mediaLAWS

Rivista di diritto dei media

2/2020 maggio

Indice
Index

Editoriale

Articles

Notes and comments
Italy

"Immuni". Un'*exposure notification* app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*

Marco Plutino

Abstract

Il governo italiano ha fatto costruire una app di notifica delle esposizioni per ridurre il rischio di contagio al Covid-19. Tale app viene esaminata nelle sue fonti di disciplina legale, nelle sue caratteristiche e nei suoi limiti tecnici e di fatto per valutarne l'impatto in termini di limitazione dei diritti fondamentali.

The Italian government has commissioned an exposure notification app to reduce the risk of contagion to Covid-19. This app is examined in its sources of legal discipline, in its characteristics and in its technical limits and in fact to assess its impact in terms of limitation of fundamental rights.

Sommario

Keywords

contact tracing – pandemia - diritti fondamentali - sicurezza nazionale – diritto alla salute

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo è stato sottoposto a referaggio anonimo.

1. Il contrasto al COVID-19 tra sicurezza e protezione dei dati in un contesto permeato dalle tecnologie digitali

L'emergenza sanitaria dovuta alla circolazione tra essere umani del nuovo virus denominato COVID-19 ha fatto compiere un salto di qualità al tema del ruolo dello Stato in relazione all'impatto dell'innovazione tecnologica nella vita quotidiana dei suoi cittadini. Si è aperta una discussione pubblica sulle potenzialità e le forme di utilizzo della tecnologia per perseguire finalità pubblicistiche che è andata oltre le nicchie in cui era confinata da un po' di tempo, connesse a questioni della sicurezza e della tutela della legalità (intercettazione telefoniche, telecamere a circuito chiuso: CCTV), come ad esempio in riferimento alle modalità di svolgimento del lavoro subordinato pubblico e privato (lavoro "agile", c.d. *smart working*) e alle sue ricadute anche nel campo dell'istruzione e della formazione (didattica a distanza). Del resto l'uso della tecnologia a tutela della salute (*digital health*, ad es. telemedicina) è già massivo, e con il progredire dell'evoluzione tecnologica si porranno e in parte già si pongono delicate questioni relative alla tutela del nucleo essenziale dei diritti fondamentali, come ad esempio in riferimento alle potenzialità e ai limiti della medicina personalizzata e della genomica, alle tecnologie di identificazione a radiofrequenza (RFID, *Radio Frequency IDentification*), con chip apponibili su superfici o inoculabili anche sotto-cutaneamente per diverse finalità possibili fino alla stupefacente frontiera dei MEMS (*Micro Electro-Mechanical Systems*), sistemi elettromeccanici miniaturizzati grandi pochi nanometri, sorta di sabbia tecnologica capace di carpire e trasmettere dati di ogni genere[1].

Entro questo dibattito già da tempo era emerso con evidenza, come nell'ultima questione appena citata, il problema dell'intreccio tra interessi commerciali ed interessi nazionali, di particolare significato quando sono in discussione l'uso di masse di dati che riguardano tendenzialmente l'intera comunità nazionale. Non appare soddisfacente la distinzione che viene spesso effettuata tra tecnologie invasive adottate da parte di soggetti statali o comunque pubblici e quelle adottate da soggetti privati, ed in particolare imprese commerciali. In un mondo in cui le informazioni, e quindi i dati, costituiscono sempre più la base di ogni *business* ed equivalgono pertanto a ricchezza e potere, la tecnologia consente per sua natura ampie possibilità di intrusioni, più o meno volute, più o meno legittime, più o meno concordate, di soggetti formalmente estranei rispetto ai titolari del contratto di utilizzo di una piattaforma, di un sistema operativo o di un software al fine di utilizzare i dati per finalità non istituzionalmente prevista dal contratto o espressamente escluse.

La realtà degli ultimi anni ha offerto un'ampia gamma di queste circostanze, con risvolti talora estremamente preoccupanti. Oggi una parte consistente dell'attività di *intelligence* di uno Stato è assorbita dal cyberspazio, cioè semplicemente dalla Rete, e anche le attività più esplicitamente ostili (c.d. *cyberwar*) avvengono con uso delle tec-

[1] Su alcune di queste tematiche v. ora M. Fasan, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del coronavirus*, in *BioDiritto – Online First,* 20 marzo 2020, 1 ss., in corso di pubblicazioni in *BioLaw Journal,* 2, 2020 C. Botrugno, *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro paese*, ivi, 13 aprile 2020, *passim*.

nologie e non con l'uso di armi convenzionali (campo nelle quali pure si pone il ruolo dell'intervento tecnologico, con particolare riguardo al tema genericamente chiamato "Intelligenza Artificiale"). Del resto, il cyberspazio consente di sovrapporre allo spazio fisico quelli che sono stati definiti nuovi "strati di senso" e di informazione che rivoluzionano la percezione individuale e collettiva circa i luoghi, il loro modo di essere e di fruizione. È pertanto normale che sia gli Stati che i soggetti privati con interessi commerciali nutrano estremo interesse per le sue potenzialità.

La confluenza operativa di soggetti pubblici e privati su un unico terreno di gioco, fortemente permeabile alle incursioni rispetto ai tentativi di alzare protezioni, difese perimetrali di una rete informatica per scongiurare accessi non desiderati alle risorse di un sistema (c.d. *firewall*), pone le questioni della sicurezza informatica tra quelle di cui uno Stato deve prendersi cura per tutelare i propri cittadini. Interessi commerciali e statali sono talora frammisti, talora conflittuali. Entità commerciali possono operare per conto di interessi statali o esser legati da accordi ignoti all'opinione pubblica. Ne deriva che possono essere sostanzialmente unitarie le preoccupazioni e grosso modo unitario dovrebbe essere l'approccio di fronte all'uso di dati (anonimi, personali o sensibili che siano) da parte di soggetti privati o pubblici.

Il nostro ordinamento appare non poco evoluto sul piano dell'approccio normativo e del resto è integrato e coordinato con l'ordinamento dell'Unione Europa che ha fatto della regolazione dei dati, quindi anche della tutela, un tratto identitario del proprio modo di collocarsi nel mondo come "comunità di diritto" e spazio di tutela dei diritti fondamentali, raggiungendo *standard* molto elevati, globalmente riconosciuti. L'Unione appare consapevole che il privato imprenditore possa operare per un tornaconto contrario all'interesse pubblico o come *instrumentum regni* al servizio di interesse pubblici previ accordi occulti. La dotazione da parte di talune entità commerciali di un enorme potere economico e, per così dire, culturale, le fa operare in modo non dissimile da entità sovrane, e del resto quanto più è grande il loro potere di fatto più gli Stati che rappresentano medie o grandi potenze, o gli Stati ove si colloca la base legale di quelle compagnie (che spesso coincidono coi primi) o anche dove l'azienda realizza i profitti, i mercati più remunerativi, cercano di garantirsene i servizi, di trarne vantaggio, o almeno di stabilire un proficuo rapporto.

I mercati remunerativi di queste compagnie sono le comunità e i loro dati, quindi i dati di una comunità nazionale che, senza le opportune garanzie, possono essere trasferiti fuori dai confini nazionali.

Queste grandi compagnie infine per la loro dimensione e il campo d'attività devono devono necessariamente delle super-potenze in tema di sicurezza informatica al fine di tutelare i propri sistemi e i propri segreti industriali. La sicurezza informatica dei sistemi statali e delle imprese nazionali è oggi al cuore del ruolo di uno Stato, parte di una "sicurezza nazionale" e della tutela di interessi nazionali. Ne deriva che gli Stati spesso hanno bisogno del ricorso alle tecnologie di questi giganti (e il tema che tratteremo ne costituisce un esempio) e che queste compagnie spesso cercano riparo e benefici sotto normative nazionali che rappresentano di fatto, e quantomeno, politiche industriali.

Si realizza in definitiva una commistione di interessi e tensioni per cui l'uso delle tecnologie, in particolare concernenti il trattamento dei dati, sul versante privato è

oggetto di interessi commerciali enormi e sul versante pubblico può finire per essere inglobata nella logica per cui "*salus rei publicae suprema lex esto*" e in nome della sicurezza nazionale tutto o quasi (tutto, in paesi non da Costituzioni democratiche) tende a essere considerato come legittimo e giustificato (ancorché non necessariamente legale), sorveglianza di massa incluse.

2. L'app Immuni e, in generale, le app di *tracing* e *exposure notification*: norme e politiche dell'Unione e scelte del d.l. 28/2020

In questo contesto radicalmente nuovo nel quale "abitiamo" (per usare un'espressione heideggeriana ad indicare la necessità di un approccio orientato alla funzione e allo scopo dell'uso delle tecnologie) l'emergenza COVID-19, a cagione della pericolosità di un virus nuovo, non poco contagioso e pericoloso e dai tratti ancora non del tutto conosciuti, ha imposto le risposte maggiormente efficaci compatibilmente con gli assetti di regime. Alcuni Stati hanno da subito contrastando la diffusione del virus con un uso massivo e inedito della tecnologia, anche informatica, dall'uso di droni per scongiurare assembramenti, alla richiesta dei dati delle "celle" telefoniche alle compagnie telefoniche per monitorare i tassi di scostamento delle popolazioni rispetto agli obblighi di contenimento presso il proprio domicilio[2], dall'installazione di applicazioni, basate su diverse tecnologie, con le più diverse funzionalità e talora incidenti, anche pesantemente, su diversi diritti (circolazione, salute, iniziativa economica, riunione ed altri, non escluse finalità repressive) all'uso di tecnologie da parte delle autorità pubbliche molto intrusive come sistemi di videosorveglianza facenti ricorso a rilevazioni biometriche, riconoscimento facciale, fino alle tecnologie diagnostiche e mediche[3].
Sono in particolare le applicazioni - c.d. app - software di grandissima diffusione e fortuna che consentono di attivare funzionalità, servizi o strumenti i prodotti tecnologici su cui gli Stati si stanno concentrando per gestire la fase intermedia di presumibile convivenza con il virus in modo da non nuocere troppo alle ragioni dell'economia, al

[2] Tale via, che richiede la collaborazione non dei c.d. *Over The Top*, ma dei fornitori di linea, quindi delle compagnie telefoniche (c.d. *Telco*), è stato largamente utilizzato, ed anche in Italia da esempio dalle regioni che hanno potuto verificare il livello di spostamenti da parte delle popolazioni mediante il monitoraggio di dati anonimi (quindi non personali) al fine di verificare i tassi presumibili di inosservanza degli obblighi di confinamento a casa durante il c.d. *lockdown*. Questi dati per quanto aggregati e anonimi hanno consentito anche di verificare le tipologie dei luoghi frequentati (es. cittadini in spiaggia, o nei boschi).

[3] Una tecnologia che riprende i vecchi braccialetti elettronici ma rientra già nel c.d. *Internet of things*, consente di misurare le distanze con le radiofrequenze, con intrusioni in parte minori per la privacy (perché non connesso ad app, con le quali può entrare però in relazione). Un simile tracciamento potrebbe monitorare la distanza (anche in casa, aprendo scenari sicuramente problematici), o misurare parametri corporei o, con efficacia, scandire la presenza di persone in luoghi affollati. Tuttavia, una tecnologia di questo tipo richiederebbe attente valutazioni, proprio per il tipo di controllo costante cui darebbe corso, molto simile – soprattutto sul piano simbolico - ad una misura limitativa della libertà personale. Del resto in Cina esso è stato utilizzato per verificare la permanenza domiciliare dove obbligate e ad Hong Kong è stato implementato su soggetti in ingresso nel paese per monitorarne gli spostamenti. Comunque, sul tema un'intervista al Presidente dell'Istituto italiano di Tecnologia, G. Metta, *Premi e bonus per stare distanti: la mia tecnologia soft per la Fase2*, in *Il Sole 24 Ore*, 9 maggio 2020.

benessere collettivo e al godimento stesso dei diritti. Si tratta di realizzare una difficile quadratura tra la necessità di tutelare eterogenei diritti dei cittadini ed assicurare altrettanto vari interessi pubblici, a partire da quelli costituzionalmente rilevanti (tra quali rientra anche la medesima tutela dei vari diritti).

In questo quadro anche l'Italia si doterà di un'applicazione, denominata "Immuni" finalizzata a contrastare la diffusione del virus in funzione delle garanzie di quel difficile e dinamico equilibrio di cui si è appena detto. Il presente contributo ha la finalità di esaminare i profili di impatto sui diritti fondamentali di questa app a poche settimane dalla sua inaugurazione alla luce dello stato attuale delle conoscenze, ormai abbastanza avanzato, al fine di verificare l'adeguatezza rispetto al quadro costituzionale, come si è venuto ormai configurando nel *multilevel government*.

Preliminarmente colpisce, nel quadro europeo, la scelta di soluzioni nazionali a fronte di una libera circolazione dei fattori (del resto in tensione) e delle persone in particolare: infatti anche su questo piano è da verificare come interferiranno le app con le libertà in questione, attualmente stressate. Va però osservato che l'intera fase nella quale i singoli Stati si stanno dotando di queste app è stata guidata dalle istituzioni comunitarie. L'Unione europea non è riuscita ad avere un approccio unitario nel contrasto iniziale del COVID-19 né circa la possibilità di dotarsi di una app unica ostando probabilmente il fatto che in ultima analisi le app potrebbero essere destinate, in fasi per lo più successive, ad essere integrate con database nazionali, gelosamente custoditi dagli Stati. Tuttavia si è rivelata capace, anche con i suoi più precisi parametri e le più compiute normative, di orientare il processo di adozione di queste app e non solo con prese di posizione politiche e orientamenti tempestivamente adottati volti ad ispirano le politiche nazionali. Al momento è da verificare se le soluzioni tecniche diversificate ma simili adottate dai vari paesi europei consentiranno il funzionamento dell'app anche oltre i confini dello Stato adottante (c.d. interoperabilità delle soluzioni), aspetto che pare fondamentale per consentire un ripristino dei movimenti di persona tra paesi UE che in questo momento attraversa una fase di tensione per la diffidenza reciproca tra gli Stati[4].

Tra le normative rilevanti vanno citate la Carta dei diritti fondamentali dell'Unione europea in part. all'art. 52, la risalente 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 (c.d. "Direttiva e-Privacy"), ancora vigente in attesa dell'adozione di un Regolamento in materia, e il 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 (che abroga la direttiva 95/46/CE; c.d. regolamento generale sulla protezione dei dati, noto anche con l'acronimo "GDPR")[5].

[4] È del resto questa la finalità ultima che ha portata al tentativo di costruire uno standard europeo di cui diremo di seguito. Su questo tema sono state diramate delle indicazioni con un report dell'European Centre for Desease Prevention and Control il 9 aprile ove si prefigura un futuribile progetto comune europeo.

[5] Una disamina sintetica del loro apporto M. Farina, *La* data protection *ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *BioDiritto – Online First*, 20 marzo 2020, in corso di

Tra le prese di posizioni merita di essere ricordata l'opinione dell'European Data Protection Board (EDPB) che chiarisce i rapporti tra la citata direttiva e il citato regolamento[6]. Un'altra presa di posizione importante è stata quella dei Comitato dei garanti europei il quale ha espresso favore sull'intendimento della Commissione europea di esprimere nella propria proposta l'adozione dell'app su base volontaria nel segno dell'adozione di una responsabilità collettiva, accompagnata pur sempre dalle più ampie garanzie in tema di protezione dei dati al fine di acquisire un atteggiamento di fiducia da parte dei cittadini europei che consente anche una migliore resa della tecnologia. Sullo sfondo l'Unione si sta incamminando verso una normativa organica sull'Intelligenza Artificiale, ad oggi a livello di un Libro Bianco della Commissione (febbraio 2020).

Di seguito si procederà a descrivere le caratteristiche tecniche dell'app "Immuni", a partire dal recente intervento con decreto legge del governo (30 aprile 2020, n. 28), il quale ha tra l'altro offerto una risposta alla prima questione relativa alla base legale di simili restrizioni dei diritti fondamentali con l'intervento di un atto con forza di legge e di cui sarà investito il parlamento in sede di conversione[7]. Il decreto intende fissare alcune disposizioni destinate ad essere in parte integrate con un successivo decreto ministeriale, previo parere del Garante della Privacy. Tale descrizione, inerente ad una materia così tecnica, intende fungere da elementare base di conoscenza al fine di procedere poi a svolgere alcune riflessioni più approfondite. Va infine chiarito che mentre scriviamo non è ancora arrivata la valutazione di impatto del Garante della privacy sull'app[8] ma che l'atteggiamento è stato finora tutt'altro che di chiusura[9] e che d'altra parte la tutela della privacy è solo uno degli aspetti toccati dalla scelta dello Stato italiano di far ricorso a questa tecnologia.

Veniamo alla descrizione di Immuni. Coloro che risiedono sul territorio nazionale (la questione dei soggiornanti occasionali rifluisce tendenzialmente in quella della c.d. interoperabilità delle app) possono installare sui propri sui dispositivi mobili dotati di

pubblicazione in *BioLaw Journal,* 2, 2020.

[6] Dal momento che la prima, pur riguardando le comunicazioni elettroniche, estende la sua portata anche ai trattamenti comuni a diverse tipologie di titolari, come ad esempio l'immagazzinamento di informazioni mediante *cookies* e si pone come *lex specialis* volta a precisare ed integrare le previsioni generali ora dettate in tema di protezione dei dati personali. Ma che viceversa il GDPR non pone obblighi supplementari rispetto alle materie che sono soggette ad obblighi specifici fissati nella direttiva del 2002, valendo per il resto la previsione dell'art. 173 del Regolamento.

[7] Ad es. C. Mirabelli, *A tempo e controllata dal Parlamento. Solo così l'app tutelerà salute e diritti*, in *Avvenire*, 24 aprile 2020. Si badi che l'autore fa riferimento all'art. 16 Cost. e alla riserva ivi contenuta per motivi sanitari; quindi parla anche della limitazione in punto di privacy che afferma dover essere proporzionata all'obiettivo. L'app per come attualmente configurata non ha la potenzialità, indicata dal giudice emerito, di tracciare gli spostamenti.

[8] E' stato reso un parere nel corso di un'audizione informale l'8 aprile 2020 dove sono state espresse preferenze che appaiono sostanzialmente confermate dalle attuali scelte.

[9] Ad esempio, il Garante ha consentito alla Protezione civile di scambiare dati sensibili con altri soggetti come forze dell'ordine, comuni, enti, anche privati, sia quale comunicazione di dati sanitari sia al fin arginare la trasmissione dei contagi, con quello che è stato, ed è, null'altro che un tracciamento svolto senza l'ausilio di tecnologie. V. d.l. 14/2020, disponente una deroga al regime ordinario di gestione dei dati personali.

sistemi operativi[10] l'applicazione software in parola. L'installazione è su base volontaria e il mancato utilizzo «non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento» (art. 6, c. 4)[11]. Prima di attivare l'app gli utenti ricevono informazioni «chiare e trasparenti, al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudo-anomizzazione utilizzate e i tempi di conservazione dei dati» (art. 6, c. 2, lett. *a*); sul concetto di pseudo-anonimizzazione cfr. *infra*). Per quest'ultimo aspetto è previsto che la conservazione dei dati relativi ai contatti, conservati «anche nei dispositivi mobili degli utenti», sarà limitata al «periodo strettamente necessario al trattamento», deciso dal Ministero della Salute, e i «dati sono cancellati in modo automatico alla scadenza del termine» (art. 6, c. 2, lett. *e*), in ogni caso con la decretazione della cessazione dello stato di emergenza (disposto con delibera del Consiglio dei ministri del 31 gennaio 2020) o entro il 31 dicembre 2020, quando in alternativa alla cancellazione può essere disposta la trasformazione in dati anonimi di tutti i dati personali trattati.

Il Ministero della Salute è infatti il titolare del trattamento dei dati e si coordina in ragione delle competenze con una vasta serie di soggetti pubblici per gli ulteriori adempimenti necessari alla gestione del sistema (art 6, c. 1) e relativamente allo stadio di avanzamento del progetto (cit.). Per quanto riguarda le finalità del sistema, e in conseguenza circa le finalità dei dati raccolti, i dati sono quelli necessari ad "allertare" gli utenti entrati in una esposizione a rischio con soggetti (a loro volta, evidentemente, utenti e utilizzatori dell'app) positivi al virus, al fine di consentire nei loro confronti, alle condizioni che descriveremo analiticamente, l'eventuale adozione nei loro confronti delle misure di limitazione dei diritti previste dall'ordinamento e delle misure di assistenza sanitaria (art. 6, c. 2 e lett. *b*). I dati raccolti non possono essere trattati per finalità diverse da quelle indicate, salvo l'utilizzo in forma aggregata o comunque anonima, per fini di sanità pubblica, profilassi, statistici e di ricerca scientifica (art 6, c. 3, con rinvio agli art. 5, par. 1, lett. *a)* e, par. 2, lett. *i)* e *j)* del Regolamento (UE) 2016/679).

I dati di prossimità dei dispositivi saranno resi anonimi o, «ove ciò non sia possibile», pseudo-anonimizzati, e in tal caso vanno adottare misure adeguata ad evitare il rischio di re-identificazione degli interessati cui si riferiscono i dati pseudo-anonimizzati oggetto di trattamento (art, 6, c. 2, lett. *d)*, il quale afferma che devono essere garantite «su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento»); viene esclusa in ogni caso il ricorso alla tecnologia della geolocalizzazione (art. 6, c. 2, lett. *c*). La valutazione di impatto viene «costantemente aggiornata» e vengono adottate dal Ministero della Salute le 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 perso-

[10] Per la telefonia mobili, i c.d. cellulari, occorre pertanto uno smartphone. Il rifermento ai sistemi operativi non costituisce solo un vincolo tecnico per l'installazione dell'app ma come si vedrà è gravida di conseguenze sul piano dell'architettura e delle funzionalità dell'app.

[11] La circostanza era già stata anticipata con nota del Ministro per l'Innovazione tecnologia e la digitalizzazione del 21 aprile 2020.

nali (art. 6, c. 2)[12]. I diritti degli interessati possono essere esercitati anche con modalità semplificate (art. 6, c. 2, lett. *f*).
La piattaforma che gestisce il sistema è di titolarità pubblica, realizzata dal Commissario straordinario di governo per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e contrasto dell'emergenza epidemiologica COVID-19 esclusivamente ricorrendo a infrastrutture localizzate sul territorio nazionale, gestite per quanto riguarda i profili attinenti ai dati dalla "Sogei", società *in house* del Ministero dell'Economia, e per quanto riguarda la tecnologia sottostante all'app da "Pago s.p.a.", interamente partecipata dallo Stato, realizzatrice dell'infrastruttura PagoPa (sistema nazionale dei pagamenti a favore della P.A.). Quanto ai programmi di titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione «sono resi disponibili e rilasciata sotto licenza aperta» (art. 6, c. 5; c.d. "*open source*", del tipo noto come MPL 2.0).

3. Profili tecnici e giuridici dell'app

La descrizione il più possibile piana delle soluzioni normative consente di approfondire alcune questioni. Il rischio che una limitazione dei diritti fondamentali, da meglio specificare, avvenisse come una base legale discutibile e insufficiente, comunque non di rango legislativo, lasciando il parlamento emarginato dal circuito decisionale, è stato fugato e la questione è stata affrontata con una fonte adeguata e dai contenuti abbastanza dettagliati.
L'app prevede che il contratto possa essere stipulato solo da persone che abbiano compiuto i 14 anni, i quali dovranno accettare la *privacy policy* e i termini di servizio. L'adozione volontaria, con cui è da intendere tanto, presupposta la gratuità per l'utente, il *download* facoltativo[13] che l'istallazione e l'uso volontario, sono certamente da intendere in prima battuta come un'espressione di libero consenso ad una eventuale limitazione dei diritti che ne consegue.
Le finalità dell'app, un aspetto determinante per valutare necessità, adeguatezza e proporzionalità delle limitazioni, è espressamente finalizzata ad una ricostruzione il più possibile tempestiva e accurata delle catene epidemiologiche. Non si tratta di una generica app "*contact tracing*" in quanto traccia "eventi" ben qualificati, e non generici "contatti" (i quali pure sono tecnicamente eventi) nè, tantomeno, "movimenti". Sarebbe pertanto più opportuno parlare, allo stato delle funzioni, di una app di *exposure notification* o, quantomeno, di mero *proximity tracing* con esclusione del *tracing* in quanto tale, che richiederebbe la geolocalizzazione quale tecnologia in grado di conoscere non solo il "se" del contatto ma anche il "dove"[14]. Occorre naturalmente specificare

[12] Che la questione non sia peregrina è dimostrato da un attacco hacker ricevuto dall'app Covid 19 Alert! predisposta con funzioni simili dal governo olandese.

[13] In opposizione al *download* automatico realizzato dal sistema in occasione di un apposito aggiornamento. Alcuni dispositivi presenti, se non sul mercato, tra gli utenti non ricevono più aggiornamenti e a questo problema tecnica andrà trovata una soluzione.

[14] La geolocalizzazione, come sappiamo dalla tante app private che si basano su di essa, ha straordinarie potenzialità che tornerebbero molto utili anche per un migliore contrasto al virus potendo indicare ad es.

quale tipo di esposizione venga rilevata. A questa funzione essenziale e basilare si potrebbero aggiungere funzionalità per garantire tramite l'app un'assistenza sanitaria per soggetti a rischio di contagio. Un'anticipazione di queste funzioni, allo stato assai poco intrusiva, è data dalla richiesta al primo accesso dell'app, da soddisfare sempre su base volontaria, di inserire la provincia di residenza dell'utente al fine di consentire alle autorità sanitaria di mostrare informazioni rilevanti a livello locale all'utente se gli venisse notificato un contratto a rischio (v. *infra)* e di contribuire alla tracciatura del quadro epidemiologico da parte delle autorità locali e del Ministero della Salute, titolare dei dati.

La volontarietà che presiede alla costruzione del sistema appare espressione del principio di autodeterminazione che è fondamentale in quanto proiezione della dignità della persona[15]. Allo stesso tempo è però da ribadire che se tale via è preferibile a condizione che l'efficacia della tecnologia sia preservata (su questo aspetto v. *infra*), allo stesso tempo non v'è dubbio in generale limitazioni dei diritti fondamentali possano anche prescindere dal consenso per finalità pubbliche e che in questa ottica il Regolamento europeo sui dati personali consente senz'altro di prescinderne per ragioni di salvaguardia della salute pubblica e per molte altre ragioni (v. art. 23 GDPR; v. anche artt. 6 e 9[16]).

La differenza tra dati anonimi, che non sono personali, e pseudo-anonimi, che sono dati personali sono basati su un ID e comunque attribuibili ad un individuo, che resta perciò individuabile attraverso il ricorso a informazioni aggiuntive, ci porta ad un aspetto tecnico di rilievo, ovvero la cifratura che attraverso un controllo con la matrice consente di risalire al nome e al cognome di una persona o comunque ad individuarlo con certezza[17]. Queste informazioni aggiuntive sono conservate separatamente e anche laddove con disposizione non proprio cristallina si afferma che i dati «resi anonimi oppure, ove non sia possibile, [siano] pseudoanonimizzati» sono previste precise garanzie per evitare che il soggetto in questione (il soggetto a rischio di contagio) possa essere identificato dalle autorità pubbliche (e non solo). Per comprendere meglio la questione occorre descrivere anche un altro profilo problematico

la qualità del contatto, la tipologia dei luoghi dove è avvenuto, la dislocazione dei focolai, consentendo facilmente la realizzazione di grafi e così via. Tutte realizzazioni che si cercherà per quanto possibile (e spesso non sarà possibile) di replicare anche con tecnologia *bluetooth* e con dati decentralizzati. Tuttavia, la geolocalizzazione con le sue potenzialità potrebbe impattare con il principio di proporzionalità e necessità di cui agli art. 8 CEDU e artt. 7 e 8 CDFUE.

[15] G. Pitruzzella – O. Pollicino, *La via europea tra libertà e solidarietà*, in *Il Sole 24 Ore*, 28 aprile 2020.

[16] Nonché il considerando 46 che recita: «Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana».

[17] È stata espressamente esclusa qualunque forma di attingimento ai dati della rubrica, alla conoscenza del numero di telefono su cui è installata l'app, come l'invio di SMS quali forme di notifiche, le notifiche essendo interne all'app.

per fare qualche considerazione d'insieme. Appare non del tutto chiaro il riferimento alla conservazione dei dati relativi ai contatti tra i dispositivi mobili nei medesimi ovvero "anche" sui dispositivi degli utenti, lasciando intendere che altra è di regola la conservazione. La disposizione non si riferisce ad una trasmigrazione di dati e loro conservazione presso un server centrale, in quanto la scelta per la decentralizzazione, ovvero di dati conservati sui dispositivi, ha sciolto molto chiaramente il dilemma decentralizzazione/centralizzazione (su server)[18], una delle principali questioni di cui si è occupato il dibattito pubblico e di cui si è interessata l'Unione europea (sono possibili del resto soluzioni intermedie). Alla fine, si è optato per la soluzione decentralizzazione, con dati confinati negli smartphone, del tipo Dp3T, *Decentralised Privacy-Preserving Proximilty Tracing*. Il riferimento a tali dati che passano su server come ai dati che non sia possibile rendere anonimi (quindi pseudo-anonimi) si dovrebbe chiarire alla luce della creazione di una piattaforma informativa finalizzata a gestire il sistema di allerta ed integrata, per le ulteriori finalità, con le «ordinarie modalità in uso nell'ambito del Sistema sanitario nazionale» (art. 6, c. 1). Questa integrazione non è forse sufficientemente chiarita dal decreto legge, e del resto occorrono provvedimenti attuativi, ma si può provare a descrivere il funzionamento specifico dell'app allo stato attuale (e quasi definitivo) delle conoscenze.

Il soggetto A scopre di essere positivo *aliunde* e non grazie all'app. L'app infatti come abbia detto non fa diagnosi ma notifica rischi accompagnate da informazioni. Il positivo che decida di utilizzare l'app può risolversi, senza averne obbligo, di inserire questo stato nell'app, entrando in un sottomenù dove visualizza una password temporanea (*one time password*). Il soggetto prende contatto con l'operatore sanitario (ad es. per via telefonica) e lo comunica al fine di essere inserito nel server, e così ecco chiarito al riferimento al server, che tornerà anche di seguito. Dopo l'inserimento il soggetto positivo valida la password e fornisce il consenso all'invio definitivo dei dati. I dispositivi degli altri scaricano quotidianamente dal server la lista dei codici dei positivi (dati pseudo-anonimi). Se l'app riconosce tra i codici della propria memoria quello di un positivo – ad esempio il soggetto A - visualizza una notifica all'utente, che attesta una situazione di rischio di contagio in quanto esiste un "tek" (una chiave a 16-bit di esposizione temporanea, *temporary exposure key*), ovvero un collegamento di esposizione tra i due soggetti nei 14 giorni antecedenti. Tale esposizione è riconoscibile e rilevata dal sistema solo nei limiti dei segnali inviati e ricevuti (che implica un riferimento spaziale) e del tempo (la durata) dell'esposizione, che sono parametri fondamentali sia per valutare l'efficacia dell'app che la sua capacità di operare conformandosi al sistema dei diritti fondamentali. L'adozione di un sistema con codici crittografati, generati casualmente, a ripetizione, rendono praticamente impossibile l'abbinamento tra il codice e la persona dell'utilizzatore del dispositivo[19]. A questo punto il soggetto B ottiene una notifica (non dal server ma direttamente dall'app) di essere entrato in contatto ed a

[18] Variamente graduabile. Ad esempio, la Germania aveva optato per un sistema semi-centralizzato, con alcuni solo dei dati conservati presso server, anche se poi ha dovuto rimettere in discussione la scelta perché l'ingresso di Google e Apple, con le API, hanno spinto verso l'adozione di sistemi decentralizzati.

[19] Nella versione precedente il dispositivo riceveva direttamente la notifica dal server di essere soggetto "a rischio", con più evidente centralizzazione dei dati.

rischio contagio, ma non sa quando ciò sia avvenuto e chi sia il soggetto in questione. Il rischio viene calcolato, secondo un algoritmo integrato nell'app, dal dispositivo. L'utente potenzialmente positivo alla luce della ricostruzione della catena del contagio riceve a sua volta informazioni e istruzioni dalle autorità sanitarie tenuto conto della sua provincia senza divenire identificabile[20].

Con successive funzionalità l'app potrebbe essere utilizzata per comunicare con le autorità e ricevere cure personalizzate ma tali funzioni sono da implementare con attenta cura alle modalità di realizzazione e alle implicazioni, quantomeno se si vogliono preservare i caratteri attuali dell'app. Attualmente spetterebbe a colui che si venisse a trovare a rischio di contagio di seguire le istruzioni dell'autorità sanitaria locale ed eventualmente prendere contatto, senza avere alcun obbligo di farlo (ma del resto avendone convenienza), con il sistema sanitario.

Pertanto, ipotizzando che il soggetto A abbia conosciuto di essere positivo da una sintomatologia a cui è seguito un tampone (o da una politica pubblica di tamponi) grazie alla sua (eventuale) segnalazione tramite app i soggetti B, C, D, ... avranno appreso con un segnale ricevuto via dispositivo di essere stati esposti al possibile contagio. Come si vede non si tratta di una vera e propria ricostruzione della catena di contagio se non limitatamente a chi è entrato in diretto contatto da un positivo, in quanto non appare possibile risalire a coloro che hanno avuto contatti con i potenziali contagiati, salvo che a loro volta non prendano contatto con le autorità e prestino consenso, nelle modalità già viste, all'invio di ulteriori *alert*. La finalità dell'applicazione è di contenere la diffusione del COVID-19 attraverso un'informazione che può condurre ad una diagnosi precoce e, prima ancora, ad adottare cautele nella vita quotidiana al fine di non esporsi a rischi. Appaiono pienamente rispettate le indicazioni del "Comitato europeo per la protezione dei dati" secondo cui anche di fronte ad un'emergenza pubblica vanno osservati necessità, proporzionalità, limitazione delle finalità e stato di diritto. Ci si può anzi chiedere se sussista un'adeguatezza della strumentazione predisposta rispetto agli obiettivi comunque di grande pregio costituzionale. Sul punto torneremo, ma va ricordato fin da ora che l'app è solo uno degli strumenti a disposizione e che in ogni caso la ricostruzione delle catene di contagio potrà proseguire a partire da un positivo nelle modalità attualmente (fisiche, per così dire) perseguite.

In una fase successiva si potrebbe arrivare ad una cartella sanitaria (o fascicolo sanitario) e prendendo contatto con il sistema sanitario si entrerebbe in un sistema nazionale di diagnostica e cura, l'app fungendo anche da diario clinico. Il Commissario Arcuri ha affermato che «sarà necessario che [l'app] si possa connettere con il Servizio sanitario, che dia informazioni perchè si possa intervenire tempestivamente ed efficacemente» lasciando intendere come la prima fase dell'app potrebbe non essere sufficiente e che nel tempo saranno rilasciate altre funzionalità.

Allo stato il soggetto potrebbe continuare a circolare liberamente senza alcuna diagnosi e quindi tendenzialmente senza poter essere monitorato, se non lo voglia, e senza poter subire una sanzione per il suo comportamento. Mentre se per qualche ragione avesse una diagnosi di positività sarebbe sottoposto a precisi obblighi a prescindere

[20] Siamo fuori dall'ambito del c.d. "caso sospetto", di cui alla circolare del Ministero della Salute del 9 marzo 2020. V. anche circolare del 20 marzo 2020.

dall'app e tra di essi non sopravverrebbe quello di utilizzare l'app, con tutto ciò che ne consegue.

Il processo complessivo appare in linea e forse leggermente scarso rispetto alle indicazioni OMS, le quali affermano: «trova il contagiato, isolalo, testalo, tratta ogni caso e traccia ogni contagiato» (le famose tre T: *testing*, *tracing*, *treating*)[21]. L'app ruota sui positivi e consente di trovare i contagiati ma senza che l'autorità pubblica lo sappia, affidandosi per questo alla responsabilità dell'individuo, sul quale non incombe un obbligo di auto-segnalarsi, e sulla fiducia che essa può suscitare.

In termini di garanzie sulla tutela dei dati personali, attualmente queste garanzie sono pressocchè assolute. I dati di prossimità delle app che si incrociano tra loro possono dare origine a dati potenzialmente sensibili[22], in quanto relativi a condizioni di salute, ma i dati sono crittografati (anonimizzati) direttamente sui dispositivi (e non su server). Ad un certo punto sono destinati a diventare veri dati personali (pseudo-anonimi) in quanto il ruolo di un server (pubblico) è di diramare la lista dei codici anonimi dei contagiati. Non c'è un server che disponga insieme degli identificativi dei dispositivi (i codici ID) e delle chiavi di crittografia.

Nelle ultimissime "demo" dell'app i dati anonimi volontariamente messi in condivisione dall'utente tramite l'inserimento della provincia di appartenenza possono essere condivisi dal titolare del trattamento dei dati con gruppi di ricerca in forma aggregata e anonima e per scopi di ricerca, come per scoprire altri aspetti del virus (ad es. le caratteristiche all'area aperta). Si tratta di virtualità rese semplici da scelte di centralizzazione dei dati ma che anche con un sistema decentralizzato non precludono attività significative come la realizzazione di grafi sociali rappresentativi dello stato dei contagi.

Un aspetto davvero problematico è che la natura volontaria dell'app cade in un contesto tecnologico e culturale, quello italiano, non dei più innovativi e avanzati. Solo il 66% delle persone ha uno smartphone e solo il 53% di costoro installa la più nota app in uso. La volontarietà dell'app riguarda ogni aspetto del processo dalla scelta del *download* al suo utilizzo o al modo in cui la si intende utilizzare. Funzionando con il *bluetooth* l'app può essere con grande facilità attivata e disattivata (senza essere disinstallata). Nessuna penalizzazione è prevista a riguardo, neanche dopo un conclamato stato di positività. Inizialmente sono state offerte stime con modelli matematici e statistici sull'utilizzazione ottimale dell'app al di fuori della possibilità italiane palesate da questi dati. Successivamente il ministro ha fissato informalmente dei *target* molto più bassi in ragione del fatto che la misura interagirà con altre.

Ciò non vuol dire che l'app sia inutile sotto determinate soglie, come affermano molto medici e scienziati. Un siffatto approccio implica un uso del tutto parziale della "razionalità" scientifica, indifferente a vincoli giuridici e al bilanciamento ragionevole tra gli interessi che costituiscono a loro volto esercizio di altre forme razionalità scientifica, di scienze come quella giuridica di discipline come il diritto costituzionale il cui ogget-

[21] V. raccomandazioni del 27 febbraio 2020, frutto della missione congiunta OMS-Cina (16-24 febbraio 2020) e linee guida del 13 marzo 2020. Sul punto G. Perrone, *Il regolamento sanitario internazionale dell'OMS alla prova dell'emergenza COVID*, in *BioDiritto – Online First*, 26 marzo 2020, in corso di pubblicazione in *BioLaw Journal,* 2, 2020.

[22] Appartenente alle "categorie particolari" di cui all'art. 9 del GDPR.

to di studio integra anche parametri teleologici[23].
Da un lato per incapace che possa essere *di per sé* a garantire l'obiettivo massimo potenziale (in caso di utilizzo dell'app da parte di tutta la politica si porrebbero del resto una serie ulteriore di questioni giuridiche e di fatto) l'app può incidere comunque in modo positivo sull'indice di contagio. Essa non nasce certo per "mimare" condizioni simili a quelle dell'immunità di gregge, ma solo per evidenziare l'esposizione ad un rischio. In secondo luogo, è la politica che deve prendere una decisione ragionevole e valutabile in questi termini sul bilanciamento non solo tra diritti ma anche tra possibilità della tecnica (obiettivi potenziali) e soluzioni pratiche alla luce del suddetto bilanciamento.
La questione fondamentale dunque non è tanto che l'app debba condurre ad una stima precisa dei contagiati (censiti e no) perché il suo obiettivo è una più possibile diffusa individuazione precoce dei casi e tracciare, per quanto possibile, le catene di contagio. Dall'app non deve giungere alcuna falsa sensazione di sicurezza e non è una alternativa al distanziamento, vera via maestra per combattere il virus, e del resto ogni app finora, anche quelle più intrusive, è stata sempre accompagnata da politiche specifiche (test sierologici, etc.). Dovrebbe servire per indicare quando il distanziamento non è stato tenuto, si intende nei limiti dei parametri tecnici dettati dalle autorità pubbliche e delle possibilità tecniche.
Semmai problemi derivano da questi ultimi aspetti, ulteriori rispetto al prevedibilmente limitato utilizzo dell'app. La tecnologia *bluetooth* è assai meno offensiva della geolocalizzazione, con la quale la nostra posizione è costantemente segnalata e memorizzata, per non dire dell'incrocio di consimili dati degli smartphone con quelli delle carte di credito o addirittura delle telecamere pubbliche[24]. Con il *bluetooth* e senza ulteriori interazioni con altre tecnologie in via molto generale e generica due persone che si incrociano a distanza ravvicinata sono in condizione di scambiarsi dati con segnali tramite i dispositivi che si cercano con un raggio a intermittenza (*beacon*) e, con il potenziale contatto, riconoscono a vicenda. Se il caso coreano mostra che anche dati in teoria anonimi possono condurre, per circostanze di fatto, a concrete identificazioni da parte di privati, e successivamente dell'opinione pubblica, di positivi o di soggetti a rischio, ma questo rischio è sempre insito nel prodursi di particolari circostanze e non certo esclusivo del ricorso alla tecnologia, il caso di Singapore invece mostra come queste app, di cui Immuni è certamente una versione al tempo più prudente e più perfezionata, portano problemi e non solo benefici. A Singapore non solo l'app è stata poco scaricata dalla popolazione ma anche utilizzata in modo non ottimale, e non ha rilevato la metà dei contagi fino a richiedere un *lockdown* a seguito di una seconda

[23] La sequenza ideata da S. Blackburn, *Filosofia*, Bari, 2011, 112 descrive perfettamente il lavoro di squadra delle scienze: «L'elettrone ha la stessa carica a Londra, Parigi, Dehli e Pechino. Ci è voluto una fortunata coincidenza di forze politiche, sociali, economiche e culturali per consentirci di scoprirlo». Ci sono profili su cui le scienze possono pretendere di avere l'ultima parola, profili in cui solo l'interazione tra le scienze può avere l'ultima parola, e profili dove la politica può avere l'ultima parola sulla base delle risultanze di una scienza o dell'integrazione di diversi contributi scientifici.

[24] Sul punto v. D. De Falco - M. L. Maddalena, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *federalismi.it,* 13 aprile 2020, 2 ss. ove però manca, a dispetto del titolo, un confronto davvero serrato sui profili tecnici caratteristici del caso coreano, il quale del resto sembra contrastare con il principio della minimizzazione delle limitazioni rispetto agli scopi.

ondata di contagi più pesante della prima (per quanto il numero dei decessi sia rimasto limitato).

Nel caso italiano sarà fondamentale una informazione pubblica chiara e trasparente perché paradossalmente mentre si continuano a regalare dati personali a grandi compagnie con i rischi che si è detto in apertura, fanno capolino nell'opinione pubblica correnti di opinioni sfavorevoli a queste "App di Stato" (come se l'auspicabile digitalizzazione della P.A. non si basasse in definitiva su di esse...). A tale proposito, per indugiare ancora sul tema della volontarietà, non dovrebbe essere escluso il ricorso ad incentivi all'utilizzo dell'app, dove l'espressione andrebbe chiarita e specificata visto che in teoria può far riferimento tanto al *download* (o alla istallazione) che all'utilizzo, ma è solo quest'ultimo che interessa effettivamente ai poteri pubblici e che è esposto non solo a pratiche di discontinuità, del tutto legittime, ma verrebbe a rischiare anche potenziali mendacità che senza incentivi dovrebbero essere quasi del tutto escluse[25]. Ogni incentivazione dovrebbe pertanto dispiegarsi senza pregiudicare i caratteri fondamentali dell'app, a partire dall'uso di dati anonimi o semi-anonimi e comunque decentralizzati.

Del resto, l'utilizzo dell'app e il suo gradimento presso i cittadini dipendono anche da alcune specifiche tecniche, come la capacità di non consumare troppa energia della batteria (infatti dovrebbe funzionare in tecnologia BLE, *bluetooth law energy*, come già in altre precedenti esperienze) e sul modo più o meno soddisfacente con cui si integrerà con i sistemi operativi.

Qui sorgono altre questioni specifiche, dove si sono registrati sviluppi nel corso della costruzione dell'app degni di interesse e che in parte abbiamo anticipato. L'app dovrà funzionare in *background*, cioè deve poter restare aperta e correttamente funzionante sullo smartphone anche quando si utilizzano altre funzioni[26].

Per preservare la volontarietà dall'app nel senso pieno dovrebbe essere possibile disattivarne il funzionamento senza disinstallarla, spegnando il *bluetooth;* soluzione anzi prevista di *default* da alcuni sistemi operativi attuali in funzione di risparmio energetico; dall'altro dovrà essere possibile anche prevedere che una volta installata volontariamente possa, sempre su base volontaria, restare sempre attiva (salva sopravvenuta

[25] Restano possibili situazioni particolarissime, al netto di quanto si dirà in conclusione. Si immagini l'ipotesi in cui il dispositivo venga lasciato a casa o su una scrivania a lavoro con il *bluetooth* acceso e un positivo si avvicini per un tempo sufficiente di esposizione. L'*alert* qui darebbe luogo ad un caso di falso positivo. Per il resto, l'incentivo rappresenta senza dubbio una (modesta) incisione sul libero consenso inteso nel senso più rigoroso, ma i veri ostacoli appaiono altri, ovvero che i meccanismi di incentivazione per restare legittimi dovrebbero a loro volta essere conformi alle norme in tema di tutela della privacy ed altri parametri (come le normative anti-discriminazione) per cui ad es. non sarebbe possibile un accredito monetario che dovrebbe interagire giocoforza con altre app che richiedono identificazione, e anche le paventate partecipazioni a lotterie *ad hoc* riservate a coloro che installano l'app dovrebbe avvenire esclusivamente tramite la app e senza pregiudicare la privacy. Si può discutere se debbano essere esclusi alla luce del criterio del«rispetto del principio di parità di trattamento» (art. 6, c. 4, d.l. 28/2020) incentivi basati su categorie ad es. considerate a rischio per condizioni di salute o stili di vita. Tendenzialmente la parità di trattamento, se intesa come principio di eguaglianza e divieto di non discriminazione, nei contesti europei introietta la c.d. regola di giustizia che consente differenziazioni ragionevolmente giustificate.

[26] Una delle ragioni per cui il modello Singapore non ha dato buona prova è che occorreva tenere sempre l'app sempre in primo piano.

volontà contraria, del resto facilmente perseguibile anche con la disinstallazione...). Questi aspetti ci fanno entrare nel merito delle questioni poste dall'intervento delle grandi compagnie tecnologiche, due delle quali sono oligopolisti del mondo dei sistemi operativi per i dispositivi (Android di Google e IOs per Apple). Successivamente ed anche in conseguenza delle prime problematiche offerte dalle app si è prodotta una novità che ha sconvolto non poco anche il processo di ideazione delle app, perchè ha inciso sulla loro architettura in alcuni casi, come in quello italiano, già a processo avviato. Oggi le app sono integrate con i sistemi operativi dei dispositivi mobili, una soluzione praticamente necessitata per un funzionamento ottimale e quindi anche al fine di conquistare la fiducia e simpatia dei cittadini. Inizialmente l'app Immuni ne prescindeva ma i problemi operativi che ne discendevano hanno non solo in Italia portato ad affrontare il problema e sciogliere il nodo alla radice. Le due *big tech* proprietarie dei sistemi operativi hanno stretto una (inedita) alleanza per allineare i sistemi *bluetooth* ai rispettivi sistemi operativi mobili e su quel "framework" hanno proceduto a concludere accordi con i vari governi per mettere a disposizione le proprie soluzioni per una implementazione ottimale delle app nazionali, anche in tal caso stabilendo la natura *open source* di queste API (*Application Program Interface*, ovvero una interfaccia di programmazione; porte che permettono agli sviluppatori di interfacciarsi con il software) dove nome, aspetto, interfaccia e dinamiche di funzionamento sono ampiamente personalizzabili dal programmatore. Ciò ha portato ad una radicale riorganizzazione delle app, le quali in prospettiva potrebbero essere addirittura superate, con necessità peraltro di affrontare gli aspetti legali della questione[27], che si ritrovano una più o meno necessitata interposizione di interfacce che integrano meglio l'app nel sistema operativo. Queste API d'altro canto interagiscono in modo ottimale solo con applicazioni che adottano il sistema di gestione dei dati decentralizzato. Una soluzione tecnica tra l'altro preferita (a scanso di un primo orientamento) dall'Unione europea in quanto foriera di minori rischi perché evita concentrazioni di dati in server, per quanto pubblici, ed ormai praticamente obbligata.

Ma il tema delle API non rileva solo per la scelta della decentralizzazione ma anche perchè il miglioramento funzionale delle app dipende in parte significativa dai programmatori dei sistemi operativi (e delle suddette API) che fanno interagire i sistemi operativi con le specifiche tecniche dei dispositivi mobili. Il punto fondamentale è che sul mercato sono disponibili una varietà enorme di modelli sia pure con un numero limitato di sistemi operativi e questi ultimi si adattano il più possibile alle specifiche del modello in ragione della gamma di prezzo e non solo. Ciò ha condotto ad affrontare diverse questioni, dal modo di *download* dell'app (con l'aggiornamento dei sistemi operativi o meno) al funzionamento ottimale dell'app rispetto ai consumi e al problema del funzionamento in *background*, al modo di ottimizzare la tecnologia prescelta per far "girare" l'app, il *bluetooth*[28].

[27] L'ingresso di Apple e Google nel campo consentirebbe che le funzioni attualmente svolte dall'app potrebbero essere di seguito svolte direttamente dal sistema operativo, rendendo inutili le app, sempre preservando la volontarietà e la decentralizzazione dei dati. Ciò appare un discorso futuribile, in quanto richiederebbe una modifica degli aspetti normativi.

[28] Per ragioni tecniche Google, a differenza di Apple, richiede che l'app funzionerà con il dispositivo con la funzione di geolocalizzazione attiva nel sistema operativo (Android), per un funzionamento

È proprio quest'ultima la questione più rilevante in punto di diritto che intendiamo trattare prima di trarre delle conclusioni. Con questa tecnologia i dispositivi si riconoscono ad una determinata distanza. La potenza del segnale del *bluetooth* è calibrabile dagli sviluppatori mediante appositi algoritmi proprio grazie alla API, in modo da tener conto dei singoli modelli di dispositivi, di diverso valore e dunque potenzialità[29].
Appare fondamentale per valutare l'app comprendere chi riceverà il segnale di allerta (il *trigger*, grilletto) per verificare se siano ragionevoli le condizioni, in quanto da esse dipendono possibili, anche se non automatiche, restrizioni ai diritti fondamentali. E per questo una questione non da poco è quella del tempo di esposizione al rischio. La soglia rilevante di questa prossimità non è stata ancora definita e non c'entra con la fissazione della misura da parte delle autorità del distanziamento fisico, ma è destinata ad interagire in modo problematico con essa. Verosimilmente il *bluetooth* funzionerà a distanze maggiori rispetto a quelle previste dalla legge e del resto il rischio di esposizione richiede di considerare anche un altro aspetto molto rilevante, che è il tempo di esposizione.
Nelle caratteristiche attuali non potrà arrivare un *alert* per aver sfiorato o toccato una persona (risultata positiva) incrociata camminando o essere rimasto per diversi secondi o qualche minuto in sua prossimità (come alla fermata di un autobus). Ma sarebbe azzardato affermare che tale situazione non è considerata perché ha potenzialità inoffensive (v. *infra).* Secondo il protocollo di Google e Apple il tempo di esposizione che sarà memorizzato sul dispositivo sarà solo quello tra i 5 minuti e i 30 minuti. Un contatto inferiore è considerato irrilevante e uno superiore non sarà registrato in quanto tale, ma saranno registrati i singoli eventi di durata significativa che sono avvenuti nel corso di un tale contatto. L'app non contiene alcuna virtualità di tracciamento di rapporti interpersonali o di abitudini sociali.
La tecnologia *bluetooth* del resto è assai meno precisa della geolocalizzazione, la quale non è essa stessa in grado di rilevare una differenza di poche decine di centimetri. Il *bluetooth* a seconda dei modelli può rilevare altri dispositivi anche a diverse decine di metri (fino a cento, attualmente nei modelli di alta gamma), come ovviamente a distanza minime, ma individua un dispositivo entro un raggio d'azione e non lo colloca in una posizione specifica, per quanto imprecisa, e rilevata come tale.
Infine, attualmente non è risolta la questione dell'integrazione tra l'infrastruttura dell'app e le strutture tecnologiche del Sistema sanitario nazionale. Al momento i dati non sarebbero messi in contatto con il SSN perché allo stato l'app non ha le caratteristiche tecniche per integrarsi e dialogare con quelle strutture. Il server allo Stato serve a consentire tecnicamente di avere un hub per inviare le liste mettendo a frutto gli intrecci di dati. Ulteriori funzionalità andrebbero aggiunte previo aggiornamento, volontario a sua volta.
L'integrazione dell'app nelle API infine ha un ultimo rilievo sulle app regionali. Da

ottimale, ma senza che "Immuni" acquisisca le informazioni di localizzazione. Pertanto, si ribadisce che il funzionamento sarà con tecnologia *bluetooth.*

[29] Sul mercato esistono modelli in grado di connettere via *bluetooth* due dispositivi a distanza di cento metri, e quindi il rischio di falsi positivi sarebbe enorme, come peraltro è apparso nell'esperienza di Singapore. Un cenno a questo problema nel testo *infra.*

quando le *big tech* sono entrate nel settore delle app di tracciamento ed esposizione offrendo i loro servizi è sfumata la possibilità di immaginare un ben integrato sistema repubblicano di app. Diverse regioni (es. Veneto, Lombardia, Friuli-Venzia Giulia, Toscana) stanno lavorando ad app proprie, anche già in via di sperimentazione. Queste app potrebbero ben essere utili per una circolazione locale, considerando che gran parte delle persone effettuano spostamenti limitati. Ma i due colossi *big tech* hanno dichiarato che consentiranno l'integrazione con le API di una solo app per ogni Stato e quindi queste app regionali probabilmente non saranno altrettanto raffinate e integrabili con quella statale. Del resto, incontrerebbero limiti ben maggiori nel campo dell'incisione dei diritti fondamentali.

4. Considerazioni conclusive

Nel momento in cui scriviamo sono trascorse tre settimane dalla prima riapertura del 4 maggio. Essa è avvenuta in circostanze tutt'altro che ottimali e più che altro per l'impossibilità di protrarre il *lockdown,* per cui sarebbe stato fondamentale già disporre dell'app come degli accorgimenti organizzativi (per es. nei trasporti pubblici) e delle politiche sanitarie (test sierologici, strategie precise su tamponi, etc.) volte a minimizzare i rischi. Tutto ciò è avvenuto solo molto parzialmente e non è noto ancora quando ci sarà il varo dell'app. Qualche critico si è spinto a dire che l'app ha fatto la fine delle mascherine a prezzo calmierato (che non si trovano[30]) ma il governo ha confermato che l'app è prossima ad essere rilasciata. Del resto, è destinata ad operare sulla base di una condizione di positività conclamata ma che opera in un quadro non soddisfacente di tracciamento e trattamento, se consideriamo che questo virus è reso pericoloso soprattutto dal fatto che è trasmesso prevalentemente da asintomatici (beninteso, perché la loro condizione è più insidiosa).

Alcuni aspetti dell'app devono ancora precisati, tra di essi abbiamo già fatto cenno ai modi e ai tempi di esposizione per l'*alert*. Si parla di parametri diversi a seconda delle circostanze ma il *bluetooth* ha potenzialità molto limitate in ciò. Torneremo sul punto dell'intreccio tra vincoli tecnici e giuridici, che appare dirimente.

Allo stato restano aperti alcuni problemi. Manca l'identificazione puntuale dei server e della loro collocazione, comunque pubblici e dislocati sul territorio nazionale, per quanto i rischi siano comunque limitati dalla scelta della decentralizzazione. Occorrerà certamente vigilanza su come saranno realizzate eventuali "fasi due" per le funzionalità dell'app, quando aumenteranno i soggetti coinvolti (es. regioni, Asl) e le potenzialità intrusive (col fascicolo sanitario). L'intermediazione delle API non dovrebbe invece destare alcuna preoccupazione in termini di possibile trasmigrazione di dati verso server collocati all'estero, e del resto alla base di quell'intervento è stata posta la condizione della decentralizzazione dei dati.

Attualmente l'app è stata giudicata in modo molto favorevole dall'M.I.T. anche sotto profilo della sicurezza. Il codice sorgente è stato resto noto e i tecnici saranno in grado di verificarne ogni carenza o *vulnus* in termini di sicurezza, a partire da eventuali *back-*

[30] P. Battista, *Ma che fine ha fatto l'app Immuni?*, in *Corriere della Sera*, 25 febbraio 2020.

doors[31]. Online esiste una comunità molto attiva che già sta operando quotidianamente per discutere e contribuire a migliorare efficienza e sicurezza dell'app.
In Italia il Copasir, organismo parlamentare di vigilanze sulla sicurezza nazionale, si è espresso con una relazione che promuove l'app con alcune riserve, che a dire il vero sono apparse per molti aspetti, un po' come in certi atti di indirizzo parlamentari, più dei manifesti politici dei singoli gruppi che delle preoccupazioni o dei suggerimenti concreti. La gran parte delle raccomandazioni infatti riguardano profili in realtà già definiti e in modo tale da superare quelle riserve; per il resto esistono aspetti marginali non ancora disciplinati e in tal caso non si tratta tanto di riserve ma utili indirizzi che si muovono ponendo condizioni entro linee europee già ben definite. I profili di sicurezza nazionale potenziali sono indubbi ma la relazione non dà molto spazio a diversi motivi di polemica dei giorni precedenti, a partire dalle modalità di selezione dell'azienda costruttrice dell'app, al suo modo di essere, e alla sua appartenenza ad un consorzio che lavorava su soluzioni centralizzate[32]. Lo stesso vincolo della gratuità della costruzione e dell'aggiornamento dell'app (quest'ultimo aspetto ha reso necessario un appalto di servizi, cui fa cenno l'ordinanza del Commissario datata 16 aprile 2020), sicuramente ripagata da un importante ritorno di immagine, può destare qualche perplessità sulle ragioni che portano un'azienda a impegnare decine di unità di personale per mesi e per migliaia di ore/uomo[33] senza alcun ritorno diretto, ma una risposta sta

[31] Gli sviluppatori dell'app "Immuni" avrebbero predisposto un'ulteriore cautela consistente nella produzione di "*dummy traffic*", trasmissione di dati spazzatura generati dai dispositivi in modo da inquinare il segnale per malintenzionati che volessero carpire informazioni tramite un'analisi di traffico. Inoltre, prima di essere distribuita l'App affronterà un "*penetration test*", i cui risultati dettagliati saranno divulgati.

[32] La società, una società per azioni ben nota, la Bending Spoons, ha sede legale in Italia e nel suo capitale ci sono piccole quote provenienti da stati non democratici, tramite fondi lussemburghesi gestiti da finanzieri italiani. Il Copasir anche per questa ragione si è mostrato molto interessato ad approfondire la procedura di selezione della società, molto solida e dotata di indubbia reputazione nell'ambiente sia per i risultati economici che per le soluzioni nel campo della sicurezza (150 dipendenti, 300 milioni di applicazioni scaricate, 90 milioni di dollari di ricavi nel 2019). La procedura di scelta tuttavia è stata opaca. Solo dopo l'approvazione del decreto legge che fa da base legale all'app sono stati pubblicati i documenti degli esperti della task force che avrebbe dovuto stabilire i criteri per la scelta della società incaricata di costruire l'app ed è emerso che l'organismo aveva raccomandato di testare in via parallela due app di altrettante società ma che il ministro competente non ha rispettato questa raccomandazione e ha scelto di testare una sola app, "Immuni", ritenendola «più rispondente alle attuali necessità». Inoltre, è emerso che il gruppo di esperti aveva subordinato la scelta dell'app a una serie di requisiti tecnici che quantomeno al momento della produzione del report non erano stati rispettati da alcuna società concorrente. La situazione tuttavia successivamente si era molto modificata.
Un altro fattore di interesse è stato rappresentato dal fatto che la Bending Spoons fa parte di un consorzio europeo pubblico-privato "no profit" (il cui acronimo è PEPP-PT), quindi non commerciale ma neanche istituzionale, costituito da poco per creare uno standard in tema di app di questa tipologia e con sede legale in Svizzera, sostenuto da una Fondazione avente sede a Basilea e sotto la vigilanza del governo svizzero (quindi non UE). Tale consorzio in qualche modo riconosciuto anche dalle istituzioni comunitarie – tanto che si parla di un modello europeo - ha avuto vicenda anche travagliate, con l'abbandono polemico da parte di alcuni soggetti (anche italiani). L'opinione pubblica italiana ha parlato non poco di questo consorzio, del resto operativo in tutta Europa senza grandi polemiche, ma il Copasir non ha sollevato questioni degne di rilievo. Il ruolo del Consorzio è venuto scemando con l'intervento in campo di Apple e Google che hanno portato avanti, con le proprie API, un modello decentralizzato (DP3T) che ha finito per esercitare anche una sorta di tutela o comunque porre vincoli tecnici alle società costruttrici delle app.

[33] *Sulla app nessun guadagno. Fiducia e privacy fondamentali*, in *Corriere della Sera*, 23 aprile 2020, intervista al

nella selezione che vedeva ben 319 aziende interessate, quindi indubbiamente attraente a prescindere dal compenso. Il funzionamento dell'app dovrebbe esaurirsi con la fine dell'emergenza, con la disponibilità del vaccino o la scomparsa del virus e non dovrebbe collegarsi formalmente ad altre operazioni di digitalizzazione della P.A. ed in particolare della Sanità.

In conclusione, la soluzione italiana appare sicuramente in linea sia con la Costituzione che con la normativa europea a partire dall'art. 23 del Regolamento generale sui dati personali (ad anche all'art. 15 della Direttiva e-Privacy) che, ormai sotto l'ombrello dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, consentono limitazioni a mezzo di misure legislative di alcuni diritti nella misura in cui la limitazione rispetti "l'essenza dei diritti e delle libertà fondamentali" e sia "una misura necessaria e proporzionalità in una società democratica" al fine di salvaguardare un'ampia serie di obiettivi tra cui la sicurezza pubblica e la sanità pubblica (art. 23 cit.; non dissimile l'art. 15 cit., che prevede anche che i dati siano conservati «per un periodo di tempo limitato»). La base legale è stata assicurata col decreto legge n. 28/2020. Le previsioni in esso previste sono proporzionate anche alla luce di quanto sollecitato dell'European Data Protection Supervisor in astratto (vedi rapporto annuale 2019) a mezzo della descrizione delle misure, dell'indicazione di massima dei diritti limitati, dell'indicazione della finalità della misura pianificata e della scelta delle misure meno impattanti. Il criterio della gradualità appare rispettato con la scelta delle misure meno invasive ritenute idonee e sufficienti per i fini istituzionali dell'app e optando per la piena volontarietà dell'uso dell'app. Si è rinunciato ad una tecnologia tracciante *tout court* e qualunque finalità di controllo e/o repressiva, palesandosi anzi una spiccata componente "solidaristica"[34], che rientra molto relativamente nell'idea della c.d. sorveglianza attiva tanto richiamata, e spesso auspicata in questi casi. Non solo la volontarietà ma per il modo stesso con cui funziona si stenta a considerarla come uno strumento di limitazione significativa di un qualche diritto fondamentale. Diversi diritti sono stati limitati in questi mesi a prescindere dalla app e anche in modo draconiano, poco ragionevole e proporzionato. L'ordinamento sembra aver recuperato un po' di equilibrio, e ad un esame approfondito di tipo prognostico l'app non appare gravare in modo rilevante, nello stadio delle sue funzionalità attualmente previste, su alcuno di essi. In ogni caso l'esercizio dei diritti degli interessati potrà essere esercitato «anche con modalità semplificate» (art. 6, c. 2, lett. *f*), richiamo forse anche ultroneo stante la tutela apprestata in generale dall'art. 82 GDPR[35].

La prudenza della soluzione italiana rovescia l'approccio finora invalso poco rispettoso della tutela della dignità umana alla luce dell'equilibrio che deve sussistere tra diritti e interessi che si intrecciano[36], fino al punto da potersi interrogare sul grado

dott. Ferrari, A.D. Bending Spoons.

[34] Utilizzo l'espressione di O. Pollicino, *Data tracing, no a deleghe in bianco*, in *corrierecomunicazioni.it*, 24 marzo 2020, 7.

[35] *Ibidem*. Il contributo non si riferisce alla soluzione adottata, in quanto precedente al decreto e quindi si esprime in chiave normativa. Sul ruolo del principio solidaristico anche in riferimento all'attuale emergenza v. M. Noccelli, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in *federalismi.it*, 13 marzo 2020, 2 ss.

[36] Criticato con severità ad es. da V. Baldini, *Dignità umana e normativa emergenziale: (in)osservanza di un*

di funzionalità dell'app rispetto all'obiettivo, che andrebbe valutato però nell'insieme delle soluzioni adottate, non solo di tipo tecnologico. In ogni caso qualche cenno di confronto con le soluzioni adottante o adottande all'estero può essere significativo. Limitandoci al campo democratico, in alcune esperienze estere il cittadino che usa l'app è spesso schedato come paziente (ad es. in Australia), o il server governativo è gestito da un privato (Amazon, ancora Australia); di frequente viene mappata la diffusione dei casi (sia pure con la garanzia si una rapida distruzione dei dati); in Norvegia l'app è prodotta da una no-profit governativa ma utilizza il ben più intrusivo gps e i dati stazionano per trenta giorni su un server governativo. Per non dire dei modelli asiatici democratici e tacendo ovviamente sugli altri[37]. I grandi paesi europei sono più indietro del nostro nelle risoluzioni. La Germania si sta distinguendo per il suo approccio, almeno a livello federale, assai circospetto sull'uso di simili tecnologie, anche nelle soluzioni molto riduttive all'italiana, a causa del retaggio totalitario dei sistemi di sorveglianza di massa (anche fino ad anni non troppo remoti: si pensi alla esperienza della Germania est) che porta i cittadini ad essere tendenzialmente contrari a forme di potenziale intrusione. Le amministrazioni regionali e locali sembrano più interessate a questi strumenti e aperte anche a raccolte massive di dati ma non è certo alle entità federate che spetta decidere su interessi per definizione unitari. Nel momento in cui consegniamo il lavoro il dibattito tedesco appare in un certo stallo. In Francia si fanno considerazioni non molto diverse da quelle italiane ma l'eccezione francese, a partire da una certa preferenza per il ruolo del pubblico e quindi anche per soluzioni centralizzate, ha costituito per settimane un ostacolo a fare passi importanti verso le realizzazioni, con richieste di soluzioni tecniche da parte del governo francese alle *big tech* piuttosto singolari quando ci si è resi conto dell'inevitabilità di forme di collaborazione. L'approccio francese consente di concludere sui rischi in punto di sicurezza informatica. Il rischio che *hacker* riescano a forzare i sistemi e a compiere azioni come mandare *alert* ingiustificati o provare a identificare soggetti alla luce delle persone con le quali si è stati in contatti ed altro ancora sono sempre possibili, per quanto le soluzioni invalse in Europa, a partire dalla decentralizzazione dei dati, diano buone garanzie quantomeno di danni più limitati rispetto a quelli di server certamente assai meno violabili di singoli dispositivi ma la cui violazione, cui abbiamo assistito in tanti campi negli ultimi anni, avrebbe effetti gravi.

Concludendo, piuttosto che come una minaccia diretta ai diritti fondamentali, il problema fondamentale dell'app, nella versione attuale, potrebbe essere legato alle conseguenze del rischio di alimentare direttamente o indirettamente un alto numero sia di falsi negativi che di falsi positivi. Se i primi non dipendono dall'app, essa d'altra parte può non segnalare diversi eventi rischiosi che solo una calibratura molto invadente del *bluetooth* potrebbe garantire, senza peraltro riuscire a distinguere le situazioni effettivamente a rischio dalle altre. Questa situazione è assimilabile a quella dei falsi positivi,

paradigma formale o (colpevole…) elusione di un parametro (anche) sostanziale? Aspetti problematici di un difficile equilibrio, in *dirittifondamentali.it*, 2, 2020, spec. 203 ss.

[37] Sul modello cinese utile A. Canepa, *Lotta al COVID e diritti dei cittadini nella Repubblica Popolare Cinese. Le peculiarità di un ordinamento socialista asiatico*, in *federalismi.it*, paper "Osservatorio Covid-19" (a cura di L. Cuocolo), 13 marzo 2020, 168 ss.

che magari pur avendo rispettato le distanze legali (ammesso che siano necessarie e sufficienti ad evitare il contagio, che, ricordiamo, non dipende solo dalle distanze, ma anche da norme igieniche), ricevono l'*alert*. Quindi da questo punto di vista pur essendo ogni iniziativa rimessa ai privati, si potrebbe determinare un numero eccessivo di richieste di approfondimenti a cui le strutture pubbliche potrebbero essere non in grado di far fronte rapidamente[38]. Non è peregrino il rischio di auto-confinamenti spontanei da parte di privati per ragioni prudenziali, magari sulla base di una imperfetta conoscenza delle modalità operative dell'app (la tecnologia tende ad essere ritenuta infallibile...), del tutto inutili e ingiustificati. Oppure il numero eccessivo di *alert* che un medesimo soggetto riceve porterà ad una assuefazione che rischia di travolgere anche quelle circostanze in cui la situazione ha dato luogo ad un rischio anche elevato.

Si pongono in altri termini tutti quei problemi che derivano da una certa ottusità della tecnologia, e a cui solo attenzione e buon senso (quest'ultimo assenta per definizione nelle tecnologie) degli esseri umani può porre rimedio.

Anche ammettendo un tasso alto di utilizzo di Immuni esistono molte situazioni che sfuggirebbero al suo monitoraggio e molte altre che entrerebbero nei suoi *radar* senza presenza di un effettivo rischio. Una app - almeno una app relativamente semplice - non rileva un muro o una barriera, non distingue se lo spazio è chiuso o aperto, non riconosce il ruolo peculiare che nella situazione concreta può giocare ad es. il *droplet,* non sa se le altre persone, come anche chi utilizzi Immuni, indossi dispositivi di protezione (ammesso che servano nella circostanza in questione). Immuni non potrà sapere se il prossimo incrociato dal dispositivo solo per un attimo ad una distanza limite per la legge e forse inclusa nel raggio d'azione del *bluetooth* ma ritenuta non rilevante ha fatto un colpo di tosse o se chi utilizzi l'app sia stato pochi secondi o quattro minuti a distanza non di sicurezza (in entrambi i casi, con un positivo), né potrà leggere correttamente la situazione di un lungomare affollato con persone a passeggio che rispettano le distanze di sicurezza (ma ove non fosse l'*alert* tendenzialmente mancherebbe) o di una spiaggia che è altrettanto affollata ma con una situazione ben più statica (dove l'*alert* sarebbe più probabile).

Il rischio forte è che un'app di questo tipo, pur nata per incidere in modo davvero minimo sul godimento dei diritti fondamentali, non solo serva a poco ma il suo modesto contributo sia controbilanciato da una certa confusione derivata (l'esempio del lungomare o della spiaggia appaiono emblematici). Al limite da qui potrebbe derivare una rilevante incisione sui diritti fondamentali, determinando i maggiori condizionamenti di fatto.

Le app come Immuni metaforicamente potrebbero essere descritte con varie metafore ottiche relative al campo visivo. A seconda dei limiti di fatto o tecnici, e anche per il loro incrocio, può dirsi che per quanto sia ben congegnata Immuni veda troppo per certi versi, troppo poco per altri e non vede affatto diverse "aree cieche". Si conferma

[38] Il decreto legge del 30 aprile prevede che la ricerca e gestione dei contatti per essere condotta in modo efficace deve prevedere delle risorse umane dedicate tra operatori sanitari e di sanità pubblica e personale amministrativo. In Italia si tratterebbe di circa 6.000 (una circolare del ministro della Salute quantifica queste risorse in circa una unità ogni 10.000 abitanti). Il loro compito consisterebbe nel monitorare pazienti in quarantena, eseguire tamponi, inserire tempestivamente dati nei diversi sistemi informativi.

la sua funzione assolutamente complementare, ma solo la pratica potrà dire che nel calcolo tra benefici e costi (non in termini stretti di diritto) ne valga la pena.
Mentre la politica fa le sue valutazioni, sarebbe ragionevole attendersi una campagna di informazione non solo sui profili di sicurezza dell'app ma anche sui modi di funzionamento, in modo che il fruitore possa essere messo in condizione di essere, per quanto possibile, il miglior giudice del rischio che corre. Un ulteriore aspetto di volontarietà dell'app dovrebbe consistere in questo, conformemente all'approccio europeo alla tecnologia digitale e alle risorse "esperte": le donne e gli uomini devono essere posti in condizioni di comprendere il funzionamento l'app per decidere, per non perdere il controllo della situazione, senza cui la volontarietà circa il seguito da dare agli *alert* dell'app diventa una bizza (magari per non andare a lavoro). Per avere sempre l'ultima parola, perché nell'app c'è l'algoritmo e il *software*, magari scritti ed eseguiti alla perfezione; la tecnologia può aiutare e ampliare gli spazi dell'autonomia, ma l'autonomia si misura nell'intenzionalità e nella vita vissuta, che è un'altra cosa.