CONTACT TRACING E APP IMMUNI: ATTO SECONDO*

Di Dianora Poletti

SOMMARIO*: 1. L'utilità delle app di tracciamento per contrastare la diffusione del contagio da Covid-19. – 2. Le condizioni necessarie per il loro impiego. – 3. La compliance alla data protection della app Immuni. – 4. Segue. In particolare, il superamento dei contact tracing dilemma. – 5. Le ragioni della scarsa diffusione di Immuni. – 6. L'uso dei dati alla salute (e i relativi rischi) dopo il contact tracing. – 7. La «resilienza» del GDPR e la falsa alternativa tutela della salute/protezione dei dati – 8. Segue. La «responsabilizzazione» dell'utilizzatore.*

ABSTRACT. *La App Immuni, strumento di contract tracing digitale scelto dal Governo per contrastare la pandemia, non ha avuto il successo sperato. In questo scritto si provano ad individuare le ragioni della sua scarsa diffusione, che vanno oltre i problemi generati dalla protezione dei dati inerenti alla salute. L'esperienza della App Immuni consente anche di svolgere considerazioni più generali sulla tenuta del GDPR, sul rapporto pubblico-privato e sull'assunzione di responsabilità, per il raggiungimento di fini solidaristici, richiesta ai suoi possibili utilizzatori.*

The Immuni App, the digital contract tracing tool chosen by the Italian Government to fight the pandemic, did not have the expected success. The paper tries to identify the reasons for its low diffusion, which goes beyond the problems generated by the protection of health data. The experience of App Immuni also allows to accomplish more general considerations on the resilience of the GDPR solutions, on the public-private relationship and on the assumption of responsibility for the achievement of solidarity purposes, required for its possible users.

1. L'utilità delle app di tracciamento per contrastare la diffusione del contagio da Covid-19.

Una delle principali risposte delle autorità pubbliche alla situazione determinata dalla diffusione del Covid-19, che ha costretto una larga parte della popolazione mondiale a misurarsi con vantaggi e limiti della società digitale, è rappresentata dall'impiego di sistemi che combinano soluzioni tecnologiche e utilizzo dei dati, in specie dei dati inerenti alla salute.

In questo contesto, l'uso delle applicazioni *software* (app) di *contact tracing* da installare sullo *smartphone* è stato al centro di un particolare interesse e di un vivacissimo dibattito, capace di spaziare dalle ricostruzioni del loro funzionamento, esaminate soprattutto dall'angolatura della protezione dei dati personali, fino alle disposizioni costituzionali coinvolte dal loro utilizzo[1].

Soprattutto, ha posto all'attenzione degli studiosi della *data protection* (e non solo) la considerazione degli effetti di un impiego "su larga scala"–per usare una espressione del Regolamento generale sulla protezione dei dati personali UE/2016/679 (GDPR) – di una soluzione digitale per aiutare le iniziative volte al contenimento della diffusione del Covid-19. Questo scenario oltrepassa la dimensione interindividuale del rapporto medico (o struttura ospedaliera)-paziente che ha sempre connotato il trattamento di dati "particolari" come quelli alla salute e tratteggia un orizzonte più articolato e ancora più complesso.

Chi scrive aveva già dedicato qualche rilievo al tema[2]: il presente contributo può considerarsi una sorta di secondo atto, sollecitato dal concreto impiego di queste tecniche.

É certo che le app di *contact tracing* possano rivestire un ruolo significativo nella lotta alla diffusione del contagio, molto più del tracciamento manuale, agendo come strumento digitale di aiuto al distanziamento sociale. Come evidenziato dalla Circolare del Ministero della Salute del 29 maggio 2020[3], le applicazioni mobili per *contact tracing* offrono diversi vantaggi: non si basano sulla memoria della persona rivelatasi poi contagiata (che potrebbe trovarsi anche in condizioni di grave compromissione della salute al momento del colloquio); consentono di rintracciare contatti sconosciuti a tale persona (ad esempio passeggeri che si sono seduti vicini su un mezzo di trasporto); possono accelerare il processo di *contact tracing*; possono facilitare il *follow up* dei contatti da parte delle autorità sanitarie.

La stessa Commissione europea, nella raccomandazione UE/2020/518 rivolta l'8 aprile 2020 agli Stati membri sull'uso della tecnologia e dei dati ai fini di contrasto alla pandemia, ha riconosciuto espressamente che le app di tracciamento si collocano in quel «toolbox of practical measures» che è parso necessario approntare per contenere le infezioni da Covid-19. A distanza di pochi mesi da tale raccomandazione, il Consiglio d'Europa, nel suo report pubblicato nel mese di ottobre 2020 (Digital Solutions to Fight Covid-19) riconosce che «the use of mobile apps has been one of the main technologies used by governments and companies to contain the pandemic and serving many different purposes»[4].

2. Le condizioni necessarie per il loro impiego.

Due sono le condizioni che legittimano l'impiego delle app di tracciamento.

La prima è la loro previsione sulla base di una norma legislativa.

Sotto questo profilo appare necessario considerare che il retroterra del sistema di *contact tracing* non è rappresentato solo dal GDPR ma anche dalle norme della direttiva 2002/58/CE (c.d. direttiva *e-privacy*) e dunque dai principi di riservatezza delle comunicazioni elettroniche. Le Linee guida 04/2020 dell'EDPB sull'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'epidemia di COVID-19 del 21 aprile 2020 sono molto chiare al riguardo: posto che i dati relativi all'ubicazione sono raccolti da fornitori di servizi di comunicazione elettronica (come gli operatori di telecomunicazioni mobili), gli stessi possono essere utilizzati dall'operatore solo se resi anonimi o con il

---

* Il contributo rielabora e aggiorna la relazione svolta al webinar «Riflessioni giuridiche sugli effetti della pandemia», svoltosi nei giorni 12 e 13 giugno 2020 nell'ambito delle iniziative del Dottorato di ricerca in Scienze Giuridiche dell'Università di Pisa ed è destinato al volume dei relativi atti.

[1] In argomento v., tra altri, G. Resta, *La protezione dei dati personali nel diritto dell'emergenza Covid*-19, in *Giustiziacivile.com*, 5.05.20; V. Cuffaro-R. D'Orazio, *La protezione dei dati personali ai tempi dell'epidemia*, in *Corr. giur.*, 2020, 729 ss.; F. Pizzetti, *Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei garanti*, in *MediaLaws* 29.06.2020; G. Citarella, *Considerazioni sull'APP Immuni*, in Virus in fabula. *Diritti e Istituzioni ai tempi del covid-19*, a cura di G.P. Dolso, M.D. Ferrara, D. Rossi, Trieste, 2020, 371 ss.

[2] D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* in *questa Rivista*, 2020, 65 ss.

[3] Cfr. Circolare sulla "Ricerca e gestione dei contatti di casi Covid-19 (Contact Tracing) ed App Immuni".

[4] Cfr. 2020 *Data Protection Report* (*October* 2020), 17.

consenso dei singoli. Le misure legislative che possono essere dettate a tutela della sicurezza nazionale e pubblica devono essere «appropriate, strettamente proporzionate allo scopo perseguito, necessarie in una società democratica ed essere soggette ad idonee garanzie conformemente alla Convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali». Quanto al GDPR, l'EDPB ha chiarito che la base giuridica del trattamento va ravvisata nell'esecuzione di un compito di interesse pubblico di cui all'art. 6.1.e del GDPR. Secondo l'art. 6.3 la base giuridica di cui al 6.1. deve essere stabilita dal diritto dell'Unione o dello Stato membro: per questa ragione l'impiego della app per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento deve essere previsto per legge.

Alla luce di queste precisazioni va dunque considerata la norma di diritto interno che ha legittimato l'impiego della app di tracciamento, ossia l'art. 6 del decreto legislativo 30 aprile 2020 n. 28, convertito dalla legge n. 7 del 25 giugno 2020 e modificato dall'art. 2 lettere a) e b) del d.l. n. 125 del 7 ottobre 2020. Un'osservazione è subito d'obbligo: la norma appena citata non fa alcun riferimento alla app Immuni, selezionata come noto dopo la call avviata dal Ministero dell'Innovazione. I chiarimenti riguardo al funzionamento di questa app, l'indicazione delle finalità e delle fasi successive all'individuazione di un caso, persino le definizioni che riguardano la sua applicazione (come quelle di «contatto» e di «contatto stretto») sono contenute nella citata Circolare del Ministero della salute del 29 maggio 2020. L'affidamento della più specifica regolamentazione dell'uso di questo strumento ad una circolare ministeriale contribuisce indubbiamente a rafforzare il grande disordine delle fonti nell'epoca della pandemia. Anche i pareri dell'Autorità Garante per la protezione dei dati personali del 29 aprile 2010, n. 79 e del 1° giugno 2020, n. 95 hanno concorso a tracciare il quadro di operatività della app in questione.

La seconda imprescindibile condizione è l'esclusione di ogni obbligatorietà nell'utilizzo dell'app, che – oltre a porre problemi di coercibilità (come assicurarsi che l'utente viaggi portando sempre dietro il suo *smartphone*) – per una certa parte della popolazione avrebbe significato quanto meno obbligatorietà dell'acquisto del dispositivo sul quale fare funzionare l'applicazione e problematiche relative al controllo. Secondo l'EDPB, il monitoraggio su larga scala della localizzazione o dei contatti tra le persone rappresenta una grave intrusione della sfera privata delle persone, che può essere legittimata solo in base alla volontaria adozione da parte dell'utente per la specifica finalità.

La volontarietà reca in sé un forte richiamo alla responsabilità individuale, come si dirà in seguito. Si può comunque precisare che non sono mancate le opinioni sulla previsione della obbligatorietà, in nome della salvaguardia della salute collettiva[5]. Un passo in questa direzione è per vero già stato compiuto: nella lunga successione dei DPCM, da ultimo quello datato 3 dicembre 2020, con l'intento di rendere più efficace il *contact tracing* attraverso l'utilizzo dell'App Immuni, è stato previsto l'obbligo degli operatori sanitari dei dipartimenti di prevenzione delle aziende sanitarie locali, «accedendo al sistema centrale di Immuni, di caricare il codice chiave in presenza di un caso di positività»[6].

3. La *compliance* alla *data protection* della app Immuni.

A distanza di qualche mese dalla sua adozione, la app Immuni, realizzata dalla società Bending Spoons S.p.a., scelta dal Governo nell'aprile scorso, può essere analizzata con maggiore distacco rispetto alle concitate discussioni che hanno fatto seguito alla sua adozione[7].

Anzitutto deve subito precisarsi che i dubbi sui rischi per la protezione dei dati personali sono in gran parte fugati, dato che la app Immuni ha passato il vaglio della sua *compliance* alla normativa in tema di *data protection*.

L'art. 6 del decreto legislativo 30 aprile 2020 n. 28 sancisce, tra l'altro, la necessità di una adeguata e previa informativa che gli utenti devono ricevere prima di attivare la app, il tipo di dati raccolti, le finalità della raccolta, le tecniche di pseudonimizzazione utilizzate, i tempi di conservazione dei dati.

Risulta in particolare rispettato il principio di proporzionalità, concatenato a quello di minimizzazione. Posto che, in questa direzione, sarebbero stati sovrabbondanti i dati forniti da dispositivi di geolocalizzazione, che tracciano gli spostamenti delle persone, è stato scelto il meno invasivo sistema

[5] Secondo C. COLAPIETRO- A. IANNUZZI, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, 2020, 798, non apparirebbe preclusa la strada dell'obbligatorietà, in caso di scarsa copertura dell'utilizzo dell'app, in ragione della salvaguardia della salute collettiva e secondo un percorso simile rispetto a quello che ha condotto ad estendere il novero delle vaccinazioni obbligatorie.

[6] Cfr. l'art. 5 lett. b) DPCM del 3 dicembre 2020.

[7] Per la descrizione del funzionamento v. M. PLUTINO, "*Immuni*". *Un'*exposure notification app *alla prova del bilanciamento tra tutela dei diritti e interessi pubblici*, in *dirittifondamentali.it*, 2020, 563 ss.

BLE (*bluetooth* low *energy*) per inviare *alert* agli *smartphone*, utilizzando solo nel momento in cui un individuo viene trovato infetto a seguito di test diagnostici i dati di prossimità presenti sul suo terminale.

Il principio di minimizzazione impone a sua volta la massima accortezza sulla conservazione dei dati relativi ai contatti, che anche nei cellulari, sarà limitata al tempo strettamente necessario: l'utilizzo dell'applicazione e della piattaforma e i trattamenti dei dati personali saranno interrotti nel momento in cui sarà decretata la cessazione dello stato di emergenza e comunque non oltre il 31 dicembre 2021[8].

Sul funzionamento della app Immuni si è pronunziata l'Autorità garante della protezione dei dati personali, che – chiamata a esprimersi sulla compatibilità di Immuni con il quadro europeo e nazionale di protezione dei dati personali – con proprio provvedimento del 1° giugno 2020 ha autorizzato il Ministero della Salute ad avviare il trattamento, sulla base della proporzionalità emergente dalla valutazione d'impatto trasmessa dal Ministero stesso, ma con la prescrizione di alcune misure di sicurezza, relative in particolare: all'adeguata informativa all'utente in ordine al funzionamento dell'algoritmo di calcolo utilizzato per la valutazione del rischio di esposizione al contagio, alla «particolare attenzione» da dedicare all'informativa e al messaggio di allerta, considerato che l'uso del sistema è previsto anche da parte di minori ultra quattordicenni; alla previsione della possibilità di disattivare temporaneamente l'app; alla stretta commisurazione della conservazione degli indirizzi IP dei cellulari ai tempi strettamente necessari per il rilevamento di anomalie e di attacchi.

Anche il sottogruppo "Profili giuridici della gestione dei dati connessa all'emergenza" del Gruppo di lavoro *data-driven* per l'emergenza Covid 19 formato da 74 esperti nominati dal Ministero dell'Innovazione[9] ha valutato la App Immuni tra le più idonee a contrastare la diffusione del contagio, sia per la capacità di contribuire tempestivamente all'azione di contrasto del virus, sia per la conformità al modello europeo delineato dal Consorzio PEPP-PT (*Pan-European Privacy Preserving- Proximity Tracing*), menzionato anche dalla Commissione Europea.

All'indomani della sua adozione da parte del Governo anche chi scrive aveva segnalato profili critici, *in primis* la mancanza di riferimenti al tema dell'interoperabilità auspicato dall'approccio "paneuropeo", necessario per consentire applicazioni di tracciamento dei contatti tra persone che attraversano frontiere nazionali e per agevolare lo scambio di informazioni, al fine di affrontare le catene di trasmissione transfrontaliere. La modifica apportata dall'art. 2, comma 1, lettera a) del d.l. n. 125/20 al comma 3 dell'art. 6 d.l. n. 28/20 supplisce a questo, stabilendo che per le finalità determinate dal comma 1 della norma, previa valutazione d'impatto ai sensi dell'art. 35 del GDPR, «è consentita l'interoperabilità con le piattaforme che operano, con le medesime finalità, nel territorio dell'Unione europea». Con questa modifica potranno essere evitati approcci frammentati o non coordinabili ed eliminate le esternalità negative dovute all'uso di app con funzionamento diverso.

4. *Segue*. In particolare, il superamento dei *contact tracing dilemma*

Pure il "*contact tracing* dilemma" della centralizzazione (su un server unico) o delocalizzazione (sul dispositivo *smartphone* dell'utente) della raccolta dei dati, dopo un' intensa disputa che ha visto schierarsi due fazioni, può dirsi ormai superato.

Nel modello centralizzato dei dati è il server (centrale, per l'appunto) che attribuisce un codice specifico per ogni app scaricata sullo *smartphone* e mantiene un elenco di questi codici. Nel protocollo decentralizzato la crittografia-generazione delle chiavi è svolta direttamente dall'app del dispositivo e non dal server. Nel sistema decentralizzato solo il singolo è a conoscenza del contatto con il soggetto positivo; nel sistema centralizzato, invece, anche chi ha accesso ai dati del server conosce il dato relativo al numero dei contatti tra persone contagiate e sane[10].

L'EDPB e anche il Garante italiano si erano pronunziati in favore dell'adozione di un sistema

[8] V. la modifica apportata all'art. 6 del d.l. n. 28/2020 (che prevedeva inizialmente come termine ultimo il 31.12.2020) dall'art. 2 del d.l. n. 125/2020, convertito dalla l. 27.11.2020, n. 159. Segnalava l'inopportunità di indicare una data troppo breve già sapendo di doverla prorogare: E. Tosi, *App Immuni, tracciamento digitale, anonimato e GDPR: luci e ombre dell'art. 6 del d.l. 28/20*, in *Diritto mercato tecnologia*, 16.05.2020.

[9] In data 31.03.20 il Ministro per l'innovazione tecnologica e la digitalizzazione, in accordo con il Ministero della Salute, ha nominato la commissione di esperti per valutare e proporre soluzioni tecnologiche *data driven* e affrontare l'emergenza sanitaria, sociale e economica legata alla diffusione del virus SARS-CoV-2 sul territorio italiano. I componenti della *task force* sono stati scelti in collaborazione con il Ministero della Salute, l'Istituto Superiore di Sanità e l'Organizzazione Mondiale della Sanità tra componenti direttamente designati dall'Autorità garante della concorrenza e del mercato, dall'Autorità per le garanzie nelle comunicazioni e dal Garante per la protezione dei dati personali.

[10] Ulteriori considerazioni sul modello centralizzato o decentralizzato in D. Poletti, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza,* cit., 72 ss.

decentralizzato, considerato più rispettoso della normativa in tema di *Data Protection*. Pure la Risoluzione del parlamento europeo del 17 aprile 2020 si è orientata in questa direzione[11], posto che il sistema centralizzato è meno sicuro e più vulnerabile dal punto di vista di possibili attacchi esterni e richiede uno sforzo di protezione del server centrale.

Nell'art. 6 del d.l. n. 28/2020 si prevede l'istituzione di una piattaforma unica nazionale, di titolarità pubblica, per la gestione del sistema di allerta dei soggetti che hanno installato la app; nel comma 2, lettera e) la norma stabilisce che «*i dati relativi ai contatti stretti siano conservati anche nei dispositivi mobili degli utenti*» per il periodo strettamente necessario al trattamento, la cui «*durata è stabilita dal Ministero della salute*», che assume il ruolo di titolare del trattamento[12]. Va tra l'altro rilevato che il mantenimento dei dati sul terminale dell'utente è un tipo di attività che rientra tra quelle normate dall'articolo 5, par. 3, della direttiva *e-privacy*[13].

A prima lettura, non appariva dunque del tutto chiaro se l'app adottasse un sistema centralizzato o decentralizzato. Anche a seguito dei chiarimenti provenuti dal Ministero dell'Innovazione risulta che il sistema è decentralizzato; solo quando l'utente risulta positivo, il trattamento si centralizza, posto che l'utente stesso è invitato, con una opzione presente sulla app, a trasferire le sue chiavi anonime alla piattaforma ministeriale.

Il ricorso ad un sistema «che custodisce i registri delle interazioni sociali e degli ID randomici sui singoli *devices* e la comunicazione al server centrale dei dati solo in presenza di una reale esigenza»[14] è considerato idoneo a minimizzare il rischio del trattamento dei dati personali, posto che le autorità sanitarie hanno accesso soltanto ai dati di prossimità del dispositivo della persona infetta, in modo da potere contattare le persone a rischio di infezione, come richiesto dalle linee europee[15].

5. Le ragioni della scarsa diffusione di Immuni

Se oggi, dunque, il problema del *contact tracing* attraverso la app di tracciamento non è più il "rischio privacy"[16] o la funzionalità tecnica, occorre individuare le ragioni che non hanno decretato il successo che si pronosticava per Immuni.

Al momento in cui si scrive Immuni è stata scaricata da 10 milioni di italiani, con poco più di ottantamila notifiche inviate e quasi 7.000 casi di positività al virus riscontrati[17].

É stato precisato dagli esperti che la app avrebbe potuto soddisfare l'intento per cui il Governo ne ha propugnato l'impiego quando ad utilizzarla sarebbe stata una fetta consistente della popolazione e che tutto questo sarebbe derivato dal grado di penetrazione del suo impiego - motivato sia da fini egoistici (sapere di avere corso il rischio di contagio) sia da finalità altruistiche (evitare l'ulteriore diffusione ad altri del virus) - nonché dalla capacità di affermarsi come unica app di tracciamento.

L'intento di fare diventare la app uno strumento strategico per la lotta al contagio da Covid-19 dipendeva dunque e anzitutto dalla forza della comunicazione e dal grado di persuasione di campagne informative per l'adesione volontaria, volte ad evidenziare l'assenza di rischi per le informazioni rilasciate e soprattutto la comprovata utilità del suo impiego per contenere la diffusione dei contagi.

Nella concreta attuazione della app Immuni non hanno giovato alla sua ampia diffusione molti fattori: una comunicazione non puntuale, la non dimostrata piena attendibilità dei risultati, una valutazione d'impatto eseguita solo a seguito delle sollecitazioni del Garante, il tempo intercorso tra le prime

[11] Cfr. la Risoluzione del Parlamento europeo del 17 aprile 2020 sull'azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze, che chiedeva una memorizzazione dei dati «completamente decentralizzata».

[12] Il Ministero della Salute si coordinerà, come si legge nel comma 1, con tutta una serie di altri soggetti, a partire da quelli operanti nel servizio nazionale della protezione civile, i quali potranno assumere - in forza del rinvio operato all'articolo 28 GDPR - la veste di responsabili del trattamento. In generale, sui diversi ruoli dei soggetti contemplati nel GDPR v. A. MANTELERO, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.*, 2019, 2799 ss. o

[13] Il quale, dedicato alla «*Riservatezza delle comunicazioni*», precisa che «*gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento*». Sicuramente il trattamento in questione non rientra nell'esenzione della memorizzazione tecnica al fine di effettuare o facilitare la comunicazione prevista nella stessa norma.

[14] C. COLAPIETRO- A. IANNUZZI, *App di* contact tracing *e trattamento dei dati con algoritmi: la falsa alternativa tra tutela del diritto alla salute e protezione dei dati personali*, cit., 793.

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

[16] Esplicita in questo senso G. FINOCCHIARO, *Il punto sull'app Immuni: bilanciamento tra diritti*, in *Media Laws* 9.06.2020.

[17] Dati tratti dal sito Immuni il 18.12.2020. La recrudescenza del virus nel periodo autunnale ha incrementato il *download* dell'app, che nel periodo estivo era stato alquanto contenuto.

anticipazioni dell'uso della app (tra la fine di marzo e l'inizio di aprile 2020) e la possibilità di scaricarla, avvenuta a fine giugno 2020 (quando si era ormai aperta la c.d. fase 2, che aveva generato speranze di superamento dell'emergenza, tanto da generare il convincimento di una sostanziale inutilità della *app*), non ultimo il fatto che la app al suo esordio non funzionasse con sistemi operativi di alcuni cellulari. Nella fase di avvio ha pesato anche la contrarietà di alcune regioni, propense ad impiegare, rivendicando la loro autonomia decisionale, non una app nazionale, ma app "territoriali"[18], come pure la proliferazione di app diverse di *contact tracing* di carattere aziendale, sulla cui illegittimità, per mancanza di una norma di legge che ne giustifichi il loro uso, è intervenuto anche il Garante della protezione dei dati personali[19].

Tutto questo ha finito per generare un diffuso timore, quando non una certa insofferenza, di fronte all'uso di questo strumento "governativo"[20], che stride con il grande numero di aderenti, per esempio al servizio di Whatsapp o con l'assenza di remore all'uso di braccialetti *fitness*, ricettacolo di informazioni spesso sensibili. Alla piena, in molti casi inconsapevole, fiducia nelle app private si è contrapposta con evidenza la scarsa fiducia nella app pubblica.

Le ragioni del mancato successo vanno ricercate anche sul piano dell'efficienza. Le prime proiezioni sull'uso funzionale di Immuni prevedevano che per un ottimale funzionamento l'applicazione avrebbe dovuto essere utilizzata almeno dal 60% della popolazione. Anche considerando che da fonti successive si è appreso che tale soglia può essere più contenuta, si deve osservare che nel nostro Paese può incidere sulla soddisfacente diffusione un uso non capillare degli *smarthphone*, unito al non elevato grado di alfabetizzazione digitale. Non è difficile ipotizzare che tali dispositivi non siano usati proprio nella fascia della popolazione più anziana, che specie nella prima fase del contagio si è rivelata quella più esposta al rischio. Ma anche la popolazione immigrata irregolare e gli *homeless* (oltre ai bambini)[21] vanno ad ingrossare le fila dei soggetti esclusi dalla rete del tracciamento digitale, con il rischio di generare risvolti iniqui e di rafforzare il divario digitale, nella forma del *digital divide* cognitivo, che rischia di diventare anche «*divide* biologico»[22].

La modalità di funzionamento di Immuni, che consente di individuare coloro che l'hanno scaricata sul proprio *smartphone* tramite codici identificativi, affida ad algoritmi, sulla base di dati di prossimità, il calcolo della vicinanza di ogni contatto e il relativo tempo di esposizione al virus. Ciò può generare la creazione di falsi positivi e di falsi negativi: questo esito può ulteriormente dissuadere dall'uso dell'app. Inoltre, l'impiego non generalizzato dell'applicazione comporta che tra i contatti del soggetto risultato positivo potranno essere presenti e risultare contagiate persone che non hanno scaricato Immuni, le quali continueranno a favorire la diffusione della malattia.

L'esperienza applicativa ha altresì comprovato ciò che si era da più parti evidenziato, ossia la non ottimale integrazione con gli interventi di assistenza sanitaria (il c.d. *follow up* dei soggetti coinvolti dalle autorità sanitarie), necessaria per assicurare quel sistema integrato ritenuto indispensabile dalle autorità garanti europee ed italiana per un efficace funzionamento del dispositivo.

Era stato subito chiarito dagli osservatori che, per risultare efficace, il funzionamento dell'app doveva essere seguito da altri strumenti, come rapidi test diagnostici e soprattutto da interventi di operatori del sistema sanitario, anche per consentire la tracciabilità manuale dei contatti al fine di eliminare i casi dubbi. Tutto questo avrebbe evitato la soggezione a decisioni esclusivamente automatizzate, interamente affidate all'algoritmo, come richiesto dall'art. 22 del GDPR, consentendo la correzione di possibili imprecisioni e storture, dal rilevante impatto sulla salute e sulla libertà dei singoli, dovute all'impiego di informazioni inesatte.

La citata circolare del Ministero della salute del 29 maggio 2020, che – come sopra chiarito – ha finito per integrare la norma sui sistemi di allerta covid-19 dettata dal d.l. n. 28/2020, definisce i compiti dell'operatore sanitario di fronte a un utente di Immuni risultato positivo, tranquillizzando sulla presenza dell'intervento umano (ma post-allert) e chiarendo che il tracciamento tramite l'app Immuni «prevede una stretta collaborazione tra il cittadino, il medico di medicina generale, il pediatra di libera scelta e il dipartimento di prevenzione». Tuttavia, il ritardato svolgimento dei test diagnostici, specie del secondo tampone, le difficoltà operative del sistema sanitario, in alcuni momenti anche la carenza di disponibilità dei dispositivi ha sicuramente inciso su

[18] Si ricorda la app "AllertaLom" della Regione Lombardia (che tuttavia non è una app di tracciamento) o la app "SardegnaSicura", rilasciata su sistemi operativi Ios e Android: una specifica sezione di questa app riguarda proprio il tracciamento con il sistema della geolocalizzazione.

[19] V. il comunicato del 10 agosto 2020.

[20] Rileva la presenza di fattori psicologici avversi alla app in questione T. PERTOT, *Immuni e tracciamento digitale: la protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, in *Le nuove leggi civ. comm.*, 2010, 1149.

[21] G. RESTA, *La app 'Immuni': pregi e limiti del tracciamento digitale dei contatti*, in *MediaLaws* 15.06.2020.

[22] L. FLORIDI, *App coronavirus devono essere etiche o è meglio rinunciare*, in Agendadigitale.eu 5.05.2020.

un uso efficiente della app, per il timore degli utenti di rimanere magari inutilmente e a lungo in situazione di distanziamento sociale.

6. L'uso dei dati alla salute (e i relativi rischi) dopo il *contact tracing.*

Pur con le cautele adottate per minimizzare i rischi, nella fase di *contract tracing* il sistema opera con meccanismi di intelligenza artificiale e di *Big Data analitics*. Se il Governo ha ritenuto opportuno regolare dettagliatamente, con apposito decreto, le modalità tecniche di trasmissione dei dati da parte degli operatori sanitari alla componente di *backend* del Sistema di allerta Covid-19[23], non va dimenticato che Apple e Google hanno stretto un'inedita alleanza per aiutare le agenzie sanitarie pubbliche a ridurre la diffusione del contagio, facilitando l'uso della tecnologia *bluetooth* su un'ampia gamma di dispositivi mobili. Questo non esclude che l'incrocio «dei nuovi dati (anche solo quantitativi) con tutti gli altri dati che sono in loro possesso» possa trasformare «i dati aggregati ... con relativa facilità in dati personali»[24].

Ma anche la fase che segue l'invio dell'alert è apparsa oltremodo delicata, sia perché è con riguardo ad essa che si reidentifica il destinatario, e quindi i suoi dati sanitari, non più associati a una sequenza di numeri, tornano "in chiaro", sia perché si deve evitare la creazione di uno "status" di possibile contagiato, che dovrebbe postulare un accesso in tempi brevi ai test diagnostici. In assenza di tutto ciò, il rischio di limitare i diritti del cittadino che poi risulta non infetto risulterebbero elevati.

Appare evidente che, a questo riguardo, giochino un ruolo estremamente rilevante tre fattori: l'anonimato dei dati, il loro riuso e le loro modalità di conservazione.

La lettura del testo dell'art. 6 del d. l. 28/2020 solleva qualche rilievo sotto il primo profilo, posto che i termini «anonimizzazione» e «pseudonimizzazione» sono utilizzati con una certa indifferenza, quando è noto che i dati anonimi sono sottratti al diametro operativo del GDPR, mentre i dati pseudonimizzati, in quanto ricollegabili alla persona fisica, vi rientrano appieno[25]. Proprio con riferimento ai dati relativi all'ubicazione, l'EDPB ha precisato che occorre sempre privilegiare il trattamento di dati anonimi piuttosto che di dati personali, ma con un *caveat*, anzi due. Il primo è che i dati non possono essere resi anonimi isolatamente, il che significa che solo intere serie o interi insiemi di dati sono passibili di anonimizzazione. In tal senso, qualsiasi intervento su un dato isolato o sulla serie storica di dati riferibili a un singolo interessato può essere considerato, nel migliore dei casi, una pseudonimizzazione, con soggezione alla disciplina del GDPR. Il secondo è legato al fatto le «tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità [e] pertanto, in determinate circostanze, possono essere vulnerabili ai tentativi di re-identificazione». Da qui, la segnalata esigenza di utilizzare tecnologie "robuste" di anonimizzazione e di garantire la trasparenza per quanto attiene alla mgetodologia di anonimizzazione utilizzata.

La app Immuni tratta certamente dati pseudonimizzati. Come ha avuto modo di evidenziare il Garante per la protezione dei dati personali, «nel contesto del *contact tracing* lo scopo della pseudonimizzazione, in tal modo realizzata, è di consentire la distribuzione delle chiavi TEK (vale a dire il risultato della pseudonimizzazione) ai partecipanti al sistema ma non delle chiavi di co-decodifica (vale a dire l'informazione aggiuntiva) venendo a mancare la quale sarebbe impedita in radice ai partecipanti la possibilità di risalire all'identità di qualsiasi altro partecipante».

Rispetto al riuso delle informazioni, è il comma 3 dell'art. 6 a tracciare le coordinate. I dati raccolti non potranno essere trattati per finalità diverse da quelle indicate, salvo l'utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, finalità statistiche o di ricerca scientifica. In proposito il Garante per la protezione dei dati personali ha segnalato che dovrà essere assicurata la trasparenza del trattamento a fini statistico-epidemiologici dei dati raccolti e dovranno essere individuate modalità adeguate a proteggerli, evitan-

[23] Cfr. il decreto emanato in data 3.06.20 dal Ministero dell'Economia e delle Finanze, adottato di concerto con il Segretario generale del Ministero della Salute, che detta «Modalità tecniche per il coinvolgimento del Sistema tessera sanitaria ai fini dell'attuazione delle misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19».

[24] A. SANTOSUOSSO, *La regola, l'eccezione, la tecnologia*, in *Biolaw Journal*, 2020, 615, il quale appare fortemente critico di fronte alla segnalata totale mancanza di controllo su come Apple e Google incroceranno i nuovi dati e si interroga: «Ma anche se restassero ancora aggregati, il drenaggio di una tale grande quantità di dati avrebbe comunque un valore economico enorme. Era proprio necessario fare questo *cadeaux*»? Si può aggiungere che il parere della *task force* sulla app "Immuni" riconosce che per la parte server viene utilizzata la piattaforma *Google Cloud Platform*. La relazione (Gruppo di lavoro 8- Profili giuridici, Relazione proposta n. 100) si può consultare sul sito https://innovazione.gov.it/task-force-dati-le-relazioni-delleattivita-dei-gruppi-che-hanno-valutato-le-app.

[25] Sul tema v. l'opera di chiarificazione compiuta da E. PELLECCHIA, *Dati personali, anonimi, pseudonimi, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Le nuove leggi civ. comm.*, 2020, 360 ss.

do ogni forma di riassociazione a soggetti identificabili e adottando idonee misure di sicurezza e tecniche di anonimizzazione.

Quanto infine alla conservazione, occorrerà garantire che al termine dell'emergenza, a meno che questi dati possano contribuire, in forma anonima, ai progressi della ricerca scientifica, sia previsto un efficace sistema di loro cancellazione definitiva, per evitare rischi "postumi" per i diritti e le libertà fondamentali.

7. La «resilienza» del GDPR e la falsa alternativa tutela della salute/protezione dei dati.

Al di là della persistente utilità o meno della app Immuni per un immediato futuro che si spera presto governato dall'uso dei vaccini per contrastare la pandemia, è certo che la sperimentazione del *contact tracing* digitale nel periodo emergenziale abbia costituito l'occasione «per un buon esercizio di metodo», in vista della crescente diffusione di soluzioni tecnologiche nel pianeta-sanità[26]. Pur nel suo sostanziale insuccesso, tale esperienza ha invero generato dense problematiche che si proiettano su più fronti, e che costituiscono l'eredità che essa lascerà sul piano della riflessione scientifica.

Ad una retrospettiva generale, si riesce anzitutto a cogliere nell'architettura del sistema di tracciamento un quadro dal quale è emersa l'impossibilità del pubblico di sostituirsi al privato, il coinvolgimento di quest'ultimo in compiti che altri studiosi definirebbero di servizio universale[27] e il tentativo del potere pubblico di imporre al primo i valori che ogni servizio universale deve rispecchiare.

Ma anche riguardo al GDPR possono svolgersi alcune considerazioni, che riguardano la sufficienza/tenuta del GDPR nel rapporto con la normativa emergenziale e la verifica della sua capacità di "resilienza".

Il GDPR, strumento che si può criticare per la sua insufficienza di fronte alla "datificazione" della società e all'impiego crescente dell'intelligenza artificiale[28], ha al suo interno la flessibilità idonea a governare anche lo stato di emergenza, giocata sul necessario bilanciamento tra interessi e sulla mancanza di assolutezza del diritto alla protezione dei dati personali, anche dei dati sanitari: molti valori (tra questi, proprio la sicurezza pubblica e la salute collettiva) sono atti a operare un bilanciamento con questa tutela. Basterebbe ricordare, preceduti dal Considerando 46 che menziona espressamente la pandemia[29], l'art. 6, par. 1, specie lettere c) ed e) e l'art. 9, par. 2, lettere c), g), h), i) sulle basi giuridiche che legittimano il trattamento, rispettivamente dei dati «comuni» e dei dati «particolari», l'art. 23 riguardante le limitazioni legislative degli obblighi e dei diritti oppure considerare, per il diritto interno, l'art. 2 *sexies*, lettere u), v), z) del Codice privacy («Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevanti»).

Il GDPR contiene inoltre più di una disposizione in merito al trattamento dei dati relativi alla salute per perseguire scopi di ricerca scientifica, adatte a governare anche il contesto dell'emergenza generata dal Covid-19, per creare mappe epidemiologiche e documentare il percorso del contagio, e anche per operare trasferimenti transfrontalieri. Come ha chiarito l'*European Data Protection Board* (EDPB) nelle *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* adottate il 21 aprile 2020, l'articolo 49 del RGPD prevede alcune situazioni specifiche in cui il trasferimento di dati personali può avvenire in via eccezionale: «Con riguardo all'attuale crisi dovuta al COVID-19, possono trovare applicazione le deroghe di cui all'articolo 49, paragrafo 1, lettera d) (trasferimento necessario per importanti motivi di interesse pubblico) e lettera a) (consenso esplicito)».

Questo significa che la cornice entro la quale si deve operare è, in sintesi, quella segnata dai principi generali del GDPR, ossia i principi di proporzionalità, adeguatezza e minimizzazione rimarcati anche dalla giurisprudenza europea che indicano, dunque, l'esigenza di contenere l'utilizzo dei dati inerenti alla salute nella misura strettamente necessaria a perseguire fini di rilievo pubblicistico, con il minor sacrificio possibile per gli interessati, ai quali devo-

[26] T. PERTOT, *Immuni e tracciamento digitale: la protezione dei dati personali, problemi di efficacia e qualche prospettiva futura*, cit., 1164.

[27] Spunti interessanti in O. POLLICINO, *Una nuova applicazione mobile per Giustizia Insieme fa riflettere su distonie e utopie del rapporto tra tecnologia e società*, in *Giustizia insieme*, 18 aprile 2020, il quale evidenzia come le piattaforme digitali stiano fornendo in definitiva servizi essenziali di pubblica utilità.

[28] Sul punto cfr. F. PIZZETTI, *GDPR e Intelligenza Artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di* soft law *previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA, in Regolare la tecnologia. Il reg. UE 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, a cura di A. MANTELERO-D. POLETTI, Pisa, 2018, 69 ss.

[29] «...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 le l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie in particolare in casi di catastrofi di origine naturale e umana».

no essere in ogni caso mantenuti i diritti, in un arco temporale di riduzione delle garanzie esattamente delimitato.

Un trattamento indiscriminato, lontano dalle coordinate tracciate dal GDPR e giustificato dall'emergenza rischia di avere conseguenze pregiudizievoli anche nella fase post-emergenziale, trasformando ciò che è eccezionale in una "nuova normalità".

Questa è la direzione che ha guidato l'intervento del Garante italiano, in sintonia con i Garanti europei, i cui interventi si collocano nel solco di un accresciuto potere delle *Authorities* che l'epoca della pandemia ci ha consegnato[30].

Solo usando questa chiave sarà possibile arrivare a concludere che la tutela dei dati personali, mai come oggi, non deve essere considerata un feticcio da preservare in ogni caso (come è stata considerata da coloro che hanno ritenuto la protezione dei dati personali un intralcio al contenimento della pandemia[31]), ma, all'opposto, neppure un abito delle feste che, in tempi di pandemia (e, forse, nemmeno dopo), non è più consentito indossare.

Altra considerazione riguarda l'affidamento riposto nella tecnologia, una tecnologia nel caso di specie non del tutto matura o non sufficientemente sperimentata, alla quale si è chiesto di reagire molto velocemente a situazioni permeate di grande incertezza e di difficile previsione nel loro successivo andamento (come dimostrano i continui aggiustamenti che ha ricevuto l'app al suo esordio). La tecnologia si è rivelata incapace di sostituire l'intervento umano[32] e ha rivelato la necessità di accompagnarsi ad investimenti sul funzionamento del sistema sanitario, con la necessaria inversione della politica dei contenimenti della spesa pubblica che ha rivelato i suoi drammatici effetti, in tema di carenza di personale, specie nell'acme della pandemia.

Proprio questa complementarietà rappresenta, più in generale, la cifra del rapporto tra nuovi sistemi digitali e loro impiego per la soluzione di esigenze pubbliche o per il supporto al loro soddisfacimento. In questo momento storico diviene ancora più indispensabile rafforzare il dialogo tra diritto e tecnica per non affidare unicamente alla seconda poteri salvifici, ma per assumere decisioni sorrette da grande ponderatezza, equilibrio e anche lungimiranza.

8. *Segue.* La «responsabilizzazione» dell'utilizzatore.

Un'ulteriore riflessione riguarda il fondamentale elemento della volontarietà dell'uso di Immuni.

La decisione individuale di impiegare la app è espressione della libertà di autodeterminazione dell'individuo, il quale – a prescindere dalla riconduzione di questa manifestazione di volontà al consenso al trattamento[33] o meno – deve mantenere il controllo sui propri dati e deve essere messo in grado di conoscere le elaborazioni che, anche tramite algoritmi, di questi si compiono.

La fiducia[34] è ciò che supplisce alla mancanza di obbligatorietà nell'uso della applicazione: ma la fiducia aumenta solo se si garantisce ai cittadini una puntuale informazione, oltre a un trattamento corretto e trasparente dei dati. Non può non destare preoccupazioni per il Governo il fatto che neppure la titolarità pubblica della app, con esclusione del carattere proprietario dei sistemi informatici utilizzati allo scopo, unita alla loro natura di tecnologie *open access*[35], sia valsa ad accrescere l'affidamento della popolazione.

Precisato che il mancato uso non può generare effetti stigmatizzanti (come ha espressamente previsto il più volte citato art. 6, che ha assicurato

[30] F. Pizzetti, *Pandemia, Immuni e app di tracciamento tra GDPR ed evoluzione del ruolo dei garanti*, cit.

[31] Cfr. la provocazione di V. Zeno-Zencovich, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws* 26.05.2020, che si domanda: «di fronte a reati di gravissimo allarme come quello di terrorismo le istituzioni europee hanno gettato alle ortiche non solo la *privacy* ma anche un paio di secoli di garantismo penale da Beccaria in poi. Di fronte ad una pandemia che è concausa di almeno 500 volte più di morti e di incomparabili danni all'economia individuale e collettiva, la protezione dei dati personali deve regnare sovrana e intoccabile?».

[32] Richiamato con forza da L. Bolognini, *Il bilanciamento tra diritti, libertà e interessi pubblici nel* contact tracing *è questione di alta politica*, in *Medialaws* 21.05.2020

[33] Sulla natura del consenso al trattamento dei dati personali si rinvia a S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 2 ss.

[34] Sulla natura del consenso al trattamento dei dati personali si rinvia a S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 2 ss.
del sistema adottato di *contract tracing* digitale.

[35] Si legge nell'ordinanza n. 10 del 16 aprile 2020 del Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid19 che «Bending Spoons S.p.a., esclusivamente 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, al Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19 e alla Presidenza del Consiglio dei ministri, 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».

l'assenza di alcuna conseguenza pregiudizievole derivante dal non utilizzo), pena non solo la mancata installazione ma anche l'abbandono volontario e momentaneo del dispositivo, si pone la questione dell'impiego di incentivi. Dietro l'uso dell'app vi è la consapevolezza che lo stesso non può essere prefigurato come un presupposto necessario per fruire di certi servizi: l'ipotetica previsione che un soggetto "allertato" abbia la precedenza su uno non "allertato" nell'accesso al sistema di protezione sanitaria, specie in un periodo di numero contingentato di tamponi, altererebbe proprio quella parità di trattamento che la norma che ne prevede l'applicazione (art. 6 comma 4° del citato d.l. 30 aprile 2020, n. 28) intende assicurare.

La volontarietà reca in sé un forte richiamo alla responsabilità individuale. Più precisamente, la strategia pubblica di contrasto alla pandemia richiama un «ruolo cooperativo» dell'individuo/persona, che mette a disposizione i suoi dati per contribuire a realizzare uno scopo pubblico doveroso, di rilevanza costituzionale[36], disegnando nuovi confini nei rapporti tra pubblico e privato nella disciplina della *data protection*.

Come già si è scritto[37], l'uso di Immuni è dunque il risultato dell'assunzione di comportamenti responsabili sollecitati (in certo qual modo "imposti"), dall'esigenza di preservare non solo egoisticamente la nostra incolumità ma, altruisticamente, anche quella degli appartenenti alla nostra comunità.

La responsabilità "per altri" non rappresenta solo l'effetto indotto da una drammatica stagione, ma si annoda al dettato costituzionale della solidarietà sociale[38], che specifica anche il rapporto tra tutela della salute individuale e protezione della salute collettiva dell'art. 32 Cost., la quale permette di assegnare un fondamento giuridico alle scelte individuali, che si scoprono (o si riscoprono) poste all'interno di una rete di rapporti strettamente interconnessi, e non solo virtualmente.

Ad un ultimo aspetto vale almeno la pena di accennare. La regolazione dell'emergenza ha posto obblighi di comportamento in capo ai datori di lavoro[39] o ai dirigenti scolastici, per arginare l'espansione dei contagi nei due ambienti di maggiore contatto (il luogo di lavoro e la scuola), ma tutto da definire risulta il capitolo della mancata attuazione delle indicazioni post-allert, ossia dell'omesso invio del codice numerico (OTP) da parte dell'utente all'operatore sanitario e delle conseguenze connesse[40]. Di fronte a questo comportamento si può discutere se emerga non già la violazione dei doveri morali o sociali, ma un profilo di possibile responsabilità in senso proprio. Il danno da contagio, fino ad oggi analizzato nel caso delle vaccinazioni obbligatorie e delle emotrasfusioni, con un percorso per così dire verticale, in cui il danneggiante è l'autorità, dovrà probabilmente essere analizzato nell'immediato futuro anche nel suo andamento orizzontale, con riflessi, si immagina, sulla colpa e sul nesso di causa.

Tutto ciò conferma che la salvezza e il superamento della pandemia passano necessariamente dall'assunzione di contegni individuali, che il potere pubblico ha il dovere di spronare per arginare un flagello così devastante.

[36] C. CAMARDI-C. TABARRINI, Contract tracing *ed emergenza sanitaria. "Ordinario" e "Straordinario" nella disciplina del diritto al controllo dei dati personali*, in *La nuova giur. civ. comm.*, 2020, 38.

[37] Sia consentito rinviare a D. POLETTI, *Il trattamento dei dati inerenti alla salute nell'epoca della pandemia: cronaca dell'emergenza*, cit., 75 s.

[38] Parlano di «torpore dei doveri inderogabili di solidarietà politica, economica e sociale di cui la Carta costituzionale impone l'adempimento» di fronte alla mancata propensione delle persone e fornire i propri dati in un quadro di certe garanzie per il perseguimento di un interesse collettivo V. CUFFARO-R. D'ORAZIO, *La protezione dei dati personali ai tempi dell'epidemia*, cit., 738.

[39] In argomento P. ALBI, *Sicurezza sul lavoro e responsabilità del datore di lavoro nella fase della pandemia*, in *Il lav. nella giur.*, 2020, 1117 ss.

[40] Sul punto, considerazioni in G. RESTA, *La app 'Immuni': pregi e limiti del tracciamento digitale dei contatti*, cit.