IANUS
Diritto e Finanza
UNIVERSITÀ DI SIENA 1240
Quaderni
https://www.rivistaianus.it
ISSN: 1974-9805
Quaderni - 2020

CONTACT TRACING. GOVERNANCE PUBBLICO-PRIVATA E PRIMI PROBLEMI DI TUTELA DEI DIRITTI FONDAMENTALI

Elia Cremona

CONTACT TRACING. GOVERNANCE PUBBLICO-PRIVATA E PRIMI PROBLEMI DI TUTELA DEI DIRITTI FONDAMENTALI

Elia Cremona

Dottorando in Scienza giuridiche,
Università degli Studi di Siena

1. Il percorso di adozione dell'*app* per il tracciamento dei contagi

Nel quadro delle azioni finalizzate al contrasto della diffusione del virus Covid-19, il Governo italiano ha deciso di accompagnare alle note misure di distanziamento sociale alcune soluzioni tecnologiche, in particolare al fine di poter monitorare l'evoluzione dell'epidemia contemporaneamente alla progressiva eliminazione dei limiti, vincoli e divieti alla libertà di movimento e all'esercizio di attività professionali, commerciali e produttive.

Il Ministero per l'innovazione tecnologica e la digitalizzazione, d'intesa con altri attori istituzionali, ha così lanciato il 23 marzo 2020 una *fast call for contribution* pubblica[1] per la ricognizione delle soluzioni esistenti e affidato a un gruppo interdisciplinare di esperti (informatici, *data scientist*, epidemiologi, economisti e giuristi)[2] il compito di supportare il Governo[3] nell'analisi e valutazione delle diverse soluzioni tecnologiche.

Come noto, all'esito della procedura selettiva[4] è stata individuata l'*app* di

[1] Il Ministero dell'Innovazione, dello Sviluppo Economico e il Ministero dell'Istruzione, dell'Università e della Ricerca, nell'ambito dell'Iniziativa "Innova per l'Italia", hanno lanciato, congiuntamente al Ministero della Salute, all'Istituto Superiore di Sanità, all'Organizzazione Mondiale della Sanità e un comitato scientifico interdisciplinare, una *fast call* al mondo dell'impresa e della ricerca, con l'obiettivo di individuare le migliori soluzioni digitali disponibili relativamente ad *app* di telemedicina e assistenza domiciliare dei pazienti e a tecnologie e strategie basate sulle tecnologie per il monitoraggio "attivo" del rischio di contagio, nonché di coordinare a livello nazionale l'adozione e l'utilizzo di queste soluzioni e tecnologie.

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

[3] E in particolare il Dipartimento per l'innovazione tecnologica e la digitalizzazione della Presidenza del Consiglio dei Ministri e il Ministero della Salute.

[4] Le proposte di soluzioni tecnologiche sono risultate 319 per il monitoraggio e 504 per la telemedicina.

contact tracing denominata 'Immuni', sviluppata dalla società italiana Bending Spoons S.p.A., che ha saputo confezionare un'*app* in grado di funzionare esclusivamente con tecnologia *Bluetooth Low Energy* (BLE)[5], escludendo in radice l'utilizzo della geolocalizzazione, inizialmente paventato[6]. Per l'effetto, con ordinanza del 16 aprile 2020, n. 10, il Commissario straordinario ha disposto la stipula del "contratto di concessione gratuita della licenza d'uso sul *software* di *contact tracing* e di appalto di servizio gratuito con la società Bending Spoons S.p.a."[7]. L'applicazione, alla data del 20 maggio, è in fase di test ed è in attesa di essere distribuita.

2. La disciplina del Sistema di allerta Covid-19

Il meccanismo di funzionamento del sistema di *contact tracing* è stato oggetto, dapprima, di alcuni atti di indirizzo dell'Unione europea e poi di una disciplina legislativa a livello nazionale.

In particolare, è intervenuta la Commissione europea con la raccomandazione dell'8 aprile 2020, che ha incoraggiato l'adozione di un *Toolbox* di misure condivise a livello europeo, *legally compliant*[8], e che ha

[5] Come per le soluzioni adottate da Singapore, o caldeggiate da Apple e Google, la tecnologia *Bluetooth Low Energy* (BLE) consente di mantenere i dati dell'utente sul dispositivo, assegnandogli un ID temporaneo, che cambia in continuazione e che viene scambiato tramite Bluetooth ogniqualvolta "impatta" con dispositivi vicini.

[6] L'*app* è stata sviluppata in *partnership* con il Centro Medico Santagostino e si prefigge tre obiettivi, ovvero: (i) contribuire tempestivamente all'azione di contrasto del virus; (ii) realizzare un'*app* conforme al modello europeo delineato dal Consorzio PEPP-PT (sebbene, a séguito dell'intervento di Apple e Google del 10 aprile 2020, di cui si dirà *infra*, le specifiche dell'*app* siano state parzialmente modificate); (iii) garanzia del rispetto della *privacy* degli utenti. Si legge infatti nell'Ordinanza del Commissario straordinario n. 10 del 16 aprile 2020 che l'*app Immuni* è stata *«ritenuta più idonea per la sua capacità di contribuire tempestivamente all'azione di contrasto del virus, per la conformità al modello europeo delineato dal Consorzio PEPP-PT e per le garanzie che offre per il rispetto della privacy»*.

[7] L'aggiudicataria ha concesso - sebbene alla data del 20 maggio 2020 il contratto non sia ancora stato reso pubblico - una licenza d'uso *"aperta, gratuita e perpetua"* del codice sorgente e di tutte le componenti applicative facenti parte del sistema di *contact tracing* e ha, sempre a titolo gratuito, manifestato la propria disponibilità a completare gli sviluppi informatici che si rendono necessari per consentire la messa in esercizio del sistema nazionale di *contact tracing* digitale.

[8] Le più rilevanti normative a livello europeo sono il Regolamento UE 679/2016 (GDPR) e la direttiva *e-privacy* 2002/58/CE. Per quanto riguarda l'uso delle applicazioni mobili di allerta e prevenzione del virus Covid-19, la raccomandazione ha enucleato i seguenti principi: *«1) misure di salvaguardia che garantiscano il rispetto dei diritti fondamentali e la prevenzione della stigmatizzazione, in particolare le norme applicabili alla protezione dei dati personali e alla riservatezza delle comunicazioni; 2) preferenza per le misure meno intrusive e comunque efficaci, compreso l'uso dei dati di prossimità, ma senza il trattamento dei dati relativi all'ubicazione o agli spostamenti delle persone, e l'uso di dati anonimizzati e aggregati ove possibile; 3) requisiti tecnici riguardanti le tecnologie appropriate (ad esempio Bluetooth a bassa energia) per stabilire la prossimità del dispositivo, la cifratura, la sicurezza dei dati, l'archiviazione dei dati sul dispositivo mobile, il possibile accesso da parte delle autorità sanitarie e la memorizzazione dei dati; 4) requisiti di cibersicurezza efficaci per proteggere la disponibilità, l'integrità, l'autenticità e la riservatezza dei dati; 5)*

istituito[9] la rete di assistenza sanitaria *online e-Health*[10], la quale ha a sua volta - il 15 aprile 2020 - pubblicato una rassegna dei requisiti minimi e delle funzionalità da soddisfare nel processo di sviluppo e di impiego delle misure digitali[11].

Pure è intervenuta la presidente dell'*European Data Protection Board*, con la lettera del 14 aprile 2020[12], rivolta alla Commissione europea in vista dell'adozione delle Linee Guida, che ha da un lato evidenziato la possibilità di adottare *app* pienamente compatibili con il diritto UE, e in particolare con i principi scolpiti all'art. 5 del GDPR[13], e dall'altro evidenziato come la *volontarietà* dell'utilizzo dell'*app* per il tracciamento dei contatti non significhi che la base giuridica del trattamento debba necessariamente consistere nel mero consenso, anzi auspicando l'adozione di una base giuridica di tipo *legale*.

Da ultimo, sono intervenute le Linee Guida della Commissione europea, rese pubbliche con la Comunicazione del 16 aprile 2020[14], nelle quali è stata ribadita l'opportunità di una base giuridica del trattamento di tipo legale, ai sensi dell'art. 5 della direttiva *e-privacy* 2002/58/CE, e sono stati altresì individuati gli elementi essenziali per l'utilizzo delle *app* di *contact tracing*, che ricalcano in larga parte i principi relativi al trattamento dei dati, come la proporzionalità, il consenso al trattamento, la minimizzazione dei dati, etc.

Tale impostazione è stata recepita a livello nazionale, sicché il legislatore ha

---

scadenza delle misure adottate e cancellazione dei dati personali ottenuti attraverso tali misure, al più tardi quando la pandemia sarà dichiarata sotto controllo; 6) caricamento di dati di prossimità in caso di infezione confermata e metodi appropriati per allertare le persone che hanno avuto contatti stretti con la persona infettata, che deve rimanere anonima; e 7) prescrizioni relative alla trasparenza per le impostazioni sulla privacy in modo da garantire la fiducia nelle applicazioni».

[9] L'istituzione è avvenuta a norma dell'articolo 14 (*Assistenza sanitaria online*) della direttiva 2011/24/UE, in forza del quale l'Unione sostiene e facilita la cooperazione e lo scambio di informazioni tra gli Stati membri operanti nell'ambito di una rete volontaria che collega le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri.

[10] La rete *eHealth* è composta dal *Comitato europeo per la sicurezza sanitaria*, dal *Centro europeo per la prevenzione e il controllo delle malattie*, dall'*European Data Protection Board*, dall'*Organismo dei regolatori europei delle comunicazioni elettroniche* e dal *Gruppo di cooperazione per i sistemi informativi di rete* (NIS) per il monitoraggio ed il rafforzamento dei livelli di sicurezza della rete e dei sistemi informativi (cybersecurity).

[11] I requisiti essenziali di funzionamento delle *app* nazionali sono stati individuati: (i) nella volontarietà del *download;* (ii) nell'approvazione da parte delle autorità nazionali; (iii) nella sicura protezione dei dati personali; (iv) nel vincolo alla dismissione alla fine dell'emergenza. Il documento completo è disponibile al seguente *link*: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[12] La lettera è reperibile al seguente *link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316030*.

[13] I principi applicabili al trattamento di dati personali individuati dall'art. 5, par. 1, del GDPR sono: a) liceità, correttezza e trasparenza; b) limitazione della finalità; c) minimizzazione dei dati; d) esattezza; e) limitazione della conservazione; f) integrità e riservatezza. Al par. 2, è poi individuato il principio di responsabilizzazione (c.d. *accountability*) del titolare del trattamento.

[14] Le linee guida sono disponibili al seguente *link*: https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf.

disciplinato il funzionamento dell'*app* e il conseguente trattamento dei dati personali dei soggetti interessati con il d.l. 30 aprile 2020, n. 28, attualmente in fase di conversione, all'art. 6, rubricato *Sistemi di allerta Covid-19*[15].

In particolare, la norma ha previsto l'istituzione di una *"piattaforma unica nazionale"*, di titolarità pubblica e realizzata esclusivamente con infrastrutture presenti sul territorio nazionale, per la gestione del sistema di allerta dei soggetti che hanno installato, su base volontaria, l'apposita *app* (Immuni) sui propri dispositivi.

Il titolare del trattamento dei dati è stato individuato nel Ministero della Salute, cui è demandata l'adozione[16] delle *"misure tecniche e organizzative"* idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati, sentito il Garante per la protezione dei dati personali[17].

Sarà dunque compito del Ministero della Salute assicurare: (a) una adeguata informativa agli utenti[18]; (b) il rispetto del principio di finalità e minimizzazione[19]; (c) che il tracciamento riguardi solo dati di prossimità dei dispositivi e che sia esclusa la geolocalizzazione dei singoli utenti[20]; (d) la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento[21]; (e) il rispetto

---

[15] Una prima disciplina del trattamento dei dati sanitari era stata fornita dall'art. 14 (*Disposizioni sul trattamento dei dati personali nel contesto emergenziale*) del d.l. 9 marzo 2020, n. 14, in forza del quale si è attribuita a soggetti qualificati la possibilità di effettuare trattamenti, ivi inclusa la comunicazione, dei dati personali, anche relativi alle particolari categorie di cui agli artt. 9 e 10 del GDPR, che risultassero necessari all'espletamento delle proprie funzioni. In particolare, è stato individuato uno specifico novero di soggetti operanti a vario titolo nel contrasto dell'emergenza epidemiologica (Protezione civile, Servizio Sanitario Nazionale, ecc.) a cui tale possibilità è stata attribuita allo scopo di *«assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali»*, pur nel rispetto dell'articolo 9, paragrafo 2, lettere g), h) e i), e dell'articolo 10 del GDPR, nonché dell'articolo 2-*sexies*, comma 2, lett. t) e u), del d.lgs. 30 giugno 2003, n. 196. Si rinvia al dispositivo integrale per gli ulteriori profili di disciplina.

[16] Sulla base di una valutazione di impatto, costantemente aggiornata, effettuata ai sensi dell'articolo 35 del GDPR.

[17] Ai sensi dell'articolo 36, par. 5, del medesimo GDPR e dell'articolo 2-*quinquiesdecies* del Codice in materia di protezione dei dati personali di cui al d.lgs. 30 giugno 2003, n. 196.

[18] E cioè che ai sensi degli articoli 13 e 14 del GDPR, agli utenti siano fornite *«informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati»* (art. 6, comma 2, lett. a) del d.l. 28/2020).

[19] E cioè che *«per impostazione predefinita, in conformità all'articolo 25 del Regolamento (UE) 2016/679, i dati personali raccolti dall'applicazione di cui al comma 1 siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al Covid-19, individuati secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti»* (art. 6, comma 2, lett. b) del d.l. 28/2020).

[20] E cioè che *«il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati; è esclusa in ogni caso la geolocalizzazione dei singoli utenti»* (art. 6, comma 2, lett. c) del d.l. 28/2020).

[21] E cioè che *«siano garantite su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento»* (art. 6, comma 2, lett. d) del d.l.

del principio di limitazione della conservazione[22]; (f) l'esercizio semplificato dei diritti dei soggetti interessati[23].

Precisa, sempre l'art. 6 in parola, che il *"mancato utilizzo"* dell'app *"non comporta alcuna conseguenza pregiudizievole"* e che *"è assicurato il rispetto del principio di parità di trattamento"*. L'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali saranno interrotti alla data di cessazione dello stato di emergenza, comunque non successiva al 31 dicembre 2020. Entro tale data, prevede il comma 6, tutti i dati personali dovranno essere cancellati, o resi definitivamente anonimi.

In disparte dei dubbi sollevati circa l'efficacia, non solo relativi alla capacità di utile funzionamento se non sarà raggiunta una percentuale soglia di *download* nella popolazione (secondo alcuni pari ad almeno il 60%[24]), ma anche relativi alla potenziale creazione di un alto numero di c.d. falsi positivi, ciò su cui ci si vuole brevemente soffermare in questa sede sono tre questioni, rilevanti sotto il profilo giuridico.

3. Tre questioni, prime considerazioni

3.1. Nei fatti: una *governance* pubblico-privata dell'emergenza

Una prima evidenza della gestione dell'emergenza epidemiologica è che, ai più diversi livelli, si sono declinate forme di *governance*[25] pubblico-privata dell'emergenza epidemiologica: nella definizione degli *standard* tecnologici di funzionamento dell'*app*, nella regolazione dei livelli di protezione della *privacy*, nella procedura di selezione del contraente deputato allo sviluppo del *software*, nell'implementazione dell'*app*.

Sarà lo sviluppo del contagio a rivelare se tale approccio sarà stato o meno virtuoso; certo è che la commistione di funzioni e competenze pubblico-private si

28/2020).

[22] E cioè che *«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 e specificata nell'ambito delle misure di cui al presente comma; i dati sono cancellati in modo automatico alla scadenza del termine»* (art. 6, comma 2, lett. e) del d.l. 28/2020).

[23] E cioè che *«i diritti degli interessati di cui agli articoli da 15 a 22 del Regolamento (UE) 2016/679 possano essere esercitati anche con modalità semplificate»* (art. 6, comma 2, lett. f) del d.l. 28/2020).

[24] Si veda https://www.agi.it/politica/news/2020-04-20/coronavirus-app-immuni-8392554/.

[25] Studi politologici evidenziano il fenomeno da tempo in atto: lo scostamento dai tradizionali modelli di *government*, basati su strutture 'verticali' esclusivamente pubbliche e politiche di governo, e l'approdo a modelli di *governance*, caratterizzati *«da un maggior grado di cooperazione e dall'interazione tra lo stato e attori non statuali all'interno di reti decisionali miste pubblico/private»*. Così R. Mayntz, *La teoria della governance: sfide e prospettive*, in *Rivista italiana di scienza politica*, fasc. 1, 1999, p. 3, cit. in G. Mobilio, *Cipe e costituzione. Governare attraverso i comitati ministeriali*, Napoli, 2018, pp. 296-297. Cfr, M.R. Ferrarese, *La governance tra politica e diritto*, Bologna, 2010.

è realizzata in via di fatto, in assenza di una cornice di regolamentazione giuridica.

Più in dettaglio. Le specifiche tecniche del *contact tracing* sono state inizialmente individuate nell'ambito di vari progetti privati, o pubblico-privati, internazionali: oltre al Consorzio PEPP-PT (la cui sigla sta per *Pan-European Privacy-Preserving Proximity Tracing*, pure menzionato dalla Commissione europea nelle proprie linee guida e di cui fa parte l'aggiudicataria Bending Spoons), si rammenta anche DP-3T (sigla che sta per "*Decentralized Privacy-Preserving Proximity Tracing*", ovvero la soluzione di tracciamento proposta da un *team* di vari ricercatori con base in Svizzera) e ROBERT (sigla che sta per "*ROBust and privacy-presERving proximity Tracing protocol*" e che è stata promossa dall'Istituto francese per la ricerca nell'informatica e nell'automazione e dal *Fraunhofer* AISEC).

Tali progetti hanno individuato diversi modelli di funzionamento delle piattaforme e delle *app* collegate, ora in senso "centralizzato", cioè mediante l'archiviazione di tutti i dati - pur se pseudonimizzati[26] - su di un unico server, ora in senso "decentralizzato", cioè mediante la conservazione dei dati degli utenti sui singoli *device* fino al momento della volontaria *disclosure*.

È poi intervenuto il *framework* Apple-Google, con il progetto *Privacy-Preserving Contact Tracing* che ha proposto l'adozione su scala globale di un modello fortemente "decentralizzato"[27], che si è rivelato estremamente persuasivo, visto che sono circa tre miliardi le persone usano *smartphone* con sistemi operativi iOs e Android.

Alla fine del mese di aprile i due colossi hanno rilasciato le API[28] da mettere a disposizione degli sviluppatori incaricati dai Governi nazionali di progettare le *app* per il *contact tracing* e hanno comunicato che non svilupperanno proprie *app* di tracciamento dei contatti, ma collaboreranno invece allo sviluppo tecnologia sottostante.

---

[26] La *pseudonimizzazione*, di cui al *considerando n. 26* del GDPR, consiste nel garantire che il trattamento dei dati personali avvenga in modo tale che non sia possibile risalire all'interessato senza l'utilizzo di informazioni aggiuntive, che devono essere conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

[27] Secondo il modello elaborato da Apple e Google, il *Bluetooth Contact Tracing* non utilizzerà la geolocalizzazione per il rilevamento di prossimità, ma si limiterà a rilevare la vicinanza a un altro dispositivo con *bluetooth* attivo e *app* in uso. Il *Rolling Proximity Identifier* di un utente cambierà in media ogni 15 minuti e necessiterà di una *Tracing Key* giornaliera per essere correlato all'utente. I rilevamenti di prossimità ottenuti da altri dispositivi verranno elaborati esclusivamente sul singolo dispositivo dell'utente. Se ad un utente è diagnosticato Covid-19, la *Tracing Key* è condivisa con il *Diagnosis server* solo sulla base del consenso dell'interessato. Per le specifiche, si rinvia a https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf.

[28] Le API sono le interfacce di programmazione dell'*app* che consentono l'interoperabilità fra i dispositivi, in tal caso Android e iOS, delle app sviluppate o selezionate dalle autorità sanitarie nazionali.

La scelta del modello Apple-Google si è "imposta" (pare) anche a livello nazionale, sebbene ad oggi siano soltanto notizie di stampa a riportarlo, ed è significativo rilevare come tale modello sia in realtà *più tutelante* dal punto di vista della *data protection* rispetto a quello inizialmente preso a riferimento sia a livello europeo che nazionale (e cioè quello del progetto PEPP-PT), in quanto esclude in radice la possibilità che i dati relativi al tracciamento dei contatti siano collazionati su di un server pubblico centralizzato[29].

Pure infine non deve darsi per scontata la scelta del Governo di rivolgersi al mercato con la ridetta *fast call for contributions*. Il Governo, e in particolare il Ministero dell'Economia, detiene una miriade di partecipazioni strategiche in aziende anche operanti nel settore dell'*Information and Communication Technology*, come SOGEI S.p.A., nella quale la partecipazione è totalitaria. Invece, la scelta di *policy* è stata quella di reperire il *software* nel settore privato, salvo poi acquisirlo in proprietà pubblica e assicurare la gestione della piattaforma e dei flussi di dati da parte di soggetti integralmente pubblici, pure stabiliti sul territorio nazionale.

3.2. Nei diritti: l'accesso ineguale al surplus di tutela del diritto alla salute

La prima questione squisitamente giuridica che ha lambito il dibattito pubblico è stata quella relativa all'obbligatorietà ovvero alla volontarietà del *download* dell'*app* di *contact tracing*. Il dibattito si è presto arenato, perché il Governo ha presto chiarito che l'utilizzo dell'*app* sarebbe avvenuto su base volontaria.

Senonché, per paradossale che sembri, la soluzione della volontarietà pone problemi *maggiori*, e non minori, in punto di diritto.

Si è detto diffusamente che l'obbligatorietà del *download* avrebbe costituito un pregiudizio eccessivo dei diritti della personalità connessi alla *privacy* (riservatezza, identità personale, ecc.).

A ben vedere però, se - come pare - il sistema sarà in grado di funzionare in modo interamente *decentralizzato* (e cioè se le informazioni sul tracciamento dei contatti permarranno esclusivamente sul *device* dell'interessato fino a volontaria *disclosure*), il pregiudizio per la *privacy* sarà minimizzato, se non nullificato.

Perciò, se la scelta fosse caduta sull'obbligatorietà dell'*app*, il problema che si sarebbe posto (di difficile soluzione in tempo utile al contrasto dell'emergenza) sarebbe stato piuttosto quello garantire a tutti i cittadini l'accesso all'*app*.

Da un punto di vista costituzionale, tuttavia, ci saremmo trovati di fronte ad una - pur inedita - "prestazione" imposta in base alla legge, ai sensi dell'art. 23 Cost.,

[29] Possibilità espressamente lasciata aperta dalla lettera della norma, laddove all'art. 6, comma 2, lett. e) del d.l. 28/2020, si dispone che *«i dati relativi ai contatti stretti siano conservati,* anche *nei dispositivi mobili degli utenti»*.

per finalità di tutela della salute collettiva, bene costituzionale di prim'ordine per la cui protezione sono peraltro già state costituzionalmente "giustificate" le ben più gravi limitazioni alla libertà di circolazione, di riunione etc.

Ad ogni modo, è parso a molti di poter ovviare al duplice problema (giuridico) '*privacy*' e (pratico) 'accesso universale' semplicemente rendendo *volontaria* l'*app* per il tracciamento dei contagi. Senonché, quantomeno il problema pratico non è affatto risolto ed occorre anzi sgomberare il campo dall'ambiguità di fondo che si cela nel dibattito pubblico sull'*app*: potere-non-averla non equivale a non-poterla-avere.

Non è una novità il tema del c.d. *digital divide*[30], per il quale non trascurabili platee di cittadini italiani sono esclusi dalla possibilità di fruire dei servizi di internet o anche solo di possedere uno *smartphone*, per incapacità, per basso livello di scolarizzazione, per ragioni di ordine economico. Peraltro, si tratta di un novero di soggetti probabilmente più esposti di altri ai rischi del contagio, come le persone anziane.

Ciò pone un grande problema di tutela dell'uguaglianza sostanziale tra chi è effettivamente libero di non scaricare l'*app* (perché, pur potendolo fare, non lo fa) e chi non la scarica perché non ne ha la possibilità. Il tema si rivelerà centrale proprio se l'*app* assicurerà i vantaggi attesi, che non si limitano al monitoraggio dei contagi: una persona contagiata dotata di *app* potrà verosimilmente attivarsi per diagnosi e cura *prima* (già dal momento della notifica del 'contatto') di quanto non sarà possibile ad un soggetto sprovvisto di *app*, che invece dovrà attendere i primi sintomi. Ed è stata sin qui evidente l'incidenza del fattore tempestività nella cura delle patologie conseguenti al contagio del virus: non può dubitarsi che una *diagnosi* precoce del contagio, assicurata dall'*app* tramite la notifica del contatto significativo con un soggetto positivo, non costituisca un *surplus* di tutela del bene-salute.

In più. Non è stato ancora chiarito se dalla titolarità dell'*app* discenderanno dei diritti a trattamenti sanitari (tampone, test sierologico?) o dei doveri comportamentali (obbligo di quarantena?) in caso di notifica di contatto con soggetto positivo al Covid-19. Pare ragionevole presumerlo, e ciò allarga la portata del problema, che sarà tutto da affrontare, visto che pare estremamente debole e generica, dal punto di vista giuridico, la previsione contenuta all'art. 6, comma 4, del d.l. 28/2020 secondo la quale è comunque *"assicurato il rispetto del principio della parità di trattamento"*.

[30] Secondo il Report dell'Istat "Cittadini e ICT" (Tecnologie dell'Informazione e della Comunicazione), pubblicato a dicembre 2019, la percentuale di famiglie italiane che dispongono di una connessione a banda larga è pari al 74,7%, mentre la percentuale degli individui che hanno utilizzato Internet, negli ultimi 3 mesi precedenti l'intervista, è pari al 67,9%. Cfr. https://www.istat.it/it/archivio/236920.

3.3. Scenario: i protocolli privati che prevedano un *download* obbligatorio

Nelle more dell'adozione dell'*app*, l'idea che soggetti privati titolari di posizioni di garanzia, come i datori di lavoro, gli amministratori di società, i dirigenti, etc., adottino protocolli privati che vincolino i sottoposti all'utilizzo dell'*app* appare una prospettazione meramente ipotetica. Ma non è così lontana dalla realtà.

Il punto critico consiste nel comprendere se, fermo il quadro giuridico di riferimento, debba ritenersi tutelata o tutelabile la libertà di non-entrare in contatto con persone che non siano sottoposte al tracciamento dei contatti. E dunque se sia per conseguenza giuridicamente sostenibile la legittimità della previsione dell'obbligatorio *download* dell'*app*, ad esempio, per l'accesso al luogo di lavoro o ad un esercizio aperto al pubblico.

Si tratterebbe di protocolli con livelli di sicurezza *più elevati* per intere categorie di lavoratori, magari esposti ad un margine di rischio di contagio supplementare in ragione delle specifiche mansioni affidate.

Dunque, fermo che il ridetto art. 6 del d.l. 28/2020 pone il principio della *volontarietà* del *download* dell'*app*, come opera tale norma in relazione alle fonti private che regolano i rapporti giuridici asimmetrici? In altre parole, i principi di volontarietà e parità di trattamento[31] hanno efficacia solo verticale o anche orizzontale?

È possibile svolgere una prima, pur sintetica, riflessione su questo strano (anche se forse apparente) *trade-off* tra salute e *privacy*. Mentre il diritto alla salute mostra certamente un 'volto solidaristico'[32], talché è stato ben possibile limitare gli altrui diritti di libertà (circolazione, riunione, iniziativa economica etc.), più difficile appare sostenere che lo stesso 'volto solidaristico' lo abbia la *privacy*.

In altre parole, la dimensione costituzionale del bene *privacy* non pare potersi estendere fino al punto di impedire, a chi lo voglia, di non-entrare in contatto con soggetti che si sottraggono al *contact tracing*. Ciò in quanto il tracciamento assicura un *surplus* di tutela della salute (i.e. diagnosi precoce) al quale il singolo non dovrebbe essere "costretto" a rinunciare sol perché un altro soggetto abbia esercitato la propria libertà di non-avere l'*app*.

La conseguenza di tale ragionamento, essendo in radice esclusa l'opzione

---

[31] Di cui all'art. 6, comma 4, del d.l. 28/2020.

[32] M. Noccelli, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, su *federalismi.it*, *Osservatorio emergenza Covid-19*, 11 marzo 2020, dove l'Autore ricorda come *«il diritto alla salute nella Costituzione non è solo un diritto fondamentale della persona, ma insieme e inscindibilmente, come ora si dirà, anche interesse della collettività (art. 32 Cost.). E qui viene in rilievo il risvolto o, se si preferisce, il volto meno conosciuto della salute, quale diritto "bifronte", nel suo versante solidaristico. L'interesse della collettività, di fronte a situazioni di gravissima emergenza sanitaria e alla minaccia per la salute di tutti e di ciascuno, assurge ad un valore superiore, capace di giustificare severe restrizioni alla libertà della persona e agli atti della sua vita quotidiana e di imporre rigorosi limiti ad altri diritti costituzionalmente garantiti, appunto, di tutti e di ciascuno».*

dell'obbligatorietà dell'*app*, dovrebbe perciò essere la legittimità (o meglio, la non illegittimità) di regole, direttive e protocolli privati che, a tutela della salute di lavoratori o avventori, dispongano l'obbligatorio utilizzo dell'*app* di *contact tracing*.

L'approdo porrebbe certo ulteriori problemi, non scandagliabili in questa sede, relativamente all'accesso a beni e servizi essenziali, che non potrebbe naturalmente essere subordinato all'utilizzo di una *app* per legge non obbligatoria.

Resta tuttavia una zona franca, e molto larga, di luoghi nei quali non si fa commercio di beni essenziali e dove pare ragionevole - ad avviso di chi scrive - riconoscere la libertà di condizionarne l'accesso all'utilizzo dell'*app*, per la migliore tutela della salute individuale e collettiva.

(21-05-2020)