

App di *contact tracing* e trattamento dei dati con algoritmi:

la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*

di

Carlo Colapietro e Antonio Iannuzzi*

SOMMARIO: 1. Premessa. – 2. Le tappe dello sviluppo dell'app e i principi che hanno guidato le valutazioni del Gruppo di lavoro *data driven*. – 3. La base giuridica per l'adozione dell'app. – 4. Brevi cenni sul funzionamento dell'app. – 5. Trasparenza dei lavori del Gruppo di lavoro *data driven*. – 6. Sulla necessità del trattamento da parte di un'app di *contact tracing*. – 7. Obbligatorietà vs. volontarietà. – 8. La falsa alternativa fra salute e protezione dei dati personali. – 9. Non solo app. Protezione dei dati personali e trattamento dei dati sanitari e genetici nell'emergenza COVID-19.

1. Premessa

Le misure di distanziamento sociale, che purtroppo ben conosciamo, non sono state l'unica risposta del Governo volta a contrastare la diffusione del COVID-19¹, ma c'è una gamma di soluzioni tecnologiche che sono in procinto di essere messe in campo, soprattutto per quanto concerne il monitoraggio del contagio. In particolare, è

* Benché il presente lavoro sia frutto della riflessione comune e della collaborazione dei due Autori, tuttavia, i paragrafi 1, 2, 3 e 4 sono stati redatti da Carlo Colapietro ed i paragrafi 5, 6, 7, 8 e 9 da Antonio Iannuzzi.

* Carlo Colapietro è Professore ordinario di Istituzioni di diritto pubblico presso l'Università degli Studi Roma Tre e componente del "Gruppo di lavoro *data-driven per l'emergenza COVID-19*" istituito presso il Ministero dell'innovazione tecnologica e la digitalizzazione. Antonio Iannuzzi è Professore associato di Istituzioni di diritto pubblico presso l'Università degli Studi Roma Tre e componente del "Gruppo di lavoro *data-driven per l'emergenza COVID-19*" istituito presso il Ministero dell'innovazione tecnologica e la digitalizzazione.

¹ Più in generale sull'emergenza COVID-19, cfr. V. BALDINI, *Emergenza sanitaria e Stato di prevenzione*, in *Dirittifondamentali.it*, 27 febbraio 2020; A. D'ALOIA, *Costituzione ed emergenza: l'esperienza del Coronavirus*, in *Biolaw Journal*, 14 marzo 2020; ID., *Postilla. Costituzione ed emergenza: verso la fine del tunnel, con qualche speranza e (ancora) con qualche dubbio*, *BioLaw Journal*, 2020; B. CARAVITA, *L'Italia ai tempi del coronavirus: rileggendo la Costituzione italiana*, in *Federalismi.it*, 18 marzo 2020; M. NOCELLI, *La lotta contro il coronavirus e il volto solidaristico del diritto alla salute*, in *Federalismi.it – Focus - Osservatorio Emergenza Covid-19*, 13 marzo 2020; A. IANNUZZI, *Leggi "science driven" e CoViD-19. Il rapporto fra politica e scienza nello stato di emergenza sanitaria*, in *BioLaw Journal*, 2020.

l'app Immuni che potrebbe fare la differenza, soprattutto in un frangente di progressivo allentamento dei limiti, come quello in corso. Eppure, la sua messa a disposizione, che può sì essere considerata celere rispetto a quanto avvenuto in altri Stati membri dell'Unione Europea, non è stata però così tempestiva come si sperava, dal momento che si è giunti fino alla prima decade di giugno². C'è da chiedersi, in proposito, se Immuni sarà ancora utile in questa successiva fase verso la quale l'Italia si sta avviando³ oppure se, per quando l'applicazione andrà a regime, saremo già in una fase successiva.

Ad ogni modo, è bene ripercorrere le tappe che hanno portato all'adozione dell'app e soffermarsi, in particolar modo, sul suo fondamento normativo e su qualcuno dei profili che più hanno acceso il dibattito pubblico, non ultimi quelli relativi alla protezione dei dati personali ed alla tutela della riservatezza.

Ebbene, alcuni Paesi, specialmente in Estremo Oriente, hanno già impiegato delle soluzioni *data driven* per contrastare la diffusione del coronavirus. Particolarmente noti sono i casi della Cina, della Corea del Sud e di Singapore, i quali hanno reagito anche tramite l'impiego delle più moderne tecnologie digitali, sebbene impiegando modelli molto diversi tra loro, specialmente dal punto di vista delle garanzie offerte alla tutela dei diritti fondamentali⁴. In realtà, i risultati promettenti ottenuti da questi Paesi non

² M. PLUTINO, "Immuni". Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici, in *Dirittifondamentali.it*, 26 maggio 2020, p. 605 evidenzia come già nelle prime tre settimane dalla riapertura del 4 maggio, sarebbe stato utile poter disporre dell'app, così come degli "accorgimenti organizzativi (per es. nei trasporti pubblici) e delle politiche sanitarie (test sierologici, strategie precise su tamponi, etc.) volte a minimizzare i rischi".

³ Critico sul punto V. ZENO-ZENCOVICH, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws*, 26 maggio 2020, secondo il quale, «la questione delle "app" di tracciamento appare questione probabilmente (ed auspicabilmente) superata dall'affievolirsi del virus e dei suoi contagi. Quel che resta sul tappeto come fondamentale esigenza di sistemi sanitari pubblici evoluti ed efficienti è quella della telemedicina, ovvero uso costante e generalizzato di strumenti digitali portatili (di cui lo smart-phone è l'espressione più ovvia) per monitorare a distanza e in tempo reale lo stato di salute soprattutto di soggetti a rischio. Per questo i dati relativi a stati morbili dovrebbero restare registrati nel fascicolo sanitario digitale di ciascuno, mentre quelli aggregati devono poter essere utilizzati per le preziosissime ricerche epidemiologiche che ci aiutino a capire cosa è successo in passato e come prevenire sciagure future».

⁴ G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, in *Giustizia Civile.com*, Editoriale del 5 maggio 2020, pp. 10 s., evidenzia come la soluzione cinese sia stata in realtà molto invasiva, dal momento che oltre che per finalità di diagnosi e di prevenzione, la tecnologia è stata impiegata anche per la repressione e il controllo di comportamenti

possono, però, essere attribuiti esclusivamente all'impiego della tecnologia, né tantomeno ai sistemi di sorveglianza sociale o all'apparato di misure repressive messe in campo, ma bisogna tener presente anche l'esperienza pregressa nel contrasto a fenomeni epidemiologici, acquisiti in seguito alla SARS del 2003⁵.

D'altra parte, risulta evidente che, attraverso la raccolta e l'analisi di dati, si può consentire alle istituzioni pubbliche di assumere le migliori decisioni, nonché di progettare le azioni più efficaci e di fornire servizi sempre più rispondenti ai bisogni ed alle necessità di cittadini ed imprese. Un tale risultato è evidente che può essere raggiunto soltanto con un approccio multidisciplinare al problema; pertanto la sfida è quella di mettere a punto dei sistemi che permettano contemporaneamente di monitorare in maniera efficace la diffusione del virus, proteggendo la *privacy* dei cittadini. E proprio con riguardo a quest'ultimo aspetto, occorre evidenziare un piccolo paradosso: da decenni ormai siamo disposti a rinunciare alla *privacy* relativa ai nostri dati per fruire di servizi apparentemente gratuiti, ma che, come noto a tutti, in realtà paghiamo in dati personali, mentre in questo momento di emergenza mondiale, in cui si tratta di arginare la pandemia, qualcuno solleva questioni relativamente a trattamenti di dati che sarebbero gestiti da strutture pubbliche e non da multinazionali private, che dall'analisi dei dati traggono profitto⁶.

Pertanto, il Ministro per l'innovazione tecnologica e la digitalizzazione in accordo con il Ministro della Salute, ha deciso di nominare un "Gruppo di lavoro *data driven* per l'emergenza COVID-19" – per valutare e proporre soluzioni tecnologiche e supportare il Governo e gli altri pubblici decisori nella definizione di politiche di contenimento del contagio da COVID-19 – composto da un contingente multidisciplinare di 74 esperti (giuristi, economisti, informatici, epidemiologi, sociologi

individuali, ad esempio, per il rispetto delle misure di isolamento fiduciario e quarantena; risulta, invece, meno invasiva la soluzione adottata da Singapore attraverso l'app *TraceTogether*.

⁵ Sul punto, cfr. ancora G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, cit., pp. 11 s.

⁶ Per quanto concerne quest'ultimo aspetto, si rinvia a V. ZENO-ZENCOVICH, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, cit., il quale sottolinea come il tema del monitoraggio sociale non avrebbe dovuto assurgere solo oggi agli onori del dibattito pubblico, considerando come da anni i dati personali siano oggetto di trattamento sia per finalità economiche, che anche per finalità di sicurezza.

e altri), scelti sulla base di una comprovata esperienza nelle rispettive discipline di riferimento⁷.

Tra le soluzioni tecnologiche prescelte c'è, appunto, l'app "Immuni", proposta dalla società Bending Spoons S.p.a., che è stata valutata tra le più idonee dal Gruppo di lavoro *data driven* sia per la capacità di contribuire tempestivamente all'azione di contrasto del virus, che per la conformità al modello europeo delineato dal Consorzio PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), citato anche dalla Commissione Europea⁸.

Non bisogna, infatti, dimenticare che per quanto riguarda il sistema di *contact tracing*, vi è stata prima una serie di atti di indirizzo da parte dell'Unione Europea, a cui ha fatto seguito l'iniziativa nazionale italiana.

Si segnalano, in proposito:

- 1) la raccomandazione dell'8 aprile 2020 della Commissione Europea, nella quale è stata affermata la necessità di adottare un *Toolbox* di misure condivise, che fossero coerenti con la normativa vigente;
- 2) La lettera del 14 aprile 2020 con la quale il Comitato Europeo per la Protezione dei Dati personali (European Data Protection Board – EDPB) si è rivolta alla Commissione, in procinto di adottare le Linee Guida;
- 3) Le Linee Guida della Commissione Europea del 16 aprile 2020, in cui, per quanto attiene all'utilizzo delle app di *contact tracing*, ci si richiama ai principi del GDPR, quali la proporzionalità, il consenso al trattamento, la minimizzazione dei dati;

⁷ Si tenga presente che la scelta è avvenuta in collaborazione con l'Istituto Superiore di Sanità e l'Organizzazione Mondiale della Sanità e con i 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.

⁸ Si tenga presente che «le specifiche tecniche del *contact tracing* sono state inizialmente individuate nell'ambito di vari progetti privati, o pubblico-privati, internazionali: oltre al Consorzio PEPPPT ([...] di cui fa parte l'aggiudicataria Bending Spoons), si rammenta anche DP-3T (sigla che sta per "*Decentralized Privacy-Preserving Proximity Tracing*", ovvero la soluzione di tracciamento proposta da un team di vari ricercatori con base in Svizzera) e ROBERT (sigla che sta per "*ROBust and privacy-presERving proximity Tracing protocol*" e che è stata promossa dall'Istituto francese per la ricerca nell'informatica e nell'automazione e dal *Fraunhofer AISEC*): così E. CREMONA, *Contact tracing. Governance pubblico-privata e primi problemi di tutela dei diritti fondamentali*, in *Ianus - diritto e finanza*, 21 maggio 2020, p. 5.

- 4) Le Linee Guida dell'EDPB del 21 aprile 2020, relative all'uso dei dati di localizzazione e degli strumenti di tracciamento dei contatti nel contesto dell'epidemia COVID-19.

È doveroso, inoltre, precisare che la società Bending Spoons ha deciso di concedere il codice sorgente e tutte le componenti applicative facenti parte del sistema di *contact tracing* 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 COVID-19 e alla Presidenza del Consiglio dei Ministri⁹, rendendosi disponibile a completare gli sviluppi informatici che si renderanno necessari per consentire la messa in esercizio del sistema nazionale di *contact tracing*.

2. Le tappe dello sviluppo dell'app e i principi che hanno guidato le valutazioni del Gruppo di lavoro *data driven*

Per quanto riguarda lo sviluppo di questo strumento digitale di *contact tracing*, è bene ricordare che, conformemente a quanto previsto dall'art. 122 del d.l. 17 marzo 2020, n. 18, convertito, con modificazioni, dalla legge 24 aprile 2020, n. 27, tale *software* va considerato alla stregua di un «bene strumentale utile a contenere e contrastare l'emergenza, o comunque necessario in relazione alle misure adottate per contrastarla».

Pertanto, tra il 23 e il 26 marzo 2020 è stata indetta una *fast call for contribution*¹⁰ diretta ad «individuare le migliori soluzioni digitali e tecnologiche disponibili per il

⁹ Il codice sorgente è stato messo a disposizione sul sito del Ministero per l'innovazione e la digitalizzazione: il 25 maggio u. s. è stata pubblicata una prima parte del codice sorgente relativa al "*front-end*", cioè la parte di applicazione che si interfaccia direttamente con gli utenti, a seguito della quale non sono mancate le polemiche, che si sono placate con la pubblicazione, il successivo 29 maggio, anche del codice "*back-end*" di Immuni.

¹⁰ Questa *fast call* è stata solo una delle iniziative adottate nell'ambito del progetto *Innova per l'Italia*, promosso da un'iniziativa congiunta del Ministro per l'innovazione tecnologica e la digitalizzazione, del Ministro dello Sviluppo Economico e del Ministro dell'Università e Ricerca, insieme a Invitalia ed a sostegno della struttura del Commissario Straordinario per l'emergenza Coronavirus, con il supporto tecnico di AgID. Si segnalano, infatti, sia l'ulteriore *fast call* relativa al reperimento di app e soluzioni tecniche di teleassistenza per pazienti domestici (sia per patologie legate a COVID-19, sia per altre patologie, anche di carattere croniche), che le altre tre *call for action*: per il reperimento di dispositivi di protezione individuale e respiratori artificiali; per la produzione di tamponi, elementi accessori e altri strumenti per la diagnosi facilitata e veloce; per lo sviluppo di tecnologie e strumenti per il contenimento, monitoraggio e contrasto alla diffusione del virus (per maggiori informazioni consultare il link <https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/03/24/innova-litalia-tecnologia-innovazione-lotta-al-coronavirus>). La valutazione delle proposte è stata affidata al Gruppo di

monitoraggio “attivo” del rischio di contagio, in vista dell’adozione, a livello nazionale, di tali soluzioni e tecnologie, al fine di migliorare i risultati in termini di monitoraggio e contrasto alla diffusione del COVID-19» (ordinanza del Commissario Straordinario per l'emergenza Coronavirus Arcuri n. 10/2020).

La valutazione delle proposte presentate da parte di privati, società ed enti, che hanno preso parte alla *call*, è stata affidata, appunto, al Gruppo di lavoro *data-driven* per l'emergenza COVID-19, che il Ministro per l'innovazione tecnologica e la digitalizzazione ha nominato il 31 marzo 2020. Le attività del Gruppo di lavoro sono state organizzate in otto sottogruppi, che si sono occupate dei più svariati aspetti¹¹, senza tralasciare la definizione dei profili giuridici per la gestione dei dati connessa all'emergenza.

Quest'ultimo sottogruppo, in particolare, si è occupato di valutare l'impatto delle soluzioni tecnologiche per quanto riguarda il rispetto della *privacy* e di altri diritti fondamentali, interagendo anche con il lavoro di altri gruppi, in particolare quello dedicato alla teleassistenza medica e quello dedicato alle tecnologie per il governo dell'emergenza. È stato, così, necessario studiare anche le dinamiche di funzionamento e le funzionalità tecniche, al fine di proporre dei rimedi per rendere le app più aderenti alle esigenze normative.

Certo è che il Gruppo di lavoro *data driven* per l'emergenza COVID-19 non ha ritenuto di dover abbandonare i principi generali del nostro ordinamento al fine di arginare la pandemia, ma anzi ha agito nella convinzione che «le tecnologie digitali e i dati potessero essere impiegati in maniera democratica, a beneficio della salute della collettività, nel rispetto delle libertà e dei diritti fondamentali».

Pertanto, l'azione del Gruppo di lavoro è stata ispirata sia al *principio di trasparenza* (ritenuto un pilastro fondamentale della nostra democrazia, che non può venire meno neppure nelle situazioni emergenziali, in cui anzi occorre dar conto con la massima trasparenza delle risorse tecnologiche e degli algoritmi impiegati), sia al

Lavoro costituito da Ministero della Salute, Istituto Superiore di Sanità, Organizzazione Mondiale della Sanità ed un Comitato scientifico interdisciplinare.

¹¹ 1) Coordinamento dei lavori; 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.

rispetto dei diritti fondamentali (che devono mantenere sempre la loro centralità, in quanto «in democrazia anche nelle emergenze le risposte straordinarie sono legittime proprio perché previste dal regime ordinario e dal quadro delle garanzie inviolabili»), nello spirito di un'*innovazione responsabile*, che coinvolge istituzioni pubbliche e soggetti privati chiamati a collaborare condividendo dati nel pieno rispetto dei diritti e delle libertà fondamentali, con l'intento di realizzare un *approccio data driven* di risposta all'emergenza sanitaria, utilizzando in ogni caso «un approccio etico e con al centro l'essere umano "by design"», tenendo bene a mente, nello svolgimento del lavoro, le domande relative ai valori umani e sociali che è doveroso preservare e perseguire.

In un certo senso, si può dire che il Gruppo di lavoro *data driven* per l'emergenza COVID-19 si è proposto di realizzare un "modello" di uso della tecnologia *human-centered*, in cui i diritti fondamentali dell'uomo fossero sempre e comunque garantiti, «evitando ogni compressione non necessaria e proporzionale delle libertà sulle quali è basata la nostra democrazia»; in particolare, si è avuto riguardo per il diritto alla protezione dei dati personali, la tutela del quale permette di essere cittadini, elettori e lavoratori liberi ed evita di «essere esposti a un potere incontrollabile, quale quello della sorveglianza di massa, della manipolazione politica e della persuasione commerciale»¹².

In totale, sono state valutate 319 proposte di soluzioni tecnologiche per il *contact tracing* e 504 per la telemedicina, ma la soluzione selezionata al termine di questo processo dal Ministro per l'Innovazione Tecnologica e la Digitalizzazione e dal Ministro della Salute è stata proprio l'app "Immun", risultata la soluzione più idonea per lo sviluppo del sistema nazionale di notifiche di esposizione digitale. Il risultato dei

¹² Le citazioni sono tratte dalla dichiarazione di intenti in cui i componenti del Gruppo di lavoro *data driven* per l'emergenza COVID-19 hanno formulato i principi ai quali si sono impegnati ad improntare la propria attività, ritenendo che «l'attuale situazione emergenziale vada fronteggiata sempre nel rispetto della normativa vigente e dei principi generali dell'ordinamento italiano ed internazionale», soprattutto con riferimento alla tutela della *privacy* ed alla protezione dei dati personali. Del resto, lo stesso Ministro per l'innovazione tecnologica e la digitalizzazione, Paola Pisano, ha a più riprese sottolineato che «la tecnologia non è neutra», il suo valore dipende da come la si sviluppa ed applica, pertanto, per essere un vero motore di cambiamento per la nostra società, deve essere «etica, trasparente, sicura e inclusiva» e, soprattutto, deve mettere al centro sempre e prima di tutto l'Uomo e «la scelta e l'adozione delle nuove tecnologie, anche di quelle legate all'intelligenza artificiale, deve tassativamente essere funzionale alle sue esigenze» (P. PISANO, *Intelligenza artificiale ed etica: una rivoluzione umana, molto umana*, Redazione ANSA Roma del 7 maggio 2020).

lavori del Gruppo *data driven* per l'emergenza COVID-19 è stato già comunicato il 10 aprile al Presidente del Consiglio dei Ministri, che in quello stesso giorno ha chiesto al Commissario straordinario Arcuri di procedere rapidamente a valutare le modalità con cui dare attuazione alla proposta di implementazione del sistema di *contact tracing* digitale. Queste ultime sono state individuate con l'ordinanza del 16 aprile 2020, n. 10, la quale disponeva la stipula del contratto con la società sviluppatrice della soluzione "Immunì".

Ciò nonostante, si è dovuto attendere ancora per fruire dell'app, tant'è che è proseguita fino ad oggi la polemica relativamente a questo ritardo inspiegabile agli occhi dell'opinione pubblica¹³, tanto da indurre lo stesso Ministro per l'innovazione tecnologica e la digitalizzazione, Paola Pisano, ad intervenire sul punto nell'audizione presso la Camera dei Deputati (IX Commissione) del 3 giugno u. s., sottolineando che l'Italia è «il primo Paese europeo di grandi dimensioni a dotarsi di uno strumento del genere a livello nazionale», il che ci costringe a fare i conti con la realtà, per «corrispondere al nostro dovere di rispettare le normative italiane ed europea sulla tutela della privacy delle persone e le esigenze di sicurezza del nostro Paese», dal momento che «non possiamo nasconderci che uno Stato ha e deve avere, in materia, più doveri rispetto a un privato».

¹³ Occorre evidenziare che, benché alla c.d. *Task Force Covid-19* fosse stato affidato il compito di procedere in tempi rapidi alla valutazione delle proposte formulate dai partecipanti alla *fast call*, al fine di selezionare la proposta più efficace e idonea ad essere implementata in tempi rapidi a livello nazionale, l'adozione dell'app è stata certamente più lenta di quanto avrebbe dovuto. Relativamente a questo aspetto, si può probabilmente presumere che sia stato dovuto ai tempi tecnici di rilascio dell'aggiornamento delle API - *Application Program Interface*, cioè l'interfaccia di programmazione, che consentono l'interoperabilità fra i dispositivi - da parte di Apple e Google. Come ricordato, infatti, anche da M. PLUTINO, "Immunì". *Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, cit., p. 602 «le due *big tech* proprietarie dei sistemi operativi hanno stretto una (inedita) alleanza per allineare i sistemi *bluetooth* ai rispettivi sistemi operativi mobili e su quel "*framework*" hanno proceduto a concludere accordi con i vari governi per mettere a disposizione le proprie soluzioni per una implementazione ottimale delle app nazionali, anche in tal caso stabilendo la natura *open source* di queste API [...] dove nome, aspetto, interfaccia e dinamiche di funzionamento sono ampiamente personalizzabili dal programmatore. Ciò ha portato ad una radicale riorganizzazione delle app, le quali in prospettiva potrebbero essere addirittura superate, con necessità peraltro di affrontare gli aspetti legali della questione, che si ritrovano una più o meno necessaria interposizione di interfacce che integrano meglio l'app nel sistema operativo. Queste API d'altro canto interagiscono in modo ottimale solo con applicazioni che adottano il sistema di gestione dei dati decentralizzato. Una soluzione tecnica tra l'altro preferita (a scanso di un primo orientamento) dall'Unione europea in quanto foriera di minori rischi perché evita concentrazioni di dati in server, per quanto pubblici, ed ormai praticamente obbligata».

3. La base giuridica per l'adozione dell'app

Uno dei problemi generati dalla necessità di utilizzare un'applicazione mobile per il contrasto alla diffusione del virus è stato causato dall'individuazione una valida base giuridica per la sua adozione, alla quale si è addivenuti soltanto con il del d.l. 30 aprile 2020, n. 28.

Sebbene, infatti, per quanto riguarda il trattamento dei dati personali necessario per le operazioni di *contact tracing*, un fondamento di legittimità poteva in buona parte essere individuato nel diritto eurounitario, fino all'emanazione del d.l. n. 28/2020 restavano aperte diverse questioni sulla quale si è reso necessario un intervento esplicito del legislatore.

Del resto, la stessa Carta di Nizza prevede all'art. 52 che, nel rispetto del principio di proporzionalità e qualora esse «rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui», possano essere adottate delle limitazioni all'esercizio dei diritti e delle libertà, le quali però «devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà».

Orbene, era necessario effettuare una scelta tra due modelli, relativamente alla base giuridica del trattamento: o fondare il presupposto di legittimità dei trattamenti sul consenso dell'interessato, conformemente a quanto previsto dall'art. 5 della risalente Direttiva CE 2002/58, c.d. Direttiva *e-privacy*¹⁴, e degli artt. 6 e 9 del Regolamento UE 2016/679, c.d. GDPR, da esprimere al momento dell'installazione dell'app; oppure ricorrere all'interesse pubblico, alla stregua di quanto sancito dall'art. 6, par.1, lett. d) ed e), e dall'art. 9, par. 2, lett. i) del GDPR e dall'art. 15 della Direttiva *e-privacy*¹⁵.

¹⁴ Purtroppo, ancora tarda l'adozione del c.d. Regolamento *e-privacy*, relativamente al quale si rimanda a G. SCORZA, *Prospettive de iure condendo della protezione dei dati personali nel settore delle comunicazioni elettroniche, tra Regolamento generale 2016/679 e futuro Regolamento e-Privacy*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017, pp. 741 ss.

¹⁵ G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, cit., pp. 15 ss. preferisce questa seconda posizione, ricordando come il Comitato europeo della protezione dei dati si fosse espresso in questa direzione, con l'affermazione dell'opportunità «di fondare il trattamento non già sulla base giuridica del consenso dell'interessato, bensì su quella

La decisione italiana si è orientato verso questa secondo ipotesi, ma non era possibile fondarsi sulla normativa già esistente, in quanto occorreva stabilire le modalità operative, i limiti e le garanzie per i diritti degli interessati, oltre che regolare altri aspetti quali, ad esempio, quelli relativi all'informativa, la comunicazione dei dati, il periodo di conservazioni dei dati¹⁶.

Infatti, l'art. 14 del d.l. 9 marzo 2020, n. 14, rubricato «*Disposizioni su trattamento dei dati personali nel contesto emergenziale*», non poteva fungere da presupposto normativo per l'adozione dell'app Immuni, ma serviva una specifica norma di rango primario¹⁷.

Al riguardo, si tenga presente che tale norma era nata con tutt'altro spirito, atteso che la sua funzione era quella di riformulare la disposizione di cui all'art. 5 dell'ordinanza del Dipartimento di protezione civile 3 febbraio 2020¹⁸, spostando in una fonte di livello superiore tale previsione normativa, dedicata a garantire un'efficace gestione dei flussi e dell'interscambio di dati personali attraverso

dell'adempimento di un compito nell'interesse pubblico (EDPB, *Guidance 4/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, punti 29 e 33)». Sull'interesse pubblico come base giuridica del trattamento v. M. MIDIRI, S. PIVA, *L'interesse pubblico come base giuridica e come finalità del trattamento dei dati personali*, in S. SCAGLIARINI (a cura di), *Il "nuovo" codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. n. 101/2018*, Torino, 2019, pp. 21 ss.

¹⁶ G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, cit., p. 16.

¹⁷ In senso contrario si era espresso F.P. MICOZZI, *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, 2020, p. 6, secondo il quale «non si ravvisano – quantomeno nella vigenza del D.L. n. 14/2020 – ostacoli particolari a che i già menzionati soggetti, deputati alla gestione dell'emergenza, possano trattare i dati personali dei contagiati (anche provenienti da terze parti) al fine di effettuare attività di *contact tracing* utile a delineare i contorni del fenomeno virale». Anche il Presidente del Garante della protezione dei dati personali nel corso di un'audizione informale aveva auspicato «una norma di rango primario, (anche un decreto-legge, che assicura la tempestività dell'intervento, pur non omettendo il sindacato parlamentare né quello successivo di costituzionalità, diversamente dalle ordinanze)». Benché subordinatamente, ove non si fosse proceduto a un intervento legislativo *ad hoc*, aveva sostenuto l'opportunità di «integrare l'art. 14 d.l. n. 14/20, anche con misure di garanzia da prevedersi eventualmente con fonte subordinata» (Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus, reperibile al seguente link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9308774>).

¹⁸ Adottata con parere favorevole del Garante della protezione dei dati personali; cfr. *Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, adottato con provvedimento 2 febbraio 2020, n.15 [doc web n. 9265883].

trattamenti di dati personali anche appartenenti a categorie particolari, necessari per adempiere alle funzioni di protezione civile nel contesto emergenziale¹⁹.

Così, in virtù dell'art. 14 del d.l. n. 14/2020, sono state ribadite una serie di disposizioni riguardanti il trattamento di dati personali, sia comuni che particolari, da parte di soggetti pubblici e privati che operano nell'ambito del Servizio sanitario nazionale, nonché la loro comunicazione ad altri soggetti pubblici; nella norma è stabilito che essi devono avvenire nel rispetto dell'art. 5 del Regolamento UE 2016/679, ma che il conferimento di incarichi di trattamento ai sensi dell'art. 2-*quaterdecies* del d.lgs. n. 196/2003 può avvenire con modalità semplificate, anche oralmente, così come anche l'informativa privacy può essere resa in forma semplificata o, addirittura, omessa.

Tuttavia, è evidente tale norma non poteva essere considerata idonea quale base giuridica per l'adozione dell'app Immuni, dal momento che nulla disponeva in materia di applicazione mobile e di *contact tracing*.

Pertanto, è solo con l'art. 6 del predetto d.l. n. 28/2020 – adottato udito il parere del Garante per la protezione dei dati personali²⁰ e rubricato appunto «*Sistema di allerta Covid-19*» – che si è finalmente addivenuti all'introduzione del presupposto legale per l'utilizzo dell'app, con l'adozione di una norma primaria volta ad introdurre una specifica disciplina delle modalità di funzionamento dell'app e del relativo trattamento dei dati, al fine di assicurare, in modo forte e univoco, i presupposti di *privacy*, sicurezza e funzionamento dell'applicazione.

Tale norma, infatti, «al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19» ha istituito una piattaforma unica nazionale per gestire il «sistema di

¹⁹ Per una ricostruzione completa e puntuale cfr. G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza COVID-19*, cit., 5 ss., il quale osserva, in particolare come «tale disposizione, nel preconstituire un'autonoma base giuridica per il trattamento legittimo dei dati particolari e nel prevedere modalità affievolite di tutela, illustra bene come, nel diritto dell'emergenza, fonti normative secondarie siano state abilitate a apportare limitazioni anche profonde a libertà fondamentali in nome del supremo interesse della tutela della salute e ovviamente nei limiti della proporzionalità».

²⁰ Cfr. il *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19* - 29 aprile 2020, provvedimento del 29 aprile 2020, n. 79 [doc. web n. 9328050].

allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione (cioè Immuni) sui dispositivi di telefonia mobile». Lo stesso articolo chiarisce, altresì, al comma 4, che «il mancato utilizzo dell'applicazione [...] non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento».

La norma individua il Ministero della salute quale titolare del trattamento di dati personali, il quale è tenuto a coordinarsi, sentito il Ministro per gli affari regionali e le autonomie, con una serie di altri soggetti istituzionali, qualificabili come responsabili del trattamento *ex art. 28 del GDPR*²¹. Il comma 2 dell'art. 6 prevede, inoltre, che il Ministero della salute debba svolgere una valutazione di impatto *ex art. 35 del GDPR*, da tenere «costantemente aggiornata», e debba, altresì, approntare le «misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi elevati per i diritti e le libertà degli interessati», dopo aver proceduto alla consultazione preventiva del Garante per la protezione dei dati personali²², conformemente all'art. 36, par. 5 del *GDPR*²³.

In particolare, la lettera dell'art. 6 richiede che il Ministero della Salute:

- a) fornisca l'informativa *privacy ex artt 13 e 14 del GDPR* agli utenti prima dell'attivazione dell'applicazione, dando «informazioni chiare e

²¹ In particolare, la norma stabilisce che il Ministro della Salute «si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, con i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e con i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché con l'Istituto superiore di sanità e, anche per il tramite del Sistema Tessera Sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID-19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura».

²² Al riguardo, il Garante per la protezione dei dati personali si è espresso con il *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19* del 1 giugno 2020, n. 95 [doc. web n. 9356568]; cfr. anche *Valutazione d'impatto sulla protezione dei dati personali presentata dal Ministero della Salute relativa ai trattamenti effettuati nell'ambito del sistema di allerta Covid-19 denominato "Immuni" - Nota sugli aspetti tecnologici* del 3 giugno 2020 [doc. web n. 9357972].

²³ Il quale stabilisce espressamente che «il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica».

trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati»;

b) assicuri la *privacy by design* di cui all'art. 25 del GDPR, garantendo che «i dati personali raccolti dall'applicazione di cui al comma 1 siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, individuati secondo criteri stabiliti dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti»;

c) provveda a effettuare il trattamento dei dati basandosi sui dati di prossimità dei dispositivi, «resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati», escludendo categoricamente la geolocalizzazione dei singoli utenti;

d) garantisca non solo «la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento», ma anche «misure adeguate ad evitare il rischio di reidentificazione degli interessati cui si riferiscono i dati pseudonimizzati oggetto di trattamento»;

e) limiti il periodo di conservazione dei dati nei dispositivi mobili degli utenti «per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute», provvedendo alla cancellazione dei dati in modo automatico alla scadenza del termine;

f) assicuri l'esercizio dei diritti degli interessati di cui agli artt. 15-22 del GDPR, anche con modalità semplificate.

Il comma 3 dell'art. 6 stabilisce, inoltre, che i dati raccolti attraverso l'applicazione «non possono essere trattati per finalità diverse da quella di cui al medesimo comma 1», a meno che non vengano utilizzati in forma aggregata o comunque anonima, «per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, ai sensi degli articoli 5, paragrafo 1, lettera a) e 9, paragrafo 2, lettere i) e j), del Regolamento (UE) 2016/679».

Per di più, è previsto che l'utilizzo dell'applicazione, della piattaforma e di ogni trattamento di dati personali relativo al sistema di allerta COVID-19 vengano interrotti «alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020»; entro la stessa data, tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi.

Infine, occorre notare che la norma puntualizza che la piattaforma di gestione del sistema è di titolarità pubblica ed è realizzata dal Commissario straordinario di governo per l'attuazione e il coordinamento delle misure occorrenti per il contenimento e contrasto dell'emergenza epidemiologica COVID-19²⁴, attraverso infrastrutture localizzate sul territorio nazionale e gestite «per quanto riguarda i profili attinenti ai dati dalla "Sogei", società *in house* del Ministero dell'Economia, e per quanto riguarda la tecnologia sottostante all'app da "Pago s.p.a.", interamente partecipata dallo Stato, realizzatrice dell'infrastruttura PagoPa (sistema nazionale dei pagamenti a favore della P.A.)»²⁵.

In definitiva, i passi sinora compiuti verso l'adozione di un sistema nazionale di notifica delle esposizioni a rischi di contagio da COVID-19 confermano dunque la tesi che non ci si trova di fronte ad un diritto "eccezionale", ad una situazione di stravolgimento delle regole per quanto riguarda la gestione della pandemia, ma, al contrario, vi è comunque il pieno rispetto della legalità e dei principi generali dell'ordinamento; in particolare, come è stato ben sottolineato, «l'art. 6 del d.l. n. 28/2020 non prefigura un diritto eccezionale, ma gestisce le eccezionali esigenze di una pandemia in linea con il Reg. Europeo 2016/679 [...] con le indicazioni del Parlamento Europeo e della Commissione Europea, e con quelle tecniche del Comitato europeo per la protezione dei dati»²⁶.

²⁴ Il comma 7 prevede, altresì, che gli oneri derivanti dall'implementazione della piattaforma non possono superare 1.500.000 euro per l'anno 2020, specificando altresì che si debba provvedere utilizzando le risorse assegnate al Commissario straordinario all'emergenza per il 2020 con delibera del Consiglio dei Ministri a valere sul Fondo emergenze nazionali di cui all'art. 44 del d.lgs. 2 gennaio 2018, n. 1.

²⁵ Cfr. anche ²⁵ M. PLUTINO, "Immuni". Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici, cit., p. 592.

²⁶ G. COMANDÈ, Sintesi dell'Audizione presso Commissione Giustizia della Camera dei Deputati in materia di Covid-19 e trattamento dei dati personali, 19 maggio 2020, paper, p. 1.

4. Brevi cenni sul funzionamento dell'app

Come accennato in premessa, l'uso di una tecnologia di *contact tracing*²⁷ potrebbe, dunque, garantire un tracciamento più efficiente dei contatti, pur sempre nel rispetto delle libertà fondamentali dei cittadini, *in primis* della *privacy*. Tra l'altro, come già ricordato, il Governo ha ricevuto a più riprese il parere favorevole dell'Autorità Garante per la protezione dei dati personali, che ha ritenuto Immuni compatibile con le norme del GDPR e del nostro Codice *privacy* e proporzionato il trattamento di dati personali effettuato nell'ambito del sistema nazionale di notifica delle esposizioni a rischi di contagio da COVID-19, una volta rispettate le tre regole fissate dall'Europa per il tracciamento: tecnologia *bluetooth* (e non la geolocalizzazione), anonimato e volontarietà.

L'app, infatti, non utilizzerà il GPS, ma il segnale *bluetooth low energy* registrato dalle app degli altri utenti con le quali i soggetti entreranno in contatto. Quando un utente verrà diagnosticato contagiato dal COVID-19 il suo dispositivo trasmetterà i dati al server, che provvederà ad informare gli altri utenti di essere a rischio contagio.

Il sistema sarà gestito dal Ministero della Salute e il codice sorgente dell'app, come predetto, sarà *open source*: chiunque potrà studiarlo. Inoltre, l'app non accederà ai contatti del telefono, non chiederà il numero e non manderà SMS.

Come si può rilevare, i principi operativi in cui il sistema di allerta COVID-19 si declina, sono perfettamente in linea con quanto disposto dall'art. 5 del GDPR, il quale enuncia i principi di liceità, correttezza e trasparenza, finalità, esattezza, minimizzazione, limitazione della conservazione, integrità e riservatezza dei dati²⁸, che

²⁷ Per una ricostruzione completa relativa al funzionamento dell'app si rimanda a M. PLUTINO, "Immuni". Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici, cit., 592 ss., il quale afferma tra l'altro che «sarebbe pertanto più opportuno parlare, allo stato delle funzioni, di una app di *exposure notification* o, quantomeno, di mero *proximity tracing* con esclusione del *tracing* in quanto tale, che richiederebbe la geolocalizzazione quale tecnologia in grado di conoscere non solo il "se" del contatto ma anche il "dove"».

²⁸ Con riferimento al catalogo dei principi del trattamento ora contenuto nell'art. 5 del nuovo Regolamento sia consentito rinviare a C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, cit., pp.106 ss., in cui si sottolinea la progressiva trasformazione

«costituiscono punti di riferimento ineludibili e strumentali all'effettività del servizio offerto dalla App in questione»²⁹.

Occorre mettere in evidenza principalmente tre aspetti relativi al funzionamento dell'app resi pubblici dai rapporti del Gruppo di lavoro *data-driven*, vale a dire: a) che «l'intero sistema integrato di *contact tracing* è interamente gestito da uno o più soggetti pubblici e che il suo codice è aperto e passibile di revisione da qualunque soggetto indipendente voglia studiarlo»; b) che «i dati trattati ai fini dell'esercizio del sistema sono "resi sufficientemente anonimi da impedire l'identificazione dell'interessato"³⁰ tenuto conto dell'insieme di fattori obiettivi, tra cui i costi, le tecnologie disponibili ed il valore della reidentificazione almeno in condizioni ordinarie e salvo il verificarsi di eventi patologici»; c) «che la decisione di usare la soluzione tecnologica sarà liberamente assunta dai singoli cittadini»³¹.

Il primo aspetto è centrale per evitare di "regalare" dati a soggetti privati e per evitare che trasferendo il server che custodisce tali dati fuori dall'Unione europea si esca dall'ambito territoriale di applicazione del GDPR. Le conseguenze di questo assunto sono così limpide che non rendono necessarie ulteriori precisazioni. Sul secondo e sul terzo aspetto, invece, relativi rispettivamente alla scelta del regime della raccomandazione o dell'obbligo dell'utilizzo dell'app ed alla autodeterminazione informativa dell'interessato, ci si soffermerà puntualmente nei due paragrafi seguenti.

Ad ogni modo, non si può certo pensare che l'app possa essere una sorta di panacea di tutti i mali. Certo, una buona app, che entrasse in funzione il più presto

dell'approccio delle istituzioni europee in materia, che passa da una configurazione prevalentemente orientata al mercato ad una, invece, più garantista nei confronti dei diritti fondamentali della persona umana.

²⁹ G. COMANDÈ, *Sintesi dell'Audizione presso Commissione Giustizia della Camera dei Deputati in materia di Covid-19 e trattamento dei dati personali*, cit., p. 1.

³⁰ Cfr. in tal senso il Considerando n. 26 del GDPR. Sull'importanza della definizione "sufficientemente anonimi" si rinvia alle riflessioni di G. COMANDÈ, *Non sparate sulle app di tracing e fidiamoci del Gdpr: ecco perché*, in *Agendadigitale.eu*, 28 aprile 2020, secondo cui le moderne tecnologie hanno «virtualmente reso inesistenti i dati anonimi; o meglio hanno virtualmente reso possibile ricollegare ogni dato ad una persona fisica; o peggio ancora hanno reso possibile – entro certi termini – indirizzarsi e discriminare individui e gruppi anche senza conoscerne l'identità».

³¹ V. *amplius* Ministero per l'Innovazione tecnologica e la digitalizzazione, *Un aggiornamento sull'applicazione di contact tracing digitale per l'emergenza coronavirus*, 21 aprile 2020, al link: <https://innovazione.gov.it/un-aggiornamento-sull-applicazione-di-contact-tracing-digitale-per-l-emergenza-coronavirus/>

possibile, potrebbe dare sicuramente un ottimo apporto nella lotta contro il COVID-19, ma anche in tal caso, l'app di *contact tracing* non può rappresentare la soluzione di tutti i problemi, o meglio ancora "lo strumento" di contrasto del coronavirus, ma soltanto "uno degli strumenti", in un'ottica in cui una serie di iniziative del Governo e delle Regioni si svolgano in maniera armonica tra loro, nell'ambito di una strategia sistematica più complessiva³².

5. Trasparenza dell'apporto tecnico del Gruppo di lavoro *data driven*

Com'è sotto gli occhi di tutti, di fronte all'emergenza rappresentata dalla comparsa di un virus nuovo capace di contagiare l'uomo, la politica ha fatto ampio ricorso agli uomini della scienza. Sono proliferati i comitati tecnico-scientifici sia a livello statale sia a livello regionale. Fra questi il "Gruppo di lavoro *data-driven* per l'emergenza da COVID-19", come detto composto da 74 esperti provenienti da aree multidisciplinari.

Il Gruppo di lavoro è l'unico sin qui, da quanto risulta, che ha inteso pubblicare i rapporti consegnati al Governo, nonostante l'assenza di ogni tipo di obbligo normativo al riguardo³³. È sulla base della lettura di questi *reports* che oggi abbiamo la possibilità di arricchire la discussione, anche tecnica, sul tema della app Immuni, prescelta poi dal Commissario straordinario per l'emergenza COVID-19 e acquisita con la citata ordinanza n. 10/2020.

È una notazione specifica importante perché è parte della questione generale della trasparenza dell'apporto dei comitati tecnico-scientifici a supporto del decisore politico.

L'ordinamento italiano sconta la mancata maturazione di una cultura della trasparenza nell'interlocuzione fra politica e scienza: mentre in Italia non è possibile

³² Così anche L. FLORIDI, *Mind the app - considerations on the ethical risks of COVID-19 apps*, 18 aprile 2020 <https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html?m=1>; più in generale sulle questioni etiche legate all'app vedi anche J. MORLEY, J. COWLS, M. TADDEO, L. FLORIDI, *Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems*, 26 maggio 2020, *paper*, consultabile al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582550.

³³ I rapporti di tutti i sottogruppi sono accessibili partendo dalla seguente pagina web: <https://innovazione.gov.it/task-force-dati-le-relazioni-delle-attivita-dei-gruppi-che-hanno-valutato-le-app/>

reperire i pareri resi dal comitato tecnico scientifico, in Francia gli *Avis du Conseil scientifique* COVID-19 sono tutti disponibili sul sito del *Ministère des Solidarités et de la Santé*³⁴.

Il tema della trasparenza dell'apporto degli esperti è fondamentale perché solo la pubblicazione dei rapporti consente di discernere il contributo tecnico dalla decisione politica e permette, altresì, di far trasparire quanta parte della decisione politica è, in qualche modo, vincolata dai pareri tecnici e quant'altra, invece, solo orientata o, infine, assolutamente discrezionale.

Specialmente nel contesto attuale, in cui i provvedimenti per limitare il contagio basati sulla scienza vengono assunti come fondamento di decreti che dispongono la limitazione di diritti e libertà costituzionali, appare di gran lunga più garantista il modello adottato in altri Paesi democratici.

6. Sulla necessità del trattamento da parte di un'app di contact tracing

Pur nella varietà dell'apporto tecnico-scientifico offerto dagli epidemiologi in questa situazione, com'è d'altra parte comprensibile di fronte ad un virus nuovo, è possibile riscontrare alcuni punti fermi. Il primo è proprio rappresentato dal consenso scientifico sulla necessità di ricostruire la catena dei contagi per cercare di spezzarla e di impedire la creazione di altre catene di trasmissione.

Il consenso della comunità scientifica su questo aspetto è il punto di partenza corretto da cui partire per impostare la questione perché rende necessario il trattamento automatizzato del contact tracing, mediante algoritmi semplici. Questa considerazione è in linea con il Regolamento europeo per la protezione dei dati personali (GDPR) che ancora la liceità del trattamento a due requisiti alternativi: la necessità del trattamento o il consenso dell'interessato.

Una buona parte dei contagi avviene nel periodo in cui il soggetto affetto da COVID-19 non è ancora consapevole, per diverse ragioni (non ha ancora sintomi o ha sintomi trascurabili e non ha ancora effettuato il tampone) e pertanto non prende

³⁴ <https://solidarites-sante.gouv.fr/actualites/presse/dossiers-de-presse/article/covid-19-conseil-scientifique-covid-19>

alcuna precauzione, quale intanto può essere l'autoisolamento³⁵. È stato opportunamente affermato in proposito, sulla scorta quanto dimostrato in uno studio scientifico apparso sulla Rivista *Nature*³⁶, «che l'alta incidenza della trasmissione pre-sintomatica (quella in cui i sintomi non sono ancora evidenti) può rendere inefficaci gli interventi di isolamento nel controllo dell'epidemia, sostenendo che le tradizionali procedure di localizzazione manuale dei contatti non siano sufficientemente veloci per contrastare la diffusione del SARS-CoV-2»³⁷.

La necessità del tracciamento dei contatti è stata avanzata già inizialmente dall'Organizzazione Mondiale della Sanità (OMS). Fra le raccomandazioni contenute nel *Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)* del 16-24 febbraio 2020 si legge che è molto importante «*Immediately expand surveillance to detect COVID-19 transmission chains, by testing all patients with atypical pneumonias, conducting screening in some patients with upper respiratory illnesses and/or recent COVID-19 exposure, and adding testing for the COVID-19 virus to existing surveillance systems (e.g. systems for influenza-like-illness and SARI)*». Ancora le linee guida OMS del 13 marzo 2020³⁸ espressamente prevedono che debba essere effettuato il tracciamento di tutti i contatti dei soggetti risultati positivi, da due giorni prima dell'insorgere dei sintomi, e che i test debbano essere eseguiti su tutti i contatti dei pazienti risultanti positivi, a prescindere se essi abbiano sintomi³⁹.

³⁵ Nella letteratura scientifica vedi FERRETTI ET AL, *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*, in *Science*, 08 May 2020: Vol. 368, Issue 6491, disponibile al seguente link: <https://science.sciencemag.org/content/368/6491/eabb6936.full>

³⁶ HE, X., LAU, E.H.Y., WU, P. et al., *Temporal dynamics in viral shedding and transmissibility of COVID-19*, *Nat Med* 26, 672–675 (2020). <https://doi.org/10.1038/s41591-020-0869-5>

³⁷ «A rafforzare tale tesi lo studio pubblicato sulla rivista *Nature*, il quale, analizzata la patogenesi virale ed osservato il picco di carica virale nei tamponi oro-faringei al momento dell'insorgenza dei sintomi, ha stimato che il 44% dei casi secondari di infezione avviene durante lo stadio presintomatico dei casi primari», così G. ATTARDI – N. MARINO – E. SANTUS, *Contact tracing, perché è così importante contro il covid (anche in Italia)*, in *Agendadigitale.eu*, 21 aprile 2020, online: <https://www.agendadigitale.eu/sicurezza/privacy/contact-tracing-perche-e-cosi-importante-contro-il-covid-anche-in-italia/>

³⁸ WHO, *Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)*, 16-24 February 2020, (spec. punto 4), accessibile al seguente indirizzo: <https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf>

³⁹ D. DE FALCO – M. MADDALENA, *La politica del tracciamento dei contatti e dei test per covid-19 alla luce delle ultime direttive OMS: nessun ostacolo giuridico impedisce di utilizzare il "modello coreano" anche in Italia*, in *Federalismi.it*, Focus - Osservatorio Emergenza Covid-19, 28 marzo 2020. Gli

Lo studio già citato pubblicato su *Science* presenta le seguenti conclusioni: «*Given the infectiousness of SARS-CoV-2 and the high proportion of transmissions from presymptomatic individuals, controlling the epidemic by manual contact tracing is infeasible. The use of a contact-tracing app that builds a memory of proximity contacts and immediately notifies contacts of positive cases would be sufficient to stop the epidemic if used by enough people, in particular when combined with other measures such as physical distancing*».

Alla luce di quanto sin qui detto, da una parte il sistema di tracciamento manuale sconta i limiti che abbiamo descritto, dall'altra anche l'app di *contact tracing* da sola non è sufficiente perché non offre copertura a tutti quei soggetti che non sono in possesso di uno *smartphone* o che, a vario titolo, non hanno installato l'app. Si può concludere, perciò che i due sistemi si possono integrare per offrire una più elevata prevenzione sanitaria per raggiungere il maggior numero possibile di potenziali contagiati, così che il soggetto che sfugge con un sistema può essere rintracciato con l'altro⁴⁰.

stessi Autori fanno notare che «le misure di tracciamento e isolamento dei focolai di infezione (oggi mediante il ricorso all'intelligenza artificiale) erano già ammesse dal "Piano Nazionale di Preparazione e Risposta ad una Pandemia Influenzale" di cui il nostro Paese è dotato fin dal 2003, ma che non risulta essere stato applicato per l'emergenza Covid-19; tale piano, nel prevedere una dettagliata sequenza di azioni da intraprendere e nell'individuare livelli e di competenze decisionali, include l'adozione di modelli anche mediante l'impiego di algoritmi di contenimento e mappatura del contagio attraverso misure eccezionali e ricorso a controlli generalizzati».

⁴⁰ È bene tenere presente che «gli standard di tracciamento manuale dei contatti forniti dall'*European Center for Disease Prevention and Control* (ECDC) nel marzo 2020 relativamente all'epidemia di coronavirus indicano tuttavia in 12 ore il tempo medio per ogni operazione di *contact tracing*. L'operazione richiede l'utilizzo di tre unità di personale specializzato. Il suo tasso di successo è peraltro insufficiente a identificare tutti i contatti del soggetto che ha contratto il virus o comunque a ridurre il numero di contatti secondari infettati non identificati e isolati sotto l'unità. Dunque, la soluzione manuale non assicura di interrompere la riproduzione epidemica. L'uso della tecnologia in ambito di *contact tracing* sarebbe in grado di dare un contributo rilevante a un "tracciamento di prossimità" molto più efficiente e rapido di quello tradizionale», Ministero per l'Innovazione tecnologica e la digitalizzazione, *Un aggiornamento sull'applicazione di contact tracing digitale per l'emergenza coronavirus*, 21 aprile 2020, consultabile al seguente link: <https://innovazione.gov.it/un-aggiornamento-sull-applicazione-di-contact-tracing-digitale-per-l-emergenza-coronavirus/>

Cfr. A. SANTOSUOSSO, *La regola, l'eccezione e la tecnologia*, in *BioLaw Journal*, 2020, p. 612 per il quale «nella fase 2, invece, si esce dall'isolamento e si è attivi: allora diventano rilevanti tamponi, test sierologici per chi va al lavoro, e la telemedicina per seguire attivamente chi contrae l'infezione e ha bisogno di cure a casa piuttosto che in ospedale, e altri strumenti di medicina sul territorio».

Se è vero, e pare evidente, che le fasi 1 e 2 si sovrappongono cronologicamente, allora vuol dire che abbiamo bisogno di entrambe le visioni e di entrambi i tipi di mezzi di intervento».

Lo stesso Presidente del Garante per la Protezione dei dati personali, nel corso di un'audizione informale alla Camera dei deputati, ha avuto modo di sottolineare che l'utilizzo di tale tecnologia ha «poche valide alternative ai fini della ricostruzione della catena epidemiologica»⁴¹.

A tale conclusione dà conforto, come si è mostrato, anche la letteratura scientifica in tema, alla quale ormai il giurista deve porre attenzione nelle materie in cui emergono valutazioni tecnico-scientifiche, a meno di voler ritenere erroneamente che spetta unicamente alle Corti o al legislatore l'onere di avvalersi degli apporti tecnici offerti dalle altre scienze negli ambiti che lo richiedono.

7. Obbligatorietà vs. volontarietà.

Diverse ragioni giuridiche e tecniche depongono in favore della volontarietà dell'installazione e dell'utilizzo dell'app.

Dal punto di vista giuridico, non vi può essere dubbio che nelle democrazie costituzionali il regime della persuasione è preferibile rispetto a quello dell'obbligo. L'obbligo di un utilizzo di una applicazione tecnologica sarebbe stato vissuto dai cittadini come un'imposizione, magari ingenerando comportamenti tendenti ad eludere l'obbligo.

Ci sono anche diverse ragioni pratiche che fanno propendere per la volontarietà dell'app.

L'eventuale imposizione da parte dell'autorità pubblica del ricorso all'app presterebbe il fianco ad utilizzi derogatori, anche considerando che su internet si fa presto a far circolare istruzioni e trucchi su come giocare a guardia e ladri: si potrebbe, per esempio, installare l'app per uscire al di fuori delle mura domestiche per mostrarla nell'ipotesi di controlli salvo poi disinstallarla una volta fatto ritorno al proprio domicilio, oppure semplicemente si potrebbe inibire il funzionamento disattivando il *bluetooth* o, infine, ponendo in essere comportamenti tecnologicamente meno accorti,

⁴¹ Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus, Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati, 8 aprile 2020.

come lasciare provvisoriamente il telefono in macchina prima di entrare in qualche edificio.

La soluzione prescelta, Immuni, adotta misure tecniche ed organizzative che minimizzano i rischi di reidentificazione dell'utente in ogni fase di vita del sistema dell'applicazione attraverso l'adozione di un sistema di ID randomico, che cambia periodicamente e con grande frequenza più volte al giorno. Il registro degli ID generati è custodito, secondo un modello decentralizzato, sul singolo *device* e non di base sul server centrale, perciò tali dati sono soggetti alla previsione dell'art. 5, par. 3, della direttiva *e-Privacy*, secondo cui «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. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente»⁴².

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 reale esigenza rappresentano importanti misure tecniche per minimizzare il rischio del trattamento dei dati personali, poiché «le autorità sanitarie dovrebbero avere accesso soltanto ai dati di prossimità del dispositivo della persona infetta, in modo che possano contattare le persone a rischio di infezione»⁴³. L'altra opzione

⁴² Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

⁴³ Come suggerito nella Comunicazione della Commissione europea, *Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati* 2020/C 124 I/01, del 17 aprile 2020.

avrebbe previsto la sola conservazione dei dati pseudonimi sul server centrale gestito dalle autorità sanitarie (c.d. *server back-end*)⁴⁴.

Avendo optato per un sistema decentralizzato, nei termini appena descritti, si poteva valutare magari il ricorso alla *blockchain*, che avrebbe sì costituito una garanzia quasi assoluta in termini di presidio dei dati personali, ma d'altra parte avrebbe comportato un problema di gran lunga superiore in termini di *data retention*, poiché i dati trattati con il sistema della *blockchain* non sarebbero stati più cancellabili, per caratteristiche proprie del sistema. L'art. 6, co. 2, lett. e) del d.l. n. 28/2020, invece, prevede opportunamente l'automatica cancellazione dei dati al termine dell'emergenza sanitaria nonché al comma 8 «l'utilizzo dell'applicazione e della piattaforma, nonché ogni trattamento di dati personali effettuato ai sensi al presente articolo sono interrotti alla data di cessazione dello stato di emergenza disposto con delibera del Consiglio dei ministri del 31 gennaio 2020, e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi». Quest'ultima opzione dovrebbe consentire l'eventuale utilizzo dei dati per finalità quali la ricerca scientifica e la statistica, qualora fosse necessario⁴⁵.

All'interno di questa infrastruttura informatica così *privacy oriented* l'eventuale disinstallazione accidentale dell'app dallo *smartphone* non consentirebbe di ricollegare l'identità dell'interessato, facendo perdere pure tutta la preziosa lista di contatti sociali. Questo proprio perché l'app non raccoglie dati personali se non limitatamente all'indirizzo IP, com'è d'altra parte ineliminabile, e del dato relativo alla provincia in cui ci si trovi a dimorare che, però, non è un dato personale. La trasmissione del solo indirizzo IP rappresenta la minore raccolta possibile di informazioni⁴⁶ e indirizza

⁴⁴ Offre una riflessione tecnica molto chiara su questi aspetti F. BAIARDI, *Le proprietà di un sistema per il tracing: centralizzato, decentralizzato, open source*, in *Risk Management 360*, online: <https://www.riskmanagement360.it/analisti-ed-esperti/le-proprieda-di-un-sistema-per-il-tracing-centralizzato-decentralizzato-open-source/>

⁴⁵ Conformemente ancora agli orientamenti della Commissione europea che ha anche raccomandato, nel caso, di includere tale possibilità, ove necessaria, «fin dall'inizio nell'elenco delle finalità» e di comunicarle «in modo chiaro agli utenti».

⁴⁶ L'art. 6, co. 2, lett. b), dispone che «per impostazione predefinita, in conformità all'articolo 25 del Regolamento (UE) 2016/679, i dati personali raccolti dall'applicazione di cui al comma 1 siano esclusivamente quelli necessari ad avvisare gli utenti dell'applicazione di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19, individuati secondo criteri stabiliti

l'utilizzo dell'app verso il regime più vicino possibile all'anonimato, allo stato delle conoscenze informatiche. In questo senso va colto il ricorso alla formula di dati «resi sufficientemente anonimi da impedire l'identificazione dell'interessato», che è stata utilizzata dalla Ministra dell'Innovazione nel corso di un'audizione informale resa al Senato⁴⁷.

In realtà, l'app tratta dati pseudononimi, come disposto dall'art. 6, co., 2, lett. c) del d.l. n. 28/2020, per cui «il trattamento effettuato per allertare i contatti sia basato sul trattamento di dati di prossimità dei dispositivi, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati»⁴⁸. Come ha avuto modo di mettere in luce il Garante della 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»⁴⁹.

L'attivazione delle notifiche di esposizione mediante l'app richiedere un triplice atto di volizione da parte dell'interessato che dovrà dapprima decidere di installare

dal Ministero della salute e specificati nell'ambito delle misure di cui al presente comma, nonché ad agevolare l'eventuale adozione di misure di assistenza sanitaria in favore degli stessi soggetti».

⁴⁷ Senato della Repubblica, 8a Commissione (Lavori pubblici, comunicazioni). Seduta 29 aprile 2020. *Audizione informale del Ministro per l'innovazione tecnologica e la digitalizzazione, intervenuto in videoconferenza, sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da coronavirus*, online: <https://innovazione.gov.it/assets/docs/RelazioneAudizione2904VIICommissioneSenato.pdf>

⁴⁸ V. PAGNANELLI, *Immuni: spunti per una riflessione privacy-oriented*, in *Questione giustizia*, 11 maggio 2020, ritiene «fuorviante» l'accostamento tra anonimizzazione e pseudonimizzazione, poiché «la differenza tra pseudonimizzazione ed anonimizzazione dunque non è di poco conto, in quanto ai dati anonimi (davvero anonimi) non si applica la disciplina del Gdpr, non trattandosi più di dati personali».

⁴⁹ «A tal riguardo, l'applicazione di tecniche di cifratura asimmetriche a stato dell'arte (ad esempio, basate su algoritmi di *hash*), con una adeguata custodia delle chiavi da parte del soggetto centrale, che sarebbe l'unico in grado di consentire la re-identificazione per ragioni meramente funzionali all'operatività del sistema, si configurerebbe come una schema di pseudonimizzazione idoneo a realizzare il disaccoppiamento tra TEK e le loro chiavi di decodifica, consentendo così la corretta applicazione dell'art. 6 comma 2, lett. c) del d.l. n. 28/2020, nonché, su tale base, la pubblicazione delle TEK dei soggetti risultati positivi». Garante della protezione dei dati personali, *Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni - 1° giugno 2020*, disponibile al link: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568>

L'app, successivamente attivare e mantenere attivati l'app e il *bluetooth* e, infine, in caso di contagio, comunicare volontariamente all'autorità sanitaria il proprio ID pseudonimizzato provvisorio per caricare il dato della positività e attivare il sistema automatizzato di notifica⁵⁰. Quest'ultimo intervento consente di realizzare quell'intervento umano sul processo algoritmico richiesto dall'art. 22 del GDPR per evitare l'esclusiva soggezione umana a decisioni automatizzate, scongiurando anche l'esposizione a possibili distorsioni e inesattezze.

È bene mettere in evidenza che l'attivazione delle notifiche di esposizione mediante l'applicazione deve essere effettivamente libera e non può essere in alcun modo incentivata. Devono essere stigmatizzate quelle proposte, che sono state avanzate in diverse sedi, tendenti a proporre delle "concessioni" in cambio della disponibilità dell'app, come per esempio una maggiore possibilità di circolazione, piuttosto che una sostanziale sostituzione dei moduli di autocertificazione per uscire di casa o, peggio ancora, una corsia preferenziale per l'accesso ai tamponi o alle cure. L'utilizzo dell'app in tal modo sollecitato non potrebbe essere considerato effettivamente il frutto di una libera e informata determinazione personale. In tale direzione, l'art. 6, co. 4, del d.l. n. 28/2020 opportunamente prevede che «il mancato utilizzo dell'applicazione di cui al comma 1 non comporta alcuna conseguenza pregiudizievole ed è assicurato il rispetto del principio di parità di trattamento»⁵¹.

L'incentivazione all'uso dell'app di *contact tracing* piuttosto, come anche la maturazione di un consenso realmente informato, passa anche per la necessaria formalizzazione di canali pubblici di corretta informazione che forniscano con chiarezza ogni tipo di indicazione e che fughino qualsivoglia dubbio, a fronte del rischio che, invece, il convincimento individuale si formi sulla base delle molte *fake news* che circolano in rete⁵².

⁵⁰ Secondo M. PLUTINO, *"Immuni". Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, it., p. 593, «l'adozione volontaria, con cui è da intendere tanto, presupposta la gratuità per l'utente, il *download* facoltativo che l'installazione e l'uso volontario, sono certamente da intendere in prima battuta come un'espressione di libero consenso ad una eventuale limitazione dei diritti che ne consegue».

⁵¹ Tale disposizione è letteralmente allineata alla Comunicazione della Commissione prima citata secondo che raccomanda di non prevedere «conseguenze negative per la persona che decide di non scaricare/utilizzare l'app»

⁵² A tal fine si segnala che il Governo ha istituito un'ulteriore task force per contrastare le *fake news* sul COVID-19. Su questa esperienza si sofferma il contributo di L. RINALDI, *La task force*

La prima informazione necessaria da comunicare è che l'installazione dell'app è utile per il singolo cittadino che la utilizza e per le persone con cui vive, prima ancora che per i pubblici poteri o per il servizio sanitario nazionale, perché nel ricevere tempestivamente la notifica di potenziale contagio, l'interessato potrà porsi in auto-isolamento, non pregiudicando la salute dei suoi cari nonché richiedere l'intervento sanitario in un momento molto anticipato rispetto all'eventuale comparsa di sintomi. Questa possibilità è decisiva per offrire una maggiore tutela in termini di prevenzione sanitaria nei confronti di una patologia che, da quanto si legge, è capace di determinare, nelle forme più acute, un aggravamento repentino delle condizioni di salute a partire dalla comparsa dei primi sintomi, con eventuale ricorso alla terapia intensiva e fino a determinare l'evento della morte. Perciò, in linea con quanto sin qui sostenuto, «la finalità dell'applicazione è di contenere la diffusione del COVID-19 attraverso un'informazione che può condurre ad una diagnosi precoce e, prima ancora, ad adottare cautele nella vita quotidiana al fine di non esporsi a rischi»⁵³.

Il secondo elemento informativo da tenere in adeguata considerazione è quello relativo all'inevitabile sanguinosa compressione di alcune libertà costituzionali che si viene a determinare. I rischi derivanti dall'utilizzo di questi strumenti non possono essere taciuti ed anzi devono essere rappresentati con estrema trasparenza. Il pericolo più rilevante può derivare dal fatto che qualora tali dati non verranno trattati correttamente, poi distrutti e comunque custoditi con adeguate misure di sicurezza si possa determinare, anche attraverso il ricorso al trattamento con *big data* e algoritmi⁵⁴, una gigantesca mappatura dei dati di interazione sociale che determinerebbe

per le fake news tra protezione del diritto all'informazione e ipotesi di censura del web, in *BioLaw Journal*, 2020, pp. 653 ss. e di B. PONTI, *La libertà di informazione al tempo della pandemia. Rilievi critici in margine all'istituzione dell'«unità di monitoraggio per il contrasto della diffusione di fake news relative al CoViD-19 sul web e sui social network»*, in *BioLaw Journal*, 2020, pp. 635 ss.

⁵³ M. PLUTINO, *“Immunì”*. Un'exposure notification app, cit., p. 597, secondo l'A. perciò «appaiono pienamente rispettate le indicazioni del “Comitato europeo per la protezione dei dati” secondo cui anche di fronte ad un'emergenza pubblica vanno osservati necessità, proporzionalità, limitazione delle finalità e stato di diritto».

⁵⁴ Relativamente all'utilizzo di algoritmi da parte di Immunì il Garante ha raccomandato di «indicare puntualmente nella valutazione d'impatto, l'algoritmo, basato su criteri epidemiologici di rischio e modelli probabilistici, aggiornandolo costantemente, specificando i parametri di configurazione impiegati e le assunzioni effettuate, rendendolo disponibile alla comunità scientifica».

un'intollerabile limitazione dei diritti politici, così grave da metterebbe in ginocchio gli stessi pilastri della democrazia costituzionale.

Questo rischio di sorveglianza politica è stato ridotto dalla selezione di un'app che non geolocalizza attraverso il GPS o seguendo le celle telefoniche, secondo modelli tecnologici che pure erano stati proposti in risposta alla fast call ministeriale, che innalzavano chiaramente gli standard di efficacia ma sacrificavano eccessivamente la protezione dei dati personali⁵⁵.

Anche questo aspetto va tenuto presente per bilanciare minacce e vantaggi dell'utilizzo dell'app che, inevitabilmente offre meno funzionalità di tracciamento proprio per assicurare una maggiore cautela nell'utilizzo dei dati personali.

Nonostante quanto sin qui affermato relativamente alla volontarietà, che è bene ribadire con chiarezza è la scelta assolutamente più opportuna, tuttavia, non appare del tutto preclusa la possibilità futura di imboccare, in termini opposti, la strada dell'obbligatorietà, in caso di scarsa copertura dell'utilizzo dell'app, secondo un percorso simile rispetto a quello che ha condotto ad estendere il novero delle vaccinazioni obbligatorie.

L'installazione e l'utilizzo dell'applicazione possono essere agevolmente inquadrati come dovere di solidarietà secondo i dettami dell'art. 2 Cost.⁵⁶ e il regime dell'obbligatorietà può essere giustificato in ragione della salvaguardia della salute collettiva, ex art. 32 Cost. Penso, invece, che intendere il ricorso all'app di tracciamento come un trattamento sanitario obbligatorio possa risultare un'opzione ermeneutica che

⁵⁵ Relativamente all'efficacia del trattamento, nel citato rapporto del Gruppo di lavoro *data-driven* si legge «che la soluzione adottata - nelle sue componenti tecnologiche e non tecnologiche - possa essere considerata, almeno in una dimensione prognostica, effettivamente efficace sul piano epidemiologico giacché, in difetto, diverrebbe difficile giustificare qualsivoglia, pur modesta e eventuale, compressione di diritti e libertà fondamentali».

⁵⁶ Cfr. O. POLLICINO - F. RESTA, *Data tracing, no a deleghe in bianco all'algoritmo*, in *Corcom*, 24 marzo 2020, accessibile in <https://www.corrierecomunicazioni.it/privacy/data-tracing-no-a-deleghe-in-bianco-allalgoritmo/> i quali osservano che «la valutazione relativa all'utilizzo dei dati sulla mobilità dei soggetti contagiati, al fine di trarne indicazioni utili a ricostruire la catena epidemiologica, (...) avrebbe un fine non già repressivo ma solidaristico, individuabile cioè nell'esigenza di sottoporre ad accertamenti quanti siano entrati potenzialmente in contatto con l'interessato o comunque di adottare le misure utili a prevenire il contagio. Anche G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *laCostituzione.info*, 1 aprile 2020, suggerisce, al riguardo, di sperimentare la solidarietà nel rinunciare quotidianamente a esercitare le nostre libertà per il tempo necessario.

propone un'estensione eccessiva, dovendosi configurare, se mai, questa tecnologia come finalizzata alla prevenzione sanitaria.

A rileggere la sentenza n. 5/2018 alla luce dell'attuale emergenza sanitaria si colgono argomenti che rendono estremamente adattabile quella giurisprudenza all'eventuale estensione al profilo dell'obbligatorietà dell'app. Tra i tanti passaggi, particolarmente è da segnalare la parte motiva nella quale il giudice delle leggi afferma che «il contemperamento di (...) molteplici principi lascia spazio alla discrezionalità del legislatore nella scelta delle modalità attraverso le quali assicurare una prevenzione efficace dalle malattie infettive, potendo egli selezionare talora la tecnica della raccomandazione, talaltra quella dell'obbligo, nonché, nel secondo caso, calibrare variamente le misure, anche sanzionatorie, volte a garantire l'effettività dell'obbligo. Questa discrezionalità deve essere esercitata alla luce delle diverse condizioni sanitarie ed epidemiologiche, accertate dalle autorità preposte (sentenza n. 268 del 2017), e delle acquisizioni, sempre in evoluzione, della ricerca medica, che debbono guidare il legislatore nell'esercizio delle sue scelte in materia (così, la giurisprudenza costante di questa Corte sin dalla fondamentale sentenza n. 282 del 2002)»⁵⁷.

Lo stesso giudizio di proporzionalità, che pure può essere influenzato dalle dimensioni dell'emergenza sanitaria, può essere valutato anche in ragione del rischio in termini di limitazione dei diritti a cui si espongono solo i cittadini che utilizzino l'app, a differenza di quelli che decidono di non usarla, a fronte di un'adesione che si riveli bassa e perciò inefficace e, quindi, senza alcun vantaggio. Da questo punto di vista sarebbe stato preferibile prevedere una soglia minima di adesione al di sotto della quale il funzionamento, e dunque il trattamento dei dati, sarebbe rimasto inibito.

⁵⁷ Cfr. le dichiarazioni del Presidente del Garante per la protezione dei dati personali secondo cui «in termini generali, comunque, il fine perseguito da tale misura risulta particolarmente apprezzabile perché non già repressivo (come invece nel caso della sorveglianza del soggetto in quarantena obbligatoria mediante la sua geolocalizzazione), ma solidaristico. Lo scopo perseguito coinciderebbe, infatti, con l'esigenza di sottoporre ad accertamenti quanti siano entrati potenzialmente in contatto con un soggetto risultato positivo al virus o, comunque, di adottare le misure utili a prevenire il contagio. Si perseguirebbe, dunque, quella componente solidaristica del diritto alla salute quale interesse collettivo, valorizzata dalla giurisprudenza costituzionale sugli obblighi vaccinali». Nella stessa sede ha aggiunto anche che la previsione di un «obbligo di utilizzo sarebbe difficilmente coercibile salvo ricorrere a un vero e proprio braccialetto elettronico» (*Audizione informale, in videoconferenza, del Presidente del Garante per la protezione dei dati personali sull'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus, cit.*).

È possibile anche sostenere che questo è un caso in cui la proporzionalità tra restrizione di un diritto e finalità che si intendono raggiungere si garantisce massimamente solo se tutti aderiscono, altrimenti il risultato che andrebbe a determinarsi produrrebbe una disuguaglianza fra chi aderisce e chi no. Da qui si potrebbe persino arrivare a sostenere la preferenza per il regime dell'obbligatorietà⁵⁸.

Andando ancora oltre, pure sarebbe astrattamente possibile in futuro, in caso di una seconda ondata di contagi, che emerga nelle autorità sanitarie e politiche la tentazione (o magari anche la necessità) di ricorrere a funzioni ben più penetranti da parte dell'app di *contact tracing*. Ciò che è opportuno che non avvenga. Un'eventuale scelta di questo tipo, per il momento da tutti scongiurata, abbinata all'imposizione dell'utilizzo aprirebbe ben altri scenari ed evocherebbe ben più gravi preoccupazioni relativamente alla tutela dei diritti fondamentali.

Alla luce di tutte queste ragioni, Immuni, pur innegabilmente determinando una compressione momentanea di alcune libertà costituzionali, presenta un funzionamento temperato⁵⁹, perché implementa alcune importanti misure tecniche e organizzative minimizzando la minaccia ai dati personali, e sembra «di fronte all'eterogeneità delle opzioni possibili», seguire «un criterio di gradualità, valutando – come ricordano l'Edpb e il Presidente del Garante italiano – se le misure meno invasive possano essere sufficienti a fini di prevenzione».

È bene tenere presente ancora che ci muoviamo in un ecosistema fortemente dinamico che è la sommatoria di due giganti del Web, Apple e Google. Solo alla vigilia dell'introduzione di sistemi informatici di *contact tracing* e probabilmente anche

⁵⁸ Lo fa S. CALZOLAIO, *Nota in merito all'art. 6, d.l. 28/2020*, Audizioni informali nell'ambito dell'esame dei disegni di legge n. 1786 (dl n. 28/2020 - proroga intercettazioni e sospensioni processuali) e n. 1799 (dl 29/2020 - detenzione domiciliari e differimenti pena), Sed. n.121, 14 Maggio 2020, http://www.senato.it/application/xmanager/projects/leg18/attachments/documento_evento_procedura_commissione/files/000/124/501/NOTA_per_audizione_Senato_14.5.2020_-_Calzolaio.pdf. L'A. ha sostenuto che «se il motivo di interesse pubblico fosse di adottare misure di contrasto alla diffusione del virus, allora risulterebbe peculiare, e anche contraddittorio, che il trattamento dei dati personali non fosse obbligatorio per tutti. Si tratterebbe infatti di un caso analogo a quello delle cd. vaccinazioni obbligatorie o, al ricorrere dei presupposti, della cd. Quarantena».

⁵⁹ Esprime condivisione M. PLUTINO, *Immuni. Un'app rassicurante in punto di tutela di diritti ma a forte rischio di esternalità negative*, in *Media Laws*, 28 maggio 2020, secondo l'A. «la base legale di Immuni è sufficiente e le sue caratteristiche sono assolutamente rassicuranti. Il modo in cui i dati vengono trattati e conservati e distrutti non suscita particolari perplessità».

sollecitati dal valore economico dei dati di interazione sociale i due *Big tech* hanno deciso di sottoscrivere storico accordo e per condividere i protocolli *bluetooth*, attraverso un aggiornamento dell'*Application Programming Interface* (API). La ragione del ritardato avvio dell'app nell'ordinamento italiano è da addebitare, oltre che all'endemico passo lento della politica italiana, anche a questo aspetto che ha rivoluzionato il sistema dei protocolli *bluetooth*, rispetto al momento in cui era stata lanciata la fast call ministeriale citata, a seguito della quale erano stati presentati i progetti⁶⁰.

8. La falsa alternativa fra tutela della salute e protezione dei dati personali

È da contestare con decisione, invece, lo sbandierato *trade-off* fra salute e *privacy*: si tratta di una falsa alternativa perché tra i due diritti fondamentali non vi è un rapporto di esclusione⁶¹. La composizione fra i due valori è sempre possibile attraverso un'operazione di ragionevole bilanciamento anche se in taluni casi può risultare particolarmente gravosa. La tirannia dei valori è estranea alla nostra Costituzione, come più volte messo in luce dalla Corte costituzionale, secondo cui «tutti i diritti fondamentali tutelati dalla Costituzione si trovano in rapporto di integrazione reciproca e non è possibile pertanto individuare uno di essi che abbia la prevalenza assoluta sugli altri». La tutela deve essere sempre «sistemica e non frazionata in una serie di norme non coordinate ed in potenziale conflitto tra loro» (sentenza n. 264 del 2012). Se così non fosse, si verificherebbe «l'illimitata espansione di uno dei diritti, che

⁶⁰ A. SANTOSUOSSO, *La regola, l'eccezione e la tecnologia*, cit., p. 615, mette in guardia relativamente alla «totale mancanza di controllo su come Apple e Google incroceranno i nuovi dati (anche solo quantitativi) con tutti gli altri dati che sono in loro possesso fino a non potersi escludere che i dati aggregati possano trasformarsi con relativa facilità in dati personali. Ma anche se restassero ancora aggregati, il drenaggio di una tale grande quantità di dati avrebbe comunque un valore economico enorme».

⁶¹ Cfr. G. DELLA MORTE, *La tempesta perfetta covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDIBlog - Forum Covid-19*, 19 marzo 2020, online: <http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/>, secondo il quale «questo paradosso è solo apparente, perché frutto di un espediente retorico – piuttosto in voga, purtroppo – che pone la questione nei termini di *trade-off* tra salute e *privacy*, mentre a un più attento esame appare evidente che la questione non può essere articolata in termini alternativi/oppositivi». Opportunamente anche N. MINISCALCO, *La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?*, in *Osservatorio costituzionale*, 2020, p. 97, rileva che «la protezione dei dati personali potrebbe, in ottica di bilanciamento, arretrare, ma giammai in toto o comunque in misura irragionevole rispetto al beneficio che all'interesse prevalente, ossia al diritto alla salute, potrebbe derivarne».

diverrebbe “tiranno” nei confronti delle altre situazioni giuridiche costituzionalmente riconosciute e protette, che costituiscono, nel loro insieme, espressione della dignità della persona»⁶².

L’aspetto più positivo, dal punto di vista giuridico, relativo al dibattito sull’introduzione di queste tecnologie di tracciamento può essere individuato proprio in questa attenta ricerca di un bilanciamento possibile fra salute e protezione dei dati personali, anche attraverso il ricorso a misure di *privacy by design* e *by default*⁶³. Il risultato potrà essere valutato con diverse accentuazioni, in una giusta prospettiva critica, ma l’approccio orientato alla *privacy* che traspare con nettezza dai rapporti del Gruppo di lavoro penso rappresenti un precedente positivo.

9. Non solo app. Protezione dei dati personali e trattamento dei dati sanitari e genetici nell’emergenza COVID-19.

Il grande interesse che condivisibilmente la dottrina e la comunicazione dedicano alla app di tracciamento non deve distogliere l’attenzione su altri aspetti relativi alla protezione dei dati personali nell’attuale emergenza sanitaria⁶⁴.

Si pensi soprattutto alla imponente operazione di mappatura genetica e di dati sanitari che si sta accumulando nelle strutture sanitarie: biobanche del plasma, dei materiali biologici e genetici che si raccolgono a seguito dei test sierologici e dei tamponi che prelevano frammenti di RNA.

Il riferimento va, in primo luogo, al decreto-legge 10 maggio 2020, n. 30 recante “Misure urgenti in materia di studi epidemiologici e statistiche sul SARS-COV-2” che «in considerazione della necessità di disporre con urgenza di studi epidemiologici e statistiche affidabili e complete sullo stato immunitario della popolazione, indispensabili per garantire la protezione dall’emergenza sanitaria in atto, ai sensi

⁶² V. Corte cost., sentt. nn. 85/2013 e 58/2018.

⁶³ E questa considerazione vale ancora di più proprio nell’attuale contesto emergenziale: vi è chi ha rilevato che benché i «dd.ll. emanati a fondamento della gestione dell’emergenza sanitaria richiamassero espressamente i parametri della proporzionalità e adeguatezza», agli «atti consequenziali adottati dal Governo nazionale e dalle istituzioni di governo territoriale, è mancata ogni forma di bilanciamento di interessi concorrenti», così V. BALDINI, *Dignità umana e normativa emergenziale: (in)osservanza di un paradigma formale o (colpevole...) elusione di un parametro (anche) sostanziale? Aspetti problematici di un difficile equilibrio*, in *Dirittifondamentali.it*, 6 maggio 2020,

⁶⁴ Per un quadro d’insieme si rinvia ancora a G. RESTA, *La protezione dei dati personali nel diritto dell’emergenza Covid-19*, cit., pp. 1 ss.

dell'articolo 9, paragrafo 2, lettere g) e j), e dell'articolo 89 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies, comma 2, lettera cc), del decreto legislativo 30 giugno 2003, n. 196», autorizza «il trattamento dei dati personali, anche genetici e relativi alla salute, per fini statistici e di studi scientifici svolti nell'interesse pubblico nel settore della sanità pubblica, nell'ambito di un'indagine di sieroprevalenza condotta congiuntamente dai competenti uffici del Ministero della salute e dall'Istituto nazionale di statistica (ISTAT)»⁶⁵.

Ma anche, in secondo luogo, al tracciamento della mobilità dei cittadini in tutto il mondo da parte dei giganti del web, come sta facendo Google⁶⁶: i dati raccolti vengono aggregati e forniti ai governi nazionali e alle autorità sanitarie, ma è chiaro che provenendo dagli *smartphone* non si tratta in origine di dati anonimi.

L'auspicio è che anche su dette altre questioni il dibattito giuridico si alimenti.

⁶⁵ La questione non è sfuggita all'attenzione di M. TOMASI, *La solidarietà come vettore per uscire dalla crisi: prospettive dall'angolo di osservazione della medicina e della ricerca scientifica*, in *BioLaw Journal*, 2020, p. 333, secondo cui rappresenta un ulteriore esempio di misure derogatorie in ordine alla «raccolta e conservazione di campioni biologici e dati associati di soggetti malati e guariti, ma anche asintomatici, paucisintomatici o sani» che «mettono in luce l'irrinunciabile esigenza di derogare alle regole generalmente vigenti, ridisegnando i bilanciamenti sottesi alle stesse e adattandole alle situazioni imposte dall'emergenza».

⁶⁶ Per farsi un'idea è possibile consultare la seguente pagina web: <https://www.google.com/covid19/mobility/>