pdf.

sottoporsi ad accertamenti: in tal modo, il tracciamento sarebbe affidato a un flusso di dati pseudonimizzati, suscettibili di re-identificazione solo in caso di rilevata positività. La comunicazione tra server centrale ed App dei potenziali contagiati avverrebbe senza consentirne la re-identificazione, minimizzando l'impatto della misura sulla privacy individuale.

In alternativa all'*alert* intra-app, si potrebbe ipotizzare l'intervento diretto dell' ASL che informi e sottoponga ad accertamento le persone che, sulla scorta delle rilevazioni *bluetooth*, risultino avere avuto contatto con il soggetto positivo.

La conservazione dei dati di contatto, da parte del server, dovrebbe comunque limitarsi al tempo strettamente indispensabile alla rilevazione dei potenziali contagiati.

L'anamnesi rimessa al medico consentirebbe di evitare l'esclusiva soggezione a decisioni automatizzate, correggendo anche, così, possibili distorsioni e inesattezze nel processo algoritmico così come richiesto dal GDPR.

In ogni caso, è auspicabile che la complessa filiera del *contact tracing* possa realizzarsi interamente in ambito pubblico, fino a "prevedere specifici reati propri, suscettibili di realizzazione da parte di coloro che, potendo avere accesso ai dati per qualunque ragione anche operativa, li utilizzino per altre finalità".

"La soluzione ipotizzata ridurrebbe, verosimilmente allo stretto necessario, la sua incidenza sulla riservatezza. Tuttavia, benché non massivo, il trattamento di dati personali comunque realizzato richiederebbe, auspicabilmente, una norma di rango primario, quindi anche un decreto-legge, che assicura la tempestività dell'intervento, pur non omettendo il sindacato parlamentare né quello successivo di costituzionalità, diversamente dalle ordinanze"[39].

E sulla scorta di tale "auspicio" lo stesso Garante ha reso il Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020[40]: "la Presidenza del Consiglio dei Ministri ha richiesto il parere del Garante su una proposta normativa volta a disciplinare il trattamento di dati personali nel contesto dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del Covid-19 per finalità di tracciamento dei contatti tra i soggetti che, a tal fine, abbiano volontariamente installato un'apposita applicazione sui dispositivi mobili".

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

---

[39] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Audizione informale, in videoconferenza, del sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus - Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati', 8 aprile 2020 , riportato su sito Garante [doc. web n. 9308774], cit..

[40] Cfr. Garante per la Protezione dei Dati Personali, Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 - 29 aprile 2020 [doc. web n. 9328050].

Al comma 2 si prevede che, all'esito di una valutazione di impatto effettuata ai sensi dell'articolo 35 del Regolamento il Ministero della salute adotti misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante, assicurando, in particolare, che:

- gli utenti ricevano, prima dell'attivazione dell'App, un'idonea informativa;
- i dati personali raccolti dall'App siano esclusivamente quelli necessari ad avvisare gli utenti di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, individuati secondo criteri stabiliti dal Ministero della salute;
- il trattamento effettuato per il tracciamento sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati, con esclusione di ogni forma di geo-localizzazione dei singoli utenti;
- siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di re-identificazione degli interessati cui si riferiscono i dati pseudonimizzati;
- i dati relativi ai contatti stretti siano conservati, anche nei dispositivi mobili degli utenti, per il periodo, stabilito dal Ministero della salute, strettamente necessario al tracciamento e cancellati in modo automatico alla scadenza del termine; i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento possano essere esercitati anche con modalità semplificate.

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

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

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

Viene subito rilevato che "la norma tiene conto di molte delle indicazioni fornite dal Presidente del Garante nell'audizione tenuta in data 8 aprile u. presso la IX Commissione trasporti e comunicazioni della Camera dei deputati"(*ut supra*), così come "appare conforme, per quanto dalla stessa disciplinato e nelle sue linee generali, ai criteri indicati dalle Linee guida del Comitato europeo per la protezione dei dati del 21 aprile scorso (vedi *infra*) a proposito dei sistemi di *contact tracing*, che possono sintetizzarsi nei termini seguenti, raffrontandovi la disposizione in esame:

a) volontarietà: in ragione del rilevante impatto individuale del tracciamento, l'adesione deve essere frutto di una scelta realmente libera da parte dell'interessato. La mancata adesione al sistema non deve quindi comportare conseguenze pregiudizievoli, adottando dunque una locuzione più ampia di quella riferita al solo esercizio dei diritti fondamentali;

b) previsione normativa: il presupposto può individuarsi nell'esigenza di svolgimento di un compito di interesse pubblico, in particolare per esigenze di sanità pubblica, in base a "previsione normativa o disposizione legislativa" dell'Unione europea o degli Stati membri. Sotto questo profilo, in particolare, la scelta di una norma di rango primario soddisfa i

requisiti di cui all'articolo 9, par. 2, lett. i) del Regolamento[41] e agli articoli 2-ter e 2-sexies del Codice[42], con garanzie ulteriori che potranno essere stabilite con il previsto provvedimento del Garante da adottare ai sensi dell'articolo 2-quinquiesdecies del medesimo Codice;

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

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

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

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

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

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

In sintesi, dunque, un sistema di *contact tracing* come descritto non sarebbe in contrasto con i principi di protezione dei dati personali. Anzi, come passiamo a vedere, sono gli stessi criteri enunciati e dettagliati più volte dalle Autorità europee**.**

Già nel suo primo intervento in materia, il Comitato europeo per la protezione dei dati (EDPB, *European Data Protection Board*) ha infatti ricordato[43] che gli sforzi per utilizzare i dati di geo-localizzazione per effettuare il tracciamento dei contatti - in effetti nello stesso modo

---

[41] Regolamento generale sulla protezione dei dati (GDPR): Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale UE 127 del 23/05/2018.

[42] Decreto Legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O. n.123 alla G.U. 29/07/2003, n.174) integrato con le modifiche introdotte dal D.Lgs.10 agosto2018, n.101 (in G.U. 04/09/2018 n.205).

[43] Cfr. European Data Protection Board, Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak, 16 March, 2020 in https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en.

in cui alcuni paesi prevedono controverse - sarebbero attualmente illegali ai sensi della direttiva e-privacy[44]. Ma in determinate circostanze, comprese le questioni di sicurezza nazionale e pubblica, gli Stati membri hanno il titolo di introdurre nuove leggi che sostituiranno le loro interpretazioni esistenti della direttiva.

Nella dichiarazione leggiamo: "Le leggi nazionali di attuazione della direttiva e-privacy prevedono il principio secondo cui i dati di localizzazione possono essere utilizzati dall'operatore solo quando sono resi anonimi o con il consenso delle persone".

"Le autorità pubbliche dovrebbero in primo luogo mirare al trattamento dei dati relativi all'ubicazione in modo anonimo (ovvero l'elaborazione dei dati aggregati in modo tale da non poter essere convertiti in dati personali). Ciò potrebbe consentire di generare rapporti sulla concentrazione di dispositivi mobili in una determinata posizione ('cartografia')".

In pratica, per identificare gruppi di persone che infrangevano le regole di autoisolamento le forze dell'ordine potevano usare dati aggregati sulla posizione, basati sulla vicinanza delle persone alle torri cellulari, ma non potevano usare i dati per trovare persone che erano venute a stretto contatto con quelli che in seguito erano risultati positivi.

La dichiarazione continua: "Quando non è possibile elaborare solo dati anonimi, l'art. 15 della direttiva e-privacy[45] consente agli Stati membri di introdurre misure legislative per la sicurezza nazionale e pubblica.

"Questa legislazione di emergenza è possibile a condizione che costituisca una misura necessaria, appropriata e proporzionata all'interno di una società democratica. Se vengono introdotte misure di questo tipo, uno Stato membro è tenuto a istituire garanzie adeguate, come garantire ai singoli il diritto a un ricorso giurisdizionale."

Riguardo al GDPR[46],"prevede le basi legali per consentire ai datori di lavoro e alle autorità sanitarie competenti di trattare i dati personali nel contesto di epidemie, senza la necessità di ottenere il consenso dell'interessato".

---

[44] Direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla protezione della vita privata nel settore delle comunicazioni elettroniche (Direttiva sulla privacy e le comunicazioni elettroniche). "Conosciuta come Direttiva e-Privacy, stabilisce le regole su come i fornitori di servizi di comunicazione elettronica, come le società di telecomunicazioni e i fornitori di servizi Internet, dovrebbero gestire i dati dei loro abbonati. Garantisce inoltre i diritti per gli abbonati quando utilizzano questi servizi ". (...) "Nel giugno 2013 la Commissione ha messo in atto nuove norme specifiche per garantire che le violazioni dei dati personali nel settore delle telecomunicazioni dell'UE siano notificate allo stesso modo in ciascuno Stato membro." In https://ec.europa.eu/digital-single-market/en/news/eprivacy-directive.

[45] Il testo consolidato recita "Articolo 15 Applicazione di alcune disposizioni della direttiva 95/46 / CE - 1. Gli Stati membri possono adottare misure legislative per limitare la portata dei diritti e degli obblighi di cui all'articolo 5, all'articolo 6, all'articolo 8, paragrafo 1 , (2), (3) e (4) e dell'articolo 9 della presente direttiva quando tale restrizione costituisce una misura necessaria, appropriata e proporzionata all'interno di una società democratica per salvaguardare la sicurezza nazionale (vale a dire la sicurezza dello Stato), la difesa, la pubblica sicurezza e la prevenzione, l'indagine, l'individuazione e il perseguimento di reati o dell'uso non autorizzato del sistema di comunicazione elettronica, di cui all'articolo 13, paragrafo 1, della direttiva 95/46 / CE. A tal fine, gli Stati membri possono, tra l'altro, adottare misure legislative che prevedono la conservazione di dati per un periodo limitato giustificato dai motivi di cui al presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea. " - "1b. I fornitori istituiscono procedure interne per rispondere alle richieste di accesso ai dati personali degli utenti sulla base delle disposizioni nazionali adottate ai sensi del paragrafo 1. Forniscono all'autorità nazionale competente, su richiesta, informazioni su tali procedure, il numero di richieste ricevute, il giustificazione legale invocata e loro risposta" in https://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058 :20091219:EN:HTML.

[46] Come noto, "il Regolamento generale sulla protezione dei dati (GDPR) dell'UE garantisce che i dati personali possano essere raccolti solo a condizioni rigorose e per scopi legittimi. Le organizzazioni che raccolgono e gestiscono le tue informazioni personali devono anche proteggerle dall'uso improprio e rispettare determinati diritti" in https://ec.europa.eu/digital-single-market/en/online-privacy.

Andrea Jelinek, presidente di EDPB, afferma: "Le norme sulla protezione dei dati (come il GDPR) non ostacolano le misure prese nella lotta contro la pandemia di coronavirus. Tuttavia, vorrei sottolineare che, anche in questi tempi eccezionali, il responsabile del trattamento dei dati deve garantire la protezione dei dati personali degli interessati. Pertanto, una serie di considerazioni dovrebbero essere prese in considerazione per garantire il trattamento legale dei dati personali. "

Quindi, lo scopo principale della dichiarazione EDPB è ricordare che le protezioni del GDPR non possono semplicemente essere spazzate via anche durante una crisi di salute pubblica[47].

In effetti, a partire dal fatto che l'enorme capacità di elaborazione dei dati consentita dalla tecnologia ha un impatto significativo sulla vita di ogni singolo cittadino e in linea con il *Necessity Toolkit*[48] del 2017, che aveva delimitato la portata del concetto di necessità di limitazioni ai diritti fondamentali, il GEPD ha adottato a dicembre 2019 i nuovi «orientamenti sulla proporzionalità»[49].

Tali regole definiscono ulteriormente il contenuto e lo scopo dei diritti garantiti dalla Carta fondamentale e dal GDPR, sviluppando un'analisi giuridica approfondita volta a creare un vero test di proporzionalità e strumenti pratici per aiutare a valutare la conformità delle misure UE proposte che avrebbero un impatto sui fondamentali diritti alla privacy e protezione dei dati personali[50].

Un ultimo punto: la fase di "proporzionalità in senso stretto" esamina gli effetti dell'atto legislativo, confrontando e ponderando i benefici derivanti dal perseguimento dell'obiettivo a cui mira il legislatore e i costi, cioè i sacrifici che esso impone agli altri diritti e interessi in gioco[51].

Normalmente è la valutazione più delicata, "quella che richiede al giudice di allargare lo sguardo delle sue valutazioni, fino a proiettarsi sull'impatto effettivo della legislazione che gli viene presentata: ciò richiede una conoscenza dei dati dell'esperienza reale che la legge regola, che supera di gran lunga i dati legali positivi, strettamente inteso"[52].

In pratica il rischio che la necessaria serenità di giudizio possa essere influenzata dall'urgenza di utilizzare al più presto strumenti tecnologici pervasivi ma efficaci per limitare pandemie così contagiose come Covid-19 deve essere attentamente valutato.

---

[47] Cfr. "Sono rigorose regole di protezione dei dati per garantire il diritto fondamentale alla protezione dei dati personali. Sono fondamentali per una società democratica e una componente importante di un'economia sempre più basata sui dati. L'UE aspira a cogliere le numerose opportunità offerte dalla trasformazione digitale in termini di servizi, posti di lavoro e innovazione, affrontando al contempo le sfide che queste comportano." nella Comunicazione della Commissione al Parlamento europeo e al Consiglio, Norme sulla protezione dei dati come strumento per rafforzare la fiducia nell'UE e oltre, Bruxelles, 24.7.2019, pagina 1, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf.

[48] Cfr. Garante Europeo per la Protezione dei Dati, 'Valutare la necessità di misure che limitano il diritto fondamentale alla protezione dei dati personali: A Toolkit', 11 aprile 2017 in https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

[49] Cfr. Garante Europeo per la Protezione dei Dati, Linee guida sulla valutazione della proporzionalità delle misure che limitano i diritti fondamentali alla privacy e alla protezione dei dati personali, 19 dicembre 2019 in https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en.

[50] Vedi anche S. Guida, D. Tozzi, 'La valutazione della proporzionalità delle misure che limitano i diritti fondamentali della privacy nelle nuove linee guida del garante europeo della protezione dei dati' in European Journal of Privacy Law & Technologies, ISSN 2704-8012, Issue 2020/1 – 2020.

[51] Cfr. M. Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola', Roma, Palazzo della Consulta 24-26 ottobre 2013, Working Papers, pag.5.

[52] Ibidem.

Sostanzialmente, EDPB sembra voler riaffermare il suo orientamento secondo cui "le decisioni di progettazione tecnologica non dovrebbero dettare le nostre interazioni sociali e la struttura delle nostre comunità, ma dovrebbero piuttosto sostenere i nostri valori e diritti fondamentali"[53].

Tuttavia, non si deve mai dimenticare che "lo spettro di osservazione dell'esperienza legale (...) è particolarmente ampio e, quindi, adeguato al giudizio di ragionevolezza"[54].

E infine "Ragionevole non esprime solo pura razionalità, ma, come è stato effettivamente detto con parole pertinenti anche all'universo legale, consiste nel sottomettere la ragione all'esperienza"[55].

Tanto che pochi giorni dopo il Comitato Europeo per la Protezione dei Dati ha adottato la "Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19"[56], che per sviluppare quanto già espresso dalla Presidente, Andrea Jelinek, *ut supra*.

Il 30/03/2020 il Consiglio d'Europa (*CoE*) ha pubblicato il documento intitolato "Dichiarazione comune sul diritto alla protezione dei dati nel contesto della pandemia di COVID-19 di Alessandra Pierucci, presidente del Comitato delle convenzioni 108 e Jean Philippe Walter, Commissario per la protezione dei dati del Consiglio d'Europa"[57]. Il documento si articola in 5 punti: elaborazione di dati relativi alla salute; 2. Elaborazione dei dati su larga scala; 3. Trattamento dei dati da parte dei datori di lavoro; 4. Dati da Mobile, e da computer; 5. Elaborazione dei dati nei sistemi educativi.

Lo snodo centrale di questo documento è il seguente: secondo la Convenzione 108+ (art.11) per possibili restrizioni in tempi di pandemia le eccezioni devono essere "previste dalla legge, rispettare l'essenza dei diritti e delle libertà fondamentali e costituisce una misura necessaria e proporzionata in una società democratica".

L'8/04/2020 la Commissione europea ha pubblicato la "Raccomandazione su un approccio comune dell'Unione per l'uso della tecnologia e dei dati per combattere e uscire dalla crisi COVID-19, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati di mobilità anonimizzati"[58].

Gli obiettivi della raccomandazione sono così indicati: "questa raccomandazione istituisce un processo per lo sviluppo di un approccio comune, denominato *Toolbox*, per utilizzare i mezzi digitali per affrontare la crisi. La cassetta degli attrezzi consisterà in misure pratiche per un uso efficace di tecnologie e dati, con particolare attenzione a due aree in particolare:

(1) ***Un approccio paneuropeo per l'uso di applicazioni mobili****, coordinato a livello dell'Unione, per consentire ai cittadini di adottare misure di distanziamento sociale efficaci e più mirate e per*

---

[53] Cfr. Garante Europeo per la Protezione dei Dati, Parere 4/2015 Verso una nuova etica digitale Dati, dignità e tecnologia 11 settembre 2015, pag. 10 in https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_it.pdf.

[54] Cfr. M. Cartabia, 'I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana, Conferenza trilaterale delle Corte costituzionali italiana, portoghese e spagnola', Roma, Palazzo della Consulta 24-26 ottobre 2013, Working Papers, cit., pag.19.

[55] Ibidem.

[56] European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020 in https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en.

[57] Cfr. Council of Europe, Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, 30 March 2020 in https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

[58] Cfr. European Commission, Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data in https://ec.europa.eu/info/sites/info/files/recommendation_on apps_for_contact_tracing_4.pdf.

avvertire, prevenire e tracciare i contatti per contribuire a limitare la propagazione della malattia COVID-19. Ciò comporterà una metodologia per il monitoraggio e la condivisione delle valutazioni dell'efficacia di tali applicazioni, della loro interoperabilità[59] *e delle implicazioni transnazionali e del loro rispetto per la sicurezza, la privacy e la protezione dei dati; e*

(2) ***Uno schema comune per l'utilizzo di dati anonimi e aggregati sulla mobilità delle popolazioni*** *al fine di (i) modellare e prevedere l'evoluzione della malattia, (ii) monitorare l'efficacia del processo decisionale da parte delle autorità degli Stati membri su misure come il distanziamento sociale e confinamento e (iii) informare una strategia coordinata per uscire dalla crisi COVID-19".*

Nella stessa data, il Comitato dei Ministri del Consiglio d'Europa ha pubblicato la "Raccomandazione CM / Rec (2020) 1 del Comitato dei Ministri agli Stati membri sugli impatti dei diritti umani dei sistemi algoritmici (adottata dal Comitato dei Ministri su 8 aprile 2020 alla 1373a riunione dei deputati dei ministri)"[60]. Questa raccomandazione, breve ma con un allegato molto ampio (Linee guida), evidenzia ovviamente gli aspetti relativi ai diritti umani.

Il 21 aprile 2020, durante la sua 23a sessione plenaria, l'EDPB ha adottato linee guida sul trattamento dei dati sanitari a fini di ricerca nel contesto dell'epidemia COVID-19 e linee guida sulla geo-localizzazione e altri strumenti di tracciabilità nel contesto dell'epidemia COVID-19. Entrambe eccezionalmente non saranno sottoposte a consultazione pubblica a causa dell'urgenza della situazione attuale e della necessità di avere le linee guida prontamente disponibili.

Le "linee guida sul trattamento dei dati sanitari a fini di ricerca nel contesto dell'epidemia COVID-19"[61] mirano a far luce sulle questioni legali più urgenti relative all'uso dei dati sanitari, come la base giuridica del trattamento, l'ulteriore trattamento dei dati sanitari ai fini della ricerca scientifica, l'implementazione di garanzie adeguate e l'esercizio dei diritti dell'interessato.

Le linee guida affermano che il GDPR contiene diverse disposizioni per il trattamento dei

---

[59] In tema di "interoperabilità transfrontaliera, ci sono alcuni aspetti epidemiologici da considerare. App diverse hanno algoritmi di calcolo del rischio diversi sebbene tutti saranno basati sul tempo e sulla distanza come parametri di base. Alcuni possono utilizzare un cut-off tale che deve essersi verificata un'esposizione a meno di due metri per più di 15 minuti mentre altri possono tenere conto di diverse combinazioni di tempo e distanza, esposizione cumulativa e altri parametri come l'insorgenza dei sintomi a calcolare un punteggio di rischio. Si consiglia di scambiare informazioni tra le app in modo da consentire l'esecuzione di diversi tipi di calcoli del rischio. Tali informazioni includerebbero il tempo e la distanza delle esposizioni, comprese quelle di breve durata come cinque minuti (o meno, se del caso). Vi sono alcune considerazioni operative aggiuntive relative al viaggio. Scenario di esempio: un cittadino e un utente dell'app dal Paese A (utente A) si recano nel Paese B per un periodo di tempo. Quando si trova nel paese B, entra in contatto con un cittadino del paese B (utente B) che in seguito risulta positivo. L'utente A riceverà una notifica. Se l'utente A si trova ancora nel paese B in quel momento, le autorità sanitarie pubbliche devono considerare da quale paese / i dovrebbe ricevere la notifica. Il modo più semplice sarebbe quello di ricevere la notifica attraverso la propria app dal Paese A. Le informazioni saranno nella lingua (e) che capisce e da un'autorità fidata. Tuttavia, potrebbe non disporre di informazioni localmente appropriate. Le autorità sanitarie pubbliche potrebbero anche prendere in considerazione la possibilità di collaborare con gli sviluppatori di app per consentire di adattare i consigli di conseguenza, ad esempio fornendo un numero di follow-up da chiamare rilevante per il Paese di visita" in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.8.

[60] Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies in https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154.

[61] Cfr. European Data Protection Board, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 21 April 2020 in https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en.

dati sanitari ai fini della ricerca scientifica, che si applicano anche nel contesto della pandemia di COVID-19, in particolare per quanto riguarda il consenso e le rispettive legislazioni nazionali. Il GDPR prevede la possibilità di elaborare determinate categorie speciali di dati personali, come i dati sanitari, laddove sia necessario per scopi di ricerca scientifica.

Inoltre, le linee guida affrontano questioni legali relative ai trasferimenti internazionali di dati che coinvolgono dati sanitari a fini di ricerca relativi alla lotta contro COVID-19, in particolare in assenza di una decisione di adeguatezza o di altre garanzie appropriate.

Le "linee guida sulla geo-localizzazione e altri strumenti di tracciamento nel contesto dell'epidemia COVID-19" [62] mirano a chiarire le condizioni e i principi per l'uso proporzionato dei dati di localizzazione e degli strumenti di tracciamento dei contatti, per due scopi specifici:

1. utilizzare i dati di localizzazione per supportare la risposta alla pandemia modellando la diffusione del virus al fine di valutare l'efficacia complessiva delle misure di confinamento;

2. utilizzare il tracciamento dei contatti, che ha lo scopo di informare le persone che potrebbero essere state vicine a qualcuno che alla fine è stato confermato come portatore del virus, al fine di rompere le catene di contaminazione il prima possibile.

Le linee guida sottolineano che sia il GDPR che la Direttiva *ePrivacy* contengono disposizioni specifiche che consentono l'uso di dati anonimi o personali per supportare le autorità pubbliche e altri attori sia a livello nazionale che dell'UE nei loro sforzi per monitorare e contenere la diffusione di COVID-19. I principi generali di efficacia, necessità e proporzionalità devono guidare qualsiasi misura adottata dagli Stati membri o dalle istituzioni dell'UE che comporta il trattamento di dati personali per combattere COVID-19.

L'EDPB sostiene e sottolinea la posizione espressa nella sua lettera alla Commissione europea del 14 aprile[63] secondo cui l'uso delle app di tracciamento dei contatti dovrebbe essere volontario e non dovrebbe fare affidamento sulla traccia dei singoli movimenti, ma piuttosto sulle informazioni di prossimità riguardanti gli utenti.

La dott.ssa Jelinek ha aggiunto: "Le app non possono mai sostituire infermieri e medici. Sebbene i dati e la tecnologia possano essere strumenti importanti, dobbiamo tenere presente che hanno limiti intrinseci. Le App possono solo integrare l'efficacia delle misure di sanità pubblica e la dedizione degli operatori sanitari necessaria per combattere COVID-19. Ad ogni modo, le persone non dovrebbero essere messe di fronte a dover scegliere tra una risposta efficace alla crisi e la protezione dei diritti fondamentali".

In data 7 maggio 2020 l'Unità Tecnologie e Privacy del Garante europeo ha emanato il "documento tecnico 1/2020 sul tracciamento dei contatti con Applicazioni Mobili"[64]. Esso "ha lo scopo di fornire una descrizione fattuale di una tecnologia emergente e discutere i suoi possibili impatti sulla privacy e sulla protezione dei dati personali. I contenuti di questa pubblicazione non implicano una posizione politica del GEPD". In realtà, contiene una serie di dettagli tecnici molto importanti, ad.es.:

√ *Tracciamento di prossimità digitale*

Per supportare e integrare il tracciamento tradizionale, potrebbero essere utilizzati i

---

[62] Cfr. European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, 21 April 2020 in https://edpb.europa.eu/our-work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_en.

[63] Cfr. European Data Protection Board, Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic, 14 April 2020 in https://edpb.europa.eu/news/news/2020/twenty-first-plenary-session-european-data-protection-board-letter-concerning_it.

[64] European Data Protection Supervisor, TechDispatch #1/2020: Contact Tracing with Mobile Applications, 7 May 2020, in https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en.

sensori di onde radio integrati: lo *smartphone* potrebbe essere utilizzato, con l'installazione di un'applicazione dedicata e/o l'aggiornamento del software del sistema operativo[65], per registrare quando due persone sono abbastanza vicine per un tempo sufficientemente lungo affinché esista un rischio elevato di contagio.

√ *Quali sono le implicazioni sulla protezione dei dati?*

Il tracciamento dei contatti di prossimità sia tradizionale che digitale comporta il trattamento di dati personali. Laddove i dati si riferiscono a persone infette, si tratta di dati sanitari che richiedono una protezione speciale.

√ *Sorveglianza su larga scala*

Il tracciamento di prossimità digitale comporta nuovi rischi per la protezione dei dati in quanto prevede la registrazione preventiva e per contatto di un numero molto elevato di popolazione negli spazi pubblici e privati utilizzando segnali di onde radio.

È quindi probabile che le applicazioni di tracciamento dei contatti comportino un rischio elevato per i diritti e le libertà delle persone fisiche e richiedano una valutazione dell'impatto sulla protezione dei dati da condurre prima del loro spiegamento.

√ *Identificazione dell'utente*

I contatti di un caso possono includere familiari, vicini o colleghi di lavoro. Collegato ad altri dati, ad es. dai social network, è tecnicamente possibile risalire al nome della persona infetta, il luogo di residenza e di lavoro e una serie di altre attività e potenzialmente la sua posizione. Il numero di contatti e la loro frequenza possono persino rivelare abitudini sociali, come le pratiche religiose. Il collegamento con i dati sulla posizione, come accade con la traccia basata sul GPS, potrebbe consentire di dedurre un'immagine dettagliata della routine quotidiana.

Le tecnologie di minimizzazione dei dati e di miglioramento della privacy possono quindi prevenire danni attraverso l'identificazione di contatti e casi infetti.

Poiché le App di tracciamento possono funzionare senza l'identificazione diretta dei loro utenti, è necessario adottare misure appropriate per prevenire la re-identificazione. Ad es., poiché i dati sulla posizione sono inclini alla re-identificazione, è meglio evitare la traccia basata sulla posizione. Le applicazioni per *smartphone* di tracciamento di prossimità digitale non richiedono il monitoraggio della posizione dei singoli utenti. Invece, dovrebbero essere utilizzati i dati di prossimità, in particolare ottenuti tramite Bluetooth BLE (*ut supra*).

Le App di tracciamento possono utilizzare identificatori pseudonimizzati per i contatti di prossimità e modificarli periodicamente, ad esempio ogni 30 minuti. Ciò riduce il rischio di collegamento e re-identificazione dei dati. Gli schemi di condivisione segreti consentono di dividere gli identificatori in parti e di diffondere la loro trasmissione in un determinato periodo di tempo. Eventuali attaccanti che tentassero di rivelare e mappare i contatti dovrebbero attendere per ricevere il numero minimo di parti necessarie per riassemblare nuovamente l'identificatore.

Il servizio che fornisce test e conferma dello stato di infezione può operare indipendentemente dal servizio centrale al quale i casi caricano i dati di tracciamento dei contatti per impedire il collegamento dei dati di tracciamento ai file dei casi medici. Per garantire comunque che i dati vengano caricati solo da casi confermati, il servizio centrale potrebbe richiedere una prova digitale.

√ *Limitazioni delle finalità*

E' necessario determinare in anticipo per quali scopi specifici (come il tracciamento dei contatti e/o la ricerca scientifica) i dati personali possono essere utilizzati, da chi e per quanto tempo possono essere conservati.

[65] Come infatti sta avvenendo in tutte le app sia in corso di realizzazione che operanti in vari Paesi.

- √ Una volta che l'epidemia si è fermata e le applicazioni di tracciamento dei contatti non sono più necessarie, è necessario predisporre una procedura per arrestare la raccolta di identificativi (disattivazione globale dell'applicazione, istruzioni per disinstallare l'applicazione, disinstallazione automatica, ecc.) Ed eliminare tutti i dati raccolti da tutti i database (applicazioni e server mobili).
- √ *Mancanza di trasparenza*

Le App di tracciamento possono raggiungere la loro massima efficienza solo se utilizzate dalla quota più ampia possibile della popolazione. La mancanza di spiegazioni su come funzionano le App di tracciamento e su come proteggono la privacy dell'utente potrebbe creare una mancanza di fiducia. Pertanto l'uso delle App di tracciamento dovrebbe essere volontario e trasparente per l'utente. Le informazioni raccolte dovrebbero risiedere sullo *smartphone* dell'utente.

- √ Per consentire a tutti gli attori coinvolti nello sviluppo e nel funzionamento delle App di tracciamento dei contatti di aderire sin dall'inizio alle leggi sulla protezione dei dati dell'UE, l'European Data Protection Board (2020) e l'European Commmission (2020) hanno pubblicato linee guida dettagliate cui attenersi.

2. Razionale scientifico e richiami tecnici.

I dettagli biologici della trasmissione del virus sono noti in termini generali: questi virus possono passare da un individuo all'altro attraverso quattro diversi percorsi di trasmissione che sono strettamente allineati alle loro implicazioni per la prevenzione:

I. *sintomatica*: diretta da un individuo sintomatico, attraverso un contatto che può essere facilmente ricostruito dal destinatario.

II. *pre-sintomatica*: diretta da un individuo che si verifica prima che l'individuo di origine manifesti sintomi evidenti.

III. *asintomatica*: diretta da individui che non manifestano mai sintomi evidenti. Ciò può essere stabilito solo dal follow-up, poiché l'osservazione di un singolo punto temporale non può distinguere completamente gli individui asintomatici da quelli pre-sintomatici.

IV. *ambientale*: tramite contaminazione, e in particolare in un modo che non sarebbe tipicamente attribuibile al contatto con la fonte in una ricognizione dei contatti (vale a dire, ciò non include le coppie di trasmissione che erano in stretto contatto, ma per chi in realtà il contagio passa attraverso l'ambiente anziché più direttamente). Questi potrebbero essere identificati in un'analisi dei movimenti spaziali.

Nel Paese in cui l'epidemia ha avuto inizio, la Cina, la lotta al Coronavirus è stata portata avanti attraverso misure di contenimento "draconiane", a partire dalla quarantena totale della città di Wuhan (con quasi 15 milioni di abitanti) e dal blocco di ogni forma di trasporto anche negli altri centri principali dello Hubei. In parallelo, il governo ha realizzato una campagna per identificare i cittadini affetti da Covid-19, attraverso un'App in grado di valutare il rischio delle persone assegnando ad ogni cittadino un diverso grado di pericolosità epidemica: una volta immessi alcuni dati, il sistema è in grado di tracciare gli spostamenti e gli incontri delle persone e assegna un codice (verde, giallo o rosso) a seconda del proprio stato di salute o rischio di infezione. Le persone non possono muoversi senza mostrare prima il codice memorizzato sull'App. Il timore è però che, superata la fase di emergenza, determinati strumenti tra cui anche i software di riconoscimento facciale, non vengano abbandonati[66].

Anche la Corea del Sud è riuscita ad ottenere risultati molto positivi grazie a diverse

[66] Cfr. L. Kuo, 'The new normal': China's excessive coronavirus public monitoring could be here to stay', The Guardian, 9 Mar 2020 in https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

applicazioni mobili, tra cui "Corona 100M", in grado di geo-localizzare gli utenti, avvisando se nel raggio di 100 metri dalla loro posizione si sia precedentemente registrata la presenza di persone contagiate da Covid-19 e in quale data[67].

Lo schema tipo di questa impostazione è il seguente:

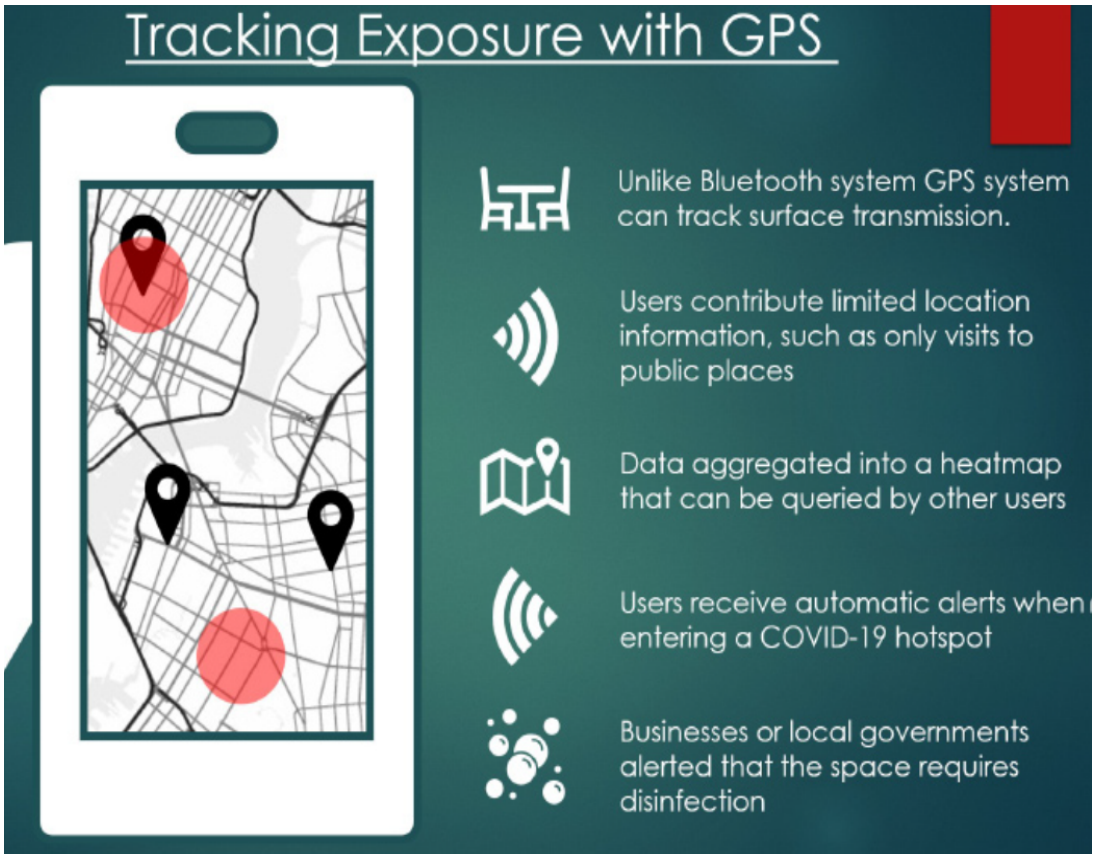


Figura 3: Metodi di tracciamento dell'esposizione con GPS (Credit: M Eifler).

Secondo qualche commentatore "si tratta, in sostanza, di un'opera ben strutturata di 'spionaggio' a tappeto degli individui realizzata grazie alla combinazione dei dati di geo-localizzazione dell'oltre un milione di utenti che ha effettuato il download dell'App, con quelli forniti dal governo"[68].

Invece di pensare a un *lockdown* di proporzioni nazionali, la Corea ha invece agito sul fronte tecnologico, attraverso la tempestiva individuazione dei soggetti positivi e la ricostruzione dei loro spostamenti. "A farne le spese la privacy, certo, ed è per questo che le misure di contenimento del virus messe in campo da Seul, in Europa hanno fatto discutere"[69].

Naturalmente, simili misure sono "agli antipodi di quanto previsto dalla normativa europea in materia di protezione e circolazione dei dati, poiché comportano un controllo 'assoluto', da parte dello Stato, dei dati personali dei cittadini – inclusi, in particolare, i dati relativi alla salute – fatti confluire in un database centralizzato e resi, in parte, accessibili agli utilizzatori delle App"[70].

---

[67] Cfr. A. Lisi, 'Coronavirus: lockdown vs. download. La privacy alla radice del contrasto della pandemia' | L'HuffPost online, 17/03/2020.
[68] Ibidem.
[69] Ibidem.
[70] Ibidem.

Tecnicamente il concetto di tracciamento dei contatti è abbastanza semplice[71]: quando si scopre che qualcuno è stato infettato da un determinato agente patogeno, si tenta di trovare tutti coloro con cui quella persona potrebbe avere avuto un contatto mentre la persona era infettiva[72]. Qualcuno infetto fornisce agli "investigatori"- che potrebbero essere medici, infermieri, volontari o studenti in medicina e infermieristica - un elenco di persone con cui è stato in contatto per un determinato periodo di tempo, di solito circa una finestra di otto giorni prima e dopo di quando hanno iniziato a mostrare sintomi. I Centri per il controllo e la prevenzione delle malattie (CDC) definiscono il "contatto" in questo caso come avvenuto a una distanza di 1,8 metri circa o meno, per 10 o più minuti[73].

Riferendosi a questa persona come caso-indice, l'App conterrebbe anche un "diario clinico" per la *early detection*, al fine di individuare precocemente le infezioni[74].

La condivisione dei dati da parte delle società tecnologiche sta aiutando i governi a combattere la vertiginosa diffusione del coronavirus monitorando il rispetto delle distanze sociali e degli ordini di restare in casa[75]. "Esiste un comprensibile desiderio di mettere insieme tutti gli strumenti a nostra disposizione per aiutare a far fronte alla pandemia", ha affermato Michael Kleinman, direttore della Silicon Valley Initiative di Amnesty International. "Tuttavia, gli sforzi dei paesi per contenere il virus non devono essere usati come una scusa per creare un sistema di sorveglianza digitale notevolmente ampliato e più intrusivo[76]".

In realtà, nuove pratiche di condivisione dei dati stanno avvenendo a molti livelli.

Google[77]ha annunciato che rilascerà nuovi dati su come la pandemia ha ridotto il traffico

---

[71] Cfr. B. Y. Lee, 'To Help Stop COVID-19 Coronavirus, What Is Contact Tracing, How Do You Do It', Apr 17, 2020 in https://www.forbes.com/sites/brucelee/2020/04/17/what-is-contact-tracing-why-is-it-key-to-stop-covid-19-coronavirus/.

[72] Tra i parametri più importanti, vi sono A) "Come le app determinano il rischio: a seconda del design dell'app, potrebbe essere possibile programmare un cut-off definito, ad esempio tutti i contatti che soddisfano le definizioni di esposizione a meno di due metri per più di 15 minuti vengono avvisati. Alcune app consentono anche di calcolare un punteggio di rischio totale in base a diverse combinazioni di tempo e distanza, in modo che un'esposizione inferiore a 15 minuti ma a distanza molto ravvicinata possa comunque attivare una notifica. Potrebbe anche esserci la possibilità di includere altri parametri per calcolare il rischio, ad esempio il giorno in cui si è verificato il contatto relativamente all'insorgenza dei sintomi nel caso. Il risultato di tale calcolo del rischio sarebbe un punteggio di rischio totale. Determinare quale sarebbe un limite adeguato per la notifica alle persone di contatto richiederà una valutazione e una calibrazione. B) Considerazioni sulla determinazione delle impostazioni: le autorità sanitarie pubbliche devono garantire che le impostazioni di tempo e distanza siano sufficientemente ampie da "catturare" i contatti più a rischio. Tuttavia, se le impostazioni sono tali che un gran numero di persone viene indicato come "contatti" e gli viene chiesto di adottare misure come l'auto-quarantena, ciò potrebbe comportare un onere per gli individui e la società e nel tempo probabilmente ridurrà l'accettabilità e l'adozione dell'app. A seconda dell'intensità del follow-up dei contatti, un gran numero di contatti aggiuntivi tracciati attraverso le app potrebbe poi comportare un onere per le autorità sanitarie pubbliche" in European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag.8.

[73] Cfr. anche "indagano sui contatti di Bob se hanno trascorso oltre 15 minuti insieme entro 2 metri" in T. Pueyo, 'Coronavirus: How to Do Testing and Contact Tracing', Medium 28/4/2020 in https://medium.com/@tomaspueyo/coronavirus-how-to-do-testing-and-contact-tracing-bde85b64072e, pag. 17.

[74] Cfr. A. Rahinò, 'App per tracciare i contagi: tra diritto alla salute e diritto alla privacy', 26 Marzo 2020 in https://studiolegalelisi.it/approfondimenti/app-per-tracciare-i-contagi-tra-diritto-alla-salute-e-diritto-alla-privacy/.

[75] Cfr. B. Brody, N. Nix, 'Pandemic Data-Sharing Puts New Pressure on Privacy Protections', Bloomberg Technology, 5 aprile 2020 in https://www.bloomberg.com/news/articles/2020-04-05/pandemic-data-sharing-puts-new-pressure-on-privacy-protections?srnd=technology.

[76] Ibidem.

[77] Cfr. N. Lomas, 'Google is now publishing coronavirus mobility reports, feeding off users' location history', Techcrunch, 03/04/2020 in https://techcrunch.com/2020/04/03/google-is-now-publishing-coronavirus-mobility-reports-feeding-off-users-location-history/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8 &guce .

pedonale verso centri di transito, negozi al dettaglio e parchi pubblici in oltre 130 paesi. La società ha dichiarato di rispondere alle richieste di funzionari della sanità pubblica che vogliono sapere come le persone si spostano in città come un modo per combattere meglio la diffusione di Covid-19, la malattia causata dal virus. Google ha ribadito che, nei suoi rapporti sulla mobilità, utilizza dati anonimizzati e aggregati[78].

Apple Inc. ha lanciato la sua iniziativa[79] quando ha annunciato che "Apple ha rilasciato oggi uno strumento di tendenze dei dati sulla mobilità da Apple Maps per supportare il lavoro di impatto in corso in tutto il mondo per mitigare la diffusione di COVID-19. Questi dati sulla mobilità possono fornire utili spunti ai governi locali e alle autorità sanitarie e possono anche essere utilizzati come base per nuove politiche pubbliche mostrando il cambiamento nel volume delle persone che guidano, camminano o prendono il trasporto pubblico nelle loro comunità.

Maps non associa i dati di mobilità all'ID Apple di un utente e Apple non conserva una cronologia della posizione dell'utente. Utilizzando i dati aggregati raccolti da Apple Maps, il nuovo sito Web indica le tendenze di mobilità per le principali città e 63 Paesi o regioni. Le informazioni vengono generate contando il numero di richieste fatte ad Apple Maps per le indicazioni. I set di dati vengono quindi confrontati per riflettere un cambiamento nel volume di persone che guidano, camminano o prendono il trasporto pubblico in tutto il mondo. La disponibilità dei dati in una particolare città, paese o regione è soggetta a una serie di fattori, tra cui le soglie minime per le richieste di direzione effettuate ogni giorno.

Apple ha integrato la privacy nel nucleo di Maps sin dall'inizio. I dati raccolti da Maps, come i termini di ricerca, il percorso di navigazione e le informazioni sul traffico, sono associati a identificatori casuali e rotanti che si ripristinano continuamente, quindi Apple non ha un profilo dei tuoi movimenti e ricerche. Ciò consente a Maps di offrire un'esperienza eccezionale, proteggendo al contempo la privacy degli utenti".

Restano però indispensabili due cautele:

1) "l'importanza di applicare misure adeguate per garantire la trasmissione sicura dei dati dai fornitori di telecomunicazioni. Sarebbe inoltre preferibile limitare l'accesso ai dati agli esperti autorizzati in epidemiologia spaziale, protezione dei dati e scienza dei dati"[80].
2) "La necessità di una pronta distruzione dei set di dati al termine dell'emergenza - è un altro elemento chiave della *guidance* tecnica[81].

---

[78] Su https://www.google.com/covid19/mobility/ si legge infatti che "I rapporti sugli spostamenti della comunità sono stati sviluppati in modo da fornire informazioni utili in conformità con i nostri rigidi protocolli sulla privacy e nel rispetto della privacy degli utenti. In nessun caso vengono messe a disposizione informazioni che consentono l'identificazione personale quali posizione, contatti o spostamenti di un individuo. Le informazioni presenti in questi rapporti sono basate su set di dati aggregati e anonimizzati degli utenti che hanno attivato l'impostazione Cronologia delle posizioni, che è disattivata per impostazione predefinita. Gli utenti che hanno attivato la Cronologia delle posizioni possono decidere di disattivarla in qualsiasi momento dal proprio Account Google e possono sempre eliminare i dati della Cronologia delle posizioni dalla sezione Spostamenti. Usiamo inoltre la stessa tecnologia di anonimizzazione di altissimo livello usata quotidianamente nei nostri prodotti per mantenere privati e protetti i dati relativi alle tue attività". Infine, "questi rapporti saranno disponibili per un periodo di tempo limitato, ossia finché i funzionari della sanità pubblica li riterranno utili per la loro attività finalizzata ad arrestare la diffusione della malattia COVID-19".

[79] Cfr. Apple Newsroom, 'Apple makes mobility data available to aid COVID-19 efforts', April 14, 2020 in https://www.apple.com/newsroom/2020/04/apple-makes-mobility-data-available-to-aid-covid-19-efforts/.

[80] Cfr. N. Lomas, 'Telco metadata grab is for modelling COVID-19 spread, not tracking citizens, says EC', Techcrunch, March 27, 2020 in https://techcrunch.com/2020/03/27/telco-metadata-grab-is-for-modelling-covid-19-spread-not-tracking-citizens-says-ec/.

[81] Ibidem.

3. Centralizzazione vs. Decentralizzazione di dati e Informazioni: differenze e conseguenze su *data protection* e privacy.

Abbiamo visto come la Commissione Europea abbia chiesto un approccio comune dell'UE per rafforzare l'efficacia degli interventi digitali e garantire il rispetto dei diritti e delle libertà chiave[82].

L'organo esecutivo dell'Unione europea vuole infatti garantire che gli sforzi individuali degli Stati membri per utilizzare i dati e gli strumenti tecnologici nella lotta al COVID-19 siano allineati e 'interoperabili' e quindi essere più efficaci, dato che il virus non rispetta i confini nazionali.

Allo stesso tempo, la sua raccomandazione[83] pone un forte accento sulla necessità di garantire che i diritti fondamentali dell'UE non vengano superati nella corsa per mitigare la diffusione del virus, con la Commissione che esorta le autorità di sanità pubblica e gli istituti di ricerca a osservare il principio di minimizzazione dei dati durante l'elaborazione di dati personali per la lotta al coronavirus. In particolare, scrive che tali organismi dovrebbero applicare quelle che definisce "garanzie appropriate", elencando la pseudonimizzazione, l'aggregazione, la crittografia e il decentramento come esempi di buone pratiche.

Concettualmente, ma anche per i risvolti pratici, nell'approccio verso le App di tracciamento dei contatti del coronavirus un forte "scisma" sta continuando a dividere l'Europa[84], dove il principale punto di contesa tra i gruppi è: centralizzazione vs decentralizzazione.

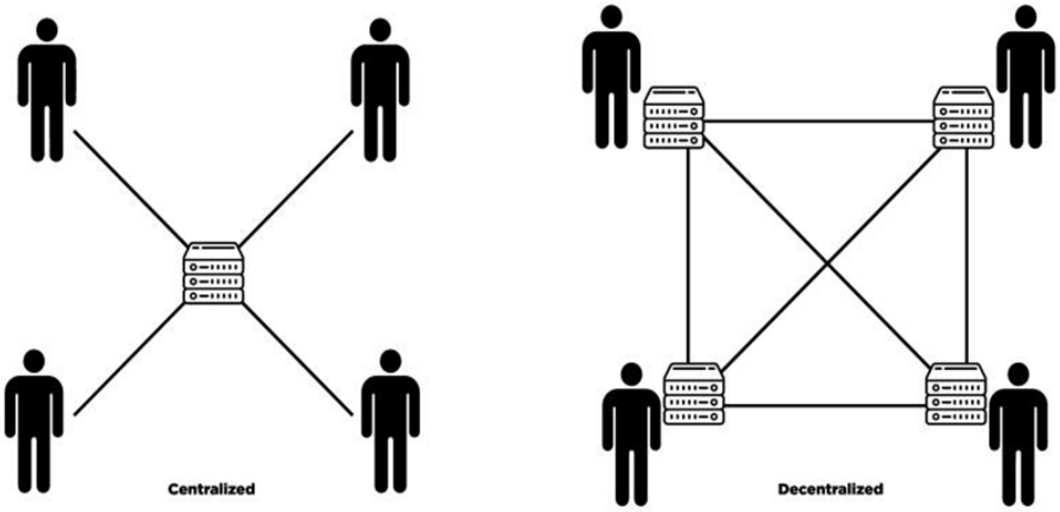


Figura 4: Impostazione centralizzata oppure decentralizzata.

Verso il lato del primo *framework* c'è un consorzio di accademici e parti interessate della *business community* che convergono sotto l'ombrello PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing). Questo gruppo ha creato una cosiddetta soluzione di

[82] Si veda anche N. Lomas, 'Call for common EU approach to apps and data to fight COVID-19 and protect citizens' rights', April 8, 2020 in https://techcrunch.com/2020/04/08/call-for-common-eu-approach-to-apps-and-data-to-fight-covid-19-and-protect-citizens-rights/.

[83] Cfr. European Commision, Recommendation C(2020) 2296 of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, cit..

[84] Cfr. L. Clarke, 'PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear', 20 /04/ 2020 in https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear.

tracciamento dei contatti Covid-19 "*privacy preserving*", in quanto "PEPP-PR è stato esplicitamente creato per aderire ai forti leggi e principi europei in materia di privacy e protezione dei dati", scrive il gruppo in un manifesto online[85] e uno dei suoi membri, Christophe Fraser, professore presso il Dipartimento di Medicina di Nuffield presso l'Università di Oxford, è anche coinvolto nello sviluppo dell'app NHSX del governo britannico.

Dall'altro lato c'è DP-3T[86], un gruppo di accademici attenti alla privacy che ha sviluppato una soluzione totalmente decentralizzata per il tracciamento dei contatti del coronavirus che conserva i dati sui portatili, piuttosto che inviarli a un database centralizzato gestito, ad esempio , dal servizio sanitario di un paese.

Verso la decentralizzazione sono anche Apple e Google che stanno collaborando (cfr. anche *supra*) allo sviluppo di un sistema decentralizzato per la ricerca dei contatti che potrà funzionare ininterrottamente utilizzando il *bluetooth* sui telefoni Apple e Android. Invece per le App centralizzate in grado di funzionare continuamente, un telefono dovrebbe essere lasciato sbloccato in ogni momento .

PEPP-PT ha suscitato critiche sulla sua mancanza di trasparenza e poi sono iniziate le defezioni: il professore EPFL Marcel Salathé si è dimesso dall'iniziativa, seguito rapidamente dagli istituti di ricerca KU Leuven, EPFL, ETH Zürich e CISPA. Tutti sono migrati sul progetto DP-3T.

Intanto PEPP ha pubblicato[87] su Github vari documenti sulla "architettura di protezione dei dati e sicurezza delle informazioni" per l'implementazione tedesca di PEPP-PT, che hanno chiamato NTK: l'App funziona utilizzando la funzione *Bluetooth Low Energy* (BLE) (*ut supra*) di uno *smartphone* per monitorare la vicinanza di altri telefoni. Se un utente inserisce una diagnosi di Covid-19, l'App scorre l'elenco dei contatti del telefono nelle ultime tre settimane e valuta per ciascuno un "punteggio di rischio" in base al grado e alla durata della prossimità, nonché ad altre popolazioni fattori epidemiologici di livello. Per quelli ritenuti a rischio, una notifica *push* li informa della necessità di autoisolarsi.

In termini di privacy, l'App assegna a ciascun portatile un identificatore persistente (PUID) che viene utilizzato per creare "ID effimeri"(EBID) per il portatile che cambiano periodicamente. Questi vengono creati crittografando il PUID con una chiave di trasmissione globale che viene rinnovata periodicamente. Dopo quattro settimane, la chiave viene eliminata. Sono gli EBID effimeri che vengono trasmessi dal telefono e gli EBID di altri telefoni nelle immediate vicinanze che vengono registrati. Una volta diagnosticato un paziente, con il consenso e l'autorizzazione del paziente da parte di un'autorità sanitaria, l'App carica sul server tutti gli EBID registrati nelle tre settimane precedenti, insieme all'ora del contatto, ai metadati[88] *Bluetooth* e ad altre informazioni. Il server back-end utilizza quindi le

---

[85] Pan European Privacy Protecting Proximity Tracing (PEPP-PT), 'Context and Mission' in https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf.

[86] Cfr. N. Lomas, 'EU privacy experts push a decentralized approach to COVID-19 contacts tracing', Techcrunch, April 6, 2020 in https://techcrunch.com/2020/04/06/eu-privacy-experts-push-a-decentralized-approach-to-covid-19-contacts-tracing/.

[87] Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) on Github in https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany. pdf.

[88] "I metadati sono dati sui dati. In altre parole, sono le informazioni utilizzate per descrivere i dati contenuti in qualcosa come una pagina Web, un documento o un file. Un altro modo di pensare ai metadati è come una breve spiegazione o un riassunto di quali siano i dati. Un semplice esempio di metadati per un documento potrebbe includere una raccolta di informazioni come l'autore, le dimensioni del file, la data di creazione del documento e le parole chiave per descriverlo" come si legge*, inter alia*, in M. Chapple, 'What Is Metadata? Metadata is critically important for website and database management', Lifewire, January 04, 2020 in https://www.lifewire.com/metadata-definition-and-examples-1019177.

chiavi di trasmissione globali per decrittografare gli EBID, rivelando il PUID (e quindi l'identità pseudonimizzata) di tutti i dispositivi vicini alla persona infetta nell'intervallo di date specificato.

Il gruppo DP-3T ha pubblicato rapidamente un'analisi di sicurezza e privacy del documento di PEPP-PT, in cui rileva un paio di importanti divergenze nel modo in cui funzionano i due sistemi. In particolare, su DP-3T, il calcolo del rischio viene eseguito sul telefono dell'utente dell'App, anziché dal server, il che significa che i dati non devono lasciare il telefono dell'utente. In termini di problemi di privacy, DP-3T ha messo in evidenza il potenziale per il 'creep funzionale' (*function creep*[89]): ad es., se il database viene violato, l'anonimato fornito dalla rotazione degli pseudonimi viene annullato e gli individui possono essere rintracciati più facilmente. Inoltre non si può escludere il rischio di 'sorveglianza' statale.

L'analisi di DP-3T afferma infatti che, poiché l'utente *backend* crea gli identificatori effimeri, il server backend può collegare qualsiasi identificatore passato o futuro (EBID) con l'identificatore permanente (PUID). Ciò significa che il server back-end può identificare qualsiasi individuo specifico e pseudonimo. Con una piccola quantità di dati aggiuntivi –viene utilizzato l'esempio di filmati CCTV o dati di carte di viaggio intelligenti - l'identità dell'individuo potrebbe essere rivelata. Secondo il gruppo quindi esiste un elevato potenziale per il '*creep* funzionale' e la trasformazione di uno strumento di tracciamento dei contatti del coronavirus in uno strumento di sorveglianza. Il documento afferma anche che dato un EBID target (ad esempio uno raccolto dalle forze dell'ordine o in un punto di controllo del passaporto), i movimenti di un utente specifico potrebbero essere rintracciati senza accesso al database.

L'analisi sostiene inoltre che il design centralizzato di NTK consente al back-end di apprendere l'intero grafico di contatto di un individuo infetto, nonché gli incontri tra individui non infetti. Sostiene che ciò viola il principio di minimizzazione dei dati del GDPR in quanto il server back-end ha accesso a più informazioni di quelle necessarie.

Come accennavo, un altro gruppo di esperti europei in materia di privacy ha proposto un sistema decentralizzato per la tracciabilità dei contatti COVID-19 basato su Bluetooth che secondo loro offre una maggiore protezione contro l'abuso dei dati.

Il protocollo Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) (cioé 'tracciamento di prossimità decentralizzato che preserva la privacy), è stato progettato da circa 25 accademici di almeno sette istituti di ricerca in Europa, tra cui l'Istituto Federale Svizzero di Tecnologia, ETH Zurigo e KU Leuven in Belgio.

Come si legge nel 'Libro bianco' che hanno pubblicato[90], l'elemento chiave è che il design prevede l'elaborazione locale della traccia e del rischio dei contatti sul dispositivo dell'utente, in base ai dispositivi che generano e condividono identificatori Bluetooth effimeri ("EphID"), come schematizzato nella seguente infografica[91]:

---

[89] "Il *'function creep*' si verifica quando le informazioni vengono utilizzate per uno scopo che non è lo scopo originale specificato. Ad esempio, un datore di lavoro può installare un sistema di sicurezza che richiede ai dipendenti di accedere o disconnettersi dal luogo di lavoro, allo scopo di impedire l'accesso non autorizzato. Tuttavia, l' organizzazione potrebbe finire per utilizzare queste informazioni sui singoli dipendenti per tenere traccia delle presenze. Questa potrebbe essere una violazione della privacy se ad es., l'organizzazione raccoglie le informazioni per tracciare la presenza dei dipendenti senza informarli dello scopo per il quale le informazioni vengono raccolte", come si legge in S. Young, 'Technology and function creep', February 22, 2018 in https://oipc.sk.ca/technology-and-function-creep-2/.

[90] Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) on Github in https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

[91] L"infografica originale '*Engagement Comic*' è in https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon. Questa è la versione italiana, realizzata da S. Guida e R. Serpe (*Founder* e *Co-Founder*,

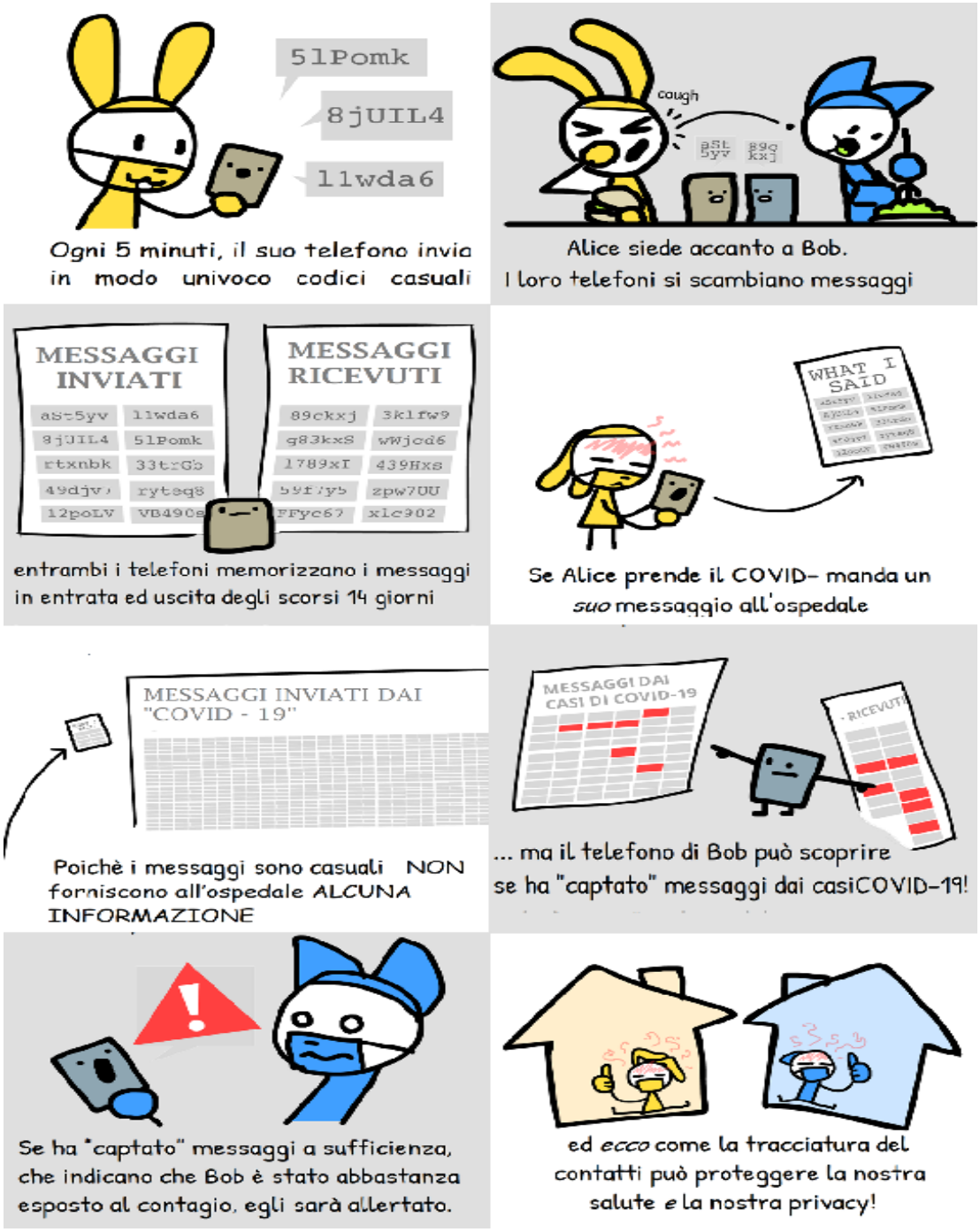


Figura 5: infografica che spiega al pubblico come funziona DP-3T (Credit: Nicky Case).

Un server back-end viene utilizzato per inviare i dati ai dispositivi, ad esempio quando una persona infetta viene diagnosticata con COVID-19, un'autorità sanitaria sancisce il caricamento dal dispositivo della persona di una 'rappresentazione compatta' (lista) di EphID nel periodo infettivo che verrebbe inviato ad altri dispositivi in modo che possano calcolare

nell'ambito della *pre-marketing strategy* relativa al progetto di 'Startup innovativa Legal Design IT Lab'), approvata e archiviata in https://github.com/DP-3T/documents/tree/master/public_engagement/cartoon/it/version_c.

localmente se esiste un rischio e avvisare l'utente di conseguenza.

In base a questo *framework* non è necessario centralizzare gli ID pseudonimizzati, in cui i dati aggregati costituirebbero un rischio per la privacy. Il che a sua volta dovrebbe rendere più semplice persuadere i cittadini dell'UE a fidarsi del sistema - e scaricare volontariamente l'app di tracciamento dei contatti utilizzando questo protocollo - dato che è progettato per resistere a eventuale riutilizzo per ipotetica 'sorveglianza' statale a livello individuale.

Il gruppo discute alcune altre potenziali minacce - come quelle poste da utenti esperti di tecnologia che potrebbero intercettare i dati scambiati localmente e decompilare / ricompilare l'app per modificare elementi - ma la tesi generale è che tali rischi sono piccoli e più gestibili rispetto alla creazione di *database* centralizzati di dati che rischiano di spianare la strada al "*creep* di sorveglianza" (*surveillance creep*)[92], vale a dire ove mai qualche Stato pensasse di utilizzare una crisi di salute pubblica come un'opportunità per creare e conservare l'infrastruttura di localizzazione a livello di cittadino.

Anche (e forse proprio per questo) la DP-PPT è stata progettata pensando allo smantellamento totale, una volta terminata la crisi della salute pubblica.

"Il nostro protocollo è una dimostrazione del fatto che sono possibili approcci rispettosi della tutela della privacy al tracciamento di prossimità e che paesi o organizzazioni non devono accettare metodi che supportano il rischio e l'uso improprio". "Laddove la legge richiede rigorose necessità e proporzionalità e il supporto della società sostiene il 'tracciamento di prossimità', questo design decentralizzato offre un modo resistente agli abusi per realizzarlo"[93].

Infine, il metodo decentralizzato (DP-3T) si adatta meglio al modello di protezione dei dati dell'UE anche con riferimento all'interoperabilità, come accennato: "i telefoni di utenti che visitano paesi stranieri, sia per lavoro che per svago, deve essere in grado di catturare i beacon dagli utenti nei paesi che visitano e includere i beacon dei pazienti con diagnosi COVID-19 in quei paesi nel loro calcolo dell'esposizione. Allo stesso modo, i residenti di un paese devono essere in grado di ricevere notifiche se a un visitatore del loro paese viene diagnosticata la COVID-19". "Tutti e tre i progetti proposti supportano l'interoperabilità tra. L'interoperabilità è possibile purché diversi operatori di diverse regioni utilizzino uno dei progetti decentralizzati proposti in questo documento"[94].

Conclusions.

"La tecnologia non tiene lontano l'uomo dai grandi problemi della natura, ma lo costringe a studiarli approfonditamente, scriveva Antoine de Saint-Exupéry"[95].

In effetti, "analizzando le azioni dei paesi dove il contagio è stato efficacemente contenuto e quelle che pensano di mettere in campo altri paesi, si capisce che la tecnologia è la chiave per realizzare soluzioni che integrino sistema sanitario, forze dell'ordine e istituzioni"[96].

---

[92] Si parla di "*surveillance creep*, quando la sorveglianza sviluppata per uno scopo limitato, come combattere una pandemia o filmare le violazioni del traffico, viene utilizzata in modi sempre più pervasivi e permanenti", come si legge in R. A. Calvo, S. Deterding, R. M. Ryan, 'Health surveillance during covid-19 pandemic. How to safeguard autonomy and why it matters', 06 April 2020, *BMJ* 2020; 369 doi: https://doi.org/10.1136/bmj.m1373.

[93] Cfr. Decentralized Privacy-Preserving Proximity Tracing (DP-PPT) on Github in https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf, cit..

[94] Ibidem.

[95] Cfr. A. Rahinò, 'App per tracciare i contagi: tra diritto alla salute e diritto alla privacy', 26 Marzo 2020 in https://studiolegalelisi.it/approfondimenti/app-per-tracciare-i-contagi-tra-diritto-alla-salute-e-diritto-alla-privacy/, cit..

[96] Cfr. M. Proverbio, 'Privacy, salute e ripresa delle attività sociali e produttive: il bilanciamento efficace che serve' - Il Sole 24 ORE, 4/4/2020 in https://www.ilsole24ore.com/art/privacy-salute-e-ripresa-attivita-sociali-e-produttive-bilanciamento-efficace-che-serve-ADwPs3H.

Ma con tutta evidenza il tema relativo al tracciamento dei contatti in relazione al suo impatto sulla privacy e sulla protezione dei dati ha anche profonde implicazioni etiche.

Da un lato, le Linee guida ECDC parlano espressamente di "*Data altruism*": come si è visto "lo scopo principale delle app è di tracciare la prossimità e avvisare le persone che sono state in contatto con persone infette al fine di rompere le catene di trasmissione. (..) Gli sviluppatori di app possono abilitare un'opzione in cui gli utenti possono acconsentire a caricare ulteriori informazioni epidemiologicamente rilevanti relative a se stessi, ad esempio l'età, alle autorità sanitarie pubbliche. Gli utenti potrebbero essere più motivati a farlo se vengono informati che il caricamento di tali dati potrebbe consentire alle autorità sanitarie pubbliche di comprendere meglio la situazione epidemiologica nel paese e le dinamiche di trasmissione. Tali dati dovrebbero essere conservati per un periodo di tempo limitato in conformità con le normative locali e dovrebbero essere garantiti sicurezza e riservatezza. Le autorità sanitarie pubbliche dovrebbero essere consapevoli di come questa richiesta sarebbe percepita dalla popolazione e se rischi di limitare l'adozione dell'app"[97].

D'altronde, come è stato autorevolmente affermato [98], "stiamo entrando in aree inesplorate dell'etica digitale. La strada da percorrere potrebbe consistere nel progettare le giuste politiche che incentivano l'adozione dell'app (volontaria, obbligatoria o una combinazione delle due) e / o in una diversa architettura dell'app (ad es. Più centralizzata, utilizzando i dati GPS ecc.) e / o la natura dell'hardware richiesto (pensa a un tracker basato su Bluetooth economico e distribuito liberamente, come quelli che puoi collegare ai tuoi tasti per trovarli a casa) e / o come viene utilizzata l'app (pensa di un hub app, in grado di supportare un'intera famiglia attraverso un solo telefono cellulare, in connessione con altri tracker Bluetooth). Ma qualsiasi soluzione dovrebbe prendersi cura delle sue implicazioni etiche ed essere abbastanza flessibile da essere rapidamente migliorata, per correggere potenziali carenze e sfruttare nuove opportunità, man mano che le pandemie si sviluppano".

E ancora "Per una volta, il problema difficile è _non privacy_. Un'app basata su Bluetooth può utilizzare dati anonimi, registrati solo nel telefono cellulare, utilizzati esclusivamente per inviare avvisi in caso di contatto con persone infette, in modo non centralizzato. Non è facile ma è fattibile. Certo, è banalmente vero che ci sono e potrebbero esserci sempre problemi di privacy. Il punto è che, in questo caso, possono essere resi molto meno urgenti rispetto ad altri problemi. Tuttavia, una volta (o, se uno è più scettico di me, anche se), la privacy è curata, altre difficoltà etiche devono essere risolte. Riguardano l'efficacia e l'equità dell'app".

Una strategia molto positiva, ancor più perché in controtendenza in un mondo ormai pervaso dal «capitalismo di sorveglianza», in cui «un altro aspetto radicale riguarda la distribuzione dei diritti alla privacy e con essa la conoscenza e la scelta". (...) In realtà, privacy e segretezza non sono opposti ma piuttosto momenti di una sequenza» [99].

Ecco perché i regolatori hanno avvertito fortemente la necessità di porre limiti alla tecnica, quella che Shoshana Zuboff ha «chiamato la dimensione materiale di potere[100] in cui sistemi impersonali di disciplina e controllo producono una certa conoscenza del comportamento umano indipendentemente dal consenso». Perciò non posso che concordare *in toto* con il nostro Garante Privacy, quando afferma che[101]"se gestita con 'metodo democratico', anche

---

[97] Cfr. European Centre for Disease Prevention and Control, 'Mobile applications in support of contact tracing for COVID-19 - A guidance for EU/EEA Member States', 10 June 2020, cit., pag. 9.

[98] Cfr. L. Floridi, 'Mind the app - considerations on the ethical risks of COVID-19 apps', April 18, 2020 in https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html.

[99] Cfr.. S. Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization', in Journal of Information Technology (2015) 30 in , https://journals.sagepub.com/doi/10.1057/jit.2015.5, pag. 82.

[100] *Ibidem*, pag. 81.

[101] Cfr. A. Soro, Presidente del Garante per la protezione dei dati personali, 'Tracciamento contagi coronavirus, ecco i criteri da seguire', in Agenda Digitale, 29 marzo 2020, riportato su sito Garante [doc. web n. 9301470].

l'emergenza può risolversi in una parentesi destinata a lasciare inalterata- persino per certi versi più forte- la nostra democrazia. La chiave è nella proporzionalità, lungimiranza e ragionevolezza dell'intervento, oltre che naturalmente nella sua temporaneità. Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l'efficienza e la delega cieca all'algoritmo per la soluzione salvifica. Così, una volta cessata quest'emergenza, avremo anche forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell'uomo".