ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
4 / 2020

OTTOBRE - DICEMBRE

L'app Immuni quale requisito per lo svolgimento di attività a rischio (di diffusione del contagio)? Una proposta per incentivare l'uso delle ICT nella lotta alla pandemia

Diana-Urania Galetta e Gherardo Carullo

Alla luce delle numerose misure restrittive adottate in Italia, come in molti altri paesi, per contenere l'epidemia di SARS-CoV-2, gli autori esaminano i termini entro i quali l'uso dell'App Immuni potrebbe essere qualificato come condizione legittimante per lo svolgimento di attività a rischio di contagio al fine di dare maggiore effettività alle misure di contenimento dell'epidemia e, quindi, meglio calibrare le limitazioni alle libertà personali. In questa prospettiva, l'attenzione degli autori si concentra sull'analisi del funzionamento dell'app Immuni, specie in un'ottica di protezione dei dati personali ed alla luce dell'analisi delle norme europee in materia, analizzate anche attraverso il prisma del principio di proporzionalità.

[The Immuni app as a requirement for carrying out activities at risk (of widespreading the contagion)? A proposal to encourage the use of ICT in the fight against the pandemic] In light of the numerous restrictive measures adopted in Italy, as in many other countries, to contain the SARS-CoV-2 epidemic, the authors examine the terms with which the use of the "App Immuni" could be qualified as a legitimate condition for carrying out activities at risk of infection. Digital contact tracing could give greater effectiveness to the measures taken to contain the epidemic and, therefore, lead to a better calibration of the limitations to personal freedoms. In this perspective, the authors' attention is focused on analyzing the functioning of the app Immuni, especially in view of protecting personal data and in light of the analysis of the relevant European standards, also analyzed through the prism of the principle of proportionality.

1. Introduzione[1]

Con l'inizio dell'autunno i dati sulla diffusione della pandemia in Italia hanno determinato un nuovo ciclo di misure volte a contrastare il diffondersi del virus SARS-CoV-2, conosciuto anche come COVID-19 (acronimo di COronaVIrus Disease 19). Le nuove misure hanno ancora una volta limitato in modo molto incisivo diritti e libertà fondamentali garantiti sia a livello nazionale sia da norme sovranazionali[2]. Ne sono un emblematico esempio i d.P.C.M. da ultimo adottati[3], che hanno sancito limitazioni in ordine allo svolgimento di molteplici attività.

Le Autorità hanno dunque dovuto prendere atto che il regime di prevenzione adottato durante la pausa estiva non è risultato idoneo, quantomeno con l'arrivo dell'autunno, ad arrestare efficacemente il virus, imponendo di conseguenza un più rigido regime di contenimento. Tra le numerose limitazioni imposte con i d.P.C.M. dall'inizio dell'emergenza sanitaria ad oggi non appare tuttavia previsto un uso particolarmente significativo della tecnologia quale mezzo per fronteggiare il diffondersi dei contagi.

Eppure, l'utilità delle soluzioni digitali è stata evidenziata proprio dal Commissario Straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19. Come chi scrive aveva già suggerito sin dall'inizio della pandemia[4], anche il Commissario Straordinario ha sottolineato che il tracciamento dei contatti, o *contact tracing*, può «*aiutare ad identificare individui potenzialmente infetti prima che emergano sintomi e, se condotto in modo sufficientemente rapido, può impedire la trasmissione successiva dai casi secondari*», espressamente evidenziando che «*l'uso della tecnologia in ambito di contact tracing appare in grado di dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale che non sempre si rivela efficace e comporta maggior dispendio di risorse*»[5].

Pur a fronte delle oggettive complessità organizzative che la pandemia ha determinato per le amministrazioni pubbliche[6], e le severe limitazioni imposte sin dal principio della pandemia, il legislatore, prima in forma di decreto d'urgenza, poi in sede di conversione, ha ritenuto di prevedere l'uso dell'app *Immuni* come meramente volontario. In altri termini, le autorità hanno ritenuto

preferibile lasciare ai cittadini la scelta se scaricare, o meno, l'app *Immuni* su di un dispositivo *mobile* su cui tale applicazione possa essere installata.
Una tale opzione poteva effettivamente apparire condivisibile nei primi mesi della pandemia, ossia in un momento di relativa incertezza[7]. Dopo la pausa estiva, in ragione della nuova impennata dei contagi, è tuttavia apparsa evidente la necessità di contrastare il virus con nuove misure di contenimento. L'esperienza ha infatti dimostrato che sono necessarie misure di prevenzione particolarmente rigide, pena la non effettività delle stesse. Senonché nel contempo si sono registrate forti proteste contro le limitazioni delle libertà personali[8], il che ha indotto le autorità a rinviare quanto più possibile un *lockdown* totale quale quello della primavera del 2020.
Alla luce dunque della necessità di limitare le attività dei privati, e della scarsa effettività delle misure di contenimento sino ad oggi adottate dopo il suddetto *lockdown*, la perdurante scelta di non prevedere un uso più deciso delle tecnologie digitali – ed in particolare di quelle già disponibili e pronte all'uso quali l'app *Immuni* – risulta poco comprensibile.
Alla luce dei recenti fatti, appare infatti ragionevole domandarsi in che modo sarebbe possibile utilizzare la tecnologia ai fini di un più capillare tracciamento dei contagi, introducendo altresì appropriate misure di *follow-up* in caso di contatto con un positivo[9], specialmente al fine di dare maggiore effettività alle misure di contenimento dell'epidemia. A tal fine, considerato che l'app *Immuni* è già disponibile e scaricabile, appare anzitutto opportuno analizzarne il funzionamento.

2. Le questioni tecniche più rilevanti in ordine al funzionamento dell'app *Immuni*

L'app *Immuni* – scaricabile gratuitamente dai negozi digitali dei maggiori fornitori di dispositivi *mobile*[10] – è stata creata per aiutare a combattere la pandemia causata dal virus COVID-19. Secondo quanto spiegato nel sito web ufficiale «*gli utenti che vengono avvertiti dall'app di un possibile contagio possono isolarsi per evitare di contagiare altri. Così facendo, aiutano a contenere l'epidemia e a favorire un rapido ritorno alla normalità*»[11].
L'app utilizza dunque la tecnologia per avvisare gli utenti che sono stati esposti al

virus, anche se asintomatici. Lo scopo è interrompere la catena delle infezioni informando le persone che sono state potenzialmente esposte al virus. Tale risultato viene conseguito non monitorando gli spostamenti dei singoli utenti, ma piuttosto ricorrendo ai sensori normalmente presenti nei dispositivi mobili per intercettare possibili contatti con persone infette. Si spiega che «*a chi si è trovato a stretto contatto con un utente risultato positivo al virus del COVID-19, l'app invia una notifica che lo avverte del potenziale rischio di essere stato contagiato. Grazie all'uso della tecnologia Bluetooth Low Energy, questo avviene senza raccogliere dati sull'identità o la posizione dell'utente*»[12]. L'obiettivo è di tracciare i contatti ed allertare gli utenti di un possibile contagio, al contempo garantendo la privacy degli utenti, riducendo al minimo o addirittura escludendo completamente la raccolta dei dati personali.

Si sottolinea che «*Immuni è stata progettata e sviluppata ponendo grande attenzione alla tutela della privacy. I dati, raccolti e gestiti dal Ministero della Salute e da soggetti pubblici, sono salvati su server che si trovano in Italia. I dati e le connessioni dell'app con il server sono protetti*»[13]. In particolare, secondo il sito web ufficiale, *Immuni* non raccoglie il nome, il cognome o la data di nascita di alcuna persona, né il numero di telefono, l'indirizzo e-mail, l'identità delle persone incontrate dall'utente o il luogo o movimenti degli utenti. In modo ancor più netto, nel quadro di sintesi dell'«*informativa privacy*» dell'app viene espressamente indicato che «*Immuni non può risalire alla tua identità o a quella delle persone con cui entri in contatto*» e che «*Immuni non raccoglie alcun dato di geolocalizzazione*»[14]. Quanto alla geolocalizzazione, occorre evidenziare che questa, su alcuni dispositivi, deve essere attiva affinché l'app *Immuni* funzioni. Anche in tali casi, tuttavia, l'app non ha accesso a tali dati in quanto non viene richiesta al sistema la relativa autorizzazione – che l'utente dovrebbe espressamente concedere –, sicché si può affermare con sicurezza che in ogni caso nessuna informazione al riguardo può essere raccolta da *Immuni*[15].

In sostanza, secondo quanto spiegato sul sito web ufficiale, l'app funziona come segue[16]: ogni *smartphone* su cui *Immuni* è installato invia in modo continuo un segnale *Bluetooth Low Energy* che contiene un codice alfanumerico. Quando due *smartphone* su cui *Immuni* è installata si trovano nelle immediate vicinanze, memorizzano reciprocamente il codice pubblico dell'altro, prendendo nota di quell'evento. I due *smartphone* annotano anche quanto è durato l'evento e la

distanza approssimativa tra i due dispositivi. Se il proprietario di uno *smartphone* su cui *Immuni* è installato risulta successivamente positivo al SARS-CoV-2, grazie all'aiuto di un operatore sanitario l'utente è in grado, restando anonimo, di trasferire le proprie chiavi di esposizione giornaliere su un server pubblico, che possiamo qui identificare come "cloud delle chiavi di esposizione". Tale condivisione delle chiavi di esposizione giornaliere sul "cloud" permette agli altri utenti di essere allertati di essere venuti a contatto con un positivo, senza che ne sia svelata l'identità.

Più precisamente, sotto un profilo tecnico, il funzionamento dell'app si basa sulla tecnologia di *Exposure Notification* sviluppata da Apple e Google, appositamente per permettere il *contact tracing* digitale nella pandemia da COVID-19[17]. Per meglio comprendere come tali codici alfanumerici siano generati e scambiati occorre dunque analizzare tale tecnologia.

Secondo la documentazione tecnica rilasciata congiuntamente da Apple e Google[18], alla base del sistema di creazione dei suddetti codici alfanumerici vi è la *Temporary Exposure Key* (TEK), ossia la chiave di esposizione giornaliera[19]. Questa è generata da una funzione denominata CNRG, che, secondo quanto riportato, «*designates a cryptographic random number generator*». La TEK è quindi generata del tutto casualmente senza alcun riferimento né all'utente né al *device*. Viene quindi in rilievo la *Rolling Proximity Identifier Key* (RPIK) che è derivata dalla chiave di esposizione giornaliera (la TEK) e viene utilizzata per generare i *Rolling Proximity Identifiers* (RPI). Questi ultimi sono i codici alfanumerici che vengono effettivamente scambiati dai dispositivi *mobile* che si trovano nelle vicinanze. Insieme a questi vengono anche inviati dei metadati (*Associated Encrypted Metadata*, AEM).

Tali metadati contengono informazioni tecniche relative alla versione del protocollo utilizzato dal dispositivo dell'utente ed alla potenza di trasmissione del segnale *Bluetooth*, utili per una migliore approssimazione della distanza del contatto[20]. Sicché nemmeno questi dati contengono alcun riferimento all'utente.

Tali metadati sono criptati utilizzando una chiave di cifratura (*Associated Encrypted Metadata Key*, AEMK) che è ricavata dalla chiave di esposizione giornaliera. La ragione per cui tali dati sono cifrati è in sostanza di consentire il tracciamento anonimo dei contatti. Per decifrarli è condizione necessaria e

sufficiente conoscere la chiave di esposizione giornaliera utilizzata per generare la chiave di cifratura dei metadati (AEMK). Conoscendo infatti la chiave di esposizione giornaliera, è possibile generare nuovamente la AEMK e quindi decifrare i metadati. Il che è alla base del meccanismo che consente di verificare se un utente sia venuto a contatto con un soggetto poi risultato positivo.
Come accennato sopra, in caso di positività vengono caricate "nel cloud" le chiavi di esposizione giornaliera. Parallelamente, tutti gli altri utenti, i cui dispositivi controllano periodicamente l'esistenza di nuove chiavi di esposizione nel cloud, scaricando le chiavi possono verificare se con queste – generando le relative AEMK – siano in grado di decifrare i metadati salvati nel corso dei contatti con altri utenti. Se così è, significa che il soggetto è entrato in contatto con un positivo, ed utilizzando le informazioni contenute nei metadati è possibile calcolare la distanza approssimativa del contatto e, quindi, la probabilità del contagio.

3. La neutralità dell'App *Immuni* rispetto alla protezione dei dati personali

Alla luce del suesposto quadro tecnico relativo al funzionamento di *Immuni*, onde valutare se, ed in che termini, *Immuni* risulti presentare criticità in relazione alla disciplina sulla protezione dei dati personali, occorre anzitutto ricordare che, ai sensi dell'articolo 2, paragrafo 1, il Regolamento 2016/679/UE (Regolamento) «*si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*».
In forza di tale previsione dell'articolo 2 si può agevolmente ritenere che, ove i dati raccolti non siano qualificabili come personali, a ben vedere il Regolamento non dovrebbe trovare applicazione *tout court*. Occorre dunque anzitutto acclarare se i codici alfanumerici sulla base dei quali funziona l'app *Immuni* (come esposto sopra) possano essere qualificati come dati personali.
In proposito, secondo la definizione fornita dal Regolamento stesso, ai sensi dell'art. 4, comma 1, n. 1, per dati personali si intende «*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")*». Lo stesso comma aggiunge che «*si considera identificabile la persona fisica che può*

essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

È necessario sottolineare che anche un mero dato alfanumerico, apparentemente anonimo, può talvolta assurgere a dato personale. Sul punto il considerando 30 del regolamento spiega che «*le persone fisiche possono essere associate a identificatori in linea forniti dai loro dispositivi, applicazioni, strumenti e protocolli, quali indirizzi di protocolli internet, identificatori di cookie o altri identificatori come i tag di identificazione a radiofrequenza. Ciò può lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*». A questo proposito, per analogia, è anche possibile ricordare che la Corte di giustizia ha dichiarato «*che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone*»[21].

Venendo all'app *Immuni*, secondo quanto riportato nell'«*informativa privacy*» consultabile dall'app stessa, e per quanto riguarda il funzionamento locale dell'app – ossia sul dispositivo dell'utente –, non risulta che la stessa raccolga od elabori alcun dato che, anche congiuntamente agli altri, possa in alcun modo rendere «*una persona fisica identificata o identificabile*».

Tra tali dati, per lo più consistenti in codici alfanumerici privi di una qualsiasi riferibilità ad una persona fisica[22], viene anche prevista la «*provincia di domicilio*». Nonostante tale espressione sia normalmente usata in contesti in cui vi è una raccolta di dati personali, in questo caso occorre evidenziare che tale informazione, da sola od anche congiuntamente a tutti gli altri dati gestiti dall'app *Immuni*, non è in alcun modo in grado di consentire l'identificazione di una persona fisica.

Quanto ai codici alfanumerici, occorre sgombrare il campo da un equivoco di

fondo. Detti codici alfanumerici, come esposto sopra, sono generati da algoritmi a partire da elementi casuali, ivi inclusa la chiave di esposizione[23], senza alcun riferimento all'utente. Rispetto alla terminologia del Regolamento 2016/679/UE, non pare quindi si sia addirittura nemmeno in presenza di pseudonimizzazione[24], che postula l'esistenza di un qualche dato riferibile ad una persona fisica[25], né di pseudo-anonimizzazione[26], ma di vera e propria totale anonimizzazione, in quanto tali dati non sono in alcun modo generati a partire da dati personali, né sono mai a questi associati.

In condizioni di normale funzionamento in locale – ossia sul dispositivo dell'utente –, dunque, non pare che l'app *Immuni* possa dirsi in alcun modo interferire con la disciplina del Regolamento, in quanto non sono trattati dati personali. La stessa «*informativa privacy*» dell'app, che pur risulta redatta con espressioni che riecheggiano il Regolamento, espressamente afferma, in relazione alla «*Tipologia di dati*» trattati, che «*per impostazione predefinita, i dati personali raccolti dall'App non consentono l'identificazione diretta dell'utente, o del suo dispositivo*». Dal che se ne dovrebbe desumere confermata la non applicabilità *tout court* del Regolamento[27].

Considerato l'uso dell'aggettivo «*diretta*» nella suddetta informativa laddove viene esclusa la possibilità di identificazione dell'utente, occorre tuttavia domandarsi se sia possibile un'identificazione «*indiretta*» che possa comunque attrarre il sistema nell'ambito di applicazione del Regolamento.

In proposito qualche preoccupazione potrebbe solo sorgere in relazione al momento in cui le chiavi di esposizione giornaliere sono caricate sul server dopo che un paziente risulti positivo. Per fare ciò deve essere generato un codice monouso (OTP) che deve essere validato da un operatore sanitario. Il che dunque potrebbe offrire un modo per associare le chiavi ad una persona fisica. Laddove si conservassero i dati relativi a tale associazione, potrebbe essere in un secondo momento collegata l'identità di una persona alle chiavi.

Pur nella remota ipotesi in cui tale associazione avvenisse – ed occorre ribadire che non vi è alcun elemento tecnico-normativo che porti a pensare ciò – il trattamento dei dati dovrebbe in ogni caso avvenire nel rispetto della normativa europea e nazionale, ed in particolare in ossequio alle specifiche misure di garanzia dettate ai sensi dell'art. 2-*septies* del d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, «*per il trattamento dei dati genetici, biometrici e relativi alla*

salute».

Ad ogni modo, tale possibilità di associazione resta del tutto teorica in quanto, stando alla documentazione tecnica disponibile, all'atto del caricamento delle chiavi sul server non viene registrata l'associazione tra chiavi ed identità del paziente.

Non si può in ogni caso sottacere che laddove una tale associazione tra chiavi e persona fisica avvenisse, si dovrebbero di conseguenza considerare dette chiavi come dati personali.

Senonché, anche tale eventualità non pone a ben vedere alcuna concreta e seria preoccupazione in relazione alla riservatezza degli individui[28]. In primo luogo, la sola chiave di esposizione non fornisce alcuna informazione utile in sé. I contatti sono tracciati, come detto, attraverso lo scambio dei codici RPI e dei relativi metadati. Sicché per ottenere una qualche informazione occorrerebbe conoscere tuti i codici RPI e relativi metadati. Ciò tecnicamente richiederebbe però l'accesso ad ogni singolo *device* in quanto i codici RPI ed i metadati, come detto, sono conservati sui singoli dispositivi e non sono mai caricati su alcun server.

Anche a voler ipotizzare che qualcuno riuscisse ad acquisire i codici RPI ed i metadati, per poterli distinguere, come detto, sarebbe necessario decifrare i metadati. Per fare ciò, tuttavia, sarebbe necessario ottenere la chiave di esposizione giornaliera utilizzata per creare la chiave di cifratura dei metadati (AEMK), analizzare tutti i codici RPI, e quindi operare le relative associazioni. Sicché occorrerebbe conoscere anche tutte le chiavi di esposizione giornaliera di tutti gli utenti di *Immuni* e la relativa associazione all'identità fisica di questi.

Si può dunque concludere che la concreta possibilità di desumere informazioni personali di qualsiasi natura dall'App *Immuni* sia tanto remota da non poter fondare alcun ragionevole timore in relazione alla riservatezza degli individui.

Senza contare poi che, anche laddove così non fosse, e quindi si ritenesse che in realtà l'app *Immuni* tratti dati personali – cosa che, è bene ribadirlo, ad oggi risulta da escludere – il Regolamento 2016/679/UE potrebbe consentire in ogni caso il trattamento coatto di detti dati personali.

Il consenso dell'interessato non è infatti necessariamente richiesto per il trattamento dei dati personali, ove sussistano altre condizioni di liceità. Nel caso specifico, il trattamento dei dati personali potrebbe benissimo essere fondato sulla condizione di liceità di cui all'articolo 6, comma 1, lett. e), GDPR. Ai sensi

di tale norma, il trattamento è lecito quando è «*necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare*». Appaiono in proposito particolarmente lungimiranti le ipotesi esemplificate dal legislatore europeo nel Regolamento stesso, ove si chiarisce espressamente che «*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*»[29].

In tali casi, il Regolamento UE richiede che la base del trattamento sia stabilita dal diritto europeo o dal diritto dello Stato membro cui è soggetto il titolare del trattamento e che tale trattamento soddisfi un obiettivo di interesse pubblico e sia proporzionato allo scopo legittimo perseguito[30]. Il che ha trovato puntuale attuazione, con decretazione d'urgenza proprio per far fronte all'epidemia e fintanto che perduri lo «*stato di emergenza*», esattamente al fine di consentire agli operatori sanitari di «*effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni ad essi attribuite nell'ambito dell'emergenza determinata dal diffondersi del COVID-19*»[31].

Data la gravità e l'unicità dell'attuale crisi sanitaria, sembra ragionevole sostenere che il monitoraggio delle infezioni risponda a uno specifico interesse pubblico. È innegabile che, al fine di contenere la diffusione del virus, possa essere estremamente utile tenere traccia dei contatti con persone infette, in modo da identificare e isolare immediatamente nuovi focolai. Sicché, anche ove si ritenesse che l'app *Immuni* raccolga dati personali – cosa che ancora una volta si deve ribadire ad oggi non risulta – ciò non parrebbe comunque ostativo all'imposizione di un obbligo di qualche tipo all'uso della stessa che prescinda dalla prestazione del consenso da parte dell'interessato. Si tratta infatti in sostanza di una valutazione che può essere ricondotta ad un giudizio di proporzionalità.

4. Segue. Uso obbligatorio dell'app *Immuni* e tutela della privacy: una questione di proporzionalità

La situazione pandemica SARS-CoV-2 corrisponde allo scenario caratteristico in cui gli interessi della società ed i diritti umani devono diventare parte di una

struttura giuridica unificata che, allo stesso tempo, determina la portata dei diritti umani e ne consente la limitazione. Un contesto in cui tipicamente entra in gioco il principio di proporzionalità[32].

Al momento di decidere se rendere o meno obbligatorio l'utilizzo di un'app come *Immuni* occorre infatti realizzare un equilibrio complesso. Da un lato, c'è l'interesse pubblico a contenere la diffusione del virus, essenziale a fini di tutela della salute pubblica e della vita delle persone. Dall'altro lato, c'è la necessità di tutelare un diritto fondamentale come la protezione dei dati personali, a sua volta essenziale per l'autonomia e la tutela della dignità umana.

Proprio in un contesto siffatto si applica certamente il principio di proporzionalità, che è uno strumento di bilanciamento inteso a fissare i criteri per adeguatamente ponderare tra il beneficio marginale per il bene pubblico, da un lato, ed il sacrificio marginale che è possibile imporre a diritti umani fondamentali, dall'altro[33].

Di derivazione dal diritto tedesco ed ampiamente utilizzato nel contesto del diritto dell'Unione europea, il principio di proporzionalità è stato infatti utilizzato sin dal principio proprio allo scopo di effettuare bilanciamenti così complessi[34].

Con il suo test strutturato in tre fasi, il principio in parola ha il vantaggio di limitare una troppo ampia discrezionalità in capo agli organi pubblici preposti ad operare detto bilanciamento, rendendolo dunque «*più trasparente, più strutturato e più prevedibile*»[35].

La prima fase della valutazione della proporzionalità è il test di idoneità, che implica una previsione da effettuare sulla base di un giudizio *ex ante*. Nel caso di specie, peraltro, si tratta di un giudizio che deve essere espresso il più rapidamente possibile, pena l'inutilità delle misure adottare in quanto *inutiliter data*!

Il presupposto di base, per quel che concerne questo primo step del test di proporzionalità, è che Legislatore e Pubblica Amministrazione possiedano una specifica competenza che consenta loro di effettuare valutazioni e accertamenti complessi i quali, almeno in linea di principio, devono poi essere rispettati nell'ambito della valutazione *ex post* effettuata da un giudice.

Ciò, se è vero in genere, è certamente ancora più vero in relazione all'attuale situazione sanitaria.

Il secondo passo è invece il test di necessità (o necessarietà), che è la parte più

importante della valutazione strutturata della proporzionalità. L'idea di fondo è ben descritta dall'espressione: "imposizione del mezzo più mite". Se esiste una scelta tra vari mezzi, tutti astrattamente idonei al raggiungimento dell'obiettivo prefissato, si deve scegliere quello che comporta le conseguenze meno negative per la libertà/diritto/opposto interesse in gioco.

Non c'è dubbio che, in considerazione di quanto detto nei paragrafi che precedono, l'efficacia di un'app come *Immuni* sia tanto maggiore quanto maggiore è il numero di persone che effettivamente la utilizzano. Di tal che, un uso obbligatorio nei termini qui proposti della app *Immuni* non avrebbe fondamentalmente alternative dal punto di vista dell'efficacia dei mezzi utilizzati.

Quanto alla proporzionalità *stricto sensu*, ossia la terza parte del test, questa consiste in un ulteriore confronto: nella fattispecie si tratterebbe di mettere a confronto i mezzi utilizzati (il presunto uso obbligatorio nei termini qui proposti dell'app) e il suo impatto sul diritto alla *privacy* degli utenti.

Una volta posizionati sui due diversi piatti della bilancia, il problema normalmente è come "assegnare una pesata" che consenta di confrontare effettivamente entrambi gli elementi posti sulla bilancia. Questo problema diventa molto più facile da risolvere in casi come quello di cui ci occupiamo qui, in quanto l'obiettivo di tracciare efficacemente le infezioni al fine di contenere la diffusione del virus SARS-CoV-2 (e prevenire la probabile morte di molte persone) è sicuramente obiettivo di pubblico interesse dal valore inestimabile. Sicché, in una situazione del genere non si pone effettivamente un problema di successiva verifica della proporzionalità in senso stretto: Vale a dire che, se l'imposizione dell'obbligo di utilizzare la app *Immuni* nelle circostanze di cui si è detto supera il test di idoneità e necessarietà (come certamente pare a chi scrive!), non sarà possibile per un giudice verificare *ex post* la sua proporzionalità *stricto sensu* senza scivolare in un controllo nel merito di quella che è una decisione a carattere eminentemente politico. Decisione che è per di più adottata dagli organi a ciò istituzionalmente preposti avendo come obiettivo ultimo la tutela di beni di valore inestimabile come la vita e la salute, il diritto alla salute dovendo ovviamente essere inteso nella sua duplice dimensione di diritto fondamentale della persona e di interesse della collettività[36].

Tornando dunque alla questione qui di nostro specifico interesse, come ha di recente affermato la Corte di giustizia dell'UE, «*per soddisfare il requisito di*

proporzionalità secondo cui le deroghe alla protezione dei dati personali devono operare nei limiti dello stretto necessario, la normativa controversa che comporta l'ingerenza deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi. In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario»[37].

Il problema qui è dunque, piuttosto, di identificare quale sia il livello di governo più appropriato per adottare la decisione di rendere l'utilizzo della app *Immuni* obbligatorio, anche e soprattutto allo scopo di fare sì che detta decisione, oltre che appropriata, risulti anche essere una decisione che massimizza l'efficacia dei risultati conseguibili.

Più in generale va sottolineato che, in un contesto di Governo multilivello come quello attuale, dove le competenze sono spesso condivise (dal livello comunale fino al livello dell'Unione Europea), può non essere sempre facile individuare quale sia l'amministrazione competente. La relativa verifica deve essere svolta di volta in volta sulla base delle misure concrete da adottare. Nel caso di specie occorre altresì tenere in debita considerazione il fatto che il virus, come ogni elemento naturale, ignora i confini legali che le nostre società si sono poste. Pertanto, in aree geograficamente interconnesse o comunque collegate, è necessaria un'azione almeno condivisa.

Questo è vero sia a livello nazionale che sovranazionale, a cominciare dal livello dell'Unione Europea. Con il problema, tuttavia, che – come è stato già autorevolmente sottolineato – «*Le istituzioni dell'Unione non possono, intervenire nella crisi sanitaria [...] se non attraverso la diffusione di informazioni e l'organizzazione di riunioni*»[38], non possedendo l'UE alcuna competenza in materia.

5. La necessità di un'adozione su larga scala di *Immuni* per garantirne la piena effettività

Un fenomeno particolarmente diffuso nel mondo della tecnologia è quello

relativo alla necessità che gli strumenti ICT abbiano una diffusione molto ampia per potere essere veramente efficaci. Il fatto che una massa critica di persone utilizzi un determinato servizio o piattaforma affinché quel servizio o piattaforma digitale sia effettivamente utile è un problema infatti molto noto. Ciò può essere apprezzato, ad esempio, in relazione ad un qualsiasi *social network*. Un servizio come *Facebook* risulta di una qualche utilità per gli utenti solo se un numero sufficiente di persone lo utilizza. Lo stesso vale anche per i servizi di messaggistica: per quanto rapidi ed efficienti, sono completamente inutili senza altre persone a cui scrivere. Questo perché un elemento essenziale di questi sistemi è che hanno lo scopo di mettere in contatto le persone. Allo stesso modo, l'utilità di un'app come *Immuni* risulta grandemente ridotta se questa non viene utilizzata da un vasto pubblico di utenti[39].

In condizioni normali di mercato sappiamo che la tecnologia, per vari motivi qui non analizzabili, tende alla standardizzazione, sia per quanto riguarda le tecnologie utilizzate per la realizzazione dei sistemi informatici stessi[40], sia per quanto riguarda le applicazioni utilizzate dagli utenti. Un fenomeno importante è noto come il «*tipping point*»[41]: se un servizio riesce ad acquisire una certa soglia di utenti, il cui numero varia in funzione di diversi fattori, si ha una tendenza alla convergenza del mercato verso questa soluzione.

Come si era suggerito sin dall'inizio della pandemia[42], nel caso di specie la convergenza verso un unico standard ed applicativo è stata assicurata da una decisione pubblica: quella adottata dal Commissario Straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, il quale ha individuato nell'app *Immuni* lo strumento software di *contact tracing*[43]. V'è peraltro da sottolineare che, sulla base dei dati ufficiali resi noti dal Governo, i *download* dell'app hanno segnato un costante aumento, sino ad arrivare, nelle ultime settimane di ottobre, ad oltre nove milioni[44].

Pur a fronte di tali confortanti dati, bisogna tuttavia tenere presente che l'emergenza coronavirus richiede un'azione particolarmente rapida e tempestiva. Con il dilagare dell'epidemia, gli effetti negativi della crisi si aggravano di giorno in giorno, sia in termini strettamente sanitari, sia da un punto di vista economico e sociale. Ciò suggerirebbe quindi l'opportunità di superare i normali tempi di diffusione di queste tecnologie, velocizzando quanto più possibile la loro rapida

adozione su larga scala.
Al fine di facilitare la diffusione di soluzioni tecnologiche che possano aiutare a combattere la pandemia sarebbe perciò auspicabile che fosse l'Autorità pubblica, quantomeno a livello nazionale, a prevedere forme di incentivazione all'uso dell'app *Immuni* che possano davvero portare alla effettiva rilevazione automatizzata dei contagi e, quindi, alla tempestiva adozione di misure di *follow-up*. In che limiti ciò possa avvenire, tuttavia, è problema di non facile soluzione.

6. La proposta: un uso dell'app *Immuni* quale condizione legittimante allo svolgimento di attività a rischio (di diffusione del contagio)

Al di là degli specifici aspetti di tutela della privacy di cui si è poc'anzi detto, per valutare in che termini l'adozione dell'app *Immuni* da parte della popolazione potrebbe effettivamente essere resa obbligatoria nei termini di cui si è detto, occorre avviare l'analisi dall'art. 6 del d.l. del 30 aprile 2020, n. 28[45]. Ai sensi di tale norma è espressamente previsto che l'installazione debba avvenire «*su base volontaria*»; e che la piattaforma deve essere limitata alla finalità di «*allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19*».
Alla luce di quanto detto sino ad ora in merito al funzionamento di *Immuni*, pare opinabile che, per la realizzazione di una tale piattaforma, nei termini esclusivamente volontaristici in cui è attualmente proposta, fosse necessaria una norma *ad hoc*. Il fatto dunque che si sia stabilito con una norma espressa il carattere volontario del *download* deve far ritenere che il legislatore abbia implicitamente voluto escludere che, con una norma di rango secondario, possa essere introdotto un generale obbligo di installazione di *Immuni*. Per potere adottare una simile soluzione (la obbligatorietà di utilizzo dell'app), allo stato attuale della normativa si deve dunque concludere che sarebbe necessaria una norma di rango legislativo volta a superare l'inciso dell'art. 6 del d.l. 28/2020, di cui si è detto.
Ciò non significa, tuttavia, che siano precluse altre forme di incentivazione al download dell'app. Si possono cioè valutare strade alternative per contribuire al

risultato di una più effettiva e diffusa adozione su larga scala di *Immuni*.
In tale senso, si può certamente apprezzare positivamente il fatto che il recente d.P.C.M. del 18 ottobre 2020 abbia disposto che «*al fine di rendere più efficace il contact tracing attraverso l'utilizzo dell'App Immuni, è fatto obbligo all'operatore sanitario del Dipartimento di prevenzione della azienda sanitaria locale, accedendo al sistema centrale di Immuni, di caricare il codice chiave in presenza di un caso di positività*»[46].
Tale norma, tuttavia, pur nell'apprezzabile sforzo di rendere più effettiva l'app *Immuni*, non è chiaro come possa essere attuata. Come descritto nel paragrafo 2, le chiavi di esposizione sono conservate sul dispositivo dell'utente, sicché solo quest'ultimo può materialmente caricarle sul "cloud". Viceversa, non pare che l'operatore sanitario possa procedere in tal senso autonomamente.
In ogni caso tale questione appare secondaria in quanto, a monte, resta il problema che, ad oggi, solo una parte della popolazione ha deciso di installare l'app *Immuni*. Sicché, per valutare in che termini se ne possa incentivare l'adozione si può avviare il ragionamento prendendo in esame quanto previsto dal d.l. del 25 marzo 2020, n. 19, che, nel dichiarare lo «*stato di emergenza*», ha autorizzato il Governo ad adottare, mediante decreto del Presidente del Consiglio dei Ministri, misure «*per evitare la diffusione del COVID-19*»[47].
Tale art. 1 autorizza il Governo, in sostanza, a prevedere la limitazione ovvero l'integrale sospensione di numerose attività, tra cui, come noto, gli esercizi commerciali e varie attività da svolgersi in luoghi pubblici o aperti al pubblico. Il d.P.C.M. del 24 ottobre 2020, per citarne uno tra i tanti, contiene numerosissimi divieti tra i quali, ad esempio, quello ai sensi del quale, «*dopo le ore 18:00 è vietato il consumo di cibi e bevande nei luoghi pubblici e aperti al pubblico*»[48].
A chi scrive non pare revocabile in dubbio che la sospensione totale di un'attività, o anche solo per fasce orarie, sia una misura più restrittiva e gravosa rispetto ad una mera limitazione della attività stessa che la autorizzi solo a determinate condizioni. In altri termini, laddove la prospettiva sia quella di un divieto parziale o addirittura integrale di svolgimento di numerose attività – come è avvenuto peraltro nuovamente per le Regioni incluse nella c.d. zona rossa, a seguito del più recente d.p.c.m. 3 novembre 2011 – appare allora ragionevole ritenere che, potendosi optare per una misura alternativa e che impatti meno sui diritti e libertà che vengono in tal modo limitati, questa seconda opzione sia preferibile

non solo in termini di sua maggiore "spendibilità" agli occhi dei cittadini. Pur lasciando da parte, infatti, le considerazioni di carattere socio-politologico (che, tuttavia, certamente non possono essere ignorate dal decisore pubblico, specialmente in un momento storico complesso come quello attuale!) è in punto di stretto diritto che la questione della "alternativa più mite" al divieto di esercizio parziale o totale della attività necessariamente si pone.

Piuttosto, dunque, che vietare parzialmente o totalmente determinate attività, si potrebbe prevedere (ed è questa la proposta che intendiamo qui formulare) che queste attività possano essere svolte da, ed erogate solo a favore di, soggetti che usino l'app *Immuni* e che siano in grado di dimostrare, per il suo tramite, di non essere stati a contatto con pazienti risultati positivi.

In altri termini, l'app *Immuni* potrebbe essere utilizzata quale strumento per potere consentire lo svolgimento di determinate attività, attualmente sospese o soggette ad ampie limitazioni, in sicurezza. Si potrebbe in particolare prevedere che l'esibizione dell'app all'ingresso di determinati luoghi aperti al pubblico sia condizione per l'accesso agli stessi, al pari della rilevazione della temperatura. L'accesso sarebbe quindi consentito solo a coloro che possano mostrare che l'app *Immuni* non indichi possibili contagi.

A tal fine, si potrebbe implementare nell'app una funzione che indichi – in modo chiaro e verificabile da chiunque mediante semplice esibizione – che il soggetto non sia entrato in contatto con un positivo. In tal modo *Immuni* potrebbe assurgere ad una sorta di "passaporto" abilitante allo svolgimento di attività e frequentazione di luoghi.

V'è tuttavia da dire che tale funzionalità non risulta attualmente implementata. A quanto consta, non vi è infatti un modo per verificare, ad oggi, da quanti giorni l'utente abbia installato l'app, né che lo stesso non sia effettivamente entrato in contatto con un positivo. Dall'analisi sul funzionamento dell'app di cui sopra si può tuttavia ritenere che sarebbe con ogni probabilità tecnicamente piuttosto semplice aggiungere una siffatta funzione, ad esempio implementando nella stessa un indicatore rosso o verde a seconda che vi sia stato, o meno, un contatto con un positivo negli ultimi *n* giorni. In altri termini, si potrebbe aggiungere nella schermata principale dell'app un chiaro indicatore che mostri se l'utente sia entrato a contatto con soggetti positivi ("semaforo giallo"), o se quest'ultimo sia risultato positivo al virus ("semaforo rosso"), ovvero ancora se l'utente possa

essere considerato non a rischio di contagio ("semaforo verde"). Solo in quest'ultima ipotesi – ossia solo ove l'app *Immuni* indichi l'assenza di contatti a rischio ("semaforo verde") potrebbe essere consentito l'accesso al luogo di prestazione del servizio.

Sotto un profilo operativo ed economico, peraltro, la società che ha realizzato gratuitamente *Immuni*, sempre «*a titolo gratuito, ha manifestato la propria disponibilità a completare gli sviluppi informatici che si renderanno necessari per consentire la messa in esercizio del sistema nazionale di contact tracing digitale*»[49]. Non è dunque da escludere che una tale funzione possa essere aggiunta dai medesimi sviluppatori che hanno realizzato l'app. Non solo. Anche ove tale società, per qualsiasi ragione, non potesse aggiungere essa stessa tale funzione, sviluppo di un indicatore del tipo qui proposto potrebbe essere affidato ad un qualsiasi altro soggetto con le necessarie competenze tecniche posto che la licenza con cui è stata consegnata l'app Immuni al Governo prevede espressamente la possibilità di modificare ed integrare il codice sorgente dell'app. La società che ha realizzato *Immuni* ha infatti reso disponibile in *open source*[50] il codice sorgente[51], sicché l'app può essere modificata ed integrata da chiunque senza vincoli legali e/o tecnici.

La soluzione qui proposta, ossia l'obbligo di ostensione di *Immuni* per certificare l'assenza di contatti a rischio quale condizione legittimante per lo svolgimento o la fruizione dei servizi collegati all'esercizio di determinate attività, risulterebbe peraltro essere pienamente compatibile con il carattere volontario dell'uso dell'app previsto, come si è detto, dalle norme attualmente in vigore. Posto che, allo stato, molteplici attività sono comunque precluse, per coloro che non volessero utilizzare l'app nulla cambierebbe; mentre si potrebbe garantire un maggior tracciamento tra coloro che optino per l'uso di *Immuni*.

Quanto alla possibile obiezione che, in questo modo, sarebbe però indirettamente violato lo spirito della legge, che ha sancito la volontarietà del *download*, questa non appare condivisibile. Fintanto che perduri la grave situazione pandemica, e quindi le autorità ritengano di chiudere del tutto determinate attività, un'apertura soggetta a condizioni del tipo di quella qui proposta non sarebbe tale da ledere la libertà di autodeterminarsi di alcuno. Semmai, essa contribuirebbe a ridurre le limitazioni attualmente imposte agli individui. Naturalmente sempreché tali vincoli di utilizzo dell'app siano

mantenuti solo ed esclusivamente fintanto che perduri lo «*stato di emergenza*».

7. Osservazioni critiche sulla mancata previsione, ad opera dei d.P.C.M., dell'app *Immuni* come strumento per il contenimento della pandemia

L'esperienza della pandemia di SARS-CoV-2 e la conseguente situazione di emergenza possono servire a fare emergere chiaramente la necessità di ricorrere a soluzioni tecnologiche innovative a supporto dell'attività delle Istituzioni pubbliche e con l'obiettivo di un miglior soddisfacimento degli interessi pubblici.
In questa prospettiva si è constatato come l'uso dell'app *Immuni* possa aiutare a tracciare i contagi e individuare rapidamente coloro che siano stati potenzialmente contagiati. Ciò, ove una significativa percentuale della popolazione utilizzasse l'App, consentirebbe quindi di meglio isolare i potenziali portatori del virus, così da ridurre il rischio che questi, a loro volta, lo trasmettano ad altri ed interrompere quindi la catena dei contagi.
Per altro verso si è mostrato che non vi sono particolari rischi per la *privacy* derivanti dall'utilizzo dell'app *Immuni*. Questo in quanto non vi è, per quanto è dato sapere, una diretta raccolta di dati personali. Ma anche nell'ipotesi, tutta da dimostrare, in cui si ritenesse sussistere una qualche forma di trattamento di dati personali, si è messo in evidenza come, in base al principio di proporzionalità, questa sarebbe in ogni caso compatibile ed adeguatamente bilanciata in ragione dell'esigenza primaria di tutelare la salute pubblica.
Non solo. Si deve anche considerare che l'app *Immuni* permetterebbe, se a pieno regime, di garantire una maggior sicurezza della popolazione. Si deve infatti tenere conto che l'uso dell'app *Immuni* secondo le modalità qui suggerite potrebbe consentire di porre in quarantena in modo più rapido le persone risultate positive e, quindi, eventualmente di allentare le restrizioni allo svolgimento delle normali attività, nella misura in cui si verifichi che le misure di *follow-up*[52] siano in grado di interrompere rapidamente la catena dei contagi.
La scelta di non ricorrere a tale strumento digitale per supportare gli sforzi di contenimento dell'epidemia appare perciò come non coerente con le finalità perseguite dalle Autorità, di tutela della salute pubblica. Né appare come una scelta esente da critiche il fatto di non avere considerato che il ricorso a tale

tecnologia potrebbe garantire una maggiore protezione della popolazione rispetto al rischio rappresentato dalla diffusione del virus, consentendo al contempo una minore restrizione delle libertà e dei diritti fondamentali delle persone.

Tale omesso ricorso alle tecnologie disponibili per garantire l'effettività e l'efficacia dell'azione amministrativa messa in campo a contrasto della pandemia, risulta peraltro ancor più criticabile in considerazione del fatto che l'uso dell'App *Immuni* – come si è detto – non genera alcun apprezzabile pregiudizio per i singoli utenti.

In ragione delle suesposte considerazioni, appare fortemente messa in dubbio la legittimità delle restrizioni attualmente in essere. Infatti, come si è detto, se l'app *Immuni* fosse utilizzata come qui suggerito, ossia quale condizione legittimante per lo svolgimento di attività "a rischio di contagio", si avrebbe una più effettiva realizzazione dei principi di «*adeguatezza e proporzionalità*»: principi che il d.l. 19/2020 indica espressamente quali parametri per l'adozione con d.P.C.M. delle misure urgenti per evitare la diffusione del COVID-19.

Ignorando invece l'apporto che tale strumento digitale può apportare, si può dubitare che i d.P.C.M. attualmente in vigore attuino fedelmente il disposto di cui al d.l. 19/2020, quantomeno nella parte in cui non abbiano tenuto conto che si sarebbe potuto ottenere un risultato migliore – inteso quale più efficace tracciamento dei contagi e quindi un più alto livello di sicurezza – con misure atte a valorizzare il *contact tracing* digitale.

In senso contrario non pare peraltro che possano addursi ragioni di *digital divide*, sia in relazione alle capacità informatiche dei cittadini, sia in rapporto alla capacità economica dei privati di acquistare e possedere uno *smartphone* idoneo all'uso di *Immuni*.

Sotto tale ultimo profilo, visti i danni all'economia che la pandemia ha causato e sta ancora causando, colpendo peraltro anche (se non soprattutto) le fasce più deboli della popolazione, sarebbe certamente possibile sfruttare gli aiuti economici per garantire la disponibilità di uno *smartphone* in grado di eseguire l'app a tutti coloro che non possano permetterselo. Il che, considerata l'elevatissima diffusione degli *smartphone* in Italia[53], e il costo relativamente esiguo dei modelli economici[54], sarebbe senz'altro sostenibile, o comunque potrebbe rappresentare il male minore rispetto ai costi oggi sostenuti dalla sanità pubblica[55] ed ai danni derivanti dalla chiusura degli esercizi commerciali.

Quanto, invece, alla questione relativa alle (forse insufficienti) capacità informatiche dei cittadini, è sufficiente evidenziare che l'app *Immuni*, una volta installata, non richiede alcuna interazione da parte dell'utente, sicché sarebbe sufficiente fornire adeguata assistenza al momento dell'installazione iniziale.

8. Tecnologie ICT e bilanciamento nella "emergenza protratta": riflessioni conclusive

Come sì è tentato di mettere in luce nelle pagine che precedono, allo stato attuale l'uso di strumenti forniti dalla tecnologia (e in particolare dalle ICT) potrebbe sia rafforzare l'effettività delle misure di prevenzione dei contagi già in essere, anche grazie all'apporto informativo che la raccolta dei dati sui contagi può generare[56], sia permettere di meglio modulare le limitazioni imposte alla popolazione, grazie a controlli automatizzati su larga scala che consentano di monitorare costantemente i contatti ed individuare quindi, immediatamente, possibili esposizioni al virus.

La moltitudine di strumenti digitali già disponibili rende certamente opportuna la scelta di uno standard comune e unico. Secondo quanto riportato dalle specifiche tecniche dell'app *Immuni*, tuttavia, ad oggi essa risulta già in grado di «*ricevere e condividere i codici relativi alle persone positive al Covid-19 tra le app dei paesi aderenti all'interoperabilità europea*»[57]. Grazie a tale importante caratteristica, ossia l'interoperabilità delle diverse applicazioni di tracciamento dei contatti, è possibile raccogliere efficacemente informazioni utili su larga scala sull'andamento della pandemia, superando i confini nazionali ed applicando un comune sistema nel mercato interno europeo.

Per di più la circostanza che, dopo molti mesi dall'inizio della crisi sanitaria, il virus si stia ancora diffondendo rapidamente, testimonia come le sole misure preventive tradizionali non siano sufficienti se non supportate da adeguati strumenti di controllo. Ma poiché questi controlli possono avvenire efficacemente solo se svolti in modo automatizzato, appare inevitabile che gli strumenti tecnologici più idonei vengano diffusi in modo rapido ed efficace, prevedendo precise strategie volte ad assicurare che il maggior numero di persone possibile si doti di *smartphone*, o altri dispositivi mobili, con installata l'app *Immuni*.

Né una scelta di tal fatta porrebbe dei problemi, come si è detto, dalla prospettiva del principio di proporzionalità. Anzi, per molti versi la soluzione qui proposta - ossia l'obbligo di ostensione della app *Immuni* per certificare l'assenza di contatti a rischio quale condizione legittimante per lo svolgimento o la fruizione dei servizi collegati all'esercizio di determinate attività - potrebbe essere proprio lo strumento che consente di evitare l'adozione di (ulteriori) misure maggiormente restrittive delle libertà e dei diritti degli individui: nella logica propria del principio di proporzionalità, che è sempre quella dell'imposizione del "mezzo più mite" fra tutti quelli a disposizione per potere raggiungere l'obiettivo prefissato. Come scriveva infatti già Giandomenico Romagnosi nelle sue "*Instituzioni di diritto amministrativo"* del 1814, «*[...] la seconda regola pratica direttrice dell'amministrazione pubblica, nel caso del conflitto degli interessi del privato con quelli del pubblico [...] si è "far prevalere la cosa pubblica alla privata entro i limiti della vera necessità". Lo che è sinonimo di "far prevalere la cosa pubblica alla privata col minimo possibile sacrificio della privata proprietà e libertà*"»[58].
In questa logica, ad esempio, il suo utilizzo consentirebbe di garantire un minore sacrificio di quella libertà di circolazione che è garantita dall'art. 67 TFUE e anche dalla disposizione di cui all'articolo 2 del Protocollo n. 4 alla Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali[59].
Ma, pure ove si esamini la questione dalla prospettiva del «*ragionevole bilanciamento tra una pluralità di interessi costituzionalmente rilevanti*»[60], cui fa più tradizionalmente ricorso la nostra Corte Costituzionale, è chiaro che, di fronte ad una crisi (sanitaria) grave come quella attualmente in atto e che è destinata purtroppo a protrarsi nel tempo, occorre dare fondo a tutte le risorse e fare ricorso a tutti gli strumenti potenzialmente a disposizione. Sicché pare evidente a chi scrive che, in un contesto in cui le misure sinora adottate limitano drasticamente la libertà di movimento delle persone, nonché lo svolgimento della maggior parte delle attività normalmente svolte, occorre non sottovalutare l'apporto che potrebbe invece derivare da un adeguato utilizzo della tecnologia allo scopo di operare, in prospettiva, un più "ragionevole bilanciamento" fra tutti i diritti ed interessi che entrano qui inevitabilmente in gioco. Anche e soprattutto perché un'emergenza che si protrae nel tempo non può ragionevolmente essere gestita con i medesimi strumenti messi in campo al momento della sua esplosione![61]

In conclusione, dunque, l'utilizzo dell'app *Immuni*, oltre a potere costituire un importante strumento a supporto delle altre misure adottate per il contenimento della pandemia, rendendole più efficaci ed efficienti, appare idoneo a consentire, in prospettiva, anche di meglio calibrarle per il futuro. In questo senso appare assai interessante l'esempio della Corea del Sud: che ha fatto ricorso ad un programma nazionale di tracciamento dei contatti COVID-19 allo scopo di guidare la "evidence-based policy" finalizzata a mitigare la pandemia[62]. L'obiettivo ultimo di dette "policy" (e degli strumenti giuridici intesi a realizzarle) deve infatti essere di far sì che tutti i diritti ed interessi coinvolti nel complesso e assai composito quadro, in cui il legislatore "dell'emergenza protratta" è necessariamente obbligato ad operare, siano ragionevolmente bilanciati, proprio nella prospettiva del "minor sacrificio possibile" caratteristica del principio di proporzionalità[63].

1. I paragrafi 1-3, 5 e 7 sono a cura di Gherardo Carullo. I paragrafi 4 e 8 sono a cura di Diana-Urania Galetta. Il paragrafo 6 è stato invece redatto congiuntamente da entrambi gli autori.
2. In tal senso, per tutti, v. L. Cuocolo, *Presentazione*, in L. Cuocolo (a cura di), *Osservatorio Emergenza Covid-19 n. 1 - I diritti costituzionali di fronte all'emergenza Covid-19. Una prospettiva comparata*, Federalismi.it, 2020, il quale sottolinea che «*la reazione degli ordinamenti mondiali all'emergenza sanitaria derivata dal Covid-19 ha portato alla compressione e alla limitazione di molti diritti individuali e collettivi, per lo più garantiti a livello costituzionale*». Sul punto si vedano anche gli ulteriori contributi in tale numero speciale della Rivista Federalismi a cura di L. Cuocolo.
3. V. il d.P.C.M. del 13 ottobre 2020, recante «*Ulteriori disposizioni attuative del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 25 maggio 2020, n. 35, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19", e del decreto-legge 16 maggio 2020, n. 33, convertito, con modificazioni, dalla legge 14 luglio 2020, n. 74, recante "Ulteriori misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19"*»; il d.P.C.M. del 18 ottobre 2020, recante «*Ulteriori disposizioni attuative del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 22 maggio 2020, n. 35, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19", e del decreto-legge 16 maggio 2020, n. 33, convertito, con modificazioni, dalla legge 14 luglio 2020, n. 74, recante "Ulteriori misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19"*»; il d.P.C.M. del 24 ottobre 2020 recante «*Ulteriori disposizioni attuative del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 22 maggio 2020, n. 35, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19", e del decreto-legge 16 maggio 2020, n. 33, convertito, con*

modificazioni, dalla legge 14 luglio 2020, n. 74, recante "Ulteriori misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19"»; nonché il d.P.C.M. del 3 novembre 2020 recante «*Ulteriori disposizioni attuative del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 22 maggio 2020, n. 35, recante "Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19», e del decreto-legge 16 maggio 2020, n. 33, convertito, con modificazioni, dalla legge 14 luglio 2020, n. 74, recante «Ulteriori misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19"*». Sui provvedimenti adottati a livello nazionale dall'inizio della pandemia, v. M. Gnes, *Le misure nazionali di contenimento dell'epidemia da Covid-19*, in *Giornale Dir. Amm.*, 3, 2020.

4. V. G. Carullo, *Digitalizzazione dei controlli ai tempi del coronavirus*, in *CERIDAP*, 1, 2020, *passim*.
5. V. ordinanza del 16 aprile 2020, n. 10 del Commissario straordinario per l'emergenza Covid-19, disponibile su http://www.governo.it/it/dipartimenti/commissario-straordinario-lemergenza-covid-19/14483.
6. V. C. Bottari, *Alcune riflessioni sui profili organizzativi ai tempi del coronavirus*, in *Federalismi.it*, Osservatorio Emergenza Covid-19 n. 1, 2020. Un esempio concreto è dato anche dalla, quantomeno iniziale, «*mancata disponibilità e al difficoltoso reperimento di strumenti ritenuti basilari nell'approntamento delle cure ai pazienti, quali le mascherine e i kit protettivi per gli operatori sanitari e i ventilatori polmonari e analoghi macchinari da utilizzare nelle sale di rianimazione*», F.G. Cuttaia, *La gestione dell'emergenza conseguente alla pandemia da Covid-19 con particolare riguardo alle criticità evidenziatesi nella governance dei dispositivi medici. Profili giuridici e spunti evolutivi*, in *Federalismi.it*, Osservatorio Emergenza Covid-19 n. 1, 2020.
7. In tal senso il contributo pubblicato in data 10 giugno 2020 di C. Colapietro, A. Iannuzzi, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in *dirittifondamentali.it*, 2, 2020, p. 792 e ss., i quali propendono «*per la volontarietà dell'app*» sia per ragioni giuridiche, sia per ragioni socio-psicologiche.
8. Secondo quanto riportato dalle maggiori testate giornalistiche, per tutti cfr. quanto segnalato dall'ANSA il 27 ottobre 2020: https://www.ansa.it/sito/notizie/cronaca/2020/10/27/covid-fonti-ipotesi-regia-comune-dietro-scontri-_bb699adb-39f1-46ab-9766-c723d54e949e.html.
9. Come rilevato da G. Della Morte, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Dir. umani e Dir. Int.*, 2, 2020, p. 329, una delle criticità di Immuni consiste nel non prevedere azioni di *follow-up* stringenti in caso di potenziale contatto con un soggetto risultato positivo.
10. Per una ricostruzione dell'iter di progettazione e sviluppo dell'app v. C. Colapietro, A. Iannuzzi, *App di contact tracing*, cit..
11. V. https://www.immuni.italia.it/#section1.

12. V. https://www.immuni.italia.it/#section1.
13. V. https://www.immuni.italia.it/#section2.
14. Si veda l'«*informativa privacy*» consultabile dall'app stessa. In dottrina, in assenza di geolocalizzazione, si è infatti osservato che «*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"*», M. Plutino, *"Immuni". Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *MediaLaws*, 2, 2020, p. 179.
15. I dispositivi che richiedono la geolocalizzazione attiva sono quelli con una versione del sistema operativo Android precedente alla n. 11. In tali casi, come viene spiegato dall'app *Immuni* stessa, «*a causa di una limitazione del sistema operativo, il servizio di geolocalizzazione deve essere attivo per consentire lo scambio di codici casuali via Bluetooth*». Dall'analisi del codice sorgente dell'app *Immuni* si può avere conferma che la necessità che la geolocalizzazione debba essere attiva non consente in ogni caso la raccolta dei relativi dati. Al riguardo si può menzionare che l'app esegue un controllo attraverso la funzione *exposureNotificationClient.deviceSupportsLocationlessScanning* facente parte del codice di *Exposure Notification* realizzato da Google per il sistema operativo Android. Tale funzione, come spiegato nella documentazione tecnica, ha il seguente scopo: «*Checks whether the device supports Exposure Notification BLE scanning without requiring location to be enabled first*» (v. https://developers.google.com/android/reference/com/google/android/gms/nearby/exposurenotification/ExposureNotificationClient?hl=en). Quanto riportato può essere verificato sul *repository* del codice sorgente dell'app (v. https://github.com/immuni-app/immuni-app-android), nei seguenti file:app/src/main/java/it/ministerodellasalute/immuni/ui/onboarding/fragments/viewpager/ExposureNotificationFragment.kt, righe 84-89;extensions/src/main/java/it/ministerodellasalute/immuni/extensions/nearby/ExposureNotificationManager.kt, riga 77.
16. La seguente descrizione è desunta dalle FAQ disponibili all'indirizzo https://www.immuni.italia.it/faq.html.
17. Come spiegato nel documento tecnico di cui alla successiva nota, tale tecnologia è stata implementata «*to combat the spread of the coronavirus — the pathogen that causes COVID-19 — by alerting participants about possible exposure, through someone they have recently been in contact with who has subsequently been positively diagnosed*» (p. 3).
18. V. il documento tecnico *Exposure Notification Cryptography Specification*, v 1.2.1, disponibile agli indirizzi https://blog.google/documents/69/Exposure_Notification_-_Cryptography_Specification_v1.2.1.pdf e https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.2.pdf.

19. La traduzione esatta sarebbe "chiave di esposizione temporanea", senonché, secondo la documentazione tecnica, la TEK viene rigenerata in base al *TEKRollingPeriod*, che in sostanza è equivalente a 24 ore, sicché si può considerare la chiave di esposizione come giornaliera, con ciò intendendosi un arco temporale di 24 ore e non la giornata solare (dalle 00:00 alle 23:59).
20. Questa la descrizione del documento tecnico *Exposure Notification - Bluetooth Specification*, v. 1.1, consultabile all'indirizzo https://www.blog.google/documents/62/Exposure_Notification_-_Bluetooth_Specification_v1.1.pdf. In particolare, viene spiegato a pagina 4 che tali metadati contengono: «*i. Byte 0 — Versioning. • Bits 7:6 — Major version (01). • Bits 5:4 — Minor version (00). • Bits 3:0 — Reserved for future use. ii. Byte 1 — Transmit power level. • This is the measured radiated transmit power of Bluetooth Advertisement packets, and is used to improve distance approximation. The range of this field shall be -127 to +127 dBm. iii. Byte 2 — Reserved for future use. iv. Byte 3 — Reserved for future use*».
21. Corte di giustizia dell'UE, sentenza del 19 ottobre 2016, C-582/14, *Breyer*, ECLI: EU: C: 2016: 779, p. 49.
22. Secondo quanto riportato nell'«*informativa privacy*», i dati raccolti sono: «*provincia di domicilio*»; «*indicatori di corretto funzionamento*»; «*token temporanei*»; «*indirizzo IP*»; «*ricezione notifica di esposizione*»; «*data dell'ultimo contatto a rischio*»; «*chiavi di esposizione (Temporary Exposure Key - TEK)*»; «*indicatori di rischio di precedenti contatti*»; «*Paesi di Interesse*»; «*codice OTP*»; «*data di comparsa dei sintomi o di prelievo del tampone*».
23. Secondo quanto riportato nella documentazione tecnica delle tecnologie sulla base delle quali l'app *Immuni* è realizzata, le chiavi di esposizione, note in inglese come *Temporary Exposure Key*, «*are anonymous keys shared between mobile devices to determine if two devices were sufficiently nearby to be considered "exposed" to one another*», v. https://google.github.io/exposure-notifications-server/getting-started/publishing-temporary-exposure-keys.html.
24. Parlano invece di pseudonimizzazione C. Colapietro, A. Iannuzzi, *App di contact tracing*, cit., p. 795.
25. Ai sensi dell'art. 4, p. 1, n. 5, si intende con «*pseudonimizzazione*» «*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive*». L'uso dell'avverbio «*più*» lascia intendere che i dati di partenza usati per la pseudonimizzazione potrebbero essere riferiti ad una persona fisica, cosa che nella specie invece non risulta sussistere trattandosi di codici alfanumerici casuali.
26. Ritiene che tali dati, anonimi in partenza, divengano pseudo-anonimi quando caricati, volontariamente, sul server a seguito di positività M. Plutino, *"Immuni". Un'exposure notification app*, cit., p. 183. Secondo quanto noto, tuttavia, non vi è motivo di ritenere che con il caricamento dei dati questi diventino pseudo-anonimi in quanto, stando alle specifiche tecniche rese disponibili, non risulta che vi sia in tale momento un'associazione

di tali codici alfanumerici con i dati personali del paziente.

27. Ed in effetti, anche quella dottrina che ha qualificato la modalità di gestione dei dati dell'app *Immuni* in termini di pseudonimizzazione, e non di vera e propria anonimizzazione, giunge a concludere che le modalità operative dell'app *Immuni* «*si riflettono sui diritti dell'interessato di cui agli artt.15-20 reg. 16/679/UE [...] non tanto derogandoli, quanto rendendoli sostanzialmente inapplicabili*», v. G. Citarella, *Considerazioni sull'APP Immuni*, in G.P. Dolso; M.D. Ferrara; D. Rossi (a cura di), *Virus in fabula. Diritti e Istituzioni ai tempi del covid-19*, EUT Edizioni Università di Trieste, Trieste, 2020, p. 376. Ma sul punto si deve ancora ribadire che se i dati raccolti non sono riferibili ad una persona, non sono solo i diritti dell'interessato ad essere inapplicabili, quanto il Regolamento 2016/679/UE nella sua interezza.
28. L'uso del termine riservatezza è qui da intendere non quale sinonimo di *privacy*, secondo l'idea per cui si tratta di concetti distinti in quanto da un lato vi è «*la Privacy, che mira a garantire la libertà di autodeterminazione nelle scelte di vita e dall'altro la riservatezza, che riguarda la non ingerenza di terzi nella propria sfera personale*», v. E. Falletti, *L'evoluzione del concetto di privacy e della sua tutela giuridica*, in G. Cassano; G. Vaciago (a cura di), *Diritto dell'internet*, CEDAM, Padova, 2012, p. 22,
29. V. considerando 46 del Regolamento. In dottrina, sul punto v. M. Ponari, *Il trattamento dei dati sanitari durante l'emergenza*, in M. Campagna; S.F. Manzin (a cura di), *Riflessioni sulla sanità in emergenza*, Aracne, Canterano, 2020, p. 106.
30. In tal senso, in relazione proprio al carattere volontario di *Immuni*, M. Plutino, *"Immuni". Un'exposure notification app*, cit., p. 180.
31. V. art. 17-*bis* del d.l. 17 marzo 2020, n. 18, recante «*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*».
32. A. Barak, *Proportionality and Principled Balancing*, in *Law & Ethics of Human Rights,* , 2010/1, p. 1 ss.
33. Si veda su questo punto anche la giurisprudenza della Corte europea dei diritti dell'uomo: «*A difference of treatment in the exercise of a right laid down by the Convention must not only pursue a legitimate aim: Article 14 will also be violated when it is clearly established that there is no reasonable relationship of proportionality between the means employed and the aim sought to be realized*»; GLOR v. SWITZERLAND, 13444/04 30/04/2009. La stessa logica secondo cui «*such a justification must be assessed in relation to the aim and the effects of the measure concerned and the principles which normally prevail in democratic societies*» si applica a tutti gli altri diritti protetti dalla CEDU, v. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-2724329-2974120%22]}, (data della consultazione: 30 agosto 2020).
34. Per approfondimenti: D.U. Galetta, *Principio di proporzionalità e sindacato giurisdizionale nel diritto amministrativo*, Giuffrè, Milano, 1998.
35. A. Barak, *Proportionality and Principled Balancing* cit. La traduzione è mia.
36. In tal senso si vedano G. Biscontini, E.M. Comba, E. Del Prato, L.A. Mazzarolli, A. Poggi,

G. Valditara, F. Vari, *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *Federalismi.it*, Osservatorio Emergenza Covid-19 n. 1, 2020, secondo i quali «*nel bilanciamento tra tutela della vita e della salute e tutela di alcuni diritti individuali, quanto meno in questo particolare momento, occorre dare la prevalenza ai primi, come già avvenuto anche con la restrizione, ad esempio, della libertà di circolazione*».

37. Corte di giustizia, 16 luglio 2020, C-311/18, *Facebook Ireland e Schrems*, ECLI: EU:C: 2020:559, p. 176.
38. J. Ziller, *Unione europea e Coronavirus*, in *CERIDAP*, 1, 2020, p. 5.
39. Tale criticità è sottolineata anche da G. Della Morte, *Quanto Immuni?*, cit., p. 328.
40. In tal senso v. M.A. Lemley, *Antitrust and the Internet Standardization Problem*, in *Conn. L. Rev.*, 28, 1996, p. 1041; M.L. Montagnani, *Remedies to Exclusionary Innovation in the High-Tech Sector: Is there a Lesson from the Microsoft Saga?*, in *World Competition*, 4, 2007, p. 623.
41. Cfr. M. Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*, Little, Brown, New York, NY, 2006.
42. Si era infatti suggerito che, in relazione al problema della frammentazione delle soluzioni tecnologiche, fosse «*opportuno che, in base alle rispettive competenze, ciascuna Autorità indichi quali strumenti tecnologici possano o debbano essere adottati, anche daicittadini, al fine di supportare le loro attività*», v. G. Carullo, *Digitalizzazione dei controlli ai tempi del coronavirus*, cit., p. 12. Sulla «*necessità di utilizzare degli standard per l'uso e la rielaborazione [dei dati sanitari]*», v. anche A. Monica, *Unione europea e tutela della salute: gestione di emergenze epidemiologiche a carattere transfrontaliero*, in M. Campagna; S.F. Manzin (a cura di), *Riflessioni sulla sanità in emergenza*, Aracne, Canterano, 2020, p. 86.
43. Con la già richiamata ordinanza n. 10/2020. Da sottolineare peraltro che la società realizzatrice dell'app, «*per spirito di solidarietà e, quindi, al solo scopo di fornire un proprio contributo, volontario e personale, utile per fronteggiare l'emergenza da COVID-19 in atto, ha manifestato la volontà di concedere in licenza d'uso aperta, gratuita e perpetua [...] il codice sorgente e tutte le componenti applicative facenti parte del sistema di contact tracing già sviluppate, nonché, per le medesime ragioni e motivazioni e sempre a titolo gratuito, ha manifestato la propria disponibilità a completare gli sviluppi informatici che si renderanno necessari per consentire la messa in esercizio del sistema nazionale di contact tracing digitale*».
44. V. i dati disponibili su https://www.immuni.italia.it/dashboard.html.
45. Recante «*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*».
46. V. art. 1, comma 1, lett. f) del d.P.C.M., che ha aggiunto tale inciso alla lett. a-*bis*) dell'art. 3 del d.P.C.M. del 13 ottobre 2020.

47. Così la rubrica dell'art. 1 del decreto.
48. V. d.P.C.M. 24/10/2020, art. 1, lett. ee).
49. V. la già citata ordinanza n. 10/2020
50. Come spiegato dalle *Linee Guida su acquisizione e riuso di software per le pubbliche amministrazioni* adottate dall'AgID di cui alla Determina del 9 maggio 2019, n. 115, l'espressione *open source* identifica «*una modalità con cui il software può essere concesso in licenza. Si realizza attraverso la concessione al pubblico, dei diritti di uso, copia, modifica, distribuzione di copie anche modificate, del software; per fare ciò, è necessario anche che il codice sorgente sia liberamente disponibile*». Le Linee Guida sono disponibili all'indirizzo https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf.
51. Ai sensi delle Linee Guida di cui alla nota precedente, il codice sorgente «*è il testo di un programma scritto in un linguaggio di programmazione (es. C o Visual Basic) dal quale si deriva il programma finale che l'utente usa. L'accesso al codice sorgente è essenziale per poter modificare un programma*».
52. Come già evidenziato da citato brano di G. Della Morte, *Quanto Immuni?*, cit., p. 329.
53. Secondo il report Digital 2020, nel 2020 in Italia sono presenti poco più di 80 milioni di *smartphone* per una popolazione residente di circa 60 milioni, v. https://datareportal.com/reports/digital-2020-italy.
54. L'app *Immuni* può essere installata su qualsiasi dispositivo con sistema operativo Android. Secondo quanto risultante dai più noti negozi online, *smartphone* con sistema operativo Android possono essere acquistati con budget (anche molto) al di sotto di € 100.
55. Sul che v. M. Campagna, *Covid–19 e questione ospedaliera*, in M. Campagna; S.F. Manzin (a cura di), *Riflessioni sulla sanità in emergenza*, Aracne, Canterano, 2020, *passim*.
56. In tal senso, sullo specifico caso della pandemia, cfr. A. Monti, *Scienza, tecnocontrollo e public-policy nell'era COVID-19*, in *Riv. Trim. Sc. Amm.*, 2, 2020. Più in generale, sul valore conoscitivo dei dati nella sfera pubblica, si rinvia a G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Giappichelli, Torino, 2017.
57. V. le note di aggiornamento dell'app sugli Store per iOS ed Android del 19 ottobre 2020. A proposito dell'interoperabilità europea v. ISA^2 - Interoperability solutions for public administrations, businesses and citizens, https://ec.europa.eu/isa2/home_en
58. Romagnosi, *Instituzioni di diritto amministrativo*, Milano, 1814, p. 16 s.
59. Secondo l'Art. 2 del Protocollo n. 4 alla CEDU «*1. Chiunque si trovi regolarmente sul territorio di uno Stato ha il diritto di circolarvi liberamente e di scegliervi liberamente la sua residenza. 2. Ognuno è libero di lasciare qualsiasi Paese, compreso il suo. 3. L'esercizio di questi diritti non può essere oggetto di restrizioni diverse da quelle che sono previste dalla legge e costituiscono, in una società democratica, misure necessarie alla sicurezza nazionale, alla pubblica sicurezza, al mantenimento dell'ordine pubblico, alla prevenzione delle infrazioni penali, alla protezione della salute o della morale o alla protezione dei diritti e libertà altrui. 4. I diritti riconosciuti al paragrafo 1 possono anche, in alcune zone*

determinate, essere oggetto di restrizioni previste dalla legge e giustificate dall'interesse pubblico in una società democratica», v. https://www.echr.coe.int/documents/convention_ita.pdf.

60. Corte Cost., sentenza 182/2017 (ECLI:IT:COST:2017:182), par. 3.2.
61. In argomento è interessante lo studio pubblicato dal Parlamento europeo, *Il diritto di eccezione: una prospettiva di diritto comparato - Italia: stato di emergenza*, doc. PE 651.983 – Giugno 2020, consultabile all'indirizzo https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)651983 (data della consultazione: 10 novembre 2020). Per una valutazione della legittimità degli interventi adottati durante la prima fase dell'emergenza si veda per tutti M. Luciani, *Il sistema delle fonti del diritto alla prova dell'emergenza*, in *Rivista AIC*, 2020, 2 (https://www.rivistaaic.it/images/rivista/pdf/2_2020_Luciani.pdf).
62. Si veda Y. Park, Y. Choe e. a., *Contact Tracing during Coronavirus Disease Outbreak, South Korea, 2020*, in *Emerging Infectious Diseases*, 2020, 26(10), p. 2465 ss. (https://dx.doi.org/10.3201/eid2610.201315), che descrivono il programma nazionale di tracciamento dei contatti COVID-19 in Corea del Sud fornendo dati concreti sui risultati ottenuti.
63. Su cui si rinvia, da ultimo, a D.U. Galetta, *Il principio di proporzionalità fra diritto nazionale e diritto europeo (e con uno sguardo anche al di là dei confini dell'Unione Europea)*, in *Rivista italiana di diritto pubblico comunitario*, 2019, 6, p. 903 ss. e dottrina ivi ampiamente richiamata.