dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2020
Data di pubblicazione – 10 giugno 2020

Non solo *privacy*. Pandemia, *contact tracing* e diritti fondamentali

di
Chiara Bergonzini*

1. A metà del periodo di emergenza: il ruolo delle nuove tecnologie tra contenimento della pandemia e diritti fondamentali

A metà del periodo di emergenza causato dalla pandemia da Covid-19 – emergenza dichiarata dal Governo italiano, per una durata di sei mesi, il 31 gennaio 2020[1] – è banale rilevare che la situazione che si presenta agli occhi del giurista, e del costituzionalista in particolare, è per diversi aspetti preoccupante, e chiama *contemporaneamente* in causa quasi tutti i fondamentali del diritto pubblico: finora, infatti, l'unico ramo della disciplina non (ancora) direttamente coinvolto è quello della giustizia costituzionale. Il che, se da un lato pare fisiologico, dati la brevità del periodo trascorso e soprattutto la rapidità con cui la situazione evolve, dall'altro lato si spiega guardando al settore sinora più stressato, cioè il piano delle fonti con cui l'emergenza è stata gestita, che com'è noto, salvo alcuni decreti-legge, si collocano al di sotto delle

* Ricercatrice TD in Diritto costituzionale, Università di Macerata.

[1] Delibera del Consiglio dei Ministri 31 gennaio 2020, *Dichiarazione dello stato di emergenza in conseguenza del rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, in GU, Serie generale, n. 26 del 1 febbraio 2020.

fonti primarie. Il groviglio di problemi[2] riconducibili alla produzione normativa ha subito attirato l'attenzione della dottrina e il dibattito scientifico si è innescato pressoché istantaneamente, dando luogo a un vivace scambio, tutt'ora in corso, cui in questa sede ci si limita a rinviare[3].

L'altra grande questione che impegna le riflessioni degli studiosi – qui non solo delle scienze giuridiche[4] – è ovviamente quella dei diritti fondamentali, molti dei quali hanno subito, per la prima volta nella storia repubblicana, una compressione tale da sfiorare l'annullamento, in nome di una rinnovata e per certi aspetti inedita valorizzazione del profilo solidaristico del diritto alla salute[5]. Anche in questo caso le problematiche sono molteplici; tra le tante, il tentativo di arginare la diffusione della pandemia ha acceso un riflettore sul legame tra i diritti e le nuove tecnologie, di cui sono emerse con prepotenza sia le potenzialità, sia la pervasività. Si tratta di questioni nuove, di cui non va sottovalutata la risonanza mediatica, e che in prospettiva paiono destinate a porsi con sempre maggiore frequenza, anche se auspicabilmente non in chiave emergenziale: la crisi Covid-19, insomma, sembra aver solo accelerato l'emersione della necessità di esercitare su questi temi anche la riflessione costituzionalistica, cui, man mano che la situazione evolve e le reazioni istituzionali si delineano, spetta il compito di sorvegliare, tra gli altri, gli effetti di tutela o limitazione che l'utilizzo delle nuove tecnologie può avere sui diritti fondamentali.

[2] Un esempio molto concreto – e solo apparentemente lieve – delle conseguenze, che sono ormai esperienza condivisa degli italiani, è ben tratteggiato da V. BALDINI, *Sorridere al tempo della normativa contro l'emergenza sanitaria*, in *dirittifondamentali.it*, 23/03/2020.

[3] E anche un rinvio non può che essere in generale alle riviste di settore, che nelle versioni online hanno aperto *instant forum* o numeri speciali sulla gestione dell'emergenza, alimentati quotidianamente: v. pertanto *Rivista AIC*, *BioLaw Journal*, *Consulta Online*, *federalismi.it*, *dirittifondamentali.it*, *Diritti regionali*, il *Forum di Quaderni costituzionali*, *Media Laws*. Particolarmente vivace – e spesso di spunto ad interventi di più ampio respiro – è il dibattito di taglio più divulgativo avviato *lacostituzione.info*; per gli approfondimenti tecnici, sono risultati a chi scrive particolarmente utili gli interventi pubblicati in *Agenda Digitale*.

[4] V. ad esempio i contributi alla sezione dedicata all'emergenza Covid nella versione online de *la Rivista il Mulino*, *www.rivistailmulino.it*.

[5] Tra i primi, cfr. M. NOCELLI, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in *federalismi.it* 11/03/2020; C. DEL BÒ, *Diritto alla salute e solidarietà*, in *www.rivistailmulino.it*, 06/04/2020; cfr. inoltre le sezioni dedicate di *Online First - BLJ 2/20: Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, in *www.biodiritto.org*, 15/03/2020.

Adottando quindi tale angolo di osservazione, basta innanzitutto superare il (basso) livello della comunicazione pubblica iper-semplificata[6] e osservare il quadro costituzionale nel suo insieme per rilevare, in generale, che la "questione tecnologica" non si esaurisce nella tutela della *privacy*, né il relativo bilanciamento si risolve nella dicotomia "libertà vs *privacy*". Al contrario, essa si apre in un ventaglio di ambiti, che vanno dalla *e-Health*[7] all'informazione online, dallo *smart working* agli scontrini elettronici, dalla didattica a distanza (*e-learning*) alle acuite necessità di contrasto del *cyber crime*, per citare solo i casi più noti. In un diagramma ad albero sempre più ampio[8], poi, ciascuno dei menzionati argomenti è suddivisibile in ulteriori ramificazioni sia teoriche sia pratiche, alcune generali e più familiari ai giuristi (si pensi al settore dell'informazione online), altre decisamente più specialistiche (per tutte, l'*e-Health*). È all'interno di questo quadro che andrebbe impostata, a parere di chi scrive, anche una riflessione su un tema molto specifico qual è l'uso delle nuove tecnologie per il contenimento della pandemia da Covid-19, su cui si concentreranno le pagine che seguono; pena la perdita di vista non solo dello scenario reale (tecnologico, sociale, economico) in cui le considerazioni giuridiche si devono collocare, ma anche della conseguente complessità delle operazioni interpretative sul tavolo.

Da quanto detto deriva infatti una conseguenza sul piano del metodo: quando si ragiona di misure tecnologiche di "lotta al Coronavirus" – per usare l'espressione ormai comune – è necessario operare un bilanciamento non solo tra salute e *privacy*, o tra "*privacy* e libertà", a seconda che la si guardi da punto di vista del contrasto alla malattia accertata o dell'allentamento delle misure generali di *lockdown* (anche se i tre profili sono ovviamente connessi nella pratica). Vero è che, data la «formidabile capacità intrusiva»[9] della sorveglianza digitale, la *privacy* rappresenta senza dubbio

[6] Particolarmente critico sul punto, e con numerosi esempi della comunicazione pubblica menzionata nel testo è F. CHIUSI, *App per il tracciamento digitale: in democrazia discutere di privacy e diritti è doveroso e necessario*, in *www.valigiablu.it*, 24/04/2020.

[7] La rete *e-Health* è un network europeo che, ai sensi dell'art. 2 della decisione della Commissione n. 2019/1765 del 22 ottobre 2019, «collega le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri e che persegue gli obiettivi di cui all'articolo 14 della direttiva 2011/24/UE», cioè l'assistenza sanitaria online.

[8] Ben rappresentato, ad esempio, dalla scansione individuata nell'*Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, cit.

[9] Corte cost., sent. n. 81/1993, p.to 2 *Diritto*.

uno dei pilastri del ragionamento, ma ad essa vanno *affiancati*[10] almeno: la libertà personale (art. 13 Cost.), di circolazione (art. 16), di riunione (art. 17), di associazione (art. 18) e di culto (art. 19); la libertà di impresa (art. 41); i diritti alla salute (art. 32), all'istruzione (artt. 33 e 34) e al lavoro (artt. 1, 4 e 35 ss.). Il tutto sullo sfondo dei principi di eguaglianza formale e sostanziale (art. 3 Cost.) e di solidarietà (art. 2 Cost.), e ovviamente senza dimenticare i vincoli di bilancio (art. 81 Cost.). Le nuove tecnologie, come i diritti, sono declinate al plurale: isolarne un unico aspetto pare – oltre che impreciso[11] – tanto fallace quanto lo sarebbe mettere in bilanciamento un solo diritto (ad esempio, la *privacy*) contro tutti gli altri, considerati come una sorta di amorfo monolite. Impostata così la questione, ne risulta un quadro notevolmente più complesso rispetto a un "ordinario" bilanciamento a due termini; il che rappresenta di certo una sfida per l'interprete, impegnandolo in un'argomentazione più faticosa; ma non può comunque giustificare, almeno sul piano scientifico, un'arbitraria delimitazione del campo di indagine, dietro la quale peraltro sembra celarsi una altrettanto arbitraria gerarchizzazione dei diritti fondamentali.

2. Le linee guida europee e nazionali

Sempre a metà del periodo di emergenza, si è inoltre delineato con chiarezza, almeno negli aspetti essenziali, il quadro regolatorio: per quanto in forma di *soft law*, infatti, le istituzioni europee e le autorità indipendenti di settore hanno consolidato posizione nette, innanzitutto riguardo ciò che è ammissibile o meno alla luce del quadro normativo vigente[12]. Di particolare interesse in relazione alla prospettiva di queste riflessioni risultano, per citare i riferimenti principali, la raccomandazione della Commissione europea n. 2020/518 dell'8 aprile scorso e la Comunicazione della medesima Commissione del 17 aprile, contenente *Orientamenti sulle app a sostegno della*

[10] Ovviamente, a condizione che si accetti l'idea dell'assenza di gerarchia tra i diritti inviolabili, su cui ci si limita a rinviare nella giurisprudenza a Corte cost., sent. n. 85/2013 (la cd. Sentenza ILVA) e in dottrina a R. BIN, da ultimo in *Critica della teoria dei diritti*, FrancoAngeli, 2018.

[11] Gli esperti del settore parlano infatti di approcci, o sistemi, o contesti, e non di singole tecnologie, che sono piuttosto considerate strumenti: oltre ai siti specializzati (ad es. *Redhat.com*) cfr. R. ANDERSON, *Contact Tracing in the Real World*, *in www.lightbluetouchpaper.org*, 12/04/2020; F. BAIARDI, *App Coronavirus e sicurezza informatica: tutti i problemi e come affrontarli*, in *www.agendadigitale.eu*, 23/04/2020.

[12] I riferimenti sono il reg. n. 679 del 2016 sulla protezione dei dati personali, il cd. GDPR, e la dir. n. 58 del 2002, cd. Direttiva *E-Privacy*.

pandemia di covid-19 relativamente alla protezione dei dati; dello stesso giorno (17 aprile), la risoluzione del Parlamento europeo sulla *azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze*; infine, le *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, adottate il 21 aprile 2020 dall'*European Data Protection Board* (EDPB – il Consiglio dei Garanti europeo per la protezione dei dati personali[13]).

Facendo seguito a diversi interventi precedenti, e al dichiarato scopo di uniformare per quanto possibile la risposta degli Stati al dilagare del contagio, sia i documenti della Commissione sia le *Guidelines* dell'EDPB individuano la gamma degli strumenti tecnologici teoricamente disponibili, la normativa di riferimento e le cautele necessarie per l'implementazione di soluzioni rispettose dei diritti fondamentali, il cui primo requisito è il rispetto dei principi – ormai consolidati a livello europeo – di *data protection* raccolti nel GDPR. Dal complesso delle indicazioni contenute nei tre documenti emergono diversi elementi interessanti per il dibattito giuridico.

2.1. Le tecnologie disponibili e i rischi correlati (cenni)

Prima di approfondire le linee guida europee, è utile soffermarsi un momento sullo strumentario tecnologico potenzialmente disponibile nella lotta all'epidemia. Con l'ampio margine di approssimazione inevitabile quando si prendono a prestito nozioni da altre discipline, va quindi precisato che l'utilità delle tecnologie digitali nelle azioni di contrasto del contagio sta, in sostanza, nella loro capacità di raccogliere, memorizzare e poi elaborare dati provenienti da dispositivi connessi ad Internet, in quantità inimmaginabili fino solo a pochi anni fa[14], ad una velocità gestibile solo da macchine[15] e con una precisione inquietante. I dati in questione possono essere riferiti a

[13] Tutti i documenti dell'EDPB sono reperibili nel suo sito istituzionale: *https://edpb.europa.eu/edpb_it*.

[14] L'unità di misura oggi in uso sono gli zettabyte; uno zettabyte è «pari ad un trilione di gigabyte ovvero 250.000.000.000 di DVD»: AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui Big Data*, 10/02/2020, p. 5. Il testo dell'Indagine è scaricabile dai siti delle tre Autorità che l'hanno curata.

[15] Nel caso di specie, quindi, gli strumenti digitali possono agevolare e soprattutto abbreviare in modo significativo i tempi dell'attività di tracciamento che gli epidemiologi svolgono, da decenni, in modo manuale, prima intervistando i contagiati per ricostruirne la rete di contatti, e poi avvisando, di solito per via telefonica, i soggetti a rischio: cfr. il *Report del Sottogruppo di lavoro n. 6*, impegnato sulle "Tecnologie per il governo dell'emergenza" (d'ora in poi, per

un singolo individuo – e se la persona è in qualsiasi modo identificabile loro tramite si tratta di dati personali, oggetto della tutela del GDPR[16] – oppure possono essere anonimi (*rectius*, anonimizzati[17]: nozione da tenere ben distinta da quella di pseudonimizzazione, ancora prevista dal GDPR[18] e che, come si vedrà, riveste un'importanza fondamentale nel *contact tracing*). Nel caso di dati anonimi, si entra nella categoria dei Big Data[19], il cui valore sta innanzitutto nella quantità, in vista di un'elaborazione in forma aggregata (tramite algoritmi), dalla quale è possibile trarre un sorprendente numero di informazioni, spesso nemmeno determinabili a priori perché

---

brevità, *Report del Sottogruppo Tecnologie*), pp. 3-4 e con particolare riferimento alla tempistica pp. 31-32; la *Relazione tecnico-giuridica sui profili connessi all'eventuale adozione di una soluzione di contact tracing per il contrasto al COVID-19* del Sottogruppo n. 8, impegnato sui "Profili giuridici della gestione dei dati connessa all'emergenza" (d'ora in poi, per brevità: *Relazione del Sottogruppo Profili giuridici*), p. 4. I due documenti citati, insieme ai report degli altri gruppi di lavoro istituiti presso il Ministero dell'Innovazione tecnologica, sono stati pubblicati il 30 aprile 2020 – tramite link al sito *GitHub.com* – sulla pagina web del Ministero: *www.innovazione.gov.it*.

[16] Ai sensi del reg. n. 2016/679, art. 2, p.to 1), per dato personale si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); 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 caratteristico della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[17] L'anonimizzazione consiste, in sostanza, nel raccogliere o trattare i dati in modo da impedirne in via definitiva ed irreversibile la riconducibilità a una persona. Va però tenuto presente che «la linea di demarcazione tra dati di natura personale e non [può] essere in concreto difficile da tracciare – in particolare in ragione della possibilità di riconnettere informazioni apparentemente anonime (o anonimizzate) a individui singoli a seguito delle peculiari operazioni di trattamento effettuate (nel tempo sempre più agevolmente realizzabili, sia per le aumentate capacità di calcolo, sia per la pluralità di archivi in ipotesi utilizzabili, aventi anche genesi ed utilizzi prospettici diversi al tempo della raccolta)»: AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui Big Data*, cit., p. 60, ma *passim*: il labile confine tra dati personali e anonimi/anonimizzati è infatti uno dei *fils rouges* dell'Indagine.

[18] La pseudonimizzazione (reg. 2016/679, art. 2, p.to 5) è «il trattamento dei dati personali in modo che tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile».

[19] In realtà la distinzione può essere considerata abbastanza netta solo ai fini delle riflessioni che si stanno svolgendo, perché, come si vedrà più avanti, uno dei capisaldi delle linee guida europee è che le tecniche di raccolta dei dati utilizzabili a fini di contenimento della pandemia non possono riguardare dati personali, ma al più pseudonimizzati (che rientrano comunque nella disciplina del GDPR); per cui i Big Data, in questa specifica circostanza, finiscono per coincidere con dati anonimi, come quelli sugli spostamenti raccolti da Google tramite *Maps*. Ciò non toglie che nelle definizioni di Big Data sinora elaborate possano essere compresi anche dati personali: cfr. AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui Big Data*, cit., pp. 7-8.

l'analisi può portare a scoprire correlazioni che non erano prevedibili dalla sola massa di dati grezzi[20]. Le due tipologie di dati hanno utilità diverse nella lotta all'epidemia: i primi, proprio perché riferibili con precisione ad un singolo individuo, oltre a fornire informazioni sulla persona (fino a quelle sulla salute), possono consentire di tenere traccia, nel tempo e nello spazio, dei suoi spostamenti e di tutte le attività svolte; i secondi sono utili per mappare, ad esempio, l'andamento di un'epidemia[21], o il grado di rispetto complessivo di una misura di limitazione della mobilità ricavato dall'analisi dei movimenti, su un certo territorio. È noto che le cd. *Big Tech* (Facebook, Google e Apple), hanno tempestivamente offerto la loro collaborazione a Governi ed enti di ricerca, fornendo set di dati anonimi raccolti dalle rispettive piattaforme[22].

Ebbene, mentre a livello tecnologico tutte le opzioni menzionate sono non solo disponibili, ma in alcuni casi già utilizzate, nella prospettiva costituzionale bisogna considerare che le scelte sulla tipologia di dati, sul loro grado di anonimizzazione, e sulle modalità di raccolta, memorizzazione e trattamento, sono determinanti per il livello di la tutela dei diritti fondamentali degli individui. Con l'ulteriore precisazione che non ci sono opzioni predefinite per una tipologia o per l'altra, perché le funzioni da assegnare agli strumenti tecnologici possono sfruttare sia dati personali sia dati anonimi. Ovviamente, la variabile incide sul risultato, ma va ribadito che la decisione

[20] Dando così luogo tra l'altro, nel caso in cui i dati trattati siano personali, a notevoli difficoltà in relazione al consenso, che ai sensi del GDPR deve essere esplicitamente e liberamente riferito a specifiche finalità di trattamento illustrate in modo chiaro e preciso: cfr. AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui Big Data*, cit., p. 18 ss.

[21] Nella versione per smartphone di Facebook, ad esempio, dal 3 maggio compare la richiesta di partecipare ad una *survey*, consistente in un questionario – di cui viene assicurato l'anonimato – sulla comparsa e l'evoluzione di sintomi, che aiuterà l'Università del Maryland «a monitorare e prevedere il diffondersi del coronavirus (COVID-19), per migliorare preparazione e intervento». Non risulta a chi scrive (senza escludere che la causa siano le limitate competenze tecnologiche) che il medesimo *alert* compaia nella versione desktop del *social network*.

[22] La notizia è apparsa con una certa regolarità sui media. Cfr. ad esempio: L. ZORLONI, *Il governo userà i big data nell'emergenza coronavirus. A partire da quelli di Facebook*, in *www.wired.it*, 17/03/2020; T. ROMM, E. DWOSKIN, C. TIMBERG, *U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus*, in *www.washingtonpost.com*, 18/03/2020; *Le nuove mappe di Facebook contro il coronavirus*, e L. ZORLONI, *Da Facebook a Google, che dati usa il governo nell'emergenza coronavirus*, entrambi in *www.wired.it*, rispettivamente 06/04/2020 e 07/04/2020; *Coronavirus: dopo Google-FB, anche da Apple dati sulla mobilità attraverso le mappe*, in *www.repubblica.it*, 14/04/2020; J. D'ALESSANDRO, *Coronavirus, Facebook: "Ecco la mappa di chi presenta i sintomi". E mercoledì arriva in Italia*, in *www.repubblica.it*, 20/04/2020.

resta eminentemente politica: su tale profilo, cruciale, si tornerà in conclusione (*infra*, par. 5).

Quanto appena sostenuto emerge, ad esempio, dal *considerando n. 12* della raccomandazione della Commissione n. 518 del 2020, in cui si legge che le applicazioni mobili (d'ora in poi: app) possono svolgere tre funzioni generali: informare i cittadini, fornendo loro consulenza e agevolando l'organizzazione del *follow-up* sanitario delle persone contagiate (spesso in combinazione con questionari di autodiagnosi); allertare chi si è trovato in prossimità di una persona infetta, per interrompere la catena del contagio; monitorare la quarantena e controllarne il rispetto da parte dei malati in isolamento domiciliare. È evidente che si delineano così non solo tre funzioni delle app, ma anche tre potenziali categorie di destinatari: la generalità delle persone (funzione informativa), i soggetti a rischio contagio (funzione di *contact tracing* e *alert*), e i soggetti malati (funzione di sorveglianza/monitoraggio della quarantena). È anche evidente che si tratta di situazioni in cui l'intervento pubblico può diventare progressivamente più coercitivo (e la tecnologia più invasiva): nel caso di una persona contagiata che violi le prescrizioni di isolamento è già configurabile la sanzione penale[23].

2.2. La app di *contact tracing*: obbligo o facoltà? Un dubbio solo apparente

Ebbene, un primo dato interessante è che la funzione di monitoraggio sul rispetto della quarantena compare, come appena visto, nei *considerando* della raccomandazione, mentre non trova spazio nel seguito, in cui l'intervento della Commissione (lo *scopo*, par. 1) viene ristretto alla creazione di un pacchetto di misure digitali, con particolare attenzione a: 1) un «approccio paneuropeo» all'uso delle app, «per consentire ai cittadini di adottare misure di distanziamento sociale efficaci e più mirate e per scopi di allerta, prevenzione e tracciamento dei contatti al fine di contribuire a limitare la propagazione della malattia»; e 2) un «piano comune per l'utilizzo di dati anonimizzati e aggregati sulla mobilità della popolazione» (che sfrutta i Big Data forniti dalle *Big Tech*). La successiva comunicazione della Commissione (17 aprile), nello specificare l'ambito degli orientamenti ivi esposti, prima «raccomanda l'utilizzo di app facoltative» e poi specifica che gli orientamenti «non riguardano le app finalizzate a far

[23] Cfr. M. FARINA, *La data protection ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, cit., 20/03/2020.

rispettare le prescrizioni in materia di quarantena (comprese quelle obbligatorie)»[24]. Le *Guidelines* dell'EDPB si concentrano, oltre che sull'uso di dati anonimi di localizzazione (ancora i Big Data), sul *contact tracing* a scopo non di sorveglianza ma di «supporto» alla popolazione, dato che il Garante europeo aveva già in precedenza preso posizione sul fatto che il *contact tracing* possa avvenire solo su base volontaria[25].

L'assenza di coercizione è insomma uno degli assi portanti di tutti i documenti europei e delle indicazioni del Garante per la privacy italiano[26]. L'imposizione di tecnologie potenzialmente onnipervasive quali sono quelle digitali è considerata, infatti, in contrasto con l'impostazione democratica di qualsiasi ordinamento liberale: la Commissione europea dichiara esplicitamente che un approccio comune alla crisi Covid-19 «si è reso necessario anche perché le misure adottate in certi paesi, quali il tracciamento delle persone basato sulla geolocalizzazione, l'uso della tecnologia per calcolare il livello di rischio sanitario di un individuo e la centralizzazione dei dati sensibili, sollevano interrogativi che riguardano numerose libertà fondamentali»[27].

Nonostante il Governo italiano si sia allineato – com'è noto e come si vedrà meglio più avanti analizzando il decreto-legge n. 28 del 2020 (*infra*, par. 4) – alle indicazioni europee sull'assoluta volontarietà nel download e nell'uso della app di *contact tracing* (dal poco felice nome di *Immuni*), vale la pena soffermarsi un attimo sugli argomenti a favore dell'obbligatorietà, che in effetti non appaiono inaccettabili sul piano teorico, almeno se si cerca di mantenere un approccio il più possibile "laico", e soprattutto pragmatico, alla questione di fondo (che resta la gestione di un'emergenza di livello e

[24] Commissione UE, COM 2020/C 124/01, p. 2.

[25] «The EDPB strongly supports the Commission's proposal for a voluntary adoption of such apps, a choice that should be made by individuals as a token of collective responsibility. It should be pointed out that voluntary adoption is associated with individual trust, thus further illustrating the importance of data protection principles»: EDPB, *Letter concerning the European Commission's draft Guidance on apps supporting the fight against the Covid-19 pandemic*, 14/04/2020, in *www.edpb.europa.eu*.

[26] V. ad esempio l'audizione svolta dal Presidente presso la Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati l'8 aprile 2020, il cui testo è disponibile in *www.garanteprivacy.it - Attività*. Va sottolineato che se non fosse stato pubblicato dal Garante il contenuto dell'audizione sarebbe stato impossibile da reperire, stante la natura informale dell'audizione medesima. Sul paradosso per cui le uniche procedure informative svolte dal Parlamento su un tema di tale rilevanza siano state sinora prive di pubblicità si tornerà in conclusione: v. *infra*, par. 4.

[27] Commissione UE, racc. n. 2020/518, par. 23.

dimensioni inediti nella storia repubblicana). Da diverse parti[28] si è rilevato, in estrema sintesi, che una "limitazione della privacy" (per usare le espressioni comuni) potrebbe essere ammissibile, se ne conseguisse una minor compressione di altri diritti. È innegabile, infatti, che durante il *lockdown* molte delle libertà citate in apertura siano state fortemente ristrette o temporaneamente sospese: basta pensare alla libertà di circolazione e soggiorno *ex* art. 16 Cost., o a quella di riunione *ex* art. 17. Partendo da questo dato di comune esperienza, il ragionamento di chi ha sostenuto l'opportunità di introdurre almeno qualche elemento di imposizione in merito dell'adozione della app[29] – che potrebbe tradursi nel *condizionare* la libertà di spostamento ecc. al suo utilizzo – è che in questo modo si rinuncerebbe, sì, a un po' di privacy, guadagnando però margini di godimento di altri diritti. Dal punto di vista del bilanciamento, in definitiva, secondo questa impostazione si otterrebbe di trattare tutti i diritti come pari, senza attribuire alla privacy una superiorità che, effettivamente, l'ordinamento non le assegna.

Non va sottovalutato il fatto che questo tipo di argomenti ha avuto una notevole diffusione – anche per voce di soggetti istituzionali e politici – soprattutto nell'immediatezza della seconda e più lunga proroga delle misure di isolamento, e che potrebbe facilmente dilagare anche nell'opinione pubblica, se le restrizioni venissero prolungate o se addirittura venisse imposto un nuovo *lockdown* (ipotesi non certo auspicabile ma che, a metà del periodo di emergenza, non è nemmeno possibile escludere[30]). In aggiunta, non si può negare che esso abbia un certo fascino sul piano speculativo[31], chiamando direttamente in causa la concezione del rapporto tra il potere e i singoli, la tenuta delle garanzie democratiche sui diritti fondamentali, la percezione

[28] V. l'ampia casistica raccolta da F. CHIUSI, *App per il tracciamento digitale*, cit.

[29] Non è chiaro in cosa potrebbe effettivamente concretizzarsi un obbligo parziale, per cui quella avanzata nel testo è un'ipotesi ricavata in via puramente deduttiva. Peraltro, anche la documentazione resa pubblica contestualmente all'adozione del d.l. n. 28/2020 non chiarisce del tutto il quadro, dato che in particolare nella *Relazione del Sottogruppo Principi giuridici* emerge in diversi punti, per quanto con la massima cautela, il riferimento a qualche forma di «incentivo» all'uso dell'app, che tuttavia non viene ulteriormente specificato.

[30] Il discorso può, in ogni caso, valere *pro futuro*, nella – ancora certamente non auspicabile, ma nemmeno escludibile – ipotesi di una nuova emergenza sanitaria. Interessanti sul punto le riflessioni di L. PEZZALI, *La pandemia: quattro profili morali*, in *www.rivistailmulino.it*, 31/03/2020, specialmente nella parte sul *Profilo Utilitarista*, p. 2.

[31] È proprio da tali scenari "alla cinese" che prendono spunto, ad esempio, G. PELLEGRINO, *Tracciamento e discriminazione*, in *www.rivistailmulino.it*, 14/04/2020 e in parte E. CHITI, '*Questi sono i nodi'. Pandemia e strumenti di regolazione: spunti per un dibattito*, in *www.lacostituzione.info*, 24/04/2020, pp. 2-3.

del valore che viene assegnato alla riservatezza dei dati personali in epoca di nuove tecnologie, le potenzialità invasive delle tecnologie medesime, eccetera. Insomma, se un – pur necessario – dibattito pubblico dovesse affrontare questo tema, l'esito potrebbe non essere così scontato come può sembrare a chi, affezionato all'impostazione liberale, avesse provato un'istintiva diffidenza verso qualsiasi soluzione seppur solo parzialmente coercitiva.

A ben guardare, tuttavia, i discorsi a favore dell'obbligatorietà incontrano un ostacolo ben più a monte, fondato sul rilievo per cui l'imposizione anche parziale di una app di *contact tracing* rappresenterebbe, almeno nelle attuali condizioni italiane, un obbligo inesigibile[32]. Prima di qualsiasi altra considerazione, infatti, va tenuto presente che la Costituzione italiana impone solo quando tutti sono nella condizione di adempiere, e non in senso astratto, ma nella concretezza del secondo comma dell'art. 3: o l'adempimento del dovere non incontra «ostacoli di ordine sociale ed economico» (com'era, a suo tempo, il servizio di leva), oppure spetta alla Repubblica rimuovere tali ostacoli. Bastano due esempi: l'istruzione inferiore è obbligatoria *perché* gratuita (art. 34 Cost.); i trattamenti sanitari possono essere obbligatori *perché* la Repubblica assicura cure gratuite agli indigenti (art. 32 Cost.). Traslando il discorso "ai tempi del Coronavirus", la domanda preliminare – e a questo punto sì, dirimente – diventa allora: è possibile imporre a tutti (o condizionare l'esercizio delle libertà fondamentali a) l'uso di una app che deve essere scaricata su uno smartphone? La risposta deve tenere presente almeno tre fattori: 1. uno smartphone ha un costo non irrilevante anche nelle sue versioni meno sofisticate (che magari non sarebbero sufficienti a supportare la funzionalità di un'app ad elevato livello crittografico, requisito fondamentale per non sacrificare del tutto la *privacy*); 2. ad ogni apparecchio deve essere abbinato, in qualche forma contrattuale, un adeguato traffico dati (indispensabile per il *contact tracing*) e, in ogni caso, 3. deve essere garantito in modo uniforme sul territorio nazionale l'accesso a Internet. A fronte di una risposta negativa ad anche solo uno dei tre quesiti, un eventuale obbligo non può che essere considerato, come si anticipava, inesigibile e quindi, se imposto, in violazione dell'art. 3 della Costituzione.

[32] Cfr. sul punto, con argomentazione rovesciata rispetto a quella illustrata nel testo, anche B. SAETTA, *Le linee guida del Garante europeo e i requisiti che l'App di tracciamento digitale dei contatti deve rispettare*, in *www.valigiablu.it*, 24/04/2020, p. 8.

Per concludere il ragionamento sul punto, va infine aggiunto che se l'obbligo divenisse esigibile, ad esempio perché si è trovata una soluzione tecnologica che consentirebbe di dare risposta affermativa alle tre domande appena formulate, tale soluzione dovrebbe comunque superare i test di adeguatezza e proporzionalità, anche dal punto di vista delle finanze pubbliche. In definitiva, si potrebbe realmente discutere di una soluzione coercitiva solo se fosse ragionevolmente certo – almeno per quanto possibile in via prognostica – che i costi (sia in termini di limitazione dei diritti, sia in senso stretto, cioè sul piano economico) sarebbero compensati da un sicuro effetto di contenimento dell'epidemia e quindi da un considerevole vantaggio per la salute *e* la libertà di movimento, di riunione, di associazione, di culto, eccetera.

Ecco perché l'adesione volontaria da parte della popolazione deve essere considerata precondizione (anche tecnica, come si dirà meglio più avanti: *infra*, par. 5) di qualsiasi valutazione sugli strumenti tecnologici. Salva l'ipotesi di dispositivi indossabili e non eliminabili dal soggetto (braccialetti elettronici) o – scenario giuridicamente terrificante ma tecnicamente banale – di chip iniettati direttamente nel corpo dei "sorvegliati", infatti, una strategia fondata sulle tecnologie digitali non può che passare per lo smartphone[33] (o un qualche tipo di altro *device* in grado di supportare e gestire la app). Il che comporta che le persone a) scarichino una app sul proprio apparecchio; b) la mantengano attivata; c) portino l'apparecchio (con batteria sufficiente) con sé quando escono di casa.

3. I principali nodi giuridici relativi al *contact tracing*: la tecnologia di raccolta dei dati, la gestione, la modalità di allerta

Al centro dei *rumors* mediatici sin dall'inizio dell'epidemia, le app di *contact tracing* sono state oggetto di particolare attenzione da parte delle istituzioni europee e dei garanti della privacy perché – com'è ormai noto a chiunque abbia rivolto solo uno sguardo alle cronache – se non opportunamente strutturate, sono in grado di compiere vere e proprie razzie di dati personali e consentire, grazie a questi ultimi, una serie di condotte illecite, tra cui spiccano i trattamenti discriminatori[34]. Anche escludendone

[33] Cfr. sul punto il *Report del Sottogruppo Tecnologie*, cit., p 5.

[34] In proposito è da sottolineare che l'assenza di obbligatorietà sembra sufficiente ad arginare il rischio sul versante del potere pubblico (a meno di avventurarsi in scenari orwelliani, che forse

l'obbligatorietà, pertanto, al momento dell'eventuale adozione il decisore politico si trova a dover compiere una serie di scelte decisive per la garanzia dei diritti, che ruotano intorno a quattro nodi principali.

Primo, quale tecnologia utilizzare per la raccolta dei dati, con particolare riferimento alla geolocalizzazione (il GPS), in alternativa all'uso di dati di prossimità (Bluetooth). Questo profilo chiama poi in causa un ulteriore aspetto della questione, relativo all'interoperabilità[35], per cui la medesima app deve poter funzionare su diversi sistemi operativi e deve consentire la "comunicazione" sia tra i dispositivi, sia tra essi e un server centrale (con interazioni diverse a seconda della soluzione che si dà al secondo nodo).

Secondo, come gestire l'archiviazione dei dati raccolti: si tratta di uno degli aspetti che hanno avuto maggiore risonanza mediatica, per cui è sufficiente richiamare a grandi linee l'alternativa tra un sistema centralizzato, in cui tutti i dati vengono memorizzati in un solo server, e uno decentrato, in cui i dati restano sui singoli dispositivi e vengono trasmessi nel caso in cui una persona che ha attivato l'app venga diagnosticata positiva alla malattia e sia quindi necessario attivare la funzione di allerta (*alert*).

Terzo, e di conseguenza, è necessario decidere la modalità con cui l'allerta viene trasmessa ai soggetti che, secondo i criteri epidemiologici, si sono trovati in condizione di rischio: se tramite un soggetto unico che gestisce le informazioni (ad esempio, l'autorità sanitaria), o direttamente dal *device* del singolo contagiato.

Quarto, bisogna stabilire come inserire questo meccanismo nell'ambito di una più complessiva – e complessa – strategia di gestione dei contagi. Va sottolineato infatti che l'avvertimento su cui convergono *tutte* le analisi in materia, sia istituzionali sia di

non sarebbe comunque inopportuno tenere quantomeno sullo sfondo del ragionamento costituzionalistico), ma non esclude affatto altri tipi di discriminazione ad opera del settore privato: si pensi, ad esempio, all'eventualità che dati sanitari finissero nella disponibilità di compagnie assicurative o di potenziali datori di lavoro.

[35] Cfr. raccomandazione n. 2020/518 della Commissione UE, *Considerando* n. 6, n. 19 e n. 28. Nelle *Guidelines* dell'EDPB l'interoperabilità compare sia nell'*Introduction & context* (p. 3), sia nell'*Annex* contenente l'*Analysis Guide*, in particolare tra le *Functional considerations*, (p. 17) e nella sezione dedicata a *Protection of personal data and privacy of natural persons* (p. 17). Merita infine ricordare che l'interoperabilità è oggetto del *Considerando* n. 68 del GDPR, come condizione tecnica sia per il mantenimento del controllo sui propri dati da parte dell'interessato, sia per l'esercizio del diritto alla portabilità di cui all'art. 20.

singoli studiosi, è che, anche nelle realtà in cui è stato sfruttato al suo massimo (la Corea del Sud), il *contact tracing* per avere successo deve essere coordinato con una meticolosa ed efficace attività epidemiologica e sanitaria.

3.1. I principi di protezione dei dati personali (*data protection*) come criteri di scelta per le caratteristiche della app

Rispetto ai primi tre nodi appena illustrati, i criteri interpretativi (e quindi limitativi della discrezionalità politica) sono rappresentati dai principi di protezione dei dati personali ormai consolidati nel contesto europeo; in particolare – come ribadito pressoché in ogni intervento anche dal Garante italiano – la chiave di volta è il principio di minimizzazione, secondo cui i dati personali devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati» (GDPR, art. 6.1, lett. *c)*).

È sulla base di tale principio che sia la Commissione europea[36], sia l'EDPB hanno indicato come tecnologia per la raccolta dei dati il Bluetooth (e in particolare il *Bluetooth Low Energy* - BLE, cioè a basso consumo): questo perché per il tracciamento dei contatti, il cui obiettivo «non è quello di seguire i movimenti delle persone o di far rispettare le prescrizioni»[37], i dati di localizzazione non servono[38], e il loro trattamento non sarebbe quindi giustificabile[39]. La Commissione specifica inoltre che non sono necessari

[36] La raccomandazione n. 2020/518 della Commissione UE elenca, tra i principi da osservare in materia, la «preferenza per le misure meno intrusive […] compreso l'uso dei dati di prossimità, ma senza il trattamento dei dati relativi all'ubicazione o agli spostamenti delle persone, e l'uso di dati anonimizzati e aggregati ove possibile» (par. 16).

[37] Commissione UE, Comunicazione 2020/C 124 1/01, par. 3.4.

[38] Identica la posizione dell'EDPB, *Guidelines*, cit., p.to 27, p. 7: «Contact tracing apps do not require tracking the location of the individual users. Instead, proximity data should be used». Poco più avanti, nel paragrafo relativo a *Recommendations and functional requirements*, le *Guidelines* ribadiscono (p.to 42, p. 9): «According to the principle of data minimization […], the data processed should be reduced to the strict minimum. The application should no collect unrelated or not needed information, which may include civil status, communication identifiers, equipment directory items, messages, call logs, location data, device identifiers, etc.».

[39] È interessante notare, sul punto, che il *Report del Sottogruppo tecnologie*, cit., p. 10, prima osserva che «potrebbero essersi verificati casi di contagio ambientale e quindi potrebbe essere richiesto un intervento di sanificazione dei luoghi/locali», motivo per cui «potrebbe essere opportuno che la soluzione possa conservare […] anche un timestamp e una limitata cronologia delle geolocalizzazioni» (ad esempio si pensi alle scuole o, caso tristemente noto, alle RSA). Subito dopo però precisa che «la raccolta di tali dati, anche previo opt-in [consenso informato

nemmeno l'ora o il luogo del contatto, mentre potrebbe essere utile conservare traccia del giorno, sia per chiarire il quadro clinico della persona al momento dell'eventuale contagio, sia per il successivo *follow-up*.

Dalla scelta del Bluetooth come strumento di *tracing* deriva anche, in sintesi, la risposta al problema dell'archiviazione. Di nuovo, la Commissione europea e l'EDPB concordano sulla necessità che i dati di contatto siano conservati sul dispositivo del singolo e che, sempre in ossequio al principio di minimizzazione, i dati di prossimità «dovrebbero essere generati e trattati solo se sussiste un reale rischio di infezione (in funzione della vicinanza e della durata del contatto)»[40].

A proposito del sistema – centralizzato o decentralizzato – di gestione dei dati, l'EDPB osserva che entrambe le soluzioni sono considerate percorribili e che, se accompagnate da adeguate misure di sicurezza, entrambe presentano vantaggi e svantaggi[41]. Il Garante europeo sottolinea comunque (p.to 43 delle *Guidelines*) che qualsiasi server coinvolto nel *contact tracing* deve raccogliere solo la cronologia dei contatti o gli identificatori pseudonimi di un utente diagnosticato come infetto, all'esito di un'adeguata valutazione di un'autorità sanitaria e a seguito di un'azione volontaria dell'utente stesso. In alternativa, il server deve conservare una lista degli identificativi degli utenti contagiati o la loro cronologia dei contatti solo per il tempo necessario ad avvisare le persone potenzialmente infette della loro esposizione al rischio, e non dovrebbe cercare di identificare i potenziali contagiati. Per quanto riguarda le istituzioni europee, se la comunicazione della Commissione si assesta su una linea simile a quella del Garante – per cui prende in considerazione entrambe le soluzioni,

---

alla specifica operazione] dell'utente, va attentamente valutata sulla base dei rischi di re-identificazione che essa comporta, in quanto *l'uso della posizione vanifica* – de facto – *ogni forma di approccio autenticamente* privacy-preserving» (corsivo non testuale). Non meno interessante, ai fini di quanto si dirà in conclusione (*infra*, par. 5), è l'ulteriore conseguenza che il *Report* sottolinea in merito alla raccolta dei dati di geolocalizzazione, che «*può rendere più complessa e meno efficace la strategia di comunicazione pubblica e di acquisizione di utenti che volontariamente usano la suddetta app*» (corsivo testuale).

[40] Commissione UE, Comunicazione 2020/C 124 1/01, par. 3.4. Per la posizione dell'EDPB, v. *Guidelines*, cit., p.to 27, p. 7: «the collected information should reside on the terminal equipment of the user and only the relevant information should be collected when absolutely necessary».

[41] EDPB, *Guidelines*, cit., p.to 42, p. 9. Pertanto, prosegue l'EDPB, «the conceptual phase of app development should always include thorough consideration of both concepts carefully weighing up the respective effects on data protection /privacy and the possible impacts on individual rights».

sottolineando il ruolo centrale dell'autorità sanitaria anche nella comunicazione e soprattutto che, nel caso del sistema centralizzato (del *server back-end*), potrebbe essere necessario fornire alle autorità sanitarie anche i recapiti delle persone a rischio[42] – è invece il Parlamento europeo a prendere una posizione netta a favore della decentralizzazione. Al punto 52 della risoluzione del 17 aprile, infatti, il PE sottolinea tra l'altro che «i dati generati non devono essere immagazzinati in banche dati centralizzate, il che condurrebbe a potenziali rischi di abuso e alla conseguente perdita di fiducia» e «chiede che la memorizzazione dei dati sia completamente decentralizzata».

Sciolti questi nodi principali, la maggior parte delle indicazioni relative alla app di *contact tracing* contenute nelle linee guida rappresentano un'applicazione delle regole generali del GDPR: i dati devono essere quantomeno pseudononimizzati e ne deve essere garantita la sicurezza, utilizzando «tecniche crittografiche all'avanguardia»[43]; la conservazione deve limitarsi allo stretto indispensabile, distinguendo tra persone contagiate e persone solo a rischio a seguito di un contatto; deve essere comunque garantito che, al più tardi quando la pandemia sarà dichiarata sotto controllo, i dati vengano cancellati e le app vengano disattivate, con l'ulteriore precisazione che la disattivazione non dovrebbe dipendere dalla disinstallazione da parte dell'utente[44].

Per quanto riguarda la base giuridica del trattamento, essa è rinvenibile direttamente nel GDPR dal combinato disposto degli artt. 6 e 9[45], in particolare quando il trattamento avviene da parte delle autorità sanitarie nazionali[46]. La Commissione indica però il consenso come «motivo più adeguato» per le attività pertinenti il tracciamento, ribadendo che esso deve essere libero, specifico, esplicito e informato. Da ciò deriva non solo l'esclusione di qualsiasi forma di consenso tacito, ma anche che le

[42] Commissione UE, COM 2020/C 124/01, par. 3.4.

[43] Commissione UE, COM 2020/C 124/01, par. 3.8.

[44] Commissione UE, COM 2020/C 124/01, par. 3.2.

[45] Cfr. la chiarissima ricostruzione di F. P. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il giuridicamente consentito*, in *Instant Forum - Diritto, diritti ed emergenza ai tempi del Coronavirus*, cit., pp. 4-5.

[46] Le autorità sanitarie nazionali « trattano generalmente dati personali quando esiste un obbligo legale stabilito dal diritto dell'Unione o nazionale che prevede tale trattamento e nel rispetto delle condizioni di cui all'articolo 6, paragrafo 1, lettera c), e all'art. 9, paragrafo 2, lettera i), del GDPR o quando tale trattamento è necessario per promuovere l'interesse pubblico riconosciuto dal diritto dell'UE o nazionale»: Commissione UE, COM 2020/C 124/01, par. 3.3, da cui anche la citazione che segue immediatamente nel testo.

finalità debbano essere indicate con la massima chiarezza; in particolare, nell'ipotesi in cui una app contenga diverse funzionalità, l'utente dovrebbe avere «la possibilità di scegliere tra diverse funzionalità che perseguono ciascuna una finalità distinta»[47].

Un punto interessante è relativo al titolare del trattamento: la dottrina, così come il Garante nazionale, hanno immediatamente segnalato la necessità che i dati siano affidati e gestiti esclusivamente da un soggetto pubblico, per due ordini di ragioni. In primo luogo perché, come avverte Ross Anderson, anche se si sceglie il tracciamento di prossimità e non la geolocalizzione, l'anonimato si ferma dove inizia la cura medica: «it's not about consent or anonymity, so much as being persuasive and having good bedside manner»[48]. In secondo luogo, perché nel momento in cui si autorizzasse un soggetto privato a gestire questo tipo di dati, «niente ci assicurerebbe che questa tracciatura non fosse utilizzata come merce di scambio contro denaro in una trattativa con i Google di turno, avidi di dati per alimentari i loro affari *data driven*»[49]. La Commissione europea, stante la natura dei dati in questione e le finalità del relativo trattamento, indica come soggetti più adeguati a svolgere il ruolo le autorità sanitarie[50].

Altro punto che pare indiscutibile è che nessuna conseguenza potrà derivare dal solo trattamento automatizzato di dati personali, cioè da una decisione presa esclusivamente da un algoritmo, senza un intervento umano. Si tratta ancora di un principio generale della *data protection*, contenuto all'art. 22.1 del GDPR, ai sensi del quale l'interessato (nel nostro caso, chi riceve un'allerta) «ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Vero è che tale principio può essere derogato, anche per i dati cd. sensibili e quindi per quelli relativi alla salute (co. 4), se l'interessato presta il consenso (art. 9.2, lett. *a)*) o se «il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri» (art. 9.2, lett. *g)*). Va tuttavia tenuto presente che l'ultima disposizione citata prosegue precisando che l'interesse pubblico rilevante deve «essere proporzionato alla

[47] Commissione UE, COM 2020/C 124/01, par. 3.6.
[48] R. ANDERSON, *Contact Tracing in the Real World*, cit., p. 1.
[49] G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *www.lacostituzione.info*, 1/04/2020, p. 5.
[50] Commissione UE, COM 2020/C 124/01, par. 3.1.

finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato»[51]. Qui il problema, evidenziato da tutti gli esperti del settore, è quello dei falsi positivi e, più in generale, della non affidabilità degli algoritmi, i quali sbagliano e non sono in grado di riconoscere i propri errori[52]. È quindi necessario l'intervento umano, a maggior ragione in una fase come quella della gestione delle conseguenze dell'allerta, a cui è auspicabile che non segua alcuna forma di imposizione: un eventuale obbligo di isolamento può pertanto derivare, in sostanza, solo da un accertamento medico.

Un ultimo aspetto rilevante, che ci si limita a menzionare perché su di esso convergono tutte le indicazioni istituzionali e tutte le analisi scientifiche (e perché non necessita di particolari spiegazioni) è la necessità che il codice della app sia *open source*, cioè pubblico e quindi sottoponibile a *peer review* per l'intera durata del suo utilizzo. Baiardi sottolinea, sul punto, che «la review deve analizzare il codice di tutto il sistema per la raccolta e gestione dei dati e non solo l'applicazione per lo smartphone», perché «dimenticare il back-office» – cioè l'infrastruttura hardware e software che gestisce i dati – «e focalizzarsi solo sull'adozione di una app open source può far trascurare problemi di sicurezza altrettanto importanti»[53].

4. Il contesto italiano

Venendo alla dimensione nazionale, il primo dato da rilevare è che la via italiana al *contact tracing* ha seguito un andamento a dir poco carsico[54]. Fino alla fine di aprile,

[51] Cfr. G. DE MINICO, *Virus e algoritmi*, cit., p. 4.

[52] Fabrizio Baiardi, riprendendo le considerazioni di Ross Anderson – il quale parte dall'osservazione per cui «Bluetooth also goes through plasterboard» (*Contact tracing in the Real World*, cit., p. 2) – fa l'esempio di «due stanze contigue ed una persona in ogni stanza. Non conoscendo il muro che divide le persone, una app può segnalare un contatto perché la distanza tra i cellulari è inferiore ad un valore di soglia o i due cellulari riescono a scambiarsi gli identificatori. Se le due stanze sono spazi pubblici dove si recano molte persone, ad esempio due ambulatori medici, il numero dei falsi positivi aumenta perché la app si comporta come se ogni medico avesse visitato tutti i pazienti. Se uno dei medici si ammala, solo il 50% dei contatti segnalati dalla app è avvenuto davvero»: F. BAIARDI, *App coronavirus e sicurezza informatica*, cit., p. 4 (della versione pdf-stampa).

[53] F. BAIARDI, *App coronavirus e sicurezza informatica*, cit., p. 2 (della versione pdf-stampa).

[54] Significativa l'analisi realizzata da Openpolis, *Coronavirus, chi decide durante lo stato di emergenza*, in *www.openpolis.it – Potere politico*, 07/05/2020.

infatti, il tema è emerso periodicamente nel dibattito pubblico solo tramite i media che, retroscena a parte, hanno spesso ripreso le posizioni del Garante per la privacy, cioè dell'unico soggetto istituzionale che ha svolto sin dall'inizio della vicenda una costante attività di divulgazione. Il gap di comunicazione ufficiale è stato parzialmente colmato dal Ministero dell'innovazione il 21 aprile, con la pubblicazione sul sito istituzionale di un *Aggiornamento sull'applicazione di contact tracing digitale per l'emergenza coronavirus*[55]. Il documento apre con una sorta di riepilogo della vicenda a partire dal 31 marzo, data del decreto di nomina dei gruppi di lavoro *data-driven* per l'emergenza COVID-19 (due delle famose *task force*)[56]; rende poi conto della *fast call for contribution* avviata dal Ministero per l'individuazione delle migliori soluzioni digitali (24-26 marzo), sfociata nell'ordinanza n. 10 del 16 aprile 2020 del Commissario straordinario per l'emergenza, con cui è stato stipulato il contratto con la società Bending Spoons S.p.a per l'acquisizione dell'app Immuni. L'*Aggiornamento*, nella parte finale, precisa inoltre che la società ha concluso il contratto «per spirito di solidarietà» e che, quindi, «ha concesso la licenza d'uso aperta, gratuita, perpetua e irrevocabile del codice sorgente e di tutte le componenti dell'applicazione; la società si è poi impegnata, sempre gratuitamente e pro bono, a completare gli sviluppi software necessari per la messa in esercizio del sistema nazionale di contact tracing»[57], rispettando così anche la previsione dell'art. 69 del Codice dell'Amministrazione Digitale (D. lgs. n. 82/2005, il cd. CAD). L'indicazione della scelta del Commissario straordinario per la app di Bending Spoons è preceduta, nell'*Aggiornamento* del Ministero, da una sommaria esposizione delle conclusioni del *Sottogruppo di lavoro sui principi giuridici* (il n. 8), la cui relazione è stata pubblicata, insieme alle altre, solo il 30 aprile, contestualmente all'adozione del decreto legge n. 28 del 2020.

Prima di concentrare l'attenzione sul decreto legge, va sottolineato che dalla cronologia appena illustrata emerge come tutta la documentazione "di supporto" alle scelte

[55] Il testo è pubblicato in *www.innovazione.gov.it – Notizie*.

[56] Il decreto ha istituito (art. 1) il Gruppo di lavoro data-driven per l'emergenza COVID-19 coordinato da Paolo De Rosa (co. 1), e articolato in otto sottogruppi (co. 2): 1) Coordinamento generale delle attività; 2) Infrastrutture e data collection; 3) Impatto economico; 4) Web data e impatto socio-economico; 5) Teleassistenza; 6) Tecnologie per il governo dell'emergenza; 7) Big data & AI for policies; 8) Profili giuridici della gestione dei dati connessa all'emergenza.

[57] MINISTERO PER L'INNOVAZIONE TECNOLOGICA, *Aggiornamento sull'applicazione di contact tracing digitale per l'emergenza coronavirus*, cit., p. 5.

politiche sia stata resa pubblica *dopo* che le scelte medesime sono state non solo prese, ma formalizzate; e questa osservazione vale anche per gli unici – almeno sinora – passaggi parlamentari della vicenda, cioè le audizioni svolte presso le commissioni competenti, che si sono tenute in via informale, quindi senza verbalizzazione[58]. Quest'ultima circostanza risulta particolarmente grave sia per il contesto, sia per l'oggetto delle audizioni, sia perché ha prodotto il paradossale risultato di intorbidire ulteriormente la comunicazione, dato che successivamente solo alcune audizioni sono state rese pubbliche (evidentemente per decisione degli auditi), in diversi formati, nelle sedi e con le tempistiche più varie[59]. Solo il 5 maggio, inoltre, sul sito del Ministero dell'innovazione tecnologica sono stati pubblicati il video e il testo dell'audizione informale svolta dalla Ministra il 29 aprile[60] in videoconferenza con la Commissione Lavori pubblici del Senato. Lo stesso rilievo in merito alla scarsa trasparenza (con particolare riferimento alla tempistica) vale per la documentazione: solo il 30 aprile, quindi a contratto concluso da qualche settimana e a decreto-legge pubblicato, è stato possibile leggere la raccomandazione del *Sottogruppo Tecnologie* (il n. 6), nelle cui conclusioni si scopre che le app selezionate erano in realtà due; e che il gruppo raccomandava di svolgere un test in parallelo di entrambe, «per avere la garanzia di poter disporre di almeno una soluzione da mettere in campo, anche quando si verificasse, in una sperimentazione concreta, il fallimento per qualunque motivo della funzionalità e/o dei livelli prestazionali richiesti dall'operazione alternativa»[61].

4.1. (segue) L'art. 6 del decreto-legge n. 28 del 2020

[58] Ci si riferisce alle audizioni informali svolte dalla IX Commissione (Trasporti, Poste e Telecomunicazioni) della Camera l'8 aprile 2020 e, per il Senato, dall'Ufficio di presidenza della 8° Commissione (Lavori pubblici e comunicazioni) il 29 aprile 2020 (di cui peraltro chi scrive non ha trovato traccia non solo nei verbali, ma nelle convocazioni della Commissione).

[59] A parte il caso dell'audizione della Ministra per l'Innovazione, di cui i media hanno parlato per una settimana prima che fosse possibile accedere a video e relazione (v. immediatamente nel testo), si rilevano i due estremi del Garante per la privacy, da un lato – che come d'abitudine ha pubblicato il testo dell'audizione nel proprio sito il giorno successivo al suo svolgimento – e dall'altro del Commissario straordinario all'emergenza Arcuri, la cui audizione (in formato video) è reperibile nella pagina Facebook del Corriere della Sera.

[60] Che in sostanza, oltre a una dettagliatissima cronologia delle attività svolte dalla Ministra, riprende i contenuti dell'*Aggiornamento* pubblicato la settimana precedente: v. *www.innovazione.gov.it*.

[61] *Report del Sottogruppo Tecnologie*, cit., p. 33.

La previsione normativa di fonte primaria per il *contact tracing* digitale – richiesta dal GDPR per il trattamento dei dati personali e sensibili in deroga ai limiti ordinari, da tutte le istituzioni europee e, comunque, imposta dalla riserva di legge in materia di diritti fondamentali della Costituzione italiana – è stata com'è noto inserita nell'art. 6 del decreto legge n. 28 del 30 aprile 2020, contenente per il resto misure in materia di giustizia[62].

La disposizione, che ha ricevuto il parere positivo del Garante della privacy[63], ricalca in sostanza – e in alcuni passaggi quasi letteralmente – le indicazioni in precedenza illustrate. Innanzitutto (co. 1), «al solo fine» di allertare le persone a rischio contagio e tutelarne la salute, viene istituita una «piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti» che hanno installato «su base volontaria», un'apposta app sui dispositivi di telefonia mobile. L'assenza di coercizione viene rafforzata dal successivo comma 4, ai sensi del quale il mancato utilizzo dell'app «non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento». Anche il requisito della gestione totalmente pubblica è garantito, dato che il titolare del trattamento dei dati è il Ministero della salute[64], la piattaforma «è di proprietà pubblica» ed è realizzata dal Commissario straordinario all'emergenza «esclusivamente con infrastrutture localizzate sul territorio nazionale» e gestite da Sogei e PagoPa (co. 5).

Per quanto riguarda l'applicazione vera e propria, il comma 2 dispone che il Ministro della salute, all'esito di una valutazione d'impatto costantemente aggiornata[65], sentito il

[62] Il decreto legge è intitolato *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*.

[63] Il Garante conclude che «il sistema di contact tracing prefigurato non appare in contrasto con i principi di protezione dei dati personali» e «auspica che tale misura sia idonea anche a superare il proliferare di iniziative analoghe in ambito pubblico, difficilmente compatibili con il quadro giuridico vigente»: v. *www.garanteprivacy.it – Attività e documenti*, provvedimento n. 79 del 29 aprile 2020, p.to 3.

[64] Che deve coordinarsi, sentito il Ministro per gli affari regionali, con una serie di altri soggetti pubblici: la Protezione civile, i soggetti attuatori individuati dal suo Capo Dipartimento con l'ordinanza di protezione civile n. 630 del 3 febbraio 2020, l'Istituto Superiore di Sanità e, anche per suo tramite, le strutture sanitarie pubbliche e private accreditate che operano nell'ambito del SSN. Curiosamente non è menzionato in questo comma il Commissario straordinario per l'emergenza, cui il comma 5 affida la realizzazione della piattaforma.

[65] Cui è tenuto, in qualità di titolare del trattamento, ex art. 35 del GDPR.

Garante per la privacy[66], «adotta misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati»[67]. Segue poi una serie di indicazioni specifiche, elencate per punti, con riferimenti espressi alle relative disposizioni del GDPR.

In primo luogo (lett. *a)*), gli utenti devono ricevere un'informativa chiara e trasparente, al fine di «raggiungere una piena consapevolezza» su finalità, operazioni di trattamento, tecniche di pseudonimizzazione, tempi di conservazione. La lettera *b)* prevede che «per impostazione predefinita» (*privacy by default*, art. 25 GDPR, in applicazione del principio di minimizzazione) i dati raccolti siano «esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19» in base a criteri stabiliti dal Ministro della salute, «nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti». Secondo la lett. *c)*, la tecnologia utilizzata dovrà essere il rilevamento di prossimità (il *Bluetooth Low Energy* - BLE), ed è «esclusa in ogni caso la geolocalizzazione»; i dati dovranno essere «resi anonimi, oppure, ove ciò non sia possibile, pesudonimizzati». Proprio in considerazione del fatto che l'anonimato non è imposto *di default*, la successiva lettera *d)* prescrive che devono essere garantite su base permanente riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi di trattamento, nonché «misure adeguate ad evitare il rischio di reidentificazione degli interessati». Per quanto riguarda il tempo di conservazione, la lettera *e)* prevede che i dati relativi ai contatti «siano conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento», la cui durata è determinata dal Ministero, e che i dati siano cancellati «in modo automatico alla scadenza del termine». Da ultimo, ai sensi della lettera *f)* i diritti degli interessati previsti dal GDPR possono essere esercitati anche in forma semplificata. Il riferimento espresso è agli articoli da 15 a 22 del GDPR: compreso, pertanto, il diritto a non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato (art. 22, su cui v. *supra*, par. 3.1).

L'articolo 6 specifica inoltre (co. 3) che i dati raccolti non possono essere trattati per modalità diverse da quelle indicate, salva la possibilità di utilizzo «in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca

[66] V. GDPR, art. 36.

[67] In ossequio al principio della *privacy by desing* e *by default*, di cui all'art. 25 del GDPR.

scientifica»[68] e che (co. 6) «tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi» alla data di cessazione del periodo di emergenza e comunque non oltre il 31 dicembre 2020. Entro la medesima data sono interrotti l'utilizzo dell'applicazione e della piattaforma, «nonché ogni trattamento di dati personali effettuato ai sensi del presente articolo».

Da ultimo, vale la pena segnalare che la clausola di copertura finanziaria, per una volta, non prevede la neutralità, ma stanzia a copertura degli oneri derivanti dall'implementazione della piattaforma la somma massima di 1.500.000 euro, cui si deve provvedere utilizzando le risorse assegnate per il 2020 al Commissario straordinario per l'emergenza (a valere sul Fondo emergenze nazionali previsto dal Codice della Protezione civile, il d. lgs. n. 1/2018, all'art. 44).

5. Le questioni aperte, aspettando il Parlamento

Nel momento in cui si chiudono queste riflessioni[69], il percorso parlamentare per la conversione del decreto-legge n. 28 del 2020 è appena agli inizi: il testo è stato assegnato alla Commissione 2ª (Giustizia) del Senato, che nella sua prima riunione ha tra l'altro deliberato una serie di audizioni (di nuovo informali), da parte dell'Ufficio di Presidenza e, per quanto riguarda il *contact tracing*, si è dichiarata in attesa della relazione che il Ministero per l'innovazione trasmetterà ai Presidenti delle Camere[70]. In attesa pertanto che l'iter della legge di conversione segua il suo corso, a mo' di conclusioni ci si limiterà a sottolineare alcune questioni aperte: alcune puntuali, relative al testo del decreto-legge, e una di sistema, che si ricollega alle considerazioni illustrate in apertura.

Partendo dal testo del decreto, meritano intanto segnalazione due incisi. Il primo è nella lettera *c)* del comma 2, nella parte in cui si legge che i dati di prossimità dei dispositivi sono resi anonimi o, «ove ciò non sia possibile, pseudonimizzati»: in pratica, dati riconducibili alla persona in un solo passaggio, ad esempio tramite una chiave di decrittazione. Non si tratta di un dato sorprendente, ed è peraltro il motivo per cui la disposizione esaminata si preoccupa di richiamare tutto lo strumentario di tutela del

[68] Anche in questo caso si tratta di una possibilità prevista direttamente dal GDPR: si tratta dell'art. 5.1 lett. *a)* e dell'art. 9.2 lett. *i)* e *j)*), cui la disposizione rinvia espressamente.

[69] 10 maggio 2020.

[70] Cfr. Senato, Comm. 2° Giustizia, res. somm. sed. 6 maggio 2020.

GDPR: se si trattasse di dati anonimi, il regolamento europeo non si applicherebbe (e verrebbe semmai in rilievo, per il profilo dell'accesso ai dispositivi, la direttiva cd. *E-Privacy*, la n. 58 del 2002). Se però si mette a sistema questo "dettaglio" con la previsione della lettera *a)*, relativa alla trasparenza delle informazioni da fornire agli utenti prima che scarichino la app, è bene tenere presente che una comunicazione pubblica fatta ai futuri utenti che escludesse *tout court* rischi di reidentificazione – e quindi per la privacy – non rispetterebbe quel requisito.

Il secondo inciso che suscita interesse all'occhio del giurista è quell'«anche» inserito nella lettera *e)* del comma 2, cioè la disposizione per cui il diario dei contatti è conservato «*anche* nei dispositivi mobili degli utenti»: par quindi di capire che, nonostante le dichiarazioni pubbliche di diversi esponenti politici, ancora non sia stata sciolta l'alternativa tra sistema centralizzato o decentralizzato di memorizzazione dei dati già illustrata (v. *supra*, par. 3). Anche in questo caso non si tratta di questione cruciale in sé: basti ricordare che l'EDPB non ha preso posizione sul punto, per concludere che non si è di fronte a una scelta dirimente per la tutela dei diritti. Anche qui, tuttavia, vale la riflessione appena fatta in merito alla trasparenza dell'informazione.

Ancora guardando al testo del decreto, merita segnalazione una mancanza, relativa all'*enforcement* delle disposizioni su cancellazione dei dati e loro eventuale uso illecito. Come rilevato anche dal Servizio Studi del Senato[71], in diverse occasioni di confronto con i parlamentari il Garante della privacy non solo ha sottolineato l'importanza fondamentale di un'efficacia temporale limitata della norma, ma ha anche suggerito di valutare la cancellazione dei dati nel caso in cui – all'esito dei controlli periodici previsti dal co. 2 – il sistema si riveli di scarsa utilità e, infine, di rinforzare con puntuali sanzioni la mancata cancellazione e l'eventuale uso illecito dei dati. Nessuna previsione di questo tipo compare nel testo del decreto-legge, e potrebbe quindi essere aggiunto in sede di conversione (finendo anche per rappresentare, si aggiunge, un test sia dell'approfondimento, sia della reale volontà di tutela degli utenti da parte dell'organo rappresentativo). A questo fine il Servizio Studi del Senato segnala anche

[71] V. SENATO - SERVIZIO STUDI, *Dossier 5 maggio 2020 - D.L. 28/2020 - A.S. n. 1786*, p. 63. Il Dossier è reperibile nella omonima sezione della scheda iter dell'atto, in *www.senato.it*.

come da valutare «l'opportunità di chiarire espressamente a chi competa assicurare la cancellazione dei dati personali trattati»[72].

Infine, una breve considerazione di sistema. Come si diceva in apertura, la pandemia da Covid-19 sta favorendo l'emersione di una questione molto più vasta, che nella sua massima estensione riguarda il rapporto tra la democrazia e le tecnologie digitali. Senza avventurarsi su temi che richiedono respiro, competenze e tempi di riflessione decisamente più ampi, e anzi limitandosi ad una prospettiva puntuale e concreta, la vicenda dell'app di tracciamento digitale – comunque vada a finire e al di là delle cronache[73] – sembra racchiudere in sé una parola chiave per il prossimo futuro: *consapevolezza*, in almeno tre declinazioni.

Sul brevissimo periodo, cioè per il contenimento dell'epidemia, va evidenziato che tutti gli studi, le linee guida e le relazioni menzionati nelle pagine che precedono convergono sull'avvertimento che la *consapevolezza* è la via per la fiducia; e che la fiducia è la pre-condizione per l'accettazione in chiave solidale, da parte dei singoli, dell'inevitabile (per quanto minimizzato) sacrificio dei propri diritti, su cui dovrebbero basarsi il download prima e l'uso costante poi di un app di *contact tracing*[74]. Per questo si insiste tanto sulla comunicazione e la strategia di presentazione[75], che dovrebbero essere volte alla creazione di un rapporto fiduciario e non basato esclusivamente sul timore della malattia o, all'estremo opposto, delle possibili sanzioni.

Ancora nell'emergenza, ma con lo sguardo al medio periodo, la *consapevolezza* dovrebbe poi essere pretesa dai cittadini nelle sedi istituzionali, a partire dal

[72] *Ibidem*.

[73] In questa sede si è scelto di non soffermarsi sulla cronaca mediatico-retroscenistica della scelta della app, in cui è recentemente intervenuto anche il Copasir, non tanto per l'impossibilità di rincorrere le notizie, quanto per la convinzione, già illustrata in premessa e su cui si tornerà tra breve, che si tratti di un dettaglio non indispensabile ai fini del ragionamento che si è cercato di svolgere. Discorso diverso sarebbe, ovviamente, se oggetto di analisi fossero i meccanismi decisionali, che tuttavia non possono essere chiaramente individuati finché l'intera vicenda non sarà conclusa.

[74] Ad esempio, «The EDPB firmly believes that, when processing of personal data is necessary for managing the Covid-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures»: EDPB, *Guidelines*, cit., p. 3

[75] È significativo che sul punto insistano i "tecnici" del Sottogruppo Tecnologie, il cui *Report* sottolinea – nell'ottica di un approccio europeo – che «ogni paese deve essere in grado di informare in modo trasparente i propri cittadini così da convincerli, senza usare imposizioni autoritarie, a partecipare volontariamente a tale sistema»: *Report del Sottogruppo Tecnologie*, cit., p. 6.

Parlamento. Se nelle prime fasi dell'emergenza poteva essere comprensibile un "passaggio per le vie brevi"[76], quando si iniziano a costruire precedenti normativi (di primo grado) sul modo in cui le tecnologie digitali sono autorizzate ad incidere sui diritti – e, si ribadisce, non solo quelli "digitali" – non dovrebbe considerarsi ammissibile che l'organo rappresentativo si nasconda dietro procedimenti informali e resoconti sommari[77], dai quali non è possibile nemmeno dedurre se i parlamentari stessi siano – appunto – consapevoli del materiale che stanno maneggiando. A ciò andrebbe aggiunta l'ulteriore consapevolezza, anche in questo caso evidenziata da tutti gli studi citati, che il Covid-19 non è un problema tecnologico[78], e che quindi il *contact tracing* andrebbe inserito in una strategia molto più ampia, basata innanzitutto sulla gestione sanitaria. Trattandosi del Parlamento italiano del 2020 i condizionali sono purtroppo d'obbligo, ma, anche alla luce dell'investimento economico, pare di poter affermare che in prospettiva i temi in esame somiglino sempre meno a un problema di *privacy*, e sempre più a una questione di *policy*.

Da ultimo, e sul medio-lungo periodo, la vicenda sinora esaminata inizia a delineare la *consapevolezza* come un tema di fondo che, partendo dalla tutela della privacy, sconfina nell'antitrust e nella disciplina delle comunicazioni, al punto da rendere ormai incerti i

[76] Sia consentita l'espressione a scopo puramente colloquiale, senza cioè prendere posizione in questa sede né sulla gestione dell'emergenza, né sui suoi tanti corollari, sui quali molti valenti studiosi stanno a tutt'oggi dibattendo.

[77] Non a caso la Commissione europea raccomanda (racc. Ue 2020/518, p.to 9) che «le autorità degli Stati membri e la Commissione dovrebbero garantire una comunicazione regolare, chiara e completa del pubblico in merito alle azioni intraprese a norma della presente raccomandazione e offrire al pubblico l'opportunità di interagire e partecipare alle discussioni».

[78] "The COVID-19 is not a technological problem" è il primo degli 11 punti stilati da *Algorithm Watch* nell'interessante documento *Automated decision-making systems and the fight against COVID-19 – our position*, pubblicato in *https://algorithmwatch.org/en/*, 02/04/2020. Da sottolineare anche, sul punto, la perplessità evidenziata dal *Sottogruppo sui profili giuridici*, secondo il quale, anche ammesso che la app sia scaricata e utilizzata da un numero sufficiente di persone, ciò «sarebbe, comunque, scarsamente produttivo degli effetti sperati qualora l'adozione di un'idonea soluzione tecnologica non fosse accompagnata da un'efficace organizzazione dei necessari presidi sanitari e dall'attività logistica necessaria, tra l'altro, alla distribuzione e esecuzione dei test tra i cittadini. Al riguardo occorre tenere presente – come risulta chiaro anche dalle esperienze straniere – che la componente tecnologica è, in ogni caso, "solo" una delle componenti di un sistema di contact tracing, inidonea, isolatamente considerata, a garantirne l'efficacia. […] Al riguardo non si dispone, allo stato, di elementi idonei a fondare alcuna valutazione sul punto con specifico riferimento alle soluzioni oggetto della call»: *Relazione del Sottogruppo Principi giuridici*, cit., p. 8.

confini non solo tra i settori disciplinari, ma anche tra area privatistica e pubblicistica[79]. Il ponte verso questa terza declinazione della consapevolezza sono i Big Data, il cui immenso valore economico rappresenta lo sfondo anche della vicenda del *contact tracing*: non si spiega altrimenti l'interesse immediatamente dimostrato dalle *Big Tech* sia nella collaborazione con enti di ricerca già menzionata[80], sia nello sviluppo dell'*Application Programming Interface* (API)[81] che consente di integrare app di *contact tracing* sui principali sistemi operativi degli smartphone (Android - Google e IoS - Apple)[82]. In questo senso, le Autorità garanti e la dottrina più attenta[83] segnalano come la consapevolezza degli utenti debba progressivamente allargarsi *dal valore dei dati personali* a *quello dei dati da loro prodotti anche in forma anonima*, in uno sforzo collettivo, saldamente radicato nelle basi dell'ordinamento costituzionale ma volto alla comprensione di un fenomeno tanto nuovo quanto impossibile da governare con gli strumenti attuali. Da questo punto di vista insomma – e con l'ovvio auspicio di non dover (più) ragionare nella logica dell'emergenza – la vicenda del Covid-19 è solo un inizio.

[79] Il tema è uno degli assi portanti dell'analisi svolta in AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui Big Data*, cit.

[80] V. *supra*, par. 2.1.

[81] Le API (*Application Programming Interface*, Interfaccia di programmazione delle applicazioni) sono sistemi ("librerie") che consentono a prodotti o servizi di interagire con altri prodotti o servizi senza bisogno di informazioni sulla loro implementazione, e semplificano quindi lo sviluppo delle app (con relativo risparmio in termini di costi e tempo). Specifico sul caso in esame. R. BERTI, A PELLICCIONE, *Tutti i problemi del* framework *Apple e Google contro il covid*, in *www.agendadigitale.eu*, 28/04/2020.

[82] V. ad es. R. ANGIUS, L. ZORLONI, *Ecco quanto fanno sul serio Apple e Google sul contact tracing*; L. ZORLONI, *Apple e Google dettano le regole per offrire la loro tecnologia di contact tracing*, entrambi in *www.wired.it*, rispettivamente 24/04/2020 e 04/05/2020; N. SANDON, A. VASTA, *Il contact tracing Apple e Google alla prova della normativa privacy Ue*, in *www.agendadigitale.eu*, 04/05/2020. Più in generale, v. ad es. B. CALDERINI, *Diritto alla portabilità: quanto valgono i nostri dati sfruttati dalle piattaforme digitali*, in *www.agendadigitale.eu*, 25/10/2019.

[83] Magistrale, sul tema, G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche.* Privacy e lex mercatoria, in *Dir. Pubblico,* 2019, n. 1, p. 89 ss., in cui l'Autrice svolge un tanto complesso quanto elegante ragionamento volto a individuare, tra l'altro, le condizioni alle quali «potremo contare in avvenire su individui divenuti *cives* consapevoli dei loro diritti nel contesto digitale, e meno consumatori ignari di beni del mercato *online*» (p. 114).