Special issue

Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito.

Francesco Paolo Micozzi*

TECHNOLOGIES, DATA PROTECTIONS AND COVID-19 EMERGENCY: RELATIONSHIP BETWEEN THE POSSIBLE AND THE LEGALLY PERMITTED

ABSTRACT: Technologies can be useful for dealing with emergencies such as that determined by CoViD-19. According to some studies, traditional contact tracing can be made more efficient and effective with the use of digital technologies. However, not everything that is technologically conceivable is also legally permitted (nor the consequent negative effects would be desirable). For this reason, it is necessary to establish a correct balance of rights to prevent a health emergency from turning into a democratic emergency. The article aims to examine how the use of technologies in the context of contact tracing can be done in compliance with European legislation on fundamental rights, including the General data protection regulation (GDPR).

KEYWORDS: CoViD-19; pandemic emergency; contact tracing, data protection, technologies

SOMMARIO: 1. Premessa – 2. Il *contact-tracing* tradizionale e tecnologico – 3. Tipologie di *contact-tracing* tecnologico – 4 Le soluzioni proposte in Europa: in particolare il protocollo DP-3T – 5. Il *contact tracing* tecnologico alla prova del GDPR – 6. La disciplina dell'emergenza in Italia e l'iter per l'adozione del *contact tracing* tecnologico – 7. L'art. 6 del DL 28/2020: la prima disciplina di dettaglio sul *contact tracing* digitale – 8. Conclusioni.

1. Premessa

Nel periodo a cavallo tra il 2019 e il 2020 ha iniziato a diffondersi, a livello mondiale, la pandemia di CoViD-19 (causata dal virus SARS-CoV-2). La pandemia in questione, la cui diffusione avrebbe avuto origine nella città cinese di Wuhan, arriva in Italia verso la fine del mese di gennaio 2020 con una tale viralità da imporre al Governo l'adozione, con decreti-legge e decreti ministeriali, una serie di misure emergenziali (reperibili nel *Dossier Coronavirus Italia* su *biodiritto.org*[1]). Non sono mancati, col moltiplicarsi delle notizie sull'incremento esponenziale dell'epidemia, episodi di minacce, lesioni e atti discriminatori ai danni di persone dai tratti asiatici che, per gli aggressori, erano sicuro indizio di veicolo d'infezione e per ciò solo sufficienti a certificarne la qualità di moderni untori, giustificandone, infine, la persecuzione.

* *Avvocato e professore associato di informatica giuridica, Università di Perugia. Mail: francescopaolo.micozzi@unipg.it .* *Il presente lavoro è aggiornato al 2 maggio 2020.*

[1] https://www.biodiritto.org/Dossier/Dossier-Coronavirus-Italia-In-costante-aggiornamento.

ISSN 2284-4503

Episodi tragicamente simili a quelli descritti dal Manzoni ne *I promessi sposi* (cap. XXXII), in cui ai tempi della peste a Milano (1630) le persone si convincevano dell'esistenza stessa degli untori e delle loro "unzioni" di «muraglie, porte d'edifizi pubblici e usci di case»; credenza rapidamente diffusa attraverso il chiacchiericcio. E il chiacchiericcio popolare, intriso d'isteria collettiva determinata dalla paura, si trasformava quasi inevitabilmente in conferma delle unzioni («il sentire faceva l'effetto del vedere») e nella conseguente caccia all'untore, ossia a coloro che «gli animi, sempre più amareggiati da' mali» riconoscevano come la causa del diffondersi della peste e contro i quali la gente potesse «far valere le sue vendette» («ogni atto poteva dar gelosia; e la gelosia diveniva facilmente certezza, la certezza furore»). Analoghi episodi di violenza, (forse meno cruenti) si sono registrati nella cronaca di quasi quattro secoli dopo, a seguito della diffusione del CoViD-19.

Certo, durante la pandemia descritta dal Manzoni non si disponeva delle conoscenze della medicina moderna (e al più si faceva ricorso a soluzioni pseudoscientifiche commiste a riti religiosi o, nelle migliori ipotesi, alle decameroniane "quarantene"), né ci si interrogava sul bilanciamento degli interessi nella tutela dei dati personali. Occorreranno, infatti, quasi tre secoli perché Samuel Warren e Louis Brandeis, dalle pagine della Harward Law Review, presentino al mondo "*The right to privacy*" (1890).

Benché il concetto di privacy e la rilevanza fondamentale della protezione dei dati personali siano, ai giorni nostri, largamente riconosciuti, è possibile costatare come la stessa esigenza di tutela sia percepita e abbia un impatto differenziato in ragione del contesto democratico, culturale e giuridico degli ordinamenti di riferimento. Tali differenze, tuttavia non sono "statiche" ma soggette a continue modulazioni, conseguenti sia ad eventi di rilevo locale che ad eventi in grado di coinvolgere aree molto più vaste. In tal ultimo senso, pertanto, si può osservare come la necessità di impiegare misure particolarmente stringenti di prevenzione e controllo della diffusione di una pandemia – evento di per sé eccezionale ma di largo impatto – può condurre alla necessità di revisionare il bilanciamento della tutela tra valori e beni giuridici in rilievo, sia pur limitatamente al periodo necessario a fronteggiare l'evento eccezionale.

2. Il *contact tracing* tradizionale e tecnologico

Dal punto di vista epidemiologico, infatti, quando si ha a che fare con una patologia consistente in un'infezione virale sconosciuta si adottano, generalmente, delle procedure basate sia su prassi comuni per la prevenzione e il contenimento dell'infezione (quali una maggiore cura dell'igiene personale, il distanziamento sociale, l'impiego di mascherine e altri dispositivi di protezione individuale) sia un protocollo "T3" – *test, treat, track* (iniziativa illustrata dall'Organizzazione mondiale della sanità nel 2012 al fine di contrastare la diffusione della malaria) – ossia l'esecuzione di test diagnostici, l'adozione di misure specifiche di trattamento e contenimento (quali, ad esempio, le quarantene) e il tracciamento degli episodi di contagio.

In quest'ultima misura (*track*) rientra il cosiddetto "*contact tracing*" (tracciamento dei contatti), che consiste nell'intervistare i pazienti ai quali sia stato diagnosticato il contagio da virus, al fine di risalire ai soggetti con i quali fossero entrati in contatto nei giorni antecedenti (almeno fino ai giorni in cui il paziente, sia pur asintomatico, potesse essere già contagioso) al fine di sottoporli a test diagnostici o a quarantena.

Tuttavia, il *contact tracing* rimesso alle semplici interviste fatte dal personale sanitario sconta la "debolezza" di essere rimesso alla memoria del paziente e alla sua capacità di indicare soggetti determinati. Per questo motivo in alcuni paesi, tra cui la Corea del Sud, già da qualche anno sono stati approntati sistemi tecnologici per eseguire il *contact tracing*. Impiegare le tecnologie per sopperire all'intrinseca debolezza della memoria del paziente può comportare, di converso, l'insorgere di ulteriori problematiche (sotto svariati profili) dovute all'impiego di una sorveglianza tecno-sanitaria su larga scala. Secondo quanto riportato dalla BBC[2], ad esempio, la Corea del Sud, al fine di monitorare la diffusione del CoViD-19 avrebbe messo in atto per la prima volta le misure straordinarie già varate nel 2015, in occasione della diffusione di un'altra epidemia di coronavirus simile alla SARS (MERS-CoV – *Middle East Respiratory Syndrome*). Attraverso i "messaggi di orientamento sulla sicurezza", realizzati con un invio massivo di SMS da parte del Governo sudcoreano, si sono verificate ipotesi di eccessiva diffusione di informazioni personali relative ai contagiati a causa della possibilità di incrociare il "codice del caso di contagio" con altre informazioni agevolmente reperibili in rete, tra le quali, "volto", "fotografie", "familiari" o, anche, elementi relativi a eventuali ipotesi di "adulterio" (ad esempio per essersi recati, in determinate ore del giorno, in ambienti nei quali, notoriamente, si pratica la prostituzione), con comprensibili risvolti negativi sulle vite dei soggetti coinvolti.

Ciò nonostante, l'impiego di tali tecnologie – che ha riguardato inizialmente, oltre alla Corea del sud, anche Cina, Singapore[3] e Israele – ha immediatamente affascinato anche i decisori politici di alcuni Paesi "occidentali" che, sulla scorta di ciò che è stato definito[4] «soluzionismo thatcheriano» («there is no alternative»), hanno immediatamente annunciato l'adozione di "app" o "soluzioni tecnologiche" per il *contact tracing*. La base argomentativa è stata, spesso, individuata in un documento pubblicato su Science[5] in cui diversi ricercatori hanno offerto il modello matematico a dimostrazione dell'efficacia del sistema di *contact tracing* tecnologico.

Una delle questioni[6] che ha catalizzato l'attenzione di decisori politici, tecnici e giuristi, è quella relativa all'impatto di tali soluzioni tecnologiche sulla disciplina in materia di protezione dei dati personali.

---

[2] Coronavirus privacy: *Are South Korea's alerts too revealing?*, in https://www.bbc.com/news/world-asia-51733145.

[3] In un recente articolo, J. BAY, direttore responsabile presso GovTech, l'agenzia governativa di Singapore per la digitalizzazione, pone i suoi dubbi sulla possibilità di sostituire oggi o nel prossimo futuro le interviste di *contact tracing* con i sistemi tecnologici di *contact tracing*: «if you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No. Not now and, even with the benefit of AI/ML and — God forbid — blockchain (throw whatever buzzword you want), not for the foreseeable future», in https://bit.ly/3cZDBxe.

[4] *Ex multis*: E. MOROZOV, *L'emergenza sanitaria e il rischio del totalitarismo*, in https://bit.ly/3bUbIVV; F. CHIUSI, *App per il tracciamento digitale: in democrazia discutere di privacy e diritti è doveroso e necessario*, in https://www.valigiablu.it/app-coronavirus-privacy-diritti.

[5] Science, 31.3.2020, https://science.sciencemag.org/content/early/2020/04/09/science.abb6936.

[6] Evidenziata anche dall'Organismo mondiale della sanità: «We do always have to have in the back of our minds – especially when it comes to collecting information on individual citizens or tracking their whereabouts or movements – that there are always very serious data protection, human rights principles that re involved. We're very, very cognisant of that and we want to ensure that all products that are developed are done in the most sensitive way possible and that we never step beyond the principles of individual freedoms, rights for individuals and for society», in https://bit.ly/2ZAupLC.

3. Tipologie di *contact tracing* tecnologico

Appare utile, a questo punto, illustrare, sia pur sommariamente, l'architettura e il modello di funzionamento delle diverse soluzioni proposte per il *contact tracing* tecnologico. Pur limitando la nostra indagine alle tecnologie utili al *contact tracing* digitale e il cui uso sia stato implementato (o sia in fase di implementazione nei paesi occidentali), non possiamo tuttavia tralasciare di considerare che, in una società iperconnessa, le informazioni potenzialmente idonee a localizzare e tracciare la nostra posizione sono numerose ed eterogenee.

Il *contact tracing*, infatti, potrebbe astrattamente essere attuato tramite dati GPS, installazione di applicazioni sui dispositivi di telefonia mobile, analisi delle transazioni con carte di credito o altri mezzi di pagamento, analisi dei dati di geolocalizzazione a disposizione dei gestori di telefonia mobile, ma anche attraverso l'uso dei cosiddetti *Big Data* (ossia quei dati provenienti, ad esempio, da società produttrici di *device* "smart", dall'utilizzo di tessere fedeltà dei market, dai sistemi di rilevamento delle targhe, dai sistemi di videosorveglianza con capacità di riconoscimento facciale…). Dal *mashup* di questa enorme ed eterogenea mole di informazioni personali è possibile disegnare un quadro assai definito sugli spostamenti di un'intera popolazione e dei singoli soggetti contagiati, oltre a quelli entrati con loro in contatto.

Tenendo a mente, tuttavia, che la finalità ultima è quella di tracciare gli eventuali contatti avuti da un soggetto all'interno di un limitato arco temporale, infatti, le soluzioni proposte si sono concentrate attorno, in genere, all'utilizzo di due diverse tecnologie: il *bluetooth* (standard di trasmissione dati su frequenze radio a corto raggio) e il GPS (*Global Positioning System*, un sistema di posizionamento e navigazione satellitare). Si parte dall'assunto, infatti, che queste ultime due tecnologie siano già disponibili per la maggior parte dei dispositivi comunemente "indossati" (smartphone). L'uso del GPS consentirebbe, in ipotesi, di localizzare un soggetto nello spazio e, attraverso il raffronto delle informazioni di localizzazione su larga scala, di individuare conseguentemente anche i soggetti che si siano trovati a una certa distanza (con margine di precisione dell'ordine di alcuni metri).

Restringeremo ulteriormente la nostra analisi all'ammissibilità di soluzioni di *contact tracing* che facciano ricorso alla tecnologia *bluetooth*, sia perché ritenuta la soluzione più praticabile dai differenti modelli proposti in Europa[7], sia perché, con le linee-guida n. 4 «sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al CoViD-19» del 21 aprile 2020[8], il Comitato europeo per la protezione dei dati (artt. 68 e ss., GDPR – *European Data Protection Board - EDPB*), indicando la disciplina di settore per l'impiego dei dati di geolocalizzazione, ha evidenziato i rischi e le maggiori difficoltà di anonimizzazione delle informazioni di geolocalizzazione.

Allo stato, pertanto, si è maggiormente orientati ad adottare una soluzione di *contact tracing* basata sulla tecnologia *bluetooth*, e in particolare la *bluetooth low energy*, o BLE (particolare tipo di tecnologia *bluetooth* a basso consumo energetico). La tecnologia BLE, infatti, consentirebbe ai diversi dispositivi (ad esempio smartphone) di comunicare (tra dispositivi e/o con un server centrale) informazioni

[7] Si veda, al riguardo, la guida creata il 15 aprile 2020 dall'*e-Health Network*, con il supporto della Commissione europea, per fornire indicazioni pratiche agli Stati membri che intendano impiegare soluzioni di *contact tracing* digitale https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

[8] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en.

ISSN 2284-4503

relative all'eventuale "contatto" tra diversi soggetti, all'intensità del segnale (dal quale può inferirsi la distanza alla quale i dispositivi si sono trovati) e la "durata" del contatto.

4. Le soluzioni proposte in Europa: in particolare il protocollo DP-3T

Scendendo maggiormente nel dettaglio, occorre precisare che, a seconda dello schema logico di implementazione della tecnologia BLE per il *contact tracing* impiegato, possono aversi, sotto il profilo del trattamento di dati personali, differenti modelli applicativi. Le valutazioni sulla capacità di maggiore o minore aderenza ai principi generali sul trattamento dei dati personali, previsti dall'art. 5 del GDPR, pertanto, andranno fatte non tanto sul "modello" quanto sull'applicazione pratica dello stesso. Due "modelli" di *contact tracing* tramite BLE si contendono, infatti, la primazia: uno che si appoggia a un sistema centralizzato di memorizzazione delle informazioni e un altro che, invece, non concentra le informazioni di "contatto" in un server centrale ma le memorizza all'interno del singolo dispositivo (sistema decentrato). La modalità di conservazione delle informazioni di tracciamento non è di poco momento, per quanto riguarda la disciplina sulla protezione dei dati personali, posto che nelle succitate linee-guida 4/2020 EDPB si precisa che sebbene entrambe le soluzioni siano praticabili, «*entrambe comportano una serie di vantaggi e svantaggi*» e che dovrebbero ponderarsi attentamente *gli effetti in termini di protezione dei dati e privacy nonché i possibili impatti sui diritti delle persone*», comunque, in via generale, la soluzione decentrata sarebbe maggiormente rispettosa del principio di minimizzazione[9]. Due sono i protocolli attualmente allo studio e in via di adozione nelle diverse soluzioni applicative proposte a livello europeo: PEPP-PT[10] (*Pan-European Privacy-Preserving Proximity Tracing*) che segue il modello centralizzato e; DP-3T[11] (*Decentralized Privacy-Preserving Proximity Tracing*) che, come intuibile, impiega lo schema decentralizzato.

È interessante, a questo punto, esaminare meglio la logica di funzionamento del modello DP-3T[12] che, con tutta probabilità, sarà impiegato nella soluzione tecnologica di *contact tracing* favorita dal Governo italiano. Il protocollo DP-3T prevede, come già visto, l'impiego della tecnologia BLE e un sistema decentralizzato per la memorizzazione delle informazioni. Una volta che la App venga installata nel dispositivo dell'utente, essa prenderebbe a generare gli EphID (*ephemeral identifiers*[13]), ossia codici alfanumerici anonimi (in quanto non contenenti informazioni riconducibili al dispositivo che li ha generati) ad intervalli temporali regolari e prefissati (un nuovo EphID sarebbe generato ogni 15 minuti). Gli EphID generati (dal dispositivo sul quale sia installata la App di *contact tracing*) sono memorizzati all'interno dell'App (in un registro che potremmo definire "registro dei codici generati") e, contemporaneamente, trasmessi tramite segnali radio (BLE) a tutti i dispositivi che si trovino ad una certa distanza (massimo 50 metri, circa). La stessa App memorizza, allo stesso modo, tutti gli EphID ricevuti tramite BLE dalle App dei soggetti che si trovino nelle vicinanze, all'interno di un altro registro che potremmo

[9] La soluzione centralizzata, ad esempio, è impiegata da Francia e Inghilterra, mentre quella decentrata dalla Germania.
[10] https://www.pepp-pt.org.
[11] https://github.com/DP-3T.
[12] Di questo modello è stata pubblicata la valutazione di impatto (DPIA) https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf.
[13] Codici pseudo-casuali di 32 byte generati con algoritmi crittografici di *hash*.

chiamare, ipoteticamente, «registro dei codici ricevuti» – gli analoghi codici, ricevuti dalle altre App. In tal modo la medesima App memorizzerà al suo interno sia un registro dei codici (EphID) generati e trasmessi, sia un registro dei codici (EphID) ricevuti dagli altri dispositivi.
Nel momento in cui dovesse accertarsi il contagio da SARS-CoV-2, i sanitari chiederebbero al paziente se ha installato la App e se vuole mettere a disposizione gli EphID generati dal suo dispositivo. In caso affermativo il sanitario genererebbe un codice di autorizzazione che verrebbe, poi, mostrato sotto forma di QR-Code (ossia un codice a barre bidimensionale impiegato tipicamente per memorizzare informazioni destinate a essere lette tramite la telecamera dello smartphone) e che consente all'utente di inviare al *server di backend* il suo «registro dei codici generati» che viene, così, messo a disposizione di tutti gli altri soggetti che abbiano installato la App. Questi ultimi potranno, una volta ricevuti tali codici, verificare (confrontandoli) se taluno dei codici ricevuti dal server corrisponda a uno dei codici memorizzati nel «registro dei codici ricevuti». In un sistema decentrato, quindi, qualsiasi utilizzatore della App potrà essere informato del fatto che è entrato in contatto, per un certo periodo e a una certa distanza, con un soggetto al quale sia stata diagnosticata la patologia. Tuttavia, nessuno è in grado di sapere quale sia il dispositivo che abbia generato i codici ricevuti né potrà essere individuato e contattato, nemmeno dal servizio sanitario: il fatto che egli si ponga in quarantena o decida di recarsi presso un centro medico per eseguire i controlli diagnostici, è rimesso, quindi, al suo "buon senso".
Nel quadro così delineato si inserisce anche l'accordo[14] siglato tra Apple e Google, che, nei primi giorni di aprile, hanno annunciato un'iniziativa congiunta per creare un sistema interoperabile (tra i sistemi operativi iOS e Android, rispettivamente della Apple e di Google che da soli controllano, sostanzialmente, la totalità dei dispositivi mobile: 86,6% il sistema Android e 13,4% il sistema iOS) di *contact tracing* basato sul programma DP-3T che ponga al centro la privacy dell'utente sin dalla sua progettazione. In tal modo si intende creare un sistema[15] in grado di aiutare i governi e le autorità sanitarie a ridurre la diffusione del virus. I primi giorni del mese di maggio 2020 all'interno dei sistemi operativi in questione è stata rimessa all'utente la possibilità di attivare il sistema di *contact tracing* "inglobato" nel sistema operativo.

5. Il *contact tracing* tecnologico alla prova del GDPR

L'Europa conosce, ormai da qualche anno, un Regolamento sulla protezione dei dati personali (Regolamento UE 2016/679, comunemente indicato con l'acronimo GDPR) che definisce la tutela dei dati personali come contributo «alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche» (considerando 2). Al contempo, pur riconoscendo (cons. 1) la tutela delle persone fisiche con riguardo al trattamento dei dati di carattere

[14] https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-BluetoothSpecification.pdf.
[15] Il sistema consiste nel rilascio delle API (acronimo per "*Application Programming Interface*" con il quale si indicano insiemi di protocolli e procedure già pronte da essere inglobate all'interno di altri progetti) che consentono l'interoperabilità fra i dispositivi Android e iOS delle app sviluppate dalle autorità sanitarie.

personale come diritto fondamentale ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8, par. 1) e del Trattato sul funzionamento dell'Unione europea (art. 16, par. 1), esclude che si tratti di una «prerogativa assoluta» (cons. 4) e afferma, anzi, che tale tutela vada considerata alla luce della sua funzione sociale e contemperata con altri diritti fondamentali.

La protezione dei dati personali, in situazioni emergenziali come quelle attuali, caratterizzate anche dal diffuso timore del contagio di un male inarrestabile, viene messa a dura prova. E ciò in considerazione del crescente (come si vedrà, falso) convincimento, che la riduzione delle tutele garantite in materia di protezione dei dati personali sia necessaria alla salvaguardia della salute pubblica. D'altronde lo stesso Parlamento europeo, con risoluzione del 17 aprile 2020[16] – dopo aver preso atto dello sviluppo di applicazioni di ricerca dei contatti su dispositivi mobili per avvertire l'utente di essere in prossimità di una persona infetta, nonché della raccomandazione della Commissione europea di sviluppare un approccio comune a livello dell'UE per l'uso di tali applicazioni – ha sottolineato «che le autorità nazionali ed europee sono tenute a rispettare pienamente la legislazione sulla protezione dei dati e della vita privata e ad attenersi agli orientamenti e alla sorveglianza delle autorità nazionali preposte alla protezione dei dati».

Come contemperare, allora, la protezione dei dati personali con l'interesse pubblico a che il virus non si propaghi oltre la soglia di reazione del sistema sanitario?

L'art. 6 del GDPR contempla, tra le diverse basi giuridiche di legittimità del trattamento di dati personali, sia la necessità di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica, sia la necessità di realizzare un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito il titolare (bisogna focalizzare l'attenzione sul fatto che tale trattamento debba essere "necessario" agli scopi menzionati). Il considerando 46 del GDPR, oltretutto, prevede la possibilità che alcune finalità, quale quella di tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, possano trovare il giusto inquadramento in entrambe le basi giuridiche appena menzionate.

Ogni informazione relativa allo stato di salute di una persona fisica rappresenta un dato appartenente alle «categorie particolari» di cui all'art. 9 del GDPR, che detta il divieto generale di trattare tale categoria di dati personali salvo che non ricorrano alcune specifiche eccezioni. Tra queste ultime è ricompreso il trattamento di dati relativi a una persona fisica (e specificamente al suo stato di salute) necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero, sempreché siano predisposte (dalle norme dell'UE o dello Stato) delle «misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato (quale, ad esempio, il segreto professionale)». Ciò significa, ad esempio, che – come esplicitato dal considerando 54 – il trattamento di categorie particolari di dati, in presenza di tali basi giuridiche, può prescindere dal consenso dell'interessato (che rappresenta un'altra delle basi giuridiche previste dall'art. 6 GDPR).

[16] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_IT.pdf.

6. La disciplina dell'emergenza in Italia e l'iter per l'adozione del *contact tracing* tecnologico

Occorre, a questo punto, comprendere come, nel nostro Paese, possano essere predisposte misure tecnologiche di *contact tracing* pur tenendo in considerazione che da più parti[17] si è evidenziata la mancanza di riscontri scientifici sulla efficacia del *contact tracing* digitale nel contrasto alla pandemia e che, da un punto di vista logico, tali strumenti potrebbero svolgere un ruolo determinante se attuati nella fase iniziale della diffusione dell'epidemia.

Tra le norme interne, aventi ad oggetto il trattamento dei dati personali, che vengono in rilievo nello stato di emergenza da CoViD-19 troviamo, anzitutto, quella inizialmente contemplata dall'art. 5, Ocdpc n. 630 del 3 febbraio 2020 (recante *Primi interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*), che è stata dapprima trasfusa nell'art. 14 del DL 14/2020 e, successivamente, inserita nell'art. 17-bis del DL 18/2020 (a seguito dell'abrogazione del DL 14/2020 ad opera dell'art. 1, co. 2, L. 27/2020, che ha, contestualmente, convertito, con modifiche, il DL 18/2020).

L'art. 17-*bis* del D.L. 18/2020 (come convertito dalla L. 27/2020), pertanto, prevede misure specifiche in tema di trattamento dei dati personali (efficaci fino al termine dell'attuale stato d'emergenza). In specie si prevede che, nel rispetto degli artt. 9, par. 2, lett. g), h) e i), e 10 del GDPR, determinati soggetti impegnati nel contrasto all'emergenza CoViD-19-19 (tra i quali il Servizio nazionale di protezione civile, gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale) possano trattare anche dati personali di cui agli artt. 9 e 10 del GDPR, che risultino necessari all'espletamento delle funzioni loro attribuite nella gestione dell'emergenza[18].

Non si realizza pertanto, né si poteva realizzare, una deroga alle disposizioni del GDPR (fonte gerarchicamente sovraordinata), ma si definiscono i ruoli e i compiti nel trattamento dei dati (in particolare quelli relativi allo stato di salute) per finalità di tutela della salute pubblica. Si prevede inoltre (al secondo comma dell'art. 14) la possibilità che tali dati personali vengano "comunicati" anche a soggetti diversi e, ancora, che vengano "diffusi" dati personali diversi da quelli previsti negli artt. 9 e 10 GDPR,

[17] Sul punto si vedano: la raccomandazione dell'8 aprile 2020 della Commissione europea («The effectiveness of these applications has generally not been evaluated»), reperibile al link: https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf; la ricerca dell'Ada Lovelace Institute («There is an absence of evidence to support the immediate national deployment of symptom tracking applications, digital contact tracing applications and digital immunity certificates»), reperibile al link: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf; le dichiarazioni di Jason Bay, direttore responsabile presso GovTech, l'agenzia governativa di Singapore per la digitalizzazione («If you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No. Not now and, even with the benefit of AI/ML and — God forbid — blockchain (throw whatever buzzword you want), not for the foreseeable future»), reperibile al link: https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98.

[18] In virtù di tale norma, tra l'altro, il 9 aprile 2020 il capo della protezione civile, con il benestare del capo della polizia, ha firmato un'ordinanza in base alla quale le questure o i commissariati possono mettere a disposizione delle ASL, previa ricerca nelle banche dati a disposizione del Ministero dell'interno, le utenze mobili dei soggetti entrati in contatto con una persona "positiva" nel caso in cui non sia possibile risalire in altro modo a tali soggetti al fine di poterli avvisare del potenziale contagio.

ma unicamente nelle ipotesi in cui la comunicazione o la diffusione risultino indispensabili alla gestione dell'emergenza in atto. Rilevante è, infine, l'ultimo comma, a mente del quale una volta cessato lo stato d'emergenza devono essere adottate misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali.

Inoltre, la norma in esame nulla prevede in relazione al trattamento dei dati relativi all'ubicazione di utenti o abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico. In assenza di una specifica previsione, il trattamento dei dati di ubicazione è soggetto alla disciplina di cui all'art. 126, D.Lgs. 196/03 (in conformità a quanto previsto dall'art. 9 della c.d. Direttiva e-privacy, 2002/58/CE). Le eventuali disposizioni interne, derogatorie alle limitazioni a tali trattamenti, possono essere introdotte – ai sensi dell'art. 15 della Direttiva e-Privacy – qualora tale restrizione costituisca una misura necessaria, opportuna e proporzionata all'interno di una società democratica.

Con l'art. 76 del già menzionato DL 17 marzo 2020, n. 18, inoltre, è stato istituito il *Gruppo di supporto digitale alla Presidenza del Consiglio dei ministri per l'attuazione delle misure di contrasto all'emergenza CoViD-19-19*, ossia un "contingente di esperti" che devono offrire supporto al Governo per ciò che concerne «introduzione di soluzioni di innovazione tecnologica e di digitalizzazione della pubblica amministrazione». Con relativo decreto del 31 marzo 2020[19], il Ministro per l'innovazione tecnologica e la digitalizzazione, ha nominato un contingente di 74 persone (una delle "*task force*" governative per la gestione dell'emergenza), tra i cui compiti rientra quello di «individuare possibili soluzioni offerte dalle tecnologie digitali […] e procede alla valutazione delle soluzioni proposte nell'ambito della 'Fast Call per tecnologie per il contrasto alla diffusione del CoViD-19-19». A seguito di tale "*fast call*" (pubblicata[20] sul sito del Ministero il 23 marzo) sono state proposte oltre trecento soluzioni, tra le quali è stata scelta quella della società Bending Spoons (e la relativa "app" è, attualmente, denominata "Immuni"[21]). Allo stato, in Italia, non sono state ancora rese pubbliche le specifiche tecniche di Immuni, ma, sulla scorta di quanto pubblicato sul sito del Ministero per l'innovazione, la App dovrebbe seguire il modello DP-3T e l'iter di realizzazione dovrebbe concludersi entro la seconda metà del mese di maggio 2020.

Successivamente, nel corso dell'audizione informale alla IX Commissione della Camera del 8 aprile[22], il Garante per la protezione dei dati personali, ha ribadito la possibilità di conciliare l'uso delle nuove tecnologie e della rete per contrastare l'emergenza epidemiologica da Coronavirus con le norme in materia di protezione di dati personali. Il Garante, dopo aver evidenziato che nuove e più stringenti previsioni, fondate su esigenze di sanità pubblica, richiederebbero una base normativa conforme ai principi generali in tema di protezione dei dati personali, ha individuato, con riguardo alle tecnologie di *contact tracing*, le seguenti precauzioni: 1) particolare attenzione al rispetto del principio di proporzionalità; 2) necessità di valutare che l'efficacia attesa dalla misura non può prescindere dalla capacità di reazione ai risultati di *contact tracing* con le azioni complementari (es. test diagnostici); 3) preferire

[19] https://innovazione.gov.it/assets/docs/DM%20Gruppo%20di%20lavoro%20COVID%2019-signed.pdf
[20] https://bit.ly/2LWQD2z.
[21] Sul punto si veda l'analisi giuridica del software fatta dalla task force ministeriale e reperibile a questo indirizzo https://github.com/taskforce-covid-19/documents/blob/master/sgdl_8_Profili_Giuridici_Gestione_Dati_Emergenza/sgdl8_relazione_immuni.pdf.
[22] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9308774.

sistemi fondati sulla volontaria adesione dei singoli, e in cui la mancata adesione non comporti pregiudizi di sorta; 4) preferire le soluzioni decentrate a quelle centralizzate; 5) limitare, comunque, la conservazione dei dati; 6) preferire un modello coordinato a livello europeo per garantire interoperabilità; 7) realizzare la filiera del *contact tracing* completamente in ambito pubblico; 8) prevedere una *sunset provision* efficace alla cessazione dello stato d'emergenza.

I principi tracciati dal Garante italiano sono ribaditi dal Comitato europeo per la protezione dei dati (EDPB), nelle linee-guida 4/2020[23] del 21 aprile, in cui, con specifico riguardo al *contact tracing* (senza ricorso alla geolocalizzazione) ha chiarito (e ribadito) che il sistema, per essere correttamente bilanciato con i diritti fondamentali, dovrebbe, tra l'altro:

Prevedere la volontarietà dell'eventuale adozione da parte degli utenti senza che al mancato utilizzo possano conseguire pregiudizi di qualsivoglia natura;

Individuare chiaramente le finalità perseguite in modo da consentire la verifica del rispetto del principio di limitazione e minimizzazione;

Evitare che la crisi sanitaria su trasformi in un'occasione per derogare rispetto al principio di limitazione della conservazione dei dati: successivamente alla crisi, di norma, tutti i dati personali dovrebbero essere cancellati o resi anonimi;

Rendere verificabili gli algoritmi usati nel *contact tracing* e rendere il codice sorgente pubblico in modo da assicurare la più ampia trasparenza;

Considerare che sono praticabili sia soluzioni centralizzate che decentrate, ma le misure di sicurezza dovranno essere adeguate ai rischi.

Nelle linee-guida, infine, il monito secondo cui «a nessuno dovrebbe essere chiesto di scegliere tra una risposta efficace all'attuale crisi e la tutela dei diritti fondamentali: entrambi gli obiettivi sono alla nostra portata, e i principi di protezione dei dati possono svolgere un ruolo molto importante nella lotta contro il virus».

7. L'art. 6 del DL 28/2020: la prima disciplina di dettaglio sul contact tracing digitale.

Il procedimento normativo della tecnologia di *contact tracing* trova, infine, la sua conclusione (almeno sino a questo momento) nell'art. 6 del DL 30 aprile 2020, n. 28, rubricato «Sistema di allerta CoViD-19-19». L'attuale versione è frutto anche dell'intervento del Garante per la protezione dei dati personali che ha offerto al Governo una serie di suggerimenti, con il parere del 29 aprile[24], che sono stati recepiti nella versione definitiva della norma in questione.

L'art. 6 del DL 28/2020 prevede, in sostanza, che il fine del sistema di *contact tracing* è quello di «allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione» e che il sistema è rappresentato da una piattaforma unica nazionale e dalle applicazioni installate sui dispositivi di telefonia mobile. Si prevede, inoltre, il compimento di una valutazione di impatto (o DPIA – *data protection impact assessment* – ai sensi dell'art. 35 del GDPR) che sarà – a prescindere dall'esito della stessa – comunque sottoposta alla valutazione e approvazione dell'Autorità Garante per la protezione dei dati; che al mancato utilizzo

[23] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9322501.
[24] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9328050.

ISSN 2284-4503

dell'applicazione non potranno seguire conseguenze pregiudizievoli; che ogni trattamento di dati personali ai sensi del medesimo articolo dovrà cessare alla cessazione dell'emergenza e, comunque, entro il 31 dicembre 2020.
Sebbene le previsioni normative contemplate dall'art. 6 del DL 28/2020 siano state adeguate alle indicazioni sia delle linee-guida 4/2020 EDPB che del parere del Garante, residuano margini di ambiguità. Innanzitutto, non è stato chiarito, come auspicato dal Garante nel suo parere, se il sistema di *contact tracing* sarà centralizzato ovvero decentrato nella memorizzazione e gestione delle informazioni di tracciamento. In secondo luogo, sembrerebbe che ad essere rilasciati sotto licenza aperta ai sensi dell'art. 69 del Codice dell'amministrazione digitale siano esclusivamente i programmi sviluppati per realizzare la piattaforma e utilizzare l'applicazione ma non l'applicazione medesima. In un'ottica di maggiore trasparenza dovrebbe estendersi il rilascio con licenza aperta dell'applicazione e del codice sorgente della stessa. Ciò consentirebbe di "compilare" l'applicazione partendo dal codice sorgente e di verificare appieno il funzionamento dell'applicazione reperibile presso gli *app store* (*Google Play e Apple Store*) che sarà confrontabile – con gli algoritmi di *hash* – con la medesima versione della app compilata.

8. Conclusioni

Considerando che, allo stato, non è stata ancora rilasciata l'applicazione in questione sarà necessario verificarne l'evoluzione, anche nel prosieguo, al fine di poter constatare l'effettivo rispetto delle linee-guida dell'EDPB e delle indicazioni del Garante e, in genere, il rispetto della disciplina del GDPR.
Uno degli aspetti che dovrà essere tenuto in somma considerazione, anche nella fase in cui si espleterà la DPIA (la valutazione d'impatto prevista dall'art. 35 del GDPR e, con specifico riguardo al sistema di *contact tracing* previsto dall'art. 6 del DL 28/2020) è quello relativo alla sicurezza informatica del sistema di *contact tracing*. Si dovranno tenere in considerazione sia i profili problematici connessi all'utilizzo di tecnologie *bluetooth*, sia i profili di sicurezza del *server di backend* che quelli dell'applicazione.
In conclusione, la disciplina sulla protezione dei dati personali non rappresenta un ostacolo all'efficientamento della prevenzione e contrasto della pandemia ma, al contempo, non ammette un'abdicazione alla tutela dei diritti fondamentali. Pertanto, nel perseguimento delle finalità preventive e di contenimento dell'epidemia dovranno, anzitutto, preferirsi le soluzioni tecnologiche che impieghino dati anonimi. L'uso, invece, di dati personali sarà ammissibile – in una situazione di emergenza che, comunque, come può determinare la compressione di altre libertà fondamentali (quale quella alla libera circolazione delle persone) potrà determinare anche la compressione del diritto alla protezione dei dati personali – purché le misure predisposte siano proporzionate alle esigenze di contrasto e siano circoscritte al tempo dell'emergenza. La questione, quindi, non può ridursi all'alternativa dell'utilizzo o meno delle tecnologie disponibili, ma va sapientemente condotta, con l'utilizzo delle tecnologie e dei dati personali, nel rispetto dei principi generali in materia di protezione dei dati personali anche per evitare quello che è stato individuato dal Garante per la protezione dei dati personali, durante la sua audizione dell'8 aprile, come «il rischio dello scivolamento inconsapevole dal modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per l'efficienza e la delega cieca all'algoritmo per la soluzione salvifica».