Quanto *Immuni*? Luci, ombre e penombre dell'app selezionata dal Governo italiano

Gabriele Della Morte[*]

SOMMARIO: 1. Introduzione e cenni metodologi. – 2. Sviluppo e approvazione dell'app *Immuni*. – 3. L'orientamento espresso da Commissione europea, Parlamento europeo, *European Data Protection Supervisor*, *European Data Protection Board*. – 4. I possibili modelli di tracciamento. – 5. (*segue*) l'accordo Apple-Google. – 6. Le tecnologie di contrasto all'epidemia adottate altrove. – 7. (*segue*) in ambito UE ed EFTA. – 8. (*segue*) in altre aree. – 9. Il funzionamento dell'app *Immuni.* – 10. Il fondamento giuridico. – 11. (*segue*) In particolare: il decreto-legge 30 aprile 2020, n. 28 e il documento relativo alla valutazione di impatto presentato dal Ministero della Salute e approvato dall'Autorità garante per la protezione dei dati personali il 1° giugno 2020. – 12. La conformità dell'app *Immuni* alla normativa internazionale in materia di dati personali. – 13. Le luci: quattro pregi dell'app *Immuni*. – 14. Le ombre: quattro criticità dell'app *Immuni*. – 15. Le penombre: conclusioni.

1. Introduzione e cenni metodologi

In seguito alla dichiarazione dello stato di pandemia da Covid-19 da parte dell'Organizzazione mondiale della sanità[1], è stata approntata, in diverse aree del mondo, una strategia di contrasto fondata sulle c.d. 'tre T': testare i potenziali infetti, tracciarne i contatti e trattarne i disagi (*Testing, Tracing, Treating*). Pertanto il tracciamento dei contatti (*Tracing*) è stato sin da subito identificato come una priorità da

[*] Professore associato di Diritto internazionale, Università Cattolica del Sacro Cuore (Milano), Facoltà di Giurisprudenza, Istituto di Studi Internazionali, Largo Gemelli, 1 – 20123 Milano gabriele.dellamorte@unicatt.it.

[1] «World Health Organization has been assessing this outbreak around the clock and we are deeply concerned both by the alarming levels of spread and severity, and by the alarming levels of inaction. We have therefore made the assessment that COVID-19 can be characterized as a pandemic. Pandemic is not a word to use lightly or carelessly […] we have called every day for countries to take urgent and aggressive action. We have rung the alarm bell loud and clear». Così l'*Opening Remarks* del Direttore dell'Organizzazione mondiale della sanità (OMS) al *media briefing* del 11 marzo 2020, consultabile su www.who.int. Sul ruolo dell'OMS nel corso della pandemia, v.: P. ACCONCI, "Prime considerazioni sull'effettività delle risposte normative dell'Organizzazione Mondiale della Sanità (OMS) alla diffusione del covid-19", in *SIDIBlog*, 9 aprile 2020, disponibile su www.sidiblog.org; G. BARTOLINI, "Alcune questioni dell'emergenza covid-19 in Italia in un'ottica di *International Disaster Law* (Parte I)", ivi, 22 maggio 2020; G.L. BURCI, "The Outbreak of COVID-19 Coronavirus: are the International Health Regulations fit for purpose?", in *EJILTalk!*, 27 febbraio 2020, disponibile su www.ejiltalk.org; I.R. PAVONE, "La dichiarazione di pandemia di Covid-19 dell'OMS: implicazioni di governance sanitaria globale", in corso di pubblicazione in *BioLaw Journal*, 27 marzo 2020, disponibile su www.biodiritto.org. Sempre in tema, con particolare attenzione all'Europa v. F. CASOLARI, "Prime considerazioni sull'azione dell'Unione ai tempi del Coronavirus", *Rivista Eurojus*, 2 marzo 2020, disponibile su www.rivista.eurojus.it.

ISSN: 1971-7105

parte di numerosi Governi[2]. La ragione è chiarita dal Ministro italiano per l'Innovazione: considerato che «gli standard di tracciamento manuale dei contatti forniti dall'*European Center for Disease Prevention and Control* nel marzo 2020 [indicano] in 12 ore il tempo medio per ogni operazione», l'uso della tecnologia permetterebbe un tracciamento di prossimità «molto più efficiente e rapido di quello tradizionale»[3]. In sintesi il passaggio dal *Tracing* 'analogico' a quello 'digitale' si manifesta come cruciale. Allorquando la «soluzione manuale non assicura di interrompere la riproduzione epidemica […] le App mobili hanno il potenziale per rafforzare le strategie di tracciamento dei contatti personali, che sono necessarie a contenere e invertire il corso della diffusione del Covid-19»[4].

Come esamineremo dettagliatamente nel presente studio, la scelta di avvalersi di nuove soluzioni tecnologiche per garantire la salute si iscrive nel quadro di esperienze in parte simili, già testate, con risultati alterni, in altre aree (par. 4, 5 e 6). Pur nella considerevole varietà delle soluzioni adottate nei vari contesti, tali sistemi di tracciamento sollevano questioni giuridiche che si irradiano lungo diverse direttrici: tutela dei dati personali, diritto alla salute, libertà di movimento, diritto al lavoro *etc*. Che si tratti di un sistema di stretta sorveglianza oppure di un più blando monitoraggio – la differenza risente, *in primis*, del retroterra giuridico-culturale dei diversi ordinamenti presi in esame – il centro intorno al quale orbitano le varie questioni giuridiche è rappresentato dall'emergenza di nuovi bilanciamenti.

Nel corso della presente indagine, dopo avere condotto un *excursus* sull'origine dell'applicazione (app) *Immuni* (paragrafo 2) e sulle linee guida sviluppate dall'Unione europea a riguardo (paragrafo 3), si concentrerà l'attenzione sul ventaglio di opzioni praticabili e su quella infine scelta dal Governo italiano (paragrafi 7, 8 e 9). Esaminato il fondamento giuridico di quest'ultima (paragrafi 10 e 11) e valutata la relativa conformità agli obblighi posti dall'ordinamento internazionale (paragrafo 12), si presenteranno alcune osservazioni sui pregi (paragrafo 13), sulle

[2] Per uno sguardo d'insieme sui profili giuridici delle tecnologie di tracciamento, v. G. DELLA MORTE, "La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze sorveglianza di massa", in *SIDIBlog*, 30 marzo 2020, consultabile su www.sidiblog.org; L. MCGREGOR, "Contact-tracing Apps and Human Rights", in *EJILTalk!*, 27 febbraio 2020, disponibile su www.ejiltalk.org; oltre al dibattito ospitato in *Symposium: Privacy and Contact Tracing*, disponibile su www.medialaws.eu a partire dal 21 maggio 2020 (con interventi di L. BOLOGNINI; G. D'ACQUISTO; G. DELLA MORTE; G. FINOCCHIARO; R. PANETTA; M. PLUTINO; O. POLLICINO; F. RESTA; V. ZENO ZENCOVICH). La restante, già copiosa, dottrina sarà evocata in relazione alle singole questioni di riferimento. Infine, per una ricognizione documentale, v. *Tracciamento di contatti – elementi di documentazione*, dossier a cura del Servizio Studi del Senato (aggiornato al 4 maggio 2020), disponibile su www.senato.it.

[3] Così il Ministro per l'Innovazione Tecnologica e la Digitalizzazione – d'ora in avanti Ministro per l'Innovazione – nel documento: *Un aggiornamento sull'applicazione di* contact tracing *digitale per l'emergenza coronavirus*, 21 aprile 2020, disponibile su www.innovazione.gov.it.

[4] *Ibidem*, dove si cita il rapporto elaborato dal *eHealth Network* – una rete delle autorità competenti in materia di sanità digitale istituita ai sensi dell'art. 14 della Direttiva 2011/24/EU – dal titolo *Mobile applications to support contact tracing in the EU's fight against COVID-19 – Common EU Toolbox for Member States*, 15 aprile 2020, disponibile su www.ec.europa.eu.

criticità (paragrafo 14) e, in guisa di conclusione, una riflessione sulle zone grigie emergenti da un attento scrutinio dei nuovi bilanciamenti (paragrafo 15).

2. Sviluppo e approvazione dell'app Immuni

Il concorso di idee per lo sviluppo di un'app destinata a monitorare i soggetti a rischio di contagio è stato bandito dal Ministro per l'Innovazione Tecnologica e la Digitalizzazione, in accordo con il Ministro dello Sviluppo Economico e con il Ministro dell'Università e della Ricerca, il 23 marzo 2020. Nonostante la finestra temporale fosse eccezionalmente breve – la *Fast Call* aveva come *dies ad quem* il 26 marzo 2020 – il concorso ha generato un notevole riscontro essendo pervenute, per il solo versante del bando dedicato al monitoraggio, ben 319 proposte[5].

Pochi giorni più tardi, il 31 marzo 2020, è stato nominato un gruppo di lavoro multidisciplinare – c.d. *Task Force Immuni* – incaricato di elaborare analisi utili «a supportare la Presidenza del Consiglio dei ministri e le Amministrazioni pubbliche nella definizione di politiche di contenimento del contagio da Covid-19»[6]. A seguito di una serie di interlocuzioni tra la *Task Force* e il Governo, nelle quali erano state inizialmente individuate due app degne di attenzione, con ordinanza n. 10[7], firmata

[5] Cfr. il bando telemedicina e sistemi di monitoraggio del 23 marzo 2020, consultabile a partire dal sito del Ministero per l'Innovazione: www.innovazione.gov.it. La *Fast Call* è stata adottata nel quadro di 'Innova per l'Italia', un progetto promosso da diversi ministeri e volto a raccogliere contributi da parte di aziende, università, centri di ricerca e società civile sul tema del contrasto al diffondersi del Covid-19. I principali documenti relativi all'elaborazione dell'app sono disponibili sul sito del Ministero per l'Innovazione ad esso dedicato: www.innovazione.gov.it. In tale sezione è consultabile anche l'audizione, svolta il 30 aprile 2020, del Ministro per l'Innovazione alla Camera dei Deputati.

[6] Così la pagina di presentazione ufficiale della *Task Force* nominata dal Ministero per l'Innovazione in accordo con il Ministero della Salute (www.innovazione.gov.it). Composta da ben 74 esperti, è suddivisa in otto sottogruppi dedicati, rispettivamente, a: coordinamento generale; infrastrutture e *Data Collection*; impatto economico; *web data* e impatto socio-economico; teleassistenza; tecnologie per il governo dell'emergenza; *Big Data* & AI *for Policies*; e infine profili giuridici della gestione dei dati connessa all'emergenza. Quest'ultimo, in particolare «procede all'analisi e alla mappatura dei vincoli normativi […] e predispone una strategia di garanzia dei diritti e delle libertà fondamentali nella gestione ordinaria ed emergenziale dei dati personali [nonché] alla verifica della compatibilità degli strumenti tecnologici oggetto di valutazione […] con l'ordinamento nazionale». Forniscono infine consulenza rappresentanti designati dal Ministero della Salute, dell'Autorità per la garanzia nelle comunicazioni, di quella per la concorrenza e del mercato e, infine, di quella per la protezione dei dati personali.

[7] Per una lettura critica della procedura adoperata, v. P. CLARIZIA, E. SCHNEIDER, "Luci e ombre sulla procedura di selezione di "Immuni", l'app del governo di tracciamento del contagio da Covid-19", in *IRPA-Osservatorio sullo Stato digitale*, 19 aprile 2020, disponibile su www.irpa.eu. In essa si sottolinea, *inter alia,* come: «non appare chiaro l'*iter* procedimentale utilizzato. La stipula del contratto, infatti, è presentata nell'ordinanza del Commissario straordinario come conclusione della *fast call* indetta dai Ministeri dello Sviluppo Economico, della Salute e per l'Innovazione. Tuttavia, il Commissario Straordinario non è mai citato negli atti della procedura e la *fast call* non prevedeva che le soluzioni tecnologiche sarebbero state acquisite a titolo gratuito». Sui profili internazionali relativi alla procedura di selezione, con particolare riferimento alla cornice normativa dell'Organizzazione mondiale del commercio, v. G. M. RUOTOLO, "Alcune osservazioni sulle App di tracciamento dei

il 16 aprile 2020 dal Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, si è disposta la stipula del contratto di concessione gratuita della licenza d'uso sul software di *contact tracing* c.d. *Immuni* e di appalto di servizio gratuito con la *Bending Spoons spa*, società progettatrice della app[8]. La proposta avanzata da quest'ultima, oltre a differenziarsi dalle altre per lo stato di avanzamento del progetto, vantava un'elaborazione nel quadro del *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT), un network europeo specializzato nello sviluppo di tecnologie di contrasto alla diffusione del virus rispettose della *privacy*[9]. Il 26 maggio 2020 il Ministero per l'innovazione ha reso pubblica la documentazione tecnica dell'app[10]. Nel momento in cui si licenzia questo studio è in corso la prima sperimentazione.

3. L'orientamento espresso da Commissione europea, Parlamento europeo, *European Data Protection Supervisor*, *European Data Protection Board*

Ciò premesso, va ricordato che già nel corso delle settimane precedenti e immediatamente seguenti l'adozione da parte del Governo italiano dell'app *Immuni* si è assistito, in sede di Unione europea, a un rilevante dibattito al quale hanno preso parti diversi attori.

Il 6 aprile 2020, il Garante responsabile della protezione dei dati in seno all'Unione europea (*European Data Protection Supervisor* – EDPS) ha pubblicato un appello per una strategia pan-europea nel contrasto all'epidemia[11]. Appena due giorni più tardi, l'8 aprile 2020, la Commissione europea ha adottato una raccomandazione relativa a un pacchetto di strumenti per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 attraverso un approccio comune in materia di uso di applicazioni mobili e ricorso a dati anonimizzati sulla mobilità[12]. Secondo tale raccomandazione, in particolare, tali applicazioni svolgono tre funzioni generali: la

contatti e dei contagi alla luce del diritto dell'Organizzazione mondiale del commercio", in *SIDIBlog*, 13 maggio 2020, disponibile su www.sidiblog.org.

[8] Per maggiori informazioni sulla società *Bending Spoon*, fondata nel 2013, oggi con sede a Milano, primo sviluppatore per app del sistema operativo IOS in Europa e con una pregressa esperienza nel campo della progettazione di una piattaforma di trattamento dei dati sanitari per conto di un centro medico polifunzionale, v. www.bendingspoons.com.

[9] Compito di quest'ultimo è, *inter alia*, quello di assistere le iniziative nazionali fornendo meccanismi e standard pronti all'uso, collaudi, nonché supporto per l'interoperabilità anche internazionale nel caso di tracciamento di catene di infezione che si estendono su più paesi. Maggiori informazioni sono disponibili su www.pepp-pt.org.

[10] V. *infra*, paragrafo 13.

[11] Cfr. *European Data Protection Supervisor*, *EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic* del 6 aprile 2020, disponibile su www.edps.europa.eu.

[12] Cfr. Raccomandazione (UE) 2020/518 della Commissione dell'8 aprile 2020, relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità.

prima è quella di «informare i cittadini, fornire loro consulenza e favorire l'organizzazione del *follow-up* medico delle persone sintomatiche, spesso in combinazione con un questionario di autodiagnosi»; la seconda è quella di «allertare le persone che si sono trovate in prossimità di una persona infetta per interrompere le catene di infezione ed evitare la recrudescenza delle infezioni nella fase di riapertura»; e la terza, infine, è quella di «monitorare la quarantena e controllarne il rispetto da parte delle persone infette, eventualmente in combinazione con funzionalità che valutino le loro condizioni di salute durante il periodo di quarantena[13].

Il Comitato europeo che riunisce le Autorità garanti dei dati personali di tutti gli Stati membri dell'Unione (*European Data Protection Board* – EDPB, da non confondere con il summenzionato EDPS), si è a sua volta espresso in diverse occasioni[14]. Una prima volta il 14 aprile, ovvero due giorni prima dell'adozione dell'app da parte del Governo italiano, con un parere reso alla Commissione europea e del quale è stato relatore proprio il Garante italiano per la protezione dei dati personali[15]. In esso si legge che il Comitato «accoglie con grande favore la proposta della Commissione di prevedere l'adozione di tali app su base volontaria, attraverso una scelta compiuta dai singoli nel segno di una responsabilità collettiva»; e ancora che «le app per il tracciamento dei contatti non necessitano di geolocalizzare i singoli utenti»[16]. Nel medesimo parere si puntualizza come l'esigenza di evitare le geolocalizzazioni sia giustificata dalla considerazione per cui l'obiettivo «non è seguire gli spostamenti individuali o imporre il rispetto di specifiche prescrizioni, bensì

[13] *Ibidem*, par. 12, dove si aggiunge: «In generale *l'efficacia di tali applicazioni non è stata valutata*. Le applicazioni informative e di controllo dei sintomi possono essere utili per sensibilizzare i cittadini. Tuttavia, secondo il parere degli esperti, le applicazioni che mirano a informare e allertare gli utenti appaiono le più promettenti per prevenire la propagazione del virus, tenendo conto anche del loro impatto più limitato sulla vita privata» (corsivo aggiunto).

[14] Sulla natura e sulle funzioni del Comitato europeo per la protezione dei dati, che dal 25 maggio 2018 ha sostituito il precedente Gruppo di lavoro Articolo 29, sia concesso rimandare a G. DELLA MORTE, "Articoli 68-76 del Regolamento generale per la protezione dei dati personali", in *Il sistema delle fonti nella protezione dei dati personali*, R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), Milano, in corso di pubblicazione.

[15] Cfr. la *European Data Protection Board Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, elaborata il 14 aprile 2020 nel corso della 21ª sessione di lavoro del Comitato, consultabile all'indirizzo: www.edpb.europa.eu/letters_en (la trad. italiana cui ci riferiamo è quella dell'Autorità garante dei dati personali italiana, disponibile su www.garanteprivacy.it). Sempre del Comitato europeo per la protezione dei dati personali, v. pure lo *Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak,* 16 marzo 2020, disponibile su www.edpb.europa.ec, dove si specifica che: «The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals».

[16] Cfr. *European Data Protection Board Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, cit.

individuare eventi che hanno natura probabilistica» come quello di avere contratto il contagio a causa della prossimità con un portatore del virus[17].

Le due condizioni anzidette: la non obbligatorietà dell'app e il ricorso a una tecnologia che non ricorre a geolocalizzazioni sono state propiziate anche dalla Commissione europea nel documento del 16 aprile relativo agli "Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati"[18]. Pur chiarendo che non si tratta di disposizioni vincolanti e che pertanto la relativa applicazione non pregiudica le eventuali ulteriori condizioni restrittive che gli Stati membri possono apportare, in tale documento si enunciano una serie di principi ("orientamenti" o *guidance*) dove si specificano le caratteristiche e i requisiti cui le app devono attenersi per garantire il rispetto della legislazione dell'Unione europea, tanto alla luce del regolamento generale sulla protezione dei dati quanto della direttiva *e-privacy*[19].

Sul tema è intervenuto anche il Parlamento europeo, che con una risoluzione adottata all'unanimità il 17 aprile 2020[20] ha preso atto dello sviluppo di app di tracciamento sottolineando come l'utilizzo «potrebbe non essere obbligatorio e che i dati generati non devono essere immagazzinati in banche dati centralizzate, il che condurrebbe a potenziali rischi di abuso e alla conseguente perdita di fiducia»[21].

Da ultimo sulla questione è ritornato il Comitato europeo per la protezione dei dati personali (EDPB) che, il 21 aprile 2020, ha reso noto le proprie *guidelines* sull'utilizzo dei dati di localizzazione e di tracciamento nel contesto della crisi da Covid-19[22]. Anche in tale documento si ribadisce come: «the use of contact tracing

[17] *Ibidem.* Per questa ragione, si aggiunge: «accogliere dati sugli spostamenti di una persona durante il funzionamento di un'app di tracciamento dei contatti configurerebbe una violazione del principio di minimizzazione dei dati, oltre a comportare gravi rischi in termini di sicurezza e privacy».

[18] Cfr. Comunicazione della Commissione, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati*, 2020/C 124 I/01 del 17 aprile 2020.

[19] Cfr., rispettivamente regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati; e direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche o direttiva *e-privacy*.

[20] Cfr. Risoluzione del Parlamento europeo del 17 aprile 2020 sull'azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze (2020/2616(RSP), in particolare il par. 52.

[21] Ivi, inoltre si richiede: «che la memorizzazione dei dati sia completamente decentralizzata, che vi sia piena trasparenza sugli interessi commerciali (extra UE) degli sviluppatori di queste applicazioni e che siano fornite chiare proiezioni a dimostrazione del fatto che l'uso di applicazioni per la ricerca dei contatti da parte di una fetta della popolazione, in combinazione con altre misure specifiche, porterà a un numero significativamente inferiore di contagi», e infine si raccomanda «che siano fissate clausole di temporaneità e siano pienamente rispettati i principi della protezione dei dati fin dalla progettazione e la minimizzazione dei dati».

[22] Cfr. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, adottate dal Comitato europeo per la protezione dei dati personali il 21 aprile 2020, e consultabili su www.edpb.europa.eu.

applications should be voluntary and should not rely on tracing individual movements but rather on proximity information regarding users»[23]. Entrambe le suddette caratteristiche sono state integrate nel progetto italiano.

4. I possibili modelli di tracciamento

Premesse tali considerazioni, occorre ricordare che prima della definizione di questo importante insieme di principi – che hanno rivestito le forme di 'linee guida', 'pacchetti di strumenti', 'orientamenti' *etc.* – le possibili soluzioni sul tappeto erano sostanzialmente due: la prima prevedeva il ricorso a un sistema di geolocalizzazione da attuarsi principalmente tramite *Global Positioning System* (d'ora in avanti: GPS); la seconda si basava su una semplice ricognizione dei contatti da realizzarsi attraverso il ricorso alla tecnologia *Bluetooth Low Energy* (d'ora in avanti: *Bluetooth*), ergo senza alcuna forma di geolocalizzazione. Tanto i benefici quanto i rischi di entrambe le soluzioni meritano un breve approfondimento.

Nel caso del tracciamento tramite geolocalizzazione il vantaggio consiste sostanzialmente nella trasmissione di una maggiore quantità di dati che si traduce in una maggiore precisione di analisi. Inoltre attraverso la geolocalizzazione è possibile riscontrare se un contatto è perdurato a lungo o meno, se esso è avvenuto in un luogo particolarmente affollato *etc.* A fronte di questi benefici, la geolocalizzazione rappresenta uno strumento di analisi indiscutibilmente invasivo, in quanto in grado di individuare ogni movimento della persona che reca con sé il dispositivo che consente il tracciamento (nella specie: uno smartphone, ovvero un oggetto dal quale è sempre più raro separarsi). È questa la ragione per la quale secondo il Comitato europeo per la protezione dei dati, supportato dall'Autorità europea e dalla stessa Commissione, le app per il tracciamento dei contatti non necessitano di geolocalizzazione. Se lo scopo perseguito non è quello di mappare gli spostamenti ma quello di individuare i contatti con soggetti positivi che, sulla base di un calcolo probabilistico, possono determinare un rischio di contagio, registrare i movimenti di ogni soggetto che abbia scaricato e attivato l'app significherebbe violare la regola della c.d. minimizzazione nel trattamento dei dati personali. Ci riferiamo al principio sancito all'art. 3, par. 1, lett. *c*) del regolamento generale per la protezione dei dati personali, per il quale occorre che i trattamenti dei dati siano: «adeguati, pertinenti e *limitati a quanto necessario rispetto alle finalità* per le quali sono trattati»[24].

[23] Ivi, par. 1.8.

[24] Corsivo aggiunto. Detto principio è richiamato, *ex multis*, anche al considerando n. 39 del regolamento generale per la protezione dei dati personali: «I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. [E ancora (con corsivo aggiunto):] I dati *personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi*». Inoltre, all'art. 25 del regolamento, dedicato alla "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" (si tratta della c.d. 'privacy by design') si prevede che: «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento […] il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali […] la minimizzazione».

Passando all'esame della soluzione alternativa alla geolocalizzazione, ovvero al ricorso al Bluetooth, esso consente di tracciare un contatto in modo del tutto indipendente dal luogo in cui il medesimo si è verificato. In caso di ricorso alla tecnologia Bluetooth il software si limita a registrare la prossimità tra dispositivi che abbiano scaricato e attivato l'app tramite un semplice scambio bidirezionale di dati identificativi criptati. In estrema sintesi ciò significa che per il *contact tracing* che fa riferimento solo a questa tecnologia il sistema funziona tanto nell'ipotesi in cui due smartphone si trovino nella medesima dimora per un'intera giornata, quanto nel caso in cui si incrocino occasionalmente per strada – spetterà poi ai singoli protocolli specificare le condizioni di distanza spaziale e di durata minima che consentono di registrare il segnale dell'altro dispositivo.

I vantaggi del sistema Bluetooth sul piano del rispetto del principio di minimizzazione appaiono evidenti, specialmente se comparati con il GPS. I rischi, tuttavia, sono quelli di una minore precisione e quindi di una più blanda azione di contrasto. In effetti, non solo la mancata localizzazione del contatto genera meno informazioni sul contesto in cui lo stesso è avvenuto, ma la medesima attendibilità del tracciamento può dipendere in misura notevole da alcune variabili, quali la potenza del segnale Bluetooth o la presenza/assenza di ostacoli di ordine fisico (si immagini la connessione tra due smartphone appartenenti a soggetti i quali, seppure prossimi, si trovano in due distinte automobili ferme nel traffico). Sicché, se da un lato nel caso di ricorso alla tecnologia Bluetooth le garanzie di minimizzazione sono maggiori, sono maggiori anche i rischi di falsi positivi e di falsi negativi. Proprio per questa ragione il Comitato europeo per la protezione dei dati personali, nella già menzionata lettera del 14 aprile 2020, ha sottolineato come «le app in questione non sono piattaforme per l'allarmismo sociale o per la stigmatizzazione. Tutt'altro: dovrebbero essere strumenti per dare a persone la possibilità di fare la propria parte»[25].

Esamineremo in seguito tanto il modo in cui i protocolli tecnici elaborati cerchino di contenere i rischi evocati, quanto il modo in cui il trattamento complessivo sia giuridicamente conforme, oltre che al principio di minimizzazione, anche agli altri obblighi deducibili dalle convenzioni regionali e/o settoriali di protezione dei diritti umani[26]. Tuttavia, prima di esprimerci su tali questioni alla luce del *modus operandi* di *Immuni*[27], occorre menzionare un recente accordo, stipulato tra due tra le più influenti società private del settore delle tecnologie dell'informazione, la cui incidenza sul tema complessivo non può essere sottovalutata.

[25] Cfr. *European Data Protection Board Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, nella traduzione proposta dall'Autorità garante italiana, cit.

[26] V. *infra*, paragrafo 12.

[27] V. *infra*, paragrafo 9.

5. *Segue*: l'accordo Apple-Google

L'accordo cui ci riferiamo è quello intercorso, il 10 aprile 2020, tra Apple e Google allo scopo di giungere a un protocollo di tracciamento fondato sulla tecnologia Bluetooth[28]. Detto protocollo ha suscitato l'interesse di un considerevole numero di Stati, tra i quali l'Italia. La ragione è semplice: esso presenta l'indiscutibile vantaggio di essere interoperabile tra diversi sistemi operativi, tanto nei dispositivi Apple che supportano iOS quanto negli smartphone che si avvalgano di Android[29].

Ciò premesso non può passare inosservato che, accanto al *know how* per la gestione dei protocolli uniformi e interoperabili, nell'accordo summenzionato si fa altresì riferimento alla possibilità di sviluppare una propria app. Infatti, secondo il documento anzidetto: «il piano è di implementare questa soluzione in due fasi». Nel corso della prima, programmata per il mese di maggio 2020, «le due aziende rilasceranno API [ovvero: *Application Programming Interface*: software che permette di semplificare il dialogo tra un'applicazione e un'altra] per consentire l'interoperabilità fra i dispositivi Android e iOS delle app sviluppate dalle autorità sanitarie». Nel corso della seconda fase, che invece si dichiara come «programmata nei prossimi mesi, Apple e Google lavoreranno per rendere disponibile una più ampia piattaforma di *contact tracing* basata su Bluetooth, integrando questa funzionalità nei sistemi operativi».

Il progetto è tanto più interessante in quanto, sempre secondo quanto previsto nell'accordo, la previsione di un'app 'universale' da integrare direttamente in tutti i maggiori sistemi operativi rappresenta «una soluzione più solida rispetto ad un'API e consentirebbe a un maggior numero di persone di partecipare, sempre su base volontaria»[30]. Apple e Google, in altri termini, stanno approntando un sistema di tracciamento che non richiederà più di installare un'apposita app ma che sarà precaricato sui nostri smartphone[31]. Tuttavia, si aggiunge, nel caso in cui un «match is detected» e lo stesso è notificato a un utilizzatore che non ha ancora scaricato «an official public health authority app» quest'ultimo sarà invitato a farlo quanto prima attraverso un sistema di avvisi, dal momento che «[o]nly public

[28] Una traduzione italiana dell'accordo del 10 aprile 2020 è disponibile in: www.apple.com/it/newsroom/. Premesso che i «governi e le autorità sanitarie di tutto il mondo stanno unendo le forze per trovare soluzioni alla pandemia di COVID-19», in esso si specifica che gli «sviluppatori software stanno dando il proprio contributo [e in] linea con questo spirito di collaborazione, Apple e Google […] lavoreranno insieme con l'obiettivo di rendere possibile l'utilizzo della tecnologia Bluetooth per aiutare governi e autorità sanitarie a contenere i contagi, nel pieno rispetto della sicurezza e della privacy degli utenti».

[29] Sulla stretta relazione tra interoperabilità e cybersicurezza, «two sides of the same coin», v. A. ODDENINO, in "Digital standardization, cybersecurity issues and international trade law", in *QIL–Questions of International Law*, 31 maggio 2018, disponibile su www.qil-qdi.org.

[30] Permettendo «inoltre l'interazione con un più ampio ecosistema di app e autorità sanitarie governative». Accordo Apple e Google, cit.

[31] In una sezione del sito dedicato alle *Frequently Asked Questions* si descrive più dettagliatamente il funzionamento di questo sistema 'universale': «After the operating system update is installed and the user has opted in, the system will send out and listen for the Bluetooth beacons as in the first phase, but without requiring an app to be installed». Cfr. www.apple.com.

health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control»[32].

In filigrana appare evidente come, nel settore sempre più strategico della tecnologia dell'informazione, si assista alla crescita esponenziale di un sistema misto pubblico-privato – una *governance senza governo* – in cui accanto ai tradizionali poteri pubblici si affiancano imprese private in grado esercitare – talvolta in modo più efficiente – pubbliche funzioni. Da tale prospettiva le attuali sinergie stabilite tra tecnologia ed esigenze di contenimento sanitario non sono che un tassello di un più ampio mosaico che concerne le profonde trasformazioni in corso sul versante della riconfigurazione, anche internazionale, dei centri decisori[33].

6. Le tecnologie di contrasto all'epidemia adottate altrove

Per quanto concerne gli Stati membri dell'Unione europea l'orientamento maggioritario è stato quello di uniformare i rimedi approntati in tema di tecnologia di tracciamento a quanto espressamente richiesto dai diversi soggetti evocati in precedenza[34]. Si tratta dell'approccio più garantista a livello globale, ma non bisogna sorprendersene: la protezione dei dati personali in ambito UE rappresenta un *unicum*, le cui ragioni profonde vanno comprese lungo una duplice prospettiva: economica, in ragione del valore veniale dei dati relativi ai cittadini qui interpretati come consumatori; e filosofica, dal momento che la storia dell'Unione europea è saldata con quella del Novecento, e che la storia del Novecento è a sua volta segnata dalle grandi discriminazioni attuate attraverso il ricorso a un uso distorto dei dati personali. Prova ne sia che fuori dal contesto europeo la sensibilità verso i dati si differenzia in modo significativo e con essa le soluzioni approntate in ambito di soluzioni tecnologiche per il tracciamento.

7. *Segue*: in ambito UE ed EFTA

Quanto appena sostenuto trova un immediato riscontro nell'allegato IV del rapporto pubblicato il 15 aprile 2020 dal *eHealth Network* e dedicato alle app aventi ad oggetto i sistemi di *tracing*[35]. In esso si espone un autentico inventario delle singole opzioni, sicché da un'analisi di tale documento è possibile dedurre alcune utili precisazioni[36].

[32] *Ibidem.*

[33] Sull'ampio tema sia consentito rimandare a. G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, in particolare p. 135 ss. e p. 261 ss. Più specificamente sul versante sanitario, v. U. PAGALLO, "Sovereigns, Viruses, and the Law: The Normative Challenges of Pandemic in Today's Information Societies", 13 maggio 2020, disponibile su www.ssrn.com.

[34] V. *retro*, paragrafo 3.

[35] Cfr. l'annesso (IV) *Inventory Mobile Solutions Against Covid-19*, del doc. del *eHealth Network* intitolato: *Mobile applications to support contact tracing in the EU's fight against COVID-19 – Common EU Toolbox for Member States*, cit.

[36] Il rapporto del *eHealth Network* fa riferimento agli studi condotti dall'*European mHealth hub* (www.mhealth-hub.org); dal *eHealth Hub platform* (www.platform.ehealth-hub.eu); e dalle *Solutions fo-*

Innanzitutto, per quanto concerne le soluzioni adottate o in discussione presso gli Stati membri dell'Unione europea e dell'Associazione europea di libero scambio (EFTA), si ricorda come solo Cipro[37] e Norvegia[38] abbiano approntato, alla data del 15 aprile 2020, soluzioni di carattere misto, ovvero che si riferiscono tanto alla tecnologia Bluetooth quanto a quella GPS che fa ricorso alle geolocalizzazioni. Gli altri Stati membri, pur offrendo ciascuno dei servizi diversi – controllo dei sintomi, tracciamento, informazione al pubblico, supporto ai pazienti attraverso il ricorso a servizi di telemedicina, supporto ai medici o combinazioni diversamente articolate di ciascuna di tali prestazioni –, hanno uniformato le loro iniziative a quanto richiesto dalla Commissione europea, dal Comitato europeo per la protezione dei dati personali e dall'Autorità europea per la protezione dei dati personali, oltre che dal *eHealth Network* medesimo[39]. In altre parole si sono orientati verso soluzioni tecnologiche di tipo volontaristico fondate sul tracciamento dei contagi e/o su servizi di assistenza e/o informazione.

Tra le soluzioni adottate si segnalano, oltre Italia, Cipro e Norvegia di cui si è già detto, l'Austria, che ha elaborato un sistema di *tracing* dei contatti (*Stoppcorona*) funzionante attraverso tecnologia Bluetooth e attivabile dalla persona contagiata[40]; la Francia, che ha dapprima progettato software dedicati all'analisi dei sintomi e alla cura dei pazienti a casa[41] e in seguito ha iniziato a discutere ulteriori strategie[42]; la Germania, che ha elaborato un software di raccolta di informazioni (*Leoss – Lean European Open Survey for SARS-CoV-2 Infected Patients*), oltre a un'app di

cusing on 'prevention of social isolation' and 'Feeling safe and secure at home' (www.aal-europe.eu). Attraverso detti studi si elabora un'articolata griglia che classifica ogni approccio secondo: le categorie dei proponenti («government, citizen movement initiatives, and private-company initiatives») e l'offerta di servizi («symptom checkers and self-diagnosis tools; tracking and tracing the spread of the coronavirus; trustworthy information and guidelines to public; support home bound (diagnosed) patients in their self-management; and support to medical staff, mainly to follow-up on patients confined at home»).

[37] Cfr. l'app *Tracer* disponibile su www.covid-19.rise.org.cy. Detta app, fondata su un particolare sistema di geolocalizzazione per il quale tutti i dati restano sullo smartphone dell'utilizzatore che può decidere di condividerli in forma anonima con il Governo, si basa sulla tecnologia *safepaths* (www.safepaths.mit.edu), sviluppata dal *Massachusetts Institute of Technology*.

[38] La Norvegia, oltre ad avere sviluppato una piattaforma di comunicazione gestita dall'autorità sanitaria pubblica (www.helsenorge.no) ha adottato un'app che persegue un duplice obiettivo: individuare rapidamente i soggetti a rischio di contagio e al contempo monitorare la diffusione dell'infezione attraverso una localizzazione degli utenti (www.simula.no). Per perseguire tali scopi i dati sono trattati e conservati in un archivio centrale. Nella prospettiva norvegese, infatti, è solo l'analisi dei dati aggregati e anonimi relativi alla localizzazione che rende possibile la determinazione della migliore azione di contrasto.

[39] V. *supra*, par. 3.

[40] Cfr. *Stopp Corona-App App. Jetzt. Immer., Die App im Kampf gegen das Coronavirus*, disponibile su www.participate.roteskreuz.at.

[41] Cfr. maladiecoronavirus.fr e www.service-public.fr. Quest'ultimo sistema, si specifica nel documento del *eHealth Network* del 15 aprile 2020, è adottato da due gruppi di ospedali.

[42] Ci riferiamo a *StopCovid*, «une application de suivi de contacts dont le téléchargement et l'utilisation reposeraient sur une démarche volontaire». Cfr., al riguardo, il parere rilasciato dalla *Commission nationale de l'informatique et des libertés* il 26 aprile 2020 (consultabile su www.cnil.fr).

tracciamento[43]; l'Olanda, che ha progettato un'app destinata a diffondere maggiori informazioni[44]*;* il Regno Unito che al momento della redazione del rapporto discuteva intorno a un'app destinata ad allertare i soggetti che si fossero trovati a rischio a causa della prossimità con contagiati[45]; infine la Spagna, che ha ideato un sito di informazioni e un'app che permette agli utenti di provvedere a un'auto-analisi e ancora di ottenere assistenza sulla base dei sintomi[46].

Da ultimo occorre osservare come, stante la libertà di movimento normalmente vigente in ambito UE, l'eventuale assenza di coordinamento tra gli approcci dei singoli Stati membri potrebbe riflettersi negativamente sul piano della mobilità. *Quid* se una compagnia aerea introducesse come condizione per potere accedere ai propri voli quella di disporre di una delle app considerate? Sebbene una simile ipotesi potrebbe configurare una limitazione coercitiva indiretta della libertà fondamentale di movimento (specialmente nel caso in cui la compagnia in questione rappresenti il modo esclusivo o principale per raggiungere una destinazione), al momento in cui si scrive non tutti i progetti escludono formalmente il rischio di compressioni sul piano dell'esercizio dei diritti.

8. *Segue*: in altre aree

Come si accennava in precedenza[47], distanziando lo sguardo le risposte giuridiche si moltiplicano e si differenziano in modo significativo, rispetto a quanto previsto in ambito UE. Prendendo ancora spunto dai dati forniti dal *eHealth Network* si possono raggruppare le risposte fornite dagli Stati extra-europei in due macro categorie: da un lato, quegli Stati – come Brasile o Vietnam – in cui sono state adottate delle misure destinate per lo più a scopi informativi; dall'altro, quegli altri – come Israele, Singapore, Cina – dove le misure di sorveglianza sono decisamente più stringenti.

Cominciando dal Brasile, la cui gestione della crisi epidemica è stata segnata da una significativa sottostima dell'evento, la risposta digitale promossa dal Ministro della Salute si è limitata allo sviluppo di un'app informativa in merito ai sintomi e alle condotte cui attenersi in caso di infezione[48]. Anche l'approccio seguito dal Vietnam si è concentrato sull'informazione: attraverso una specifica app (*Ncovi*)[49] i cittadini

[43] Cfr. www.dzif.de/en (per la versione in inglese) e www.corona-datenspende.de, il cui slogan è riassumibile in «Hände waschen, Abstand halten, *Daten spenden*» (lavati le mani, mantieni la distanza, *dona i dati* – corsivo aggiunto).

[44] Cfr. www.apps.apple.com.

[45] Cfr. il rapporto del *eHealth Network* del 15 aprile 2020, cit. e M. COULD e G. LEWIS, "Digital contact tracing: protecting the NHS and saving lives", 24 aprile 2020; ancora T. EDEN, "The code behind the NHS Covid-19 App", 8 maggio 2020, entrambi consultabili su www.nhsx.nhs.uk. Sebbene il Regno Unito non faccia più parte della UE lo inseriamo ancora all'interno di questo gruppo per effetto del regime transitorio.

[46] Cfr. www.covid19.es.

[47] V. *retro*, paragrafo 6.

[48] Coronavírus – SUS, disponibile su www.play.google.com.

[49] Cfr. OpenGov Asia su www.opengovasia.com.

hanno la possibilità di restare aggiornati sul diffondersi del virus nelle proprie aree residenziali.

Passando poi all'esame degli Stati che hanno adottato misure più stringenti, Israele ha adottato un'app di tracciamento (*Hamagen*)[50] che, se da un lato accede ai dati GPS degli smartphone di riferimento tracciandone i movimenti, dall'altro mantiene tali dati all'interno del dispositivo. Considerati i possibili rischi, la legittimità dell'app *Hamagen* è stata contestata dinanzi alla Corte suprema israeliana, che ha inizialmente ritenuto illegittimo il tracciamento dei pazienti Covid-19 al di fuori del controllo legislativo esercitato dalla Knesset. Sebbene l'ingiunzione sia stata revocata in seguito alla sopravvenuta autorizzazione[51], l'esempio è paradigmatico dell'interessamento, sino alle giurisdizioni di massimo grado, dei problemi che possono sorgere in caso di tracciamento.

Anche la soluzione elaborata dallo Stato di Singapore rappresenta un esempio particolarmente interessante, specie dalla prospettiva delle aspettative eccessive riposte nei sistemi di sorveglianza digitale[52]. In tale Stato, quanto meno in un primo momento, il Governo non ha proceduto ad alcun *lockdown*, ricorrendo alla sola soluzione tecnologica affidata a un'app (*Trace Together*) fondata su tecnologia Bluetooth e non abilitata a geolocalizzare i dispositivi[53]. Giacché l'app in questione era su base volontaria essa non ha prodotto i risultati attesi, essendo stata scaricata e adoperata soltanto dal 17% della popolazione[54]. Sulla scorta di questo insuccesso lo Stato di Singapore ha prontamente effettuato un *revirement* della posizione inizialmente assunta, ricorrendo alla chiusura delle attività principali.

Quanto alla Cina, l'app *Alipay Health Code* – probabilmente la più nota anche in ragione dell'ampia diffusione – dopo avere raccolto dati relativi ai contatti, allo stato di salute *etc.*, attribuisce a ciascun individuo un punteggio generato da un algoritmo ed espresso in forma di *QR-code* di diversi colori. Un *QR-Code* rosso impone un confinamento presso il proprio domicilio; quello giallo permette una mobilità soggetta a restrizioni; quello verde consente la piena libertà; e, nel caso di mancanza di un *QR-Code* sul proprio dispositivo, come la mancanza *tout court* di un dispositivo, si considera una situazione equivalente a un *QR-code* rosso[55].

[50] 'Scudo' (in israeliano), disponibile su www.play.google.com.

[51] Per una sintesi della decisione in lingua inglese, cfr. "Israel's Top Court: No Shin Bet Tracking of Coronavirus Patients Without Knesset Oversight", consultabile su www.haaretz.com, 19 marzo 2020.

[52] «[C]ome osserva in proposito il direttore del centro di ricerca sull'intelligenza artificiale dell'*Ada Lovelace Institute* britannico, «la tecnologia non è mai una soluzione magica e non lo è in particolare in questa circostanza». Ma è spesso raffigurata come tale [*silver bullet*, nel testo originale] «e questo è parte del problema». Così L. PICA CIAMARRA, citando J. Delcker, in "App, il giro di vite digitale", sul sito del CNR – Istituto per la storia del pensiero filosofico e scientifico moderno, disponibile su www.ispf.cnr.it, 19 giugno 2020.

[53] Cfr. Government Technology Agency su www.tech.gov.sg.

[54] V. L. MCGREGOR, "Contact-tracing Apps and Human Rights", cit., p. 2.

[55] Sul ruolo dello smartphone come «nuovo pilastro della società cinese» (attraverso 'l'app delle app' *WeChat* è possibile finanche produrre tutti i documenti per il divorzio, oltre a contrarre matrimonio) v. la suggestiva ricostruzione di S. PIERANNI, *Red Mirror. Il nostro futuro si scrive in Cina*, Bari, 2020, in particolare pp. 17-34.

Da ultimo sebbene non sia menzionato nel rapporto del *eHealth Network*, merita un breve cenno la strategia digitale approntata in Corea del Sud. Forte dell'esperienza accumulata in occasione del contrasto a una precedente epidemia nel 2015, la risposta di questo Stato si è caratterizzata per un uso indiscriminato del tracciamento. Quest'ultimo è avvenuto attraverso l'incrocio di informazioni ottenute attraverso tanto il ricorso a metodi tradizionali (interviste ai pazienti) quanto a metodi innovativi (dati GPS degli smartphone, archivi digitali delle farmacie e delle carte di credito, registrazioni di telecamera a circuito chiuso *etc.*). Si tratta, come facilmente intuibile, di sistemi fortemente intrusivi che risulterebbero certamente inammissibili nel continente europeo[56]. Inoltre, come rammentato in un rapporto del *Korea Center for Disease Control and Prevention*[57], essi non sono al riparo da rischi di falsi positivi e/o negativi: *quid*, ad esempio, nel caso in cui l'utilizzatore di una carta di credito sia un soggetto diverso dal relativo titolare?

9. Il funzionamento dell'app *Immuni*

Attestata l'esistenza di diversi modelli teorici di tracciamento e di numerose declinazioni pratiche di tali modelli[58], resta da verificare come funzioni l'app italiana.

Innanzitutto *Immuni* è un'app di *contact tracing* gratuita, volontaria e accessibile agli individui maggiori di 14 anni. Essa è fondata su una tecnologia Bluetooth: lo scopo, come ricordato, non è quello di geolocalizzare gli individui potenzialmente contagiosi ma identificare e allertare quanti si siano trovati in una situazione di prossimità con un soggetto risultato positivo al virus (ergo indipendentemente dal *dove* detta situazione di prossimità si sia verificata).

[56] In senso sorprendentemente contrario – la sorpresa è motivata dalle innumerevoli fonti normative in senso opposto – e pur evocando (*sic!*) il principio di proporzionalità, le opinioni di due magistrati, D. DE FALCO, M.L. MADDALENA, per i quali il quadro normativo «avrebbe giustificato e giustificherebbe anche ora l'adozione di misure di sorveglianza attiva anche tramite tecnologie di geolocalizzazione, *data tracing* ed analisi dei dati mediante il ricorso ad algoritmi, purché autorizzati da una fonte primaria unicamente nell'attuale situazione emergenziale, stante le loro strumentalità con gli obiettivi di contenimento dell'epidemia, alla luce delle recenti indicazioni OMS». Così in "La politica del tracciamento dei contatti e dei test per covid alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia", in www.federalismi.it, 28 marzo 2020, p. 10.

[57] V. "Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts", in *Osong Public Health and Research Perspectives*, vol. 11, 2020; p. 60 ss. (disponibile su ophrp.org). In esso si chiarisce come la gestione si sia articolata in quattro fasi: 1) la localizzazione del contatto (*patient route*); 2) la valutazione dell'esposizione al rischio; 3) la classificazione del contatto; e 4) la gestione del contatto. Più dettagliatamente: «The location of the contact was determined through the process of preliminary identification, by interviewing patients, and their acquaintances, and by objective verification of the investigated information. Exposure risk evaluation was performed depending on the route of disease transmission, patient characteristics, and environmental characteristics. Based on the results of the evaluation, the contacts were classified into close and casual contacts depending on the exposure. The method of managing the classified contacts was largely distinguished between movement restriction and symptom monitoring».

[58] V. *retro*, paragrafi 4. 6, 7 e 8.

Una volta scaricata e attivata l'app genera dei codici identificativi anonimi e randomizzati, ovvero che mutano a brevi intervalli di tempo, per far sì che non possano mai essere associati a una persona fisica particolare. Giacché quando due dispositivi con l'app attiva si trovano nelle vicinanze provvedono, tramite il segnale Bluetooth, a scambiarsi i rispettivi identificativi, di fatto *Immuni* consente a due smartphone di registrare – in modo bidirezionale – tale prossimità spaziale. Tale informazione, associata ad altre che si riferiscono, ad esempio, alla durata della situazione di prossimità oltre che alla forza del segnale, viene processata dall'algoritmo dell'app direttamente all'interno del singolo dispositivo. Ciò premesso, seguono due possibili scenari. Nell'ipotesi in cui un soggetto che abbia attivato l'app non abbia effettuato alcun test perché non risulti sintomatico, oppure avendo effettuato il test risulti negativo, la lista dei contatti contenuta nel proprio smartphone risulta inaccessibile e i dati saranno eliminati quando non più necessari. Diversamente, nel caso in cui il proprietario dello smartphone risulti positivo al virus, quest'ultimo potrà caricare sul server pubblico, attraverso l'assistenza di un operatore, i codici casuali che il proprio dispositivo ha generato nel corso dei giorni precedenti. Ora, poiché l'app. *Immuni* controlla periodicamente i codici presenti sul server e li confronta con quelli salvati sul dispositivo dell'utente, l'algoritmo è in grado di determinare la potenziale esposizione a un contagio attraverso un sistema sostanzialmente decentralizzato[59]. In caso di risposta affermativa, l'app avverte l'utente di mettersi in contatto con gli operatori sanitari al fine di garantire le condotte più sicure.

Da questo primo esame e in attesa di verificare il funzionamento dell'app a pieno regime, appare chiaro che tre sono i passaggi fondamentali lungo i quali si snoda l'intera procedura: la registrazione della prossimità tra gli smartphone; l'identificazione dei contatti in forma anonima; e il *follow up* della persona contagiata e di quanti si sono trovati in una situazione di rischio. Come specificheremo in seguito, ciascuno di questi passaggi presenta dei tratti peculiari[60]. Tuttavia, prima di esaminare nel dettaglio i pregi e le criticità dell'app ci sembra opportuno svolgere talune osservazioni sul piano del fondamento giuridico e su quello degli obblighi internazionali in materia.

[59] Più dettagliatamente, stando alla ricostruzione proposta da R. BERTI, A. LONGO, S. ZANETTI, "Immuni, cos'è e come funziona l'app italiana coronavirus", 15 maggio 2020, in *Agenda Digitale*, disponibile su www.agendadigitale.eu: «Quando uno dei soggetti che ha scaricato l'app risulta positivo al virus, gli operatori sanitari gli forniscono un codice di autorizzazione con il quale questi può scaricare su un server ministeriale il proprio codice anonimo (questo avviene nel modello decentralizzato che sarà la versione definitiva di Immuni. In quello precedente, usato finora nelle beta dell'app, il paziente carica la lista dei codici con cui è stato in contatto nei giorni precedenti). I cellulari con l'app prendono dal server i codici dei contagiati (nel modello precedente ricevono direttamente dal server la eventuale notifica di essere un "soggetto a rischio"). Se l'app riconosce tra i codici nella propria memoria un codice di un contagiato, visualizza la notifica all'utente (nel modello precedente, visualizza la notifica su impulso del server, come sopra accennato)».

[60] Cfr. *infra*, par. 14.

10. Il fondamento giuridico

La questione della copertura giuridica delle diverse app di *tracing* ha da subito attirato l'attenzione del Comitato europeo per la protezione dei dati, il quale, nel parere reso alla Commissione il 14 aprile 2020, ha reso noto che simili applicazioni dovessero essere installate su base volontaria dall'utente, specificando al contempo che la base giuridica del trattamento non è ravvisabile nel consenso quanto nell'interesse pubblico rilevante e proporzionato alla finalità di salute perseguita[61]. Il suddetto Comitato ha inoltre aggiunto come il relativo fondamento giuridico debba essere correttamente individuato nella promulgazione di leggi nazionali che promuovano l'impiego di app su base volontaria e senza alcuna penalizzazione per chi non intenda farne uso[62].

Tale richiesta è stata soddisfatta dal Governo italiano il 30 aprile 2020 allorquando, con l'adozione del decreto-legge n. 28, si è offerta una copertura di rango primario all'elaborazione dell'app *Immuni*[63]. In precedenza tale copertura era riferibile all'art. 14 del decreto-legge 9 marzo 2020, n. 14, che tuttavia si ascriveva alle deroghe ordinarie al trattamento dei dati personali in ragione della necessità di comunicare in forma semplificata il proprio stato di salute al fine di contrastare il rischio di contagio[64]. Appare evidente che una simile copertura non avrebbe potuto reggere un affondo nel campo del trattamento dei dati personali sensibili come quelli sanitari, ed è questa la preminente ragione per la quale si è giunti, dopo una serie di passaggi intermedi[65], all'adozione del decreto-legge di cui *supra*.

[61] Infatti, come correttamente osserva E. CIRONE, "L'app italiana di *contact tracing* alla prova del GDPR: dall'*habeas data* al *ratchet effect* il passo è breve?", in SIDIBlog, 13 maggio 2020, disponibile su www.sidiblog.org: «merita precisare che, nel caso dell'app di *contact tracing*, è corretto parlare di consenso perché la scelta di effettuare o meno il *download* dell'applicativo è rimessa al cittadino. Tuttavia, non può dirsi che il consenso costituisca la base giuridica legittimante il trattamento dei dati, che si fonda, invece, sull'interesse pubblico alla tutela della salute».

[62] Cfr. *European Data Protection Board Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, cit.

[63] Sul decreto-legge v. *infra*, il par. seguente.

[64] Cfr. l'art. 14: "Disposizioni sul trattamento dei dati personali nel contesto emergenziale". Ai sensi del primo comma di tale disposizione fino al termine dello stato di emergenza «per motivi di interesse pubblico nel settore della sanità pubblica […] le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte […] possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19». Sul punto, v. O. POLLICINO e F. RESTA, in "*Data Tracing*, no a deleghe in bianco all'algoritmo", consultabile in www.corrierecomunicazioni.it, 24 marzo 2020.

[65] Tra questi il decreto-legge 25 marzo 2020, n. 19, *Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19*, in Gazzetta Ufficiale del 25 marzo 2020). In senso critico G. DI MINICO: «se è pur vero che non ha disposto una girata in bianco al Presidente del consiglio, è però innegabile che abbia fatto meno di quanto avrebbe dovuto fare per soddisfare quella assorbente attribuzione di competenza consegnata nella riserva. L'art. 2 […] enumera le misure restrittive delle libertà, ma lascia alla valutazione politica del Presidente del consiglio la scelta di quale rendere concretamente operante, senza neanche vincolare il suo libero apprezzamento politico ai parametri della necessità, qui degradata ad

Da ultimo va aggiunto che la copertura di un'app valida per tutto il territorio nazionale attuata attraverso una fonte primaria ha servito altresì lo scopo di contrastare un'avanzata in ordine sparso delle Regioni italiane, sulla falsariga di quanto già avvenuto in tema di limitazioni alla libertà di movimento (nel corso della c.d. 'fase 1') e di riapertura degli esercizi commerciali (nel corso della c.d. 'fase 2'). Nel già menzionato documento del *eHealth Network* si riporta come, al 15 aprile 2020, alcune Regioni italiane avessero già elaborato delle app di contrasto alla diffusione del virus[66]. Queste ultime, avendo portata locale e prevedendo in alcuni casi obblighi disallineati, sollevavano diversi dubbi di legittimità costituzionale[67].

11. *Segue*: in particolare, il decreto-legge 30 aprile 2020, n. 28 e il documento relativo alla valutazione di impatto presentato dal Ministero della Salute e approvato dall'Autorità garante per la protezione dei dati personali il 1° giugno 2020

Il 30 aprile 2020 è stato pubblicato in *Gazzetta Ufficiale* il decreto-legge n. 28[68], entrato in vigore il 1° maggio 2020. Tale provvedimento, ricalcando in larga parte quanto puntualizzato dal Ministro per l'innovazione attraverso una nota di alcuni giorni prima[69], chiarisce diverse questioni, ma non tutte.

Partendo dagli aspetti positivi, si specifica che l'app *Immuni* è istituita «[a]l solo fine di allertare le persone che siano entrate in *contatto stretto* con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione

adeguatezza, e della precauzionalità, qui diluita nella proporzionalità». ID., "Virus e algoritmi. Impariamo da un'esperienza dolorosa, disponibile in www.lacostituzione.info, 1° aprile 2020.

[66] Ad esempio, il progetto promosso dalla Regione Lazio e diretto a supportare quanti si fossero auto-isolati nelle proprie dimore: www.regione.lazio.it.

[67] Specialmente nelle ipotesi in cui le limitazioni previste da tali app locali fossero state più incisive. A solo titolo di esempio il Governatore della Regione Veneto ha annunciato, il 20 aprile 2020, l'intenzione di rendere obbligatorio il ricorso a un'app di *tracing* locale (così le dichiarazioni in conferenza stampa, riportate in www.mattinopadova.gelocal.it/padova del 20 aprile 2020). Contrario alla possibilità di un'interferenza regionale in materia anche G. TROPEA, "Il *contact tracing* digitale e l'epidemia: sindrome cinese?", disponibile in www.lacostituzione.info del 9 aprile 2020: «Non mi pare che le regioni possano intervenire in materia. Sul punto può essere utile notare che quando il giudice amministrativo ha affrontato sinora *ex professo* la questione della compatibilità del potere di ordinanza con la privacy (nel caso dell'ordinanza del sindaco di Messina che, fra l'altro, imponeva la registrazione on-line dei dati personali di coloro che intendessero attraversare lo stretto) ha perentoriamente data un parere nel senso dell'illegittimità – anche su questo fronte – del provvedimento, per violazione della potestà legislativa statale (Cons. St., sez. I, 7 aprile 2020, n. 735). La fonte primaria, quindi, dovrà essere statale e non vi saranno margini per interventi regionali in materia».

[68] Cfr. decreto-legge 30 aprile 2020, n. 28, recante "Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19" (decreto-legge *Immuni*).

[69] Ci riferiamo alla nota del 21 aprile 2020, intitolata "Un aggiornamento sull'applicazione di *contact tracing* digitale per l'emergenza coronavirus", disponibile sul sito del Ministero interessato: www.innovazione.gov.it.

nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19»[70]. Inoltre si sottolinea come non solo l'app funziona su base volontaria, ma anche che «il mancato utilizzo dell'applicazione […] non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento»[71]. Ancora, si evidenzia come i programmi informatici di «titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione[72] […] sono resi disponibili e rilasciati sotto licenza aperta»[73]. Altresì si rileva come l'app è destinata alla sola finalità di tracciamento dei contatti senza provvedere alla geolocalizzazione degli interessati[74], e come essa possa essere eliminata in ogni momento con la conseguente rimozione di tutti i dati raccolti[75]. Relativamente a questo ultimo profilo si prevede ancora che la medesima app funzionerà solo sino a quando resterà in vigore lo stato di emergenza deliberato dal Consiglio dei Ministri in data 31 gennaio 2020 e comunque non oltre il 31 dicembre 2020: *dies ad quem* tutti i dati personali trattati saranno cancellati o resi definitivamente anonimi[76]. Il titolare del trattamento dei dati (*data controller*), ovvero quella figura cui il regolamento generale per la protezione dei dati personali affida il compito di decidere il 'perché'

[70] V. decreto-legge 30 aprile 2020, n. 28, art. 6, par. 1, corsivo aggiunto.

[71] Ivi, par. 4.

[72] Ivi, par. 5, dove si fa riferimento altresì alla circostanza per cui detta piattaforma «è realizzata dal Commissario di cui all'articolo 122 del decreto-legge 17 marzo 2020, n. 18 [ovvero dal Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19, NdA] convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, esclusivamente con infrastrutture localizzate sul territorio nazionale e gestite dalla società di cui all'articolo 83, comma 15, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133». Ai sensi di tale ultima disposizione si sancisce inoltre che «i diritti dell'azionista della società di gestione del sistema informativo dell'amministrazione finanziaria […] sono esercitati dal Ministero dell'Economia e delle Finanze».

[73] V. decreto-legge 30 aprile 2020, n. 28 (c.d. decreto-legge *Immuni*), art. 6, par. 5, dove si richiama – per intero, senza specificare i commi – l'art. 69 del c.d. Codice dell'amministrazione digitale, decreto-legislativo 7 marzo 2005. Tale ultima disposizione, intitolata «Riuso dei programmi informatici», prevede diversi obblighi. Al comma 1 si sancisce che le pubbliche amministrazioni titolari di programmi applicativi realizzati su indicazioni del committente pubblico sono obbligate a «darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni». A tal fine i commi 2 e 3 prevedono, rispettivamente, che i programmi sviluppati per conto dell'amministrazione «siano facilmente portabili su altre piattaforme», e che nei contratti per l'acquisizione di tali programmi siano inserite clausole che garantiscano il diritto di riuso. Al comma 4, inoltre, si prevede che nei medesimi contratti si possono includere delle clausole volte a vincolare per un determinato lasso di tempo il fornitore nel senso di obbligarlo a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso delle applicazioni.

[74] V. decreto-legge 30 aprile 2020, n. 28, art. 6, par. 2, lett. *c*: «il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi […] è esclusa in ogni caso la geolocalizzazione dei singoli utenti».

[75] *Ibidem*.

[76] *Ibidem*.

e il 'come' i dati devono essere trattati[77], è individuato nel Ministero della Salute, le cui funzioni sono esercitate in coordinamento con il Ministero per gli affari regionali e le autonomie, con i soggetti operanti nel Servizio nazionale per la protezione civile nonché con l'Istituto superiore di sanità[78].

Al Ministero della Salute è assegnata altresì la delicata stesura del documento relativo alla valutazione di impatto, prevista ai sensi dell'art. 35 del regolamento generale per la protezione dei personali[79] e approvata dall'Autorità garante per la protezione dei dati personali il 1° giugno 2020, con l'accompagnamento di un'articolata relazione nella quale si evidenziano diverse fragilità dell'app[80]. In tale ultimo documento, dopo avere analizzato il funzionamento dell'app in ogni fase[81], e dopo aver esaminato la raccolta e il trattamento degli ulteriori dati c.d. *analytics*[82],

[77] Secondo l'art. 4. par. 1, n. 7, del regolamento generale per la protezione dei dati personali, il titolare del trattamento è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le *finalità* e i *mezzi* del trattamento di dati personali».

[78] V. decreto-legge 30 aprile 2020, n. 28, art. 6, par. 1. Al Ministero della Salute, inoltre, spetta anche il controllo per cui i dati trattati dall'app *Immuni* sono «per impostazione predefinita […] esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19», individuati secondo i criteri stabiliti dal medesimo Ministero. Ivi, par. 2, lett. *b*.

[79] Ivi, par. 2. Più specificamente la valutazione di impatto è una procedura volta alla responsabilizzazione (*accountability*) del titolare del trattamento che il regolamento generale per la protezione dei dati personali richiede nelle ipotesi in cui il trattamento medesimo possa comportare un rischio elevato per i diritti e le libertà delle persone in ragione del monitoraggio sistematico dei comportamenti, del riferimento a dati sensibili *etc*. V. anche i considerando 84, 89, 93 e 95 del regolamento summenzionato, e le "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del regolamento (UE) 2016/679", adottate il 4 aprile 2017 e modificate da ultimo il 4 ottobre 2017, da parte del Gruppo di lavoro Articolo 29 per la protezione dei dati personali (oggi, come ricordato, sostituito dal Comitato europeo per la protezione dei dati personali).

[80] Cfr. "Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni", 1° giugno 2020, disponibile in www.garanteprivacy.it. Nella sezione dispositiva si evidenziano diversi punti critici (ben dodici), che fanno riferimento, *inter alia* e oltre quanto a riportato altrove: alla corretta informazione in ordine alla possibilità che l'app generi notifiche di esposizione che non riflettono una condizione di rischio; alla facoltà di disattivare temporaneamente l'app; a una maggiore attenzione al messaggio di allerta (tenendo conto del fatto che l'app è utilizzabile anche da parte di minori ultra quattordicenni); all'introduzione di misure volte ad assicurare il tracciamento delle operazioni compiute dagli amministratori di sistema; all'adozione di misure per mitigare i rischi derivanti dal caricamento di codici non riferiti a soggetti positivi a seguito di eventuali errori materiali o diagnostici.

[81] Il documento prende in esame, specificamente: *a*) l'installazione e la configurazione dell'app; *b*) l'interazione tra i dispositivi mobili degli utenti; *c*) la raccolta delle chiavi temporanee *Temporary Exposure Key* (TEK) dal dispositivo di un utente accertato positivo al Covid-19; *d*) la pubblicazione delle TEK degli utenti risultati positivi al Covid-19; ed *e*) il raffronto con gli identificativi di prossimità del dispositivo mobile denominato RPI (*Rolling Proximity Identifier*).

[82] Ci riferiamo alla circostanza per cui l'app raccoglie, oltre alle TEK degli utenti accertati positivi al Covid-19, ulteriori informazioni relative a «*Analytics* di tipo *Epidemiological Info*» e a «*Analytics* di tipo *Operational Info*». Al primo gruppo (*Analytics Epidemiological Info*) appartengono le informazioni che si trasmettono nel momento in cui si decide di effettuare il caricamento delle proprie

si presentano alcune osservazioni sul piano giuridico con riferimento a tre aspetti: *i*) la volontarietà dell'utilizzo dell'app; *ii*) le finalità dell'app; e infine *iii*) l'utilizzo dei dati pseudonimizzati.

Quanto al primo profilo l'Autorità garante osserva come la volontarietà debba permeare l'app nella sua interezza e dunque manifestarsi in modo trasparente in tutte le fasi funzionamento[83].

Per quanto concerne il secondo profilo, si ricorda che l'app persegue lo scopo «da un lato, di "allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi" e, dall'altro, di "tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legata all'emergenza Covid 19"». A tale riguardo l'Autorità garante specifica che nel trattare i dati relativi alla salute occorre rispettare quanto previsto dall'art. 9, par. 1, lett. *g*, del regolamento generale per la protezione dei dati personali e dall'art. 2 *sexies* del codice in materia dei dati personali[84]. Tali disposizioni concernono i tipi di dati che possono essere trattati, le operazioni eseguibili, l'interesse pubblico rilevante e le misure appropriate per tutelare i diritti fondamentali. Un «livello di dettaglio» che, secondo l'Autorità garante, «è riportato nella valutazione di impatto in esame».

TEK nel sistema. Dette informazioni concernono, *ex multis*: la provincia di domicilio; l'*Exposure Detection Summary*, ovvero una serie di dati relativi a *tutti* gli eventuali contatti a rischio avvenuti negli ultimi 14 giorni (ivi compresi il numero di giorni trascorsi dall'ultimo contatto a rischio, la durata aggregata dei contatti a rischio, la distinta per intervalli di intensità del segnale Bluetooth *etc.*); l'*Exposure Info*, ovvero una serie di informazioni relative a *ciascun* contatto a rischio avvenuto negli ultimi 14 giorni e che comprende, oltre a quanto riportato *supra*, il rischio di contagiosità associato alla TEK relativa al contatto a rischio.

Al secondo gruppo (*Analytics Operational Info*) appartengono i dati raccolti al fine di «capire statisticamente il livello di diffusione dell'app sul territorio e la correttezza del suo utilizzo» oltre che per «monitorare su base statistica l'epidemia, allocare in modo più efficiente le risorse sanitarie». Tali informazioni comprendono, *inter alia*: la provincia di domicilio; lo stato di attivazione dell'interfaccia Bluetooth e delle notifiche di esposizione; il sistema operativo del dispositivo mobile (iOS o Android); l'avvenuta ricezione di notifiche di esposizione al rischio; la data in cui è eventualmente avvenuta l'ultima esposizione al rischio *etc.*

[83] In particolare: «il download, l'istallazione, la configurazione, l'attivazione della tecnologia Bluetooth, il caricamento delle TEK sul *backend* di Immuni in caso di risultato positivo del tampone, la raccolta delle diverse categorie di *analytics* nelle fasi in cui si articola il trattamento, la consultazione del medico di fiducia dopo aver ricevuto un messaggio di allerta sul rischio di essere entrato in contatto stretto con soggetti risultati positivi, la disinstallazione dell'applicazione». Sul tema v. anche i punti n. 24 e 31 delle *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, elaborate dal Comitato europeo per la protezione dei dati personali il 21 Aprile 2020, cit. *retro*, par. 3.

[84] V. decreto-legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", in *Gazzetta Ufficiale* n. 174 del 29 luglio 2003, così come modificato dal decreto-legislativo 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

Per quanto concerne, infine, il ricorso ai dati pseudonimizzati, l'Autorità garante ricorda come, ai sensi dell'art. 25 del regolamento generale per la protezione dei dati personali, la pseudonimizzazione costituisca una misura c.d. di *privacy by design* che rappresenta «un adempimento e non […] una tecnica di anonimizzazione dei dati». Essa è costituita da uno speciale trattamento che non consente l'attribuzione dei dati personali a un interessato senza il ricorso a informazioni aggiuntive. Ne consegue che affinché il sistema funzioni correttamente occorre che le due componenti (dato pseudonimizzato, da un lato, e informazione aggiuntiva, dall'altro) siano ben separate. Nel contesto del *contact tracing* tale scopo è realizzato attraverso la distribuzione ai partecipanti delle chiavi TEK (ovvero del risultato della pseudonimizzazione), ma non delle chiavi di co-decodifica (ovvero delle informazioni aggiuntive). Per questa ragione l'Autorità garante conclude che, sulla base dello stato dell'arte, un adeguato sistema di custodia delle chiavi di decodifica da parte del soggetto centrale (il solo in grado di consentire la re-identificazione «per ragioni meramente funzionali all'operatività del sistema») possa configurare uno schema di pseudonimizzazione idoneo[85].

Premesse tali considerazioni, dalla lettura combinata del decreto-legge 30 aprile 2020, n. 28 e della relazione dell'Autorità garante sul documento relativo alla valutazione di impatto presentato dal Ministero della Salute emergono talune criticità, come quelle relative alle indeterminatezze in merito al regime di comunicazione tra dispositivi e server. Il punto è già evocato dalla lettura del decreto-legge c.d. *Immuni*, allorquando, al par. 2, lett. *e*, si fa riferimento alla circostanza per cui i dati «relativi ai contatti stretti siano conservati, *anche* nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della Salute» (corsivo aggiunto). A tale riguardo i dubbi che possono sorgere intorno alla congiunzione "anche" sono indirettamente avallati dall'Autorità garante per la protezione dei dati personali, la quale, sempre nel documento appena citato, specifica che «non è chiaro se vengano conservati gli indirizzi IP dei dispositivi mobili che interagiscono con il *backend*».

[85] «[C]onsentendo così la corretta applicazione dell'art. 6 comma 2, lett. *c*), del d.l. n. 28/2020, nonché, su tale base, la pubblicazione delle TEK dei soggetti risultati positivi». Secondo l'opinione di G. COMMANDÉ, «l'anonimato in quanto tale, ammesso che possa esistere, non protegge più. Non da solo almeno». Per questa ragione «sarebbe più corretto dire che il GDPR non si applica a "informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato». Salvo poi, specificare: «Eccoli i dati "sufficientemente anonimi", quei dati che l'architettura del trattamento (finalità, modalità, soggetti coinvolti...), le misure tecniche ed organizzative (comprese quelle per la sicurezza dei dati) tenuto conto delle tecnologie, dei costi e del tempo necessario per la reidentificazione permettono di considerare come anonimi *fino a quando i costi, le tecnologie e l'interesse alla reidentificazione non cambieranno*» (corsivo aggiunto). ID., "Non sparate sulla app di tracing e fidiamoci del Gdpr: ecco perché", in Agenda Digitale, 28 aprile 2020, disponibile su www.agendadigitale.eu.

12. La conformità dell'app *Immuni* alle normativa internazionale in materia di dati personali

Come osserva correttamente il Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza" della *Task Force Immuni*[86], da una prospettiva normativa «tanto che si guardi al diritto alla protezione dei dati personali, tanto che si guardi a qualsiasi altro diritto fondamentale» il problema della sostenibilità del ricorso a una soluzione del tipo di quella incorporata in *Immuni* «va, innanzitutto, affrontata e risolta in una logica di bilanciamento dei diritti […] in ossequio a un criterio di necessità e proporzionalità».

Le norme alla luce delle quali valutare detto bilanciamento sono innanzitutto, per l'Italia, il regolamento generale per la protezione dei dati personali e il decreto-legislativo 196/2003 nel testo modificato dal decreto-legislativo 101/2018[87], oltre ad altre disposizioni di derivazione internazionale.

Una disamina completa di tali norme, con particolare attenzione a quelle di rilevanza internazionale, è stata già approntata in occasione di uno scritto precedentemente richiamato[88]. In questa sede ci limiteremo a rievocare alcuni punti essenziali, concernenti i principali obblighi che si possono desumere dalla normativa internazionale, per concludere sul modo in cui detti obblighi possono entrare in bilanciamento con l'esigenza di tutela della salute espressa attraverso il ricorso a strategie di *contact tracing*.

A tale riguardo va innanzitutto rilevato che le principali norme di diritto internazionale rilevanti si collocano all'interno di alcune convenzioni a carattere settoriale e/o regionale.

Un esempio è rappresentato dall'art. 17 del Patto internazionale sui diritti civili e politici relativo al divieto di interferenze arbitrarie o illegittime nella vita privata[89].

[86] Cfr. "Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di *contact tracing* per il contrasto al COVID-19", disponibile su www.innovazione.gov.it.

[87] Cfr., rispettivamente, il decreto-legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali", cit.; e il decreto-legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679", cit.

[88] G. DELLA MORTE, "La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze sorveglianza di massa", cit., nota 1.

[89] Sul punto v. F. TAMMONE, "*Nous sommes en guerre*: la lotta globale alla pandemia alla prova del Patto internazionale sui diritti civili e politici", in *SIDIBlog*, 27 marzo 2020, disponibile su www.sidiblog.org. Al riguardo è sufficiente menzionare come il Comitato dei diritti umani ricordi che, poiché «all persons live in society, the protection of privacy is necessarily relative» (*General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 aprile 1988, par. 7). Considerato, poi che nel quadro dell'art. 17 non è prevista alcuna eccezione, si applica il regime di deroghe generali sancito dall'art. 4 del medesimo Patto. Ai sensi di tale disposizione in caso di pubblica emergenza che sia ufficialmente dichiarata e che attenti alla vita della nazione gli Stati parte hanno la possibilità di derogare agli obblighi sanciti «to the extent strictly required by the exigencies of the situation». Tuttavia

Diversamente, per quanto concerne le convenzioni a portata regionale un esempio è costituito dalle norme riscontrabili nell'ambito del Consiglio d'Europa[90] o ancora dalla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale adottata a Strasburgo il 28 gennaio 1981 (c.d. Convenzione 108)[91]. Un'attenzione speciale meritano, poi, le norme elaborate nel quadro dell'Unione europea, considerata anche l'eccezionale rilevanza che la protezione dei dati personali ha acquisito in tale ambito[92]. Il già menzionato regolamento generale per la protezione dei dati personali sancisce diverse obblighi a riguardo: innanzitutto si dispone, all'art. 23, che ogni limitazione apportata da uno Stato membro UE ai principi in esso iscritti debba garantire «l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica»; poi si prevede più dettagliatamente che tali limitazioni debbano necessariamente essere disposte, ai sensi del par. 1, «mediante misure legislative», che contengano, ai sensi del successivo par. 2, indicazioni relative a: *a*) le finalità di trattamento; *b*) le categorie di dati personali; *c*) la portata delle limitazioni introdotte; *d*) le garanzie per prevenire abusi o illeciti; *e*) l'indicazione del titolare del trattamento; *f*) i periodi di conservazione e le garanzie applicabili; *g*) i rischi per i diritti e le libertà degli interessati; e *h*) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità medesima[93].

Ulteriore attenzione è riservata al tema dalla Carta dei diritti fondamentali dell'Unione europea, il cui art. 52 dispone che eventuali limitazioni all'esercizio dei diritti e delle libertà devono essere previste dalla legge e rispettare il contenuto

anche quest'ultima disposizione deve essere interpretata alla luce del *General Comment* summenzionato. Il relativo par. 8 specifica che «relevant legislation *must specify in detail the precise circumstances* in which such interferences may be permitted» (corsivo aggiunto).

[90] È questo il caso dell'art. 8 della Convenzione europea dei diritti umani dedicato al rispetto della vita privata e familiare. Il secondo paragrafo di tale disposizione, specificando le condizioni che permettono alle autorità pubbliche di interferire con gli obblighi, fa riferimento alle seguenti tre circostanze: che le interferenze siano previste dalla legge; che siano necessarie nel quadro di una società democratica; che corrispondano agli scopi tutelati, quali, *inter alia*, la protezione della salute.

[91] Si tratta della c.d. Convenzione 108, il cui art. 6 è dedicato alla protezione delle categorie 'speciali' di dati che richiedono una tutela rafforzata. Tra questi ultimi si annoverano i dati riferibili alla salute degli individui.

[92] V. anche *retro*, paragrafo 6.

[93] Occorre poi specificare che le limitazioni in questione non concernono semplici «dati personali», ma quella categoria protetta che, ai sensi dell'art. 4, n. 15, del regolamento anzidetto concerne i dati attinenti alla salute, compresa la prestazione di servizi di assistenza sanitaria (cfr. anche i considerando n. 35 e il n. 51). Tali dati meritano una tutela rafforzata, specificata all'art. 9, par. 2, del regolamento medesimo. Anche la protezione di questi dati, tuttavia, è suscettibile di compressioni, e a noi sembra che nel novero delle eccezioni assumono rilevanza: i trattamenti necessari a scopi di diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei servizi o sistemi sanitari (lett. *h*, e considerando n. 53); e l'interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici (lett. *i*, e considerando n. 54).

essenziale di tali diritti e libertà[94]. Infine, va menzionata la direttiva *ePrivacy* del 2002[95], il cui art. 15 fissa la possibilità per gli Stati membri dell'Unione europea di limitare con disposizioni legislative gli obblighi in materia di riservatezza dei dati sul traffico, richiedendo al contempo che dette limitazioni avvengano per finalità determinate e in una misura necessaria, opportuna e proporzionata all'interno di una società democratica.

Nello studio evocato *supra*, al termine di un esame più articolato degli obblighi contenuti nei diversi strumenti internazionali, concludevamo nel senso per cui le deroghe agli obblighi internazionali in materia di tutela alla protezione dei dati personali motivate da esigenze di salute dovessero soddisfare le seguenti condizioni: (*i*) formalità; (*ii*) indispensabilità; (*iii*) finalità: (*iv*) tassatività; (*v*) temporalità; (*vi*) impugnabilità; (*vii*) proporzionalità. Molti di questi criteri, e in particolare quelli relativi ai punti (*i*), (*iii*), (*iv*), (*v*) e (*vi*) possono essere considerati assolti dall'app *Immuni*. Alcuni dubbi possono sorgere sui punti (*ii*), relativo all'indispensabilità nel quadro di una società democratica; e (*viii*) relativo alla proporzionalità dell'interferenza rispetto allo scopo perseguito. Premesso che un giudizio più maturo su questi ultimi due aspetti richiederebbe una più lunga osservazione del *modus operandi* dell'app, su tali ultimi aspetti si ritornerà nel corso dei paragrafi che seguono e, segnatamente, nelle conclusioni[96].

13. Le luci: quattro pregi dell'app *Immuni*

Premesse tutte le riflessioni avanzate sino ad ora, è giunto il momento di fissare alcuni elementi utili a una corretta comprensione delle luci e delle ombre, ovvero dei pregi e delle criticità del sistema approntato dal Governo italiano. Solo in seguito, in guisa di conclusione, si avanzeranno talune riflessioni sulle 'penombre': ovvero sul contesto e quindi sul difficile esercizio di bilanciamento.

Cominciando dagli elementi positivi, la prima caratteristica positiva dell'app, già evocata in precedenza[97], è quella relativa al fondamento giuridico. Esso è stato correttamente individuato nella salute pubblica e, come richiesto dal Comitato europeo per la protezione dei dati[98], ha assunto le vesti di un decreto-legge che promuove l'impiego di app su base volontaria senza alcuna penalizzazione per chi non intende farne uso[99].

[94] Ai sensi di tale norma si dispone inoltre che dette limitazioni devono essere adottate «nel rispetto del principio di proporzionalità [e] solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

[95] Sulla quale v. anche *retro*, paragrafo 3.

[96] V. *infra*, paragrafo 15.

[97] V. *retro*, par. 3, 10 e 11.

[98] V. *retro*, par. 3, dove si richiama il parere reso alla Commissione il 14 aprile 2020.

[99] Cfr. *European Data Protection Board Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, elaborata il 14 aprile 2020, cit.

La seconda caratteristica positiva dell'app risiede nel tratto, oltre che gratuito, volontaristico. Sebbene tale ultimo aspetto si traduca anche in un *vulnus* – dal momento che il carattere facoltativo comporta inevitabilmente una riduzione del numero di utenti – esso appare in linea, come più volte rimarcato, con quanto richiesto dalle autorità europee e dal Garante italiano per la protezione dei dati personali[100] (che ha anche sottolineato come tale tratto volontaristico debba attraverso tutte le diversi fasi nelle quali si articola il funzionamento dell'app[101]). Qualche dubbio potrebbe nascere nel caso di proposte dirette a incentivare il ricorso all'app come *condicio sine qua non* per l'accesso a taluni servizi (il Sottosegretario alla Salute, ad esempio, ha evocato a mezzo stampa la possibilità di ricevere via app i certificati del medico curante[102]). Nel caso, occorrerà vigilare scrupolosamente sulla forma e il contenuto di tali incentivi o 'associazioni di servizi' al fine di escludere manifestazioni di coercizione indiretta che svuoterebbero l'adesione volontaria del contenuto che gli è proprio[103].

Una terza caratteristica positiva dell'app è riferibile all'attenzione volta all'architettura decentralizzata e pubblica del sistema di raccolta e conservazione dei dati. Infatti, non solo *Immuni* non è in grado di geolocalizzare l'utente e non può accedere alla rubrica dei contatti né al numero di telefono, ma l'intero sistema di dati registrabili, in seguito a un parziale cambio di prospettiva rispetto ai progetti originari, si caratterizza oggi per un modello più decentralizzato. In sostanza gli sviluppatori di *Immuni*, insieme con i tecnici del Ministero per l'innovazione, hanno apportato alcune modifiche in corso di elaborazione dell'app al fine di rafforzare la sicurezza dei dati e andare incontro alle specifiche tecniche richieste dall'accordo Google-Apple[104]. Più specificamente nell'ultima versione le chiavi crittografiche sono generate direttamente nei dispositivi del singolo utente in luogo che nei server. In termini concreti ciò significa che «ogni volta che due cellulari 'si incontrano' (ovvero rimangono ad una certa distanza per un certo tempo […]), si scambiano il proprio identificativo anonimo generato localmente con crittografia»[105]. Da ciò si desume che il dispositivo che ha installato l'app porta con sé soltanto una lista di codici privi di qualsiasi elemento identificativo della persona e

[100] V. *retro*, par. 3 e par. 9.

[101] V. *retro*, par. 11.

[102] Così in un intervista del 24 aprile 2020 rilasciata al Corriere della Sera: «più che incentivi, parola che sa di commerciale, parlerei di ulteriori servizi al cittadino».

[103] È di questo parere anche il Sottogruppo di lavoro incaricato delle questioni giuridiche all'interno della *Task Force Immuni*: «sono assolutamente sconsigliate, perché di dubbia costituzionalità, forme di incentivo che graduino/limitino l'accesso dei cittadini a servizi altrimenti fruibili secondo principi di parità di trattamento o che vincolino l'esercizio di diritti di libertà all'adozione dell'app». Cfr. "Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di *contact tracing* per il contrasto al COVID-19", cit.

[104] Su tale accordo v. *retro*, par. 5.

[105] «Viene così meno una possibilità di re-identificare i soggetti. Solo chi riceve la notifica sa di esserlo stato». R. BERTI, A. LONGO, S. ZANETTI, "Immuni, cos'è e come funziona l'app italiana coronavirus", cit.

che le chiavi di decodifica sono gestite in modo separato nel rispetto di quanto richiesto dalla normativa di riferimento[106].

Infine, quarto e ultimo tratto positivo, come previsto dall'ordinanza del 16 aprile 2020 e come ribadito dallo stesso Ministero per l'innovazione con nota del 21 aprile 2020, il codice sorgente è rilasciato con licenza *open source*. Detto codice, insieme con la restante documentazione tecnica di *Immuni*, è stato reso pubblico sul sito del Ministero per l'innovazione il 26 maggio 2020 con queste parole di accompagnamento: «Il codice aperto è un *bene comune* del nostro Paese, della community degli sviluppatori italiani e internazionali» (corsivo aggiunto) [107].

14. Le ombre: quattro criticità dell'app *Immuni*

Come accennato in precedenza sono tre i passaggi peculiari intorno ai quali si struttura il funzionamento dell'app: la registrazione dei contatti di prossimità in forma pseudonimizzata, l'avviso in caso di contagio, e il *follow up* delle persone interessate dal rischio[108]. Ciascuno di questi momenti è caratterizzato da alcune criticità. Tuttavia, prima di esaminarle nel dettaglio, occorre soffermarsi su una questione preliminare che attraversa l'intero discorso sulla valutazione: la diffusione dell'app.

La prima osservazione critica concerne dunque la (probabile) scarsa diffusione dell'app e la difficoltà di scongiurare quest'evenienza. Come osserva il Sottogruppo di lavoro dedicato ai problemi giuridici di *Immuni*, «prima ancora di addentrarsi nell'esame delle questioni giuridiche […] sembra essenziale affrontare la questione della sussistenza di idonei elementi utili a ritenere che l'app […] possa effettivamente essere scaricata e utilizzata regolarmente da una percentuale rilevante della popolazione da identificarsi sulla base degli studi epidemiologici in corso»[109]. Lo

[106] V. quanto osservato *retro*, par. 11. Inoltre il server è un'infrastruttura pubblica appartenente a una Società di informatica di proprietà ministeriale (Sogei) da anni impegnata nel processo di trasformazione digitale della Pubblica Amministrazione. La questione è tanto più importante in quanto, come ricordato, oltre ai dati relativi ai contagi, anche i c.d. *analytics* svolgono una funzione importante: grazie alle elaborazioni del server sarà possibile apprendere quanti soggetti sono stati allertati in ogni provincia, quanti di questi hanno in seguito contratto il contagio *etc*. Proprio con riferimento a questa ulteriore categoria di dati nella relazione dell'Autorità garante si ricorda come «tali informazioni non possono essere considerate dati anonimi [poiché] consentono, in diversi contesti, concrete possibilità di re-identificazione degli interessati, soprattutto se associate ad altre informazioni ovvero in caso di morbilità non elevata o di ambiti territoriali con bassa densità di popolazione», sottolineando al contempo come «nella valutazione d'impatto non sono adeguatamente precisate le modalità con cui il Ministero della Salute intende trattare e conservare le diverse tipologie di *analytics* raccolti».

[107] Cfr. Ministero per l'Innovazione su www.innovazione.gov.it. Tuttavia, nella relazione dell'Autorità garante che approva il documento relativo alla valutazione di impatto predisposto dal Ministero della Sanità (sul quale sempre *retro*, par. 11) si evidenziano anche i rischi connessi a tale codice *open source* (v., in particolare il par. 7). Si menziona, ad esempio, la possibilità che le informazioni inviate con tecnologia Bluetooth possano essere rilevati anche da terzi attraverso apparati di scansione (c.d. *sniffer*) in grado di intercettare la trasmissione per usi impropri.

[108] V. *retro*, par. 9.

[109] Cfr. "Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19", cit.

stesso Sottogruppo rileva come, secondo la Commissione europea, il nostro Paese si è collocato – nel 2019 – al 24° posto fra i 28 Stati membri dell'UE secondo l'indice DESI (*Digital Economy and Society Index*) che monitora le prestazioni digitali e misura i progressi compiuti dai paesi dell'UE in termini di competitività digitale[110]. Sulla scorta di quanto osservato si evidenzia come l'obiettivo di ampia diffusione dell'app appaia «estremamente ambizioso» e all'uopo si raccomanda, prima di ogni altra valutazione, un attento esame degli strumenti comunicativi, regolamentari e tecnologici «utilizzabili al fine di rendere raggiungibile il predetto obiettivo di diffusione»[111]. La questione appare tanto più perniciosa in quanto le stime iniziali, avvalorate dall'Autorità garante per la protezione dei dati personali, si assestavano intorno a una percentuale di popolazione attiva piuttosto elevata: il 60%[112]. Appare evidente che nel caso di *Immuni*, trattandosi di un'app scaricabile solo su base volontaria nel contesto di una popolazione anziana e con scarsa dimestichezza ad adoperare le funzioni più avanzate degli smartphone, risulta estremamente difficile immaginare una diffusione su così larga scala. Anche per questa ragione nel corso di interventi successivi si è fatto riferimento a soglie decisamente più contenute (25%-30%)[113]. Né sarebbero legittime, come pure abbiamo avuto modo di osservare, forme di incentivazione diretta o indiretta a scaricare e attivare l'app, in particolare collegando l'utilizzo della medesima alla possibilità di usufruire di alcuni servizi sanitari di base[114].

La seconda criticità concerne la prima delle tre fasi evocate: quella della registrazione bidirezionale della prossimità tra due smartphone che hanno scaricato e attivato *Immuni*. Come rilevato in precedenza[115], allo stato attuale dello sviluppo tecnologico del sistema Bluetooth il rischio di un elevato numero di falsi (tanto positivi quanto negativi) è più che plausibile. Infatti, come correttamente osservato in uno studio edito dal *MIT Technology Review* se, in teoria «the amount of power is proportional to distance, so it can be used to gauge how far the two phones are

[110] Lo stesso sottogruppo di lavoro rileva che l'Italia appare, al contempo, «in buona posizione, sebbene ancora al di sotto della media dell'UE, in materia di connettività e servizi pubblici digitali». *Ibidem.*

[111] *Ibidem*.

[112] «Il *contact tracing* necessita dell'adesione di circa il 60% della popolazione: se si riesce a sensibilizzare tale quota di cittadini, il risultato potrebbe essere a un tempo rispettoso della privacy e proficuo per il contenimento dei contagi». Così il Presidente dell'Autorità garante per la protezione dei dati personali in "Le app degli spostamenti solo su base volontaria", disponibile in www.garanteprivacy.it, 17 aprile 2020. Per un approfondimento dal punto di vista epidemiologico v., *ex multis*, L. FERRETTI, CHRIS WYMANT, M. KENDALL *et al*., "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing", in *Science*, disponibile su www.science.sciencemag.org, 8 maggio 2020.

[113] Istruttiva al riguardo è l'audizione in videoconferenza del Ministro per l'Innovazione sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus, 29 aprile 2020, disponibile su www.webtv.senato.it.

[114] V. *retro*, le osservazioni già espresse nel par. precedente in merito al carattere volontario dell'app.

[115] V. *retro*, paragrafo 4.

from one another», nella pratica «many things can mess that signal up and make the data incorrect» sicché, di fatto, per funzionare correttamente attraverso Bluetooth l'app «needs bigger, better data»[116]. Purtroppo quest'ulteriore mole di dati implicherebbe proprio quelle restrizioni sul piano della *privacy* che si intendevano eludere ricorrendo, appunto, alla tecnologia Bluetooth in luogo di quella che consente una geolocalizzazione. Si consideri, *ex multis*, l'esempio di due smartphone che abbiano abilitato l'app e che registrino la reciproca presenza nonostante siano separati da una parete. Sebbene in simili circostanze non sarebbe possibile trasmettere il contagio, l'app potrebbe comunque registrarne il rischio (falso positivo), così come potrebbe non rilevare la presenza di un soggetto contagioso all'interno di uno spazio in cui il segnale di connettività Bluetooth si manifesti come scarso o disturbato (falso negativo). Sul punto il protocollo elaborato da Apple e Google svolge un ruolo essenziale perché è da esso che dipende l'elaborazione corretta del rischio contagio sulla base della distanza spaziale e temporale. Tuttavia la circostanza in sé (ovvero: la circostanza per cui simili variabili dipendano da un accordo tra società private), come specificheremo a breve esaminando le 'penombre', non è al riparo da qualche perplessità[117].

La terza criticità attiene alla natura dell'algoritmo che calcola il rischio del contagio. Nel documento con il quale l'Autorità garante approva la valutazione di impatto predisposta dal Ministero della Salute si osserva in via preliminare che non sono ancora individuati «i criteri epidemiologici di rischio e i modelli probabilistici su cui si basa l'algoritmo, né i parametri di configurazione impiegati corredati dalle assunzioni effettuate»[118]. Per questa ragione nella parte del documento menzionato dedicato alle raccomandazioni figura quella di «indicare puntualmente» le caratteristiche dell'algoritmo, «specificando i parametri di configurazione impiegati e le assunzioni effettuate [e] rendendolo disponibile alla comunità scientifica»[119].

La quarta criticità concerne il *follow up* che segue l'auto-dichiarazione di contagio, nella misura in cui l'app risulta del tutto inefficace se il Governo non fa seguire allo scambio dei dati diverse azioni di tipo positivo, a partire dal sottoporre a tampone tutti i soggetti che hanno avuto contatti con le persone contagiate. Il

[116] «Things like walls, human bodies, pockets, or even proximity to several phones at once can throw the measurements off». Così P. HOWELL O'NEIL, "Bluetooth contact tracing needs bigger, better data", in *MIT Technology Review*, 20 aprile 2020, disponibile su www.technologyreview.com.

[117] V. *infra*, paragrafo 15.

[118] In conformità con quanto disposto dall'art. 6, comma 2, lett. *b*, del decreto legge *Immuni*, il quale prevede che l'individuazione del contatto di prossimità avvenga «secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure tecniche e organizzative contenute nella valutazione d'impatto». Cfr. il "Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 – App Immuni", cit., par. 2.

[119] In merito all'esigenza di «superamento della alternativa, in materia di decisioni completamente automatizzate, fra divieto generale operante *ex ante* e diritto soggettivo *azionabile ex post*», v. le recenti osservazioni di A. ODDENINO (che schiudono interessanti prospettive di ricerca) in "Decisioni algoritmiche e prospettive internazionali di valorizzazione dell'intervento umano", in *Diritto Pubblico Comparato ed Europeo on line* 2020, disponibile su www.dpceonline.it, p. 199 ss., in particolare p. 217.

punto è delicato perché, se tali azioni positive fossero particolarmente penalizzanti – se si fosse deciso, ad esempio, di obbligare alla quarantena tutti coloro che sono stati 'tracciati' in prossimità di un soggetto poi dichiarato positivo – il risultato concreto si tradurrebbe in un drastico calo del ricorso alla medesima app[120]. In ogni caso, come rileva il Sottogruppo di lavoro dedicato alle questioni giuridiche di *Immuni*, anche immaginando una sufficiente distribuzione dell'app, detta condizione, da sola, non sarebbe comunque garanzia di efficacia, se «non fosse accompagnata da un'efficace organizzazione dei necessari presidi sanitari e dell'attività logistica necessaria, tra l'altro, alla distribuzione e esecuzione dei test tra i cittadini»[121]. Sicché, si aggiunge, «come risulta chiaro anche dall'esame delle esperienze straniere […] la componente tecnologica è, in ogni caso, "solo" una delle componenti»: in assenza del *testing* e del *treatment* che seguono l'avvertimento del rischio del contagio, l'adozione di soluzioni tecnologiche risulterebbe improduttiva di benefici significativi[122].

15. Le penombre: conclusioni

In un documento intitolato *Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems*, alcuni tra i più influenti teorici contemporanei del cyberspazio[123] hanno elaborato una griglia di riferimento in cui accanto ai parametri legali[124] si introduce un'ulteriore cornice di valutazione fondata su ben dodici «enabling factors» che a giudizio degli autori dovrebbero orientare la risposta alla questione «is the Digital tracking and tracing being developed correctly?». A tale fine si presenta per ciascuna domanda un segno positivo (+) o negativo (–), alla somma dei quali corrisponde un maggiore o minor punteggio di risposta affermativa al quesito. Considerato che la verifica di compatibilità giuridica è già stata affrontata in occasione

[120] A riguardo si è innanzitutto previsto un *call center* di primo e di secondo livello. Quello di 'primo' avrà come destinatari i cittadini che si trovano in difficoltà nell'adoperare l'app e ancora i medici che sono chiamati ad applicare 'un gestionale' della medesima. Quello di 'secondo' avrà come destinatario quanti si siano trovati in contatto con un cittadino dichiarato positivo: costoro interloquiranno con un operatore sanitario cui spetterà il compito di spiegare nel dettaglio le successive fasi. In tal senso l'audizione del Ministro per l'Innovazione del 29 aprile 2020, cit.

[121] Cfr. "Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di *contact tracing* per il contrasto al COVID-19", cit.

[122] «A cosa servirebbe la più intelligente, efficace, pervasiva ed invasiva delle applicazioni tecnologiche se, una volta scovati i soggetti a rischio, non vi fosse la capacità di eseguire test e, a valle, di impartire ad essi le protezioni e poi le cure più adeguate? A (quasi) nulla». Così L. BOLOGNINI, "Il bilanciamento tra diritti, libertà e interessi pubblici nel *contact tracing* è questione di alta politica", 21 maggio 2020, in www.medialaws.eu.

[123] Cfr. J. COWLS, L. FLORIDI, J. MORLEY e M. TADDEO, "Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems", disponibile sul sito del *Oxford Internet Institute* dell'Università di Oxford: www.oii.ox.ac.uk.

[124] Individuati nelle seguenti categorie: «Interventions must be *necessary* to achieve a specific public health objective, *proportional* to the seriousness of the public health threat; *scientifically sound* to support their effectiveness; and *time-bounded*». Per un confronto con i parametri di conformità agli obblighi internazionali adoperati nel presente scritto si rimanda a quanto espresso *retro*, paragrafo 12.

dell'esame degli obblighi internazionali in materia[125] si è ritenuto opportuno, in guisa di conclusione, sottoporre *Immuni* a quest'ultimo test, nella consapevolezza che quanto «may be ethically justifiable in a country with a small and digitally literate population, like Singapore, may not be simply importable as a solution for a country with a much larger population and a more significant digital divide»[126].

Seguendo lo schema proposto, e cioè assegnando un segno positivo oppure negativo a ogni singola questione, il risultato suggerito è il seguente: (1) si tratta di un'app volontaria? (+)[127]; (2) è un'app che attribuisce il giusto rilievo al consenso? (+); (3) si tratta di un'app che preserva l'anonimato? (+)[128]; (4) i dati trattati dall'app possono essere eliminati dagli utenti? (+)[129]; (5) la finalità dell'app è chiaramente specificata? (+); (6) la finalità dell'app è chiaramente delimitata? (+)[130]; (7) l'app è adoperata solo per fini preventivi? (+)[131]; (8) l'app è adoperata per monitorare la condotta degli utilizzatori? (+); (9) l'app è *open source*? (+); (10) l'app è scaricabile da tutti allo stesso modo? (+)[132]; (11) l'app è accessibile a tutti allo stesso modo? (+)[133]); (12) l'app prevede un termine per il proprio funzionamento? (+).

Alla luce di questo rapido esame si comprende plasticamente come il Governo italiano abbia tenuto in massima considerazione le indicazioni europee volte a rafforzare il versante delle garanzie ed in tale ampio contesto che occorre iscrivere la vicenda dell'app *Immuni*[134]. Tuttavia, giacché il c.d. *soluzionismo digitale* non rappresenta una panacea[135], *Immuni* non è in alcun modo sufficiente a risolvere da sola

[125] V. *retro*, paragrafo 12.

[126] «Similarly, what was ethically justifiable in one place yesterday may not be so tomorrow as circumstances and attitudes change».

[127] Sui rilievi dell'Autorità garante per la protezione dei dati personali in materia, v. *retro*, par. 11.

[128] Con particolare riferimento all'esclusione della geolocalizzazione e a alla decentralizzazione.

[129] Quanto meno con riferimento alla possibilità di eliminare l'app medesima.

[130] Nella misura in cui non si fa menzione della possibilità di aggiornamenti idonei ad estenderne le funzioni.

[131] Nel senso che essa è adoperata per abbattere la curva dei contagi e non per attribuire ulteriori benefici a chi ne fa uso.

[132] Al riguardo occorre tenere conto di quanti non possono disporre di uno smartphone: ad esempio i detenuti.

[133] Il punto critico è il rispetto degli standard europei in materia di accessibilità dei prodotti relativi alla tecnologia dell'informazione alle persone con disabilità dal momento che, trattando l'app informazioni relative ai dati sensibili in materia di stato di salute, l'inserimento di tali dati non potrà essere delegato a terzi. Così E. PELLINO e F. SARZANA, "App coronavirus, 10 domande urgenti al Governo italiano", in *Agenda Digitale*, 17 aprile 2020, disponibile su www.agendadigitale.eu.

[134] Secondo alcuni tale attenzione sul versante delle garanzie si è spinto sino a sacrificare l'efficacia stessa del tracciamento: «Risultato: massima tutela della privacy, almeno in astratto, ma grande debolezza in termini di efficacia […] Insomma, meccanismi di allerta più simile a una "pubblicità progresso 2.0", sensibilizzante e mirata, che a strumenti emergenziali di sanità pubblica». Così L. BOLOGNINI, "Il bilanciamento tra diritti, libertà e interessi pubblici nel *contact tracing* è questione di alta politica", cit.

[135] Come ricorda E. NADRELLI in "The emergency of digital solutionism" (disponibile su www.broadband4europe.com, 6 aprile 2020), «[t]he term "digital solutionism" was introduced in 2013 by Evgenj Morozov to indicate an approach advocating the use and diffusion of digital systems and applications as a tool for solving problems that are essentially social and actually need first and

i numerosi problemi che si manifestano sul versante del rischio epidemico. La chiave interpretativa deve essere dunque ampia e olistica[136] e all'interno di quest'ultima persistono alcune zone poco chiare, qui definite in 'penombra'. La prima concerne la questione della necessità e della proporzionalità della misura nel contesto italiano; la seconda quella dell'apporto di attori privati nell'esercizio di funzioni pubbliche.

Cominciando dalla prima questione, secondo la relazione del Sottogruppo di lavoro "Profili giuridici della gestione dei dati connessa all'emergenza" della *Task Force Immuni*[137], tra gli elementi fondativi della valutazione doveva ritenersi il seguente: che la soluzione adottata – nelle sue componenti tecnologiche e non tecnologiche – fosse considerata efficace sul piano epidemiologico almeno in una dimensione prognostica, giacché in caso contrario sarebbe risultata illegittima anche una minima compressione dei diritti e delle libertà fondamentali[138]. La questione che emerge è quella di un delicato bilanciamento: da un lato, occorre comprimere la tutela dei dati personali e, dall'altro, accertarsi che tali limitazioni siano necessarie e proporzionali ai benefici concreti che l'app è in grado di produrre sul terreno del contrasto all'epidemia. Su questo fronte il Garante europeo per la protezione dei dati personali ha redatto due documenti di grande interesse: "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit" del 11 aprile 2017; e "European Data Protection Supervisor Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data" del 19 dicembre 2020[139]. Dall'esame

foremost a political answer». L. MCGREGOR, "Contact-tracing Apps and Human Rights", cit., aggiunge: «This has led to some commentators asking whether contact-tracing apps are just another example of techno-solutionism or as Ross Anderson has suggested, 'do-something-itis'».

[136] In altri termini *Immuni* deve essere esaminata e valutata sullo sfondo di una strategia complessiva dove, accanto al *tracing*, coesistano anche il *testing* dei soggetti a rischio e soprattutto il *treatment* degli individui contagiati (ci riferiamo qui alla strategia delle c.d. tre 't' menzionate in apertura. V. *retro*, paragrafo 1).

[137] Cfr. "Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19", cit.

[138] Gli altri elementi presi in considerazione sono: (*a*) che l'intero sistema di *contact tracing* fosse gestito da soggetti pubblici e che il suo codice fosse aperto e suscettibile di revisione da qualunque soggetto indipendente intenda studiarlo; (*b*) che i dati trattati ai fini dell'esercizio del sistema fossero resi sufficientemente anonimi da impedire l'identificazione dell'interessato tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della re-identificazione almeno in condizioni ordinarie e salvo il verificarsi di eventi patologici o, almeno, pseudo-anonimi previa adozione di idonee misure idonee a limitare il rischio di identificazione degli interessati; (*c*) che la decisione di usare la soluzione tecnologica fosse liberamente assunta dai singoli cittadini; (*d*) che raggiunta la finalità perseguita tutti i dati, con l'eccezione di dati aggregati e pienamente anonimi a fini di ricerca o statistici, fossero cancellati; […] (*f*) che la soluzione adotti misure tecniche ed organizzative che minimizzino i rischi di re-identificazione in ogni fase di vita del sistema (a titolo esemplificativo con variazione periodica e casuale dell'ID anonimo dell'applicazione).

[139] Entrambi consultabili in www.edps.europa.eu. Per un primo esame, v. G. DELLA MORTE, "Necessità e proporzionalità nell'app Immuni", in *Symposium: Privacy and Contact Tracing*, cit. Attribuisce l'opportuno rilievo a tali documenti anche C. DI SOMMA, "Covid-19. Il *contact tracing*: dalla

di questi ultimi emerge la questione che segue: se si accetta come premessa che quanto più grandi saranno i vantaggi sul piano del contrasto all'epidemia tanto più legittime saranno le limitazioni sul piano della tutela dei dati personali, se ne può dedurre che se i vantaggi fossero molto contenuti o addirittura esigui anche le compressioni ammissibili ne risulterebbero estremamente limitate? La domanda non è retorica se si considera presumibile, alla stregua di quanto precedentemente esposto[140], che la percentuale di popolazione italiana che adopererà correttamente l'app sarà decisamente ridotta. Tuttavia, il tema ci sembra in 'penombra' per due ordini di ragioni: primo, perché è difficile azzardare una risposta prima di verificare sul campo, trascorso un adeguato lasso di tempo, l'efficacia dell'app nell'azione di contrasto combinato al virus (al momento in cui si licenzia questo scritto, giugno 2020, l'app attraversa una prima fase di applicazione); e, secondo, perché detta efficacia dipenderà in parte dall'evoluzione delle interfacce di programmazione delle applicazioni (API) di Google e Apple sulle quali *Immuni* si appoggia[141].

Lungo la traccia di quest'ultima constatazione ci si imbatte nel secondo e ultimo tema in 'penombra', relativo alla situazione per cui l'intera l'architettura del trattamento dei dati in *Immuni* è fondata su un sistema decentralizzato cui tuttavia fa da *pendant* una centralizzazione (sostanzialmente privata) del *know how* tecnologico[142]. I dati restano ben processati dalle regole europee ma il protocollo tecnico di processione è elaborato da insostituibili società private di *information technology*, le uniche, d'altronde, ad assicurare un livello di efficienza e di interoperabilità adeguato.

In filigrana, dietro alle diverse sensibilità occidentali e asiatiche sul *contact tracing*, e ancora dietro la considerazione per cui «i Big Data sono in tutta evidenza più efficaci nella lotta al virus rispetto alla chiusura delle frontiere»[143], si intravede un tema ancora più grande, che concerne le trasformazioni di ordine economico, sociale e politico imposte dalla rivoluzione digitale e la contestuale emergenza di poteri privati sempre più investiti dell'esercizio di funzioni pubbliche[144]. «Forse

limitazione della libertà di movimento a quella della protezione dei dati personali", in *Privacy &* 2020 (numero speciale Covid-19), p. 86 ss.

[140] V. *retro*, con particolare riferimento alla prima delle criticità richiamate al paragrafo 14.

[141] Sui problemi connessi ai falsi positivi e negativi e sul ruolo delle *Application Programming Interfaces* (APIs) di Google e Apple a riguardo, v. *retro*, rispettivamente, paragrafi 14 e 5.

[142] Sicché «di fondo c'è, poco rilevato, il paradosso di una soluzione del tutto decentralizzata che è però del tutto centralizzata a livello di sviluppo e gestione del codice nelle mani dei due colossi». Così R. BERTI, A. PELLICCIONE, "Tutti i problemi del framework Apple e Google contro il covid", in www.agendadigitale.eu, 28 aprile 2020.

[143] Così il filosofo sud-coreano B. C. HAN in "La società del virus tra Stato di polizia e isteria della sopravvivenza", in *Avvenire*, 7 aprile 2020, disponibile su www.avvenire.it.

[144] Sull'ampio tema, *ex multis*, e riportando solo alcune tra le letture più suggestive: Y.N. HARARI, "The world after coronavirus", cit. in *Financial Times,* disponibile su www.ft.com, 20 marzo 2020; S. ZUBOFF, *Il capitalismo della sorveglianza, Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019. Il punto è colto anche da *Trattamento dei contatti e democrazia. Lettera aperta ai decisori*, promossa dal Politecnico di Torino e sottoscritta, il 20 aprile 2020, da personalità del mondo accademico (disponibile su www.nexa.polito.it). In una sezione opportunamente intitolata "Non è solo un problema di privacy" si rileva come «[i]l potere generato dall'accesso e dal trattamento di grandi moli di dati

dovremmo persino ridefinire la sovranità alla luce dell'epidemia. Sovrano è chi dispone dei dati»[145]. Ma chi dispone dei dati, oggi, non sono più – soltanto – gli Stati.

ABSTRACT. How Much Immune? Lights, Shadows and Penumbra of the App Selected by the Italian Government

The recourse, made by Italy, to contact tracing apps in order to counter the outbreak of the Covid-19 virus is part of similar experiences which have been already tested, with various results, in different States. Despite the considerable variety of solutions adopted, these contact tracing systems raise different legal issues: protection of personal data, right to health, freedom of movement etc. All these factors require a delicate balance: on the one hand, it is necessary to compress the protection of personal data and, on the other, it is needed to make sure that these limitations are necessary and proportional to the concrete benefits that the app is able to produce on the ground of the contrast to the epidemic. The essay, after conducting an excursus on the origins of the Italian app "Immuni" (section 2) and on the guidelines developed by the European Union in this regard (section 3), focuses on the possible contact tracing options and on the one which has been finally selected by the Italian Government (sections 4-9). After analysing the legal basis of the latter (sections 10 and 11), the paper assesses the compliance of the above system with the obligations set by the international norms (section 12). Finally, it develops some observations on the merits (section 13), the critical aspects (section 14), and the grey areas emerging from the effort to strike a fair balance between the competing interests at stake (section 15).

Keywords: Covid-19; algorithm; big data; contact tracing; data protection; human rights.

personali è in grado di modificare profondamente i rapporti e le relazioni tra le persone e soprattutto tra i diversi attori sociali, tra consumatori e imprese e inevitabilmente tra i cittadini e lo Stato».

[145] B.C. HAN, "La società del virus tra Stato di polizia e isteria della sopravvivenza", cit.