TRACCIAMENTO TECNOLOGICO DEL CONTAGIO

CONTACT TRACING TECHNOLOGY

Actualidad Jurídica Iberoamericana Nº 12 bis, mayo 2020, ISSN: 2386-4567, pp. 868-885

Marcello
D'AMBROSIO

ARTÍCULO RECIBIDO: 8 de mayo de 2020
ARTÍCULO APROBADO: 10 de mayo de 2020

RESUMEN: Lo scritto analizza il tema dell'impiego delle TIC nel tracciamento del contagio da COVID-19. L'introduzione di "app" capaci di controllare l'epidemia suscita forti perplessità in relazione alla tutela della riservatezza. Lo studio ha lo scopo di avvalorare la tesi per la quale l'impiego delle tecnologie nella gestione dell'emergenza sanitaria non soltanto è lecito ma necessario al fine di assicurare un bilanciamento, guidato dai principi di adeguatezza, proporzionalità e ragionevolezza, tra valori fondamentali dell'ordinamento.

PALABRAS CLAVE: Tracciamento; contagio; dati personali; riservatezza.

ABSTRACT: *The paper analyzes the issue of the use of ICT in COVID-19 contact-tracing. The introduction of "app" capable of controlling epidemic raises concern about privacy. The essay sets out to highlight that the use of technologies in the management of the pandemic is lawful and necessary in order to balance fundamental rights according to the principles of adequacy, proportionality and reasonableness.*

KEY WORDS: *Contact-tracing; infection; personal data; privacy.*

1. Non c'è altra soluzione che tracciare! Sembra, questa, la conclusione a cui sono giunti i governi di molti dei Paesi, duramente, colpiti dall'epidemia di COVID-19. Il *totem* della *privacy*, baluardo della riservatezza, subisce uno degli attacchi più duri mai registrati (i rischi a cui sono esposti i dati personali sono sempre più frequenti, come rileva Perlingieri, P.: "*Privacy* digitale e protezione dei dati personali tra persona e mercato", in *Foro nap.*, 2018, p. 481 ss.; sul punto, altresì, Perlingieri, C.: *Profili civilistici dei social networks*, Napoli, 2014, p. 68 ss.; Sica, S., Zeno-Zencovich, V.: "Legislazione, giurisprudenza e dottrina nel diritto dell'*internet*", in *Dir. inf.*, 2010, p. 382). Di tal guisa, ciò che fino a qualche tempo addietro sembrava inconcepibile nelle democrazie occidentali, ovverosia una sorveglianza di massa (uno scenario, per certi aspetti, non così sconosciuto secondo Zuboff, S.: *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019; cfr., altresì, Resta, G.: "La sorveglianza elettronica di massa e il conflitto regolatorio Usa/Ue", in *Dir. inf.*, 2015, p. 697 ss.), s'impone, oggi, come la "via da seguire". Il controllo del contagio ha, in poco tempo, assunto il valore di un'opzione ineludibile, a fronte del bisogno di recuperare la "normalità" nella sua più comune retorica. Tale urgenza tradisce quanto il nostro modello socioeconomico, costruito sulle ceneri di contrapposizioni basate sulla forza delle armi e plasmato dalla matrice della società dei consumi (v. la lucida analisi di Bauman, Z.: *Consumo, dunque sono*, Bari, 2017), non sia in grado di sopportare una prolungata stasi. Con sguardo ingenuo rivolto a ripristinare "il mondo di prima", si accetta l'idea che la quotidianità possa essere monitorata, al fine di scongiurare un disastro sanitario, nella maturata consapevolezza che il prolungato distanziamento sociale, unica arma efficace nelle mani del decisore politico, risulti, ormai, socialmente insostenibile. Di qui, segue la ricerca di ogni mezzo che possa interrompere la pausa dal "vivere". Per riprendere le attività relazionali, tuttavia, occorre garantire la protezione della salute, individuale e pubblica. La tecnologia, al riguardo, offre strumenti idonei a tracciare la condizione delle persone nel tempo e nello spazio (utili, in generale, le riflessioni di Rodotà, S.: *Tecnologie e diritti*, Bologna, 1995, p. 19 ss.; Rodotà, S.: "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", in *Riv. crit. dir. priv.*, 1997, p. 586 ss.), sì che, *mutatis mutandis*, traslando il pensiero di chi fa appello alla costatazione di quanto, in certi casi, sia inutile aspettare che le cose si sistemino da sole, rinviando l'inevitabile, viene da dire: "se non ora, quando?" (Levi, P.: *Se non ora, quando?*, Torino, 1982). La sfida posta dell'emergenza, dunque, ci impegna a rispondere all'interrogativo rivolto a stabilire

• Marcello D'Ambrosio
Professore associato diritto privato, Università degli Studi di Salerno. Correo electrónico: mdambrosio@unisa.it

se non sia questo un (o il) momento nel quale accettare di 'essere controllati' in favore di un valore ritenuto preminente.

2. Al fine di rispondere al quesito posto in premessa è necessario definire, seppur sommariamente, quale sia l'esigenza che, nella sfida alla pandemia, legittimi il ricorso alle TIC. Il tracciamento del contagio può essere, infatti, realizzato attraverso soluzioni differenti (si pensi, ad esempio, alla tecnologia prevista nel progetto franco-tedesco che ha dato vita al *ROBERT Protocol*, sviluppato nell'ambito dell'iniziativa PEPP-PT, *Pan European Privacy-Preserving Proximity Tracing* ovvero le soluzioni API Apple-Google). All'attenzione dei più, il riferimento è alle c.dd. "*app*". Per questa via, in Europa, sulla scorta di pregresse esperienze internazionali, si valuta la previsione – e si apprezza l'introduzione – di applicativi che installati su *device* personali siano in grado di raccogliere, monitorare e condividere dati sulla condizione di salute e sugli spostamenti dell'utente (per una dettagliata ricostruzione, anche tecnica, delle soluzioni prospettate sul territorio europeo, cfr. "eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States", Version 1.0, 15 aprile 2020, in *https://ec.europa.eu/health/sites/health/files/ehealth/docs/COVID-19_apps_en.pdf*). Di là dai benefici paventati, la previsione di uno strumento di tal fatta genera legittime perplessità negli studiosi, a vario titolo, della materia e, di conseguenza – seppur solo in parte – nella collettività, non pienamente consapevole delle caratteristiche, delle funzionalità e dei rischi degli strumenti evocati (circa l'inconsapevolezza degli utenti di fronte all'impiego delle nuove tecnologie, D'Ambrosio, M.: "Confidentiality and the (Un)Sustainable Development of the Internet", in *Italian Law Journal*, 2, 2016, p. 252 ss.; D'Ambrosio, M.: *Progresso tecnologico, «responsabilizzazione» dell'impresa ed educazione dell'utente*, Napoli, 2017, p. 20 ss.; nonché Di Ciommo, F.: "Diritti della personalità tra media tradizionali e avvento di *internet*", in AA.VV.: *Persona e tutele giuridiche* (a cura di G. Comandè), Torino, 2003, p. 3 ss.; Perlingieri, C.: "La tutela dei minori di età nei *social networks*", in *Rass. dir. civ.*, 2016, p. 1324). La selezione dell'interesse posto alla base della "scelta" di affidare a un sistema integrato di tecnologia – *hardware* e *software* – il compito di assicurare un ritorno controllato alle ordinarie relazioni collettive è divenuta, pertanto, un piano di confronto dirimente per accertare la compatibilità con il nostro sistema ordinamentale della prospettata gestione di dati (particolarmente) sensibili.

Senza dubbio la finalità posta alla base del ricorso a strumenti di tracciamento è, in prima battuta, rinvenibile nella tutela della salute. In applicazione del diritto sancito dall'art. 32 cost., non solo come diritto del singolo ma come interesse della collettività, si giustificano forme di monitoraggio con le quali si bilanciano valori contenuti nelle disposizioni costituzionali (Bin, R.: *Diritti e argomenti: il*

bilanciamento degli interessi nella giurisprudenza costituzionale, Milano, 1992). L'opposizione all'introduzione di strumenti che indaghino e traccino la condizione di salute individuale vede, dunque, deboli argomenti contrari che possano negare la necessità e la convenienza di risposte efficaci nei confronti di un'emergenza sanitaria. Nel bilanciamento tra valori fondamentali della persona, posti alla base del nostro ordinamento, sembra legittimo, attesa l'eccezionalità della condizione attuale, accogliere un'interpretazione del dato normativo che giustifichi scelte, singolari, distanti altrimenti dalla regolare applicazione della legge, ossequiosa della libertà e della riservatezza delle persone.

Nel dibattito sull'impiego delle nuove tecnologie nella lotta all'epidemia emerge, tuttavia, un diverso interesse, la protezione del quale induce, con vigore, verso il ricorso a strumenti di tracciamento. Il riferimento è all'interesse alla ripresa delle attività economiche, per le quali la salute individuale e collettiva ha imposto una sospensione. L'art. 41 cost. è chiaro nel definire che l'iniziativa economica privata, nella sua più ampia formulazione, non possa mai svolgersi in modo da arrecare danno alla sicurezza umana (Bifulco, R., Celotto, A., Olivetti, M.: *Commentario alla Costituzione*, Torino, 2006; nonché Perlingieri, P.: *Commento alla costituzione italiana*, Napoli, 2001, p. 241 ss.).

Se la sospensione delle attività produttive e commerciali si è mostrata legittima – e lo è tuttora – lo *stress* sopportato dal mercato, acuito pure dall'incertezza sulla durata del blocco delle attività, rischia di generare effetti gravi, alcuni dei quali di medio-lungo periodo. Il morso della crisi economica, che prende larga parte della cittadinanza, compresa quella porzione che non risulta essere stata vittima sanitaria dell'emergenza, giustifica la protezione di un interesse che fa da contrappunto alla prudenza insita nel distanziamento sociale. Si osserva l'espressione di un valore di rilevanza costituzionale che reclama una ponderata caratura dei limiti a esso imposti. Nell'assunzione della decisione di offrire alla collettività strumenti di tracciamento del contagio emerge, dunque, tanto la necessità di assicurare la tutela salute della cittadinanza quanto l'esigenza di proteggere il tessuto imprenditoriale, l'iniziativa economica e con essa quella moltitudine di manifestazioni dell'autonomia negoziale che, lasciate per troppo tempo in una condizione di mera, putativa, sospensione, rischiano di compromettere l'ordinata esecuzione dei rapporti privati e di dar vita a un'inevitabile recrudescenza della litigiosità contrattuale.

A fronte delle considerazioni espresse sul bilanciamento valoriale, potrebbe, ragionevolmente, replicarsi che le esigenze illustrate non richiedono, per forza, il ricorso a strumenti di tracciamento tecnologico. Non vi sarebbe la necessità di comprimere oltre alla libertà personale anche la sfera di riservatezza delle persone. Tuttavia, prima di liquidare la questione con approssimazione argomentativa, ammettendo *in re ipsa* che le soluzioni tecniche in azione determinino, in concreto,

un tale effetto, è bene verificare se non sia il bilanciamento evocato a imporre la doverosità del ricorso a sistemi di tracciamento tecnologico del contagio.

La previsione di limitazioni a talune libertà fondamentali richiede una concreta ponderazione dell'equilibrio tra valori da effettuarsi in termini quantitativi, qualitativi e temporali. La compressione delle libertà è legittima solo se – e nella misura in cui – sia, strettamente, necessaria alla protezione della persona. La rilevanza dei valori mortificati è tale da non ammettere soluzioni incongrue rispetto al fine, ingiustificatamente più ampie rispetto allo scopo perseguito, temporalmente non calibrate in funzione del controllo dell'epidemia. Sì che sono illegittime quelle soluzioni normative che non rispondano, in base ai principi di proporzionalità (quale tratto fondamentale del neo-costituzionalismo moderno, cfr. Barak, A.: "Proportionality", in *Cambridge University Press*, 2012, p. 175 ss.; Stone Sweet, A., Mathews, J.: "Proportionality Balancing and Global Constitutionalism", in 47 *Columbia Journal of Transnational Law* 2008, p. 73), adeguatezza e ragionevolezza, all'esigenza di protezione dei valori evocati (in riferimento al principio guida della ragionevolezza, cfr. Paladin, L.: "Ragionevolezza (principio di)", in *Enc. Dir.*, agg., I, Milano, 1997, p. 899 ss.; nonché in una prospettiva attenta alla logica del bilanciamo dei valori, Perlingieri, G.: *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 102 ss.; Perlingieri, G.: "Ragionevolezza e bilanciamento nell'interpretazione recente della corte costituzionale", in *Riv. dir. civ.*, 2018, p. 716 ss.; in giurisprudenza, Corte cost., 29 maggio 1995, n. 220, in *www.cortecostituzionale.it*).

La determinazione dei provvedimenti adottabili richiede di valutare tutte le opzioni per assicurare il controllo e il superamento della situazione di crisi. Nello scenario di operatività offerto, un ruolo imprescindibile è, ormai, svolto dalla tecnologia, anche dal punto di vista sanitario (con la Raccomandazione UE 2020/518 della Commissione dell'8 aprile 2020, la Commissione europea precisa che alcune di queste applicazioni mobili "potrebbero essere considerate dispositivi medici" qualora siano destinate dal fabbricante a essere utilizzate, tra l'altro, a fini di diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie). Si pensi, inoltre, a quanto l'innovazione tecnica abbia mutato e migliorato la natura dei rapporti sociali, pure nell'emergenza, assistendo e concedendo l'esecuzione di prestazioni altrimenti impossibili. Il dato non può essere sottovalutato nella scelta delle azioni da mettere in campo. Per questa via, nello stabilire il condizionamento delle libertà deve valutarsi fino a che punto tale azione possa essere ritenuta legittima ove si riscontri che l'impiego di strumenti tecnologici (sul rapporto tra libertà e tecnologia, si rinvia alle riflessioni di Sica, S.: *La libertà fragile*, Napoli, 2014, p. 16 ss.), collocati in sicurezza, con un trattamento affidato, ad esempio, alle autorità sanitarie nazionali, assicuri una migliore esplicazione ai valori costituzionali, diversamente compromessi (Cartabia, M.: "I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale

italiana", 2013, in *www.cortecostituzionale.it*, p. 11, ricorda che "non soltanto nessun diritto costituzionale può considerarsi assoluto, tale cioè da prevalere sugli altri in misura indiscriminata; ma ogni disposizione che impone un sacrificio, una restrizione o una limitazione di un diritto costituzionale deve valere alla maggior realizzazione di un altro interesse costituzionale").

Segnatamente, può ritenersi, che se la tecnologia, nella piena conformità all'ordinamento, permetta alla libertà di circolazione e all'iniziativa economica privata di non essere limitate, ovvero di essere riprogrammate sotto altre direttrici, il mancato ricorso a tale opportunità risulterebbe disallineato rispetto a un quadro di legalità costituzionale (secondo una prospettiva, in generale, descritta da Perlingieri, P.: *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, Napoli, 2006, p. 188 ss.).

3. Definita, in astratto, la legittimità del ricorso al tracciamento tecnologico del contagio, è necessario precisare, in concreto, quale sia l'oggetto del tracciamento, al fine di stabilire se il trattamento dei dati risulti adeguato alla finalità prefissata.

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), si avverte che date "l'elevata invasività" delle soluzioni di tracciamento tecnologico e le sfide che esso comporta, prima di ricorrere a questa opzione è necessario effettuare un'attenta analisi. La Commissione raccomanda l'utilizzo di applicazioni facoltative. Le funzionalità contenute nelle *app*, infatti, "possono incidere in misura diversa su un'ampia gamma di diritti sanciti dalla Carta dei diritti fondamentali dell'UE: dignità umana, rispetto della vita privata e familiare, protezione dei dati di carattere personale, libertà di circolazione, non discriminazione, libertà d'impresa, libertà di riunione e di associazione. L'interferenza con la vita privata e il diritto alla protezione dei dati di carattere personale può essere particolarmente significativa dato che alcune delle funzionalità si basano su un modello ad elevata intensità di dati". In conclusione, *condicio sine qua non* per lo sviluppo, l'accettazione e l'utilizzo di tali applicazioni da parte delle persone è la "fiducia", che presuppone la dimostrazione che gli utenti mantengono il pieno controllo dei propri dati.

La Commissione europea ha definito il perimento di operatività delle applicazioni mobili facoltative di tracciamento, suddividendole in quelle che: danno informazioni sulla pandemia di COVID-19 (per tali applicazioni si rileva che, in base al principio di minimizzazione dei dati, non v'è bisogno di raccogliere, conservare e trattare informazioni personali, salvo che nell'ipotesi nella quale il dato sia necessario per fornire il servizio di informazione: un esempio è l'*app* "AllertaLom",

messa appunto dalla Regione Lombardia e utilizzata per ricevere le comunicazioni della Protezione Civile, nonché notifiche e informazioni); allertano le persone che si sono trovate per un certo tempo in prossimità di un soggetto infetto, per dare informazioni sulla collocazione in auto-quarantena (per questa categoria di applicazioni la Commissione europea raccomanda l'impiego di tecnologia BLE, la quale permette di tracciare i contatti in maniera più precisa ed evita di raccogliere dati di geolocalizzazione); offrono alle persone questionari di autovalutazione dei sintomi e di orientamento alla condotta (funzionalità di controllo dei sintomi) o un canale di telemedicina (questo tipo di strumenti, trattando dati personali relativi alla salute, richiedono l'applicazione di un più rigido regime normativo ai sensi del GDPR).

In particolare, per gli utenti che utilizzano la funzionalità "controllo dei sintomi", le informazioni contenute nell'apparecchiatura terminale possono essere trattate solo nella misura necessaria per consentire all'*app* il suo funzionamento. La Commissione europea precisa che la funzionalità "controllo dei sintomi" può essere utile agli Stati membri "per indirizzare i cittadini verso eventuali test, fornire informazioni sull'isolamento e sulle tempistiche e le modalità di accesso all'assistenza sanitaria". Questa funzionalità può, inoltre, "integrare l'assistenza sanitaria di base e aiutare a comprendere quali sono i tassi di infezione da COVID-19 nella popolazione". Al fine di raggiungere lo scopo si dovrebbe chiarire che i dati personali relativi alla salute sono trattati allo scopo a) di fornire alla persona la possibilità di autovalutare, sulla base di una serie di domande, se ha sviluppato sintomi della malattia, oppure b) di ottenere una consulenza medica nel caso in cui abbia effettivamente sviluppato tali sintomi. I dati raccolti dovrebbero essere cancellati dopo un periodo massimo di un mese (quantificazione temporale che corrisponde al periodo di incubazione, aumentato di un margine di sicurezza) o dopo che la persona è stata sottoposta al tampone con esito negativo. Alle autorità sanitarie potrebbe essere accordato il potere di conservare i dati per periodi più lunghi a fini di sorveglianza e per attività di ricerca, "a condizione che ciò avvenga in forma anonima".

Non si conoscono, ancora, i dettagli tecnici del sistema di tracciamento tecnologico adottato in Italia. L'autorità pubblica si è limitata a divulgare solo alcune informazioni in merito alla selezione di un prodotto *software*, tra una schiera di alternative, offerte da soggetti privati (Ordinanza n. 10 del 16 aprile del Commissario per l'emergenza, in *http://www.governo.it/sites/new.governo.it/files/CSCOVID-19_Ord_10-2020_txt.pdf*). Si è appreso che lo strumento, facendo tesoro di opzioni programmate in passato, impiegherà la tecnologia degli applicativi installabili su dispositivi mobili, così come operato in altri ordinamenti.

Di fronte alla scelta di tracciare il contagio si richiede la raccolta di informazioni personali dell'utente, allo scopo di conoscere la sua condizione di salute e i suoi spostamenti. La raccolta delle informazioni dovrà essere guidata dal principio di minimizzazione dei dati, sancito dall'art. 5, par. 1, lett. c, del GDPR (un principio emblematicamente definito nel suo momento applicativo da Corte giust., 8 aprile 2014, C-293/12 e C-594/12, Digital Rights Ireland e Seitlinger e a., in *www.curia.europa.eu*), per il quale solo i dati personali che sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità possono essere trattati. Tecnicamente, sono molte altre le informazioni che potrebbero essere acquisite, direttamente o indirettamente, dalle applicazioni mobili, ma in coerenza con le previsioni normative in materia, non è concesso raccogliere dati che non siano aderenti alle finalità del trattamento.

Al livello europeo si sta tentando un coordinamento dell'azione degli Stati membri in materia (apprezzato anche dal Garante europeo: cfr. Lettera della Presidente del Comitato Europeo per la Protezione dei Dati alla Commissione europea sul Progetto di linee-guida in materia di app per il contrasto della pandemia dovuta al COVID-19, del 14 aprile 2020, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9316030*). In tal senso, la Commissione europea ha, con la Raccomandazione (UE) 2020/518, par. 3, riconosciuto che è «necessario mettere a punto un approccio comune» all'uso delle tecnologie e dei dati digitali in risposta all'attuale crisi. Tale azione è protesa a costituire un sostegno efficace per le autorità nazionali competenti, in particolare per le autorità sanitarie, fornendo dati per comprendere l'evoluzione dell'epidemia. Si rileva che le tecnologie digitali possono consentire ai cittadini di "adottare misure efficaci e maggiormente mirate di distanziamento sociale". L'approccio proposto, nondimeno, è utile a preservare l'integrità del mercato unico e "a tutelare i diritti e le libertà fondamentali, in particolare il diritto alla vita privata e alla protezione dei dati personali".

In questo solco, L'EDPB ha elaborato delle linee guida sull'uso dei dati di localizzazione e degli strumenti per il tracciamento del contagio (Linee-guida 04/2020 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, in *www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9322501*). Anche il Garante europeo ha riconosciuto che, ove sia necessario ricorrere al trattamento di dati personali per gestire la pandemia, la protezione delle informazioni personali sia "indispensabile per generare un clima di fiducia, creare le condizioni per l'accettabilità sociale di qualsiasi soluzione e garantire, pertanto, l'efficacia di tali misure". La raccolta delle informazioni, si precisa, non deve essere protesa a controllare le persone quanto ad assicurare nuovi strumenti utili alla collettività,

tenuto conto che i dati e le tecnologie possono essere, di certo, strumenti importanti, ma solo in maniera complementare ad altre misure di sanità pubblica.

L'azione condotta dagli Stati membri non può che essere guidata dai principi generali di "efficacia, necessità e proporzionalità" (ai sensi dell'art. 52 della Carta fondamentale dei Diritti dell'Unione europea e dell'art. 5 TUE). Si propone, dunque, un uso "proporzionato" (secondo la prospettiva delineata da Corte giust., 21 dicembre 2016, C-203/15 e C- 698/15, Tele2 Sverige AB, in *www.curia.europa.eu*) dei dati di localizzazione e degli strumenti di tracciamento, individuando due ambiti specifici: 1) utilizzo dei dati di localizzazione "a supporto della risposta alla pandemia tramite la definizione di modelli della diffusione del virus, al fine di valutare l'efficacia complessiva di misure di isolamento e quarantena"; 2) utilizzo del tracciamento dei contatti "per informare le persone che sono probabilmente entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio".

Secondo quanto ricostruito, prende vita un modello di tecnologia in virtù della quale le persone possano essere avvertite: a) mediante l'invio automatico di un'allerta "ai contatti ravvicinati quando un utente informa l'app – con l'approvazione o la conferma dell'autorità sanitaria, ad esempio mediante un codice QR o TAN – di essere risultato positivo al test (trattamento decentralizzato)"; b) mediante "identificativi temporanei" pseudoanonimizzati, generati in modo arbitrario e conservati su un *server back-end* tenuto dall'autorità sanitaria o decentrati sull'apparecchiatura dell'utente, in virtù dei quali gli utenti, che sono stati in contatto ravvicinato con un utente risultato positivo al test, ricevono una segnalazione sul loro *device* (cfr. Comunicazione della Commissione europea Orientamenti sulle *app*, cit.). È bene ricordare che l'identità della persona infetta "non dovrebbe essere comunicata" alle persone con le quali è stata in contatto epidemiologico, essendo sufficiente allertarle che sono state in contatto con un individuo risultato infetto nel corso degli ultimi 16 giorni.

4. I dati relativi all'ubicazione delle persone possono essere raccolti soltanto alle condizioni previste dal sistema europeo di protezione dei dati personali (sul punto, utile è il rinvio alle Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19, del 21 aprile 2020: in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9326465*). La Commissione europea ha esortato a definire con chiarezza la base giuridica del trattamento, sì da: a) stabilire con precisione i caratteri del trattamento di dati relativi alla salute, specificandone le finalità; b) indicare con precisione il titolare del trattamento, ossia l'entità incaricata della gestione dei dati, e chi, oltre al titolare del trattamento, può avere accesso a tali informazioni;

c) escludere la possibilità di trattare tali dati per finalità diverse da quelle elencate nella normativa e d) prevedere garanzie specifiche. Al fine di non compromettere l'utilità pubblica e l'accettazione delle *app*, il legislatore nazionale dovrebbe prestare particolare attenzione al fatto che la soluzione scelta sia quanto più inclusiva possibile nei confronti dei cittadini (ancora Comunicazione della Commissione europea Orientamenti sulle *app*, cit.).

Si ricorda che talune informazioni ai sensi della Direttiva 2002/58/CE, come recepita dal Codice della *privacy*, compresi i dati sull'ubicazione dell'utente, possono essere raccolti direttamente sul dispositivo dell'utente e a essi può essere consentito l'accesso solo a condizione che sia stato prestato il consenso dell'utente e la memorizzazione, oltre all'accesso, siano strettamente necessari alla fornitura del servizio (sul ruolo del consenso Viterbo, F.G.: *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008, p. 181 ss.; nonché Perlingieri, C.: *Profili civilistici dei social networks*, cit., p. 66 ss.; e, più di recente, Bravo, F.: "Il consenso e le altre condizioni di liceità del trattamento di dati personali", Aa.Vv.: *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali* (diretto da Finocchiaro, G.), Bologna, 2017, p. 101 ss.; Vivarelli, A.: *Il consenso al trattamento dei dati nell'era digitale*, Napoli, 2019, p. 25 ss.). In merito, il Garante europeo ricorda che in conformità al principio di minimizzazione, "i dati trattati dovrebbero essere limitati a quelli strettamente necessari". L'*app* non dovrebbe raccogliere informazioni non correlate o non necessarie "come, per esempio, dati anagrafici, identificativi di comunicazione, voci di *directory* del dispositivo, messaggi, registrazioni di chiamate, dati relativi all'ubicazione, identificativi del dispositivo, ecc.". Inoltre, si aggiunge che i dati trasmessi dall'applicazioni "devono includere solo identificatori univoci e pseudonimi", generati dall'applicazione e specifici di tale strumento. Tali identificatori devono essere rinnovati regolarmente, "secondo una frequenza compatibile con lo scopo di contenere la diffusione del virus e sufficiente a limitare il rischio di identificazione e di localizzazione fisica delle persone" (Linee-guida 04/2020, cit., § 3.2, punto 40-41).

In ogni caso, i dati relativi all'ubicazione possono essere trasmessi all'autorità o a terzi soltanto a condizione che siano stati resi anonimi ovvero se l'utente ha manifestato, preventivamente, il proprio consenso, tutto nella misura e per la durata necessari alla fornitura del servizio, sebbene, rispetto al quadro delineato, a norma dell'articolo 15 della Direttiva, siano ammesse delle deroghe ai diritti e agli obblighi previsti quando costituiscono una misura necessaria, adeguata e proporzionata all'interno di una società democratica per determinati obiettivi (cfr. Corte giust., 29 gennaio 2008, C-275/06, Productores de Musica de España Promusicae c. Telefonica de Espana SAU, in *www.curia.eruopa.eu*.). In relazione alla possibilità di riutilizzare i dati raccolti ai sensi dell'art. 5, comma 3, della Direttiva 2002/58/CE, essi possono ritenersi oggetto lecito di trattamento ove ricorra una

delle condizioni previste dall'art. 23 del GDPR. Anche l'EDPB ha ricordato, infatti, che il quadro normativo europeo prevede un sistema disciplinare che consente l'uso di dati anonimi o personali per realizzare l'interesse collettivo relativo al tracciamento dell'epidemia.

Quanto alla richiesta del consenso dell'interessato al trattamento, la previsione varia a seconda delle circostanze. Ove ricorrano le condizioni di cui all'art. 5, par. 3, della Direttiva 2002/58/CE, per la memorizzazione e l'accesso ai dati anonimi, necessario per l'erogazione della fornitura all'utente, non sarebbe richiesto il consenso. Nel caso in cui, invece, si faccia riferimento alle ipotesi di trattamento di cui all'art. 6, par. 1, lett. a, il trattamento dei dati sarà lecito soltanto dietro manifestazione di volontà espressa dell'interessato. Nondimeno, deve essere tenuto in conto che l'art. 6, par. 1, lett. e, del GDPR stabilisce che il trattamento è, comunque, lecito se "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento". Pertanto, se la finalità della gestione fosse stabilità all'interno di un atto normativo, allo scopo di svolgere un compito nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, tale base giuridica dovrebbe contenere disposizioni specifiche che prevedano: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire una gestione delle informazioni lecita e corretta. Su questi presupposti nulla impone che il trattamento dei dati personali debba basarsi sul consenso (linee-guida 04/2020, cit., § 3.1, punto 29-31) allo scopo di creare un rapporto di fiducia con l'utente (al riguardo, Comunicazione della Commissione europea Orientamenti sulle *app*, cit.).

All'interno di tale perimetro normativo è stata introdotta, con decretazione di urgenza, una normativa sul sistema di allerta COVID-19 a livello nazionale (art. 6 del d.l. 30 aprile 2020, n. 28, recante misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonchè disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta COVID-19). Sulla conformità della disciplina alla regolamentazione in materia è stato anche reso un parere dal Garante per la protezione dei dati personali (Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 del 29 aprile 2020, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050*). Il decreto legge prevede l'istituzione di una piattaforma informatica unica nazionale (nella esclusiva titolarità pubblica ai sensi dell'art. art. 6, comma 5, del d.l. n. 28 del

2020) per la gestione del sistema di allerta in riferimento ai casi di infezione relativi a utenti che hanno installato l'applicazione mobile di tracciamento.

In particolare, si prevede (art. 6, comma 2, del d.l. n. 28 del 2020) che gli utenti ricevano, prima dell'attivazione dell'applicazione (ai sensi degli articoli 13 e 14 del GDPR), informazioni chiare e trasparenti allo scopo di raggiungere piena consapevolezza, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati. L'istallazione dell'applicazione è facoltativa e non possono essere previste conseguenze pregiudizievoli per il suo mancato utilizzo (art. 6, commi 1 e 4, del d.l. n. 28 del 2020). In ossequio del richiamato principio di minimizzazione, i dati personali raccolti dall'applicazione devono essere, esclusivamente, quelli necessari ad avvisare gli utenti di rientrare tra i contatti stretti di altri utenti accertati positivi al COVID-19. Il trattamento dovrà essere realizzato, come ammonito a livello europeo, su dati di prossimità, resi anonimi oppure, ove ciò non sia possibile, pseudonimizzati, essendo esclusa, in ogni caso, la geolocalizzazione dei singoli utenti (art. 6, comma 2, lett. c, del d.l. n. 28 del 2020). Dovranno essere adottate tute le misure che garantiscano la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, nonchè le misure adeguate a evitare il rischio di re-identificazione degli interessati (art. 6, comma 2, lett. d, del d.l. n. 28 del 2020). I dati relativi ai contatti stretti potranno essere conservati, anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento (art. 6, comma 2, lett. e, del d.l. n. 28 del 2020). Si prevede che i diritti di accesso dell'interessato, i diritti di rettifica e di cancellazione, il diritto di limitazione del trattamento, il diritto alla portabilità, il diritto di opposizione e il diritto a non essere sottoposti a processo di trattamento automatizzato possano essere esercitati anche in modalità semplificata (art. 6, comma 2, lett. f, del d.l. n. 28 del 2020). Infine, l'utilizzo dell'applicazione e della piattaforma, nonchè ogni trattamento di dati personali saranno interrotti alla data di cessazione dello stato di emergenza e, comunque, non oltre il 31 dicembre 2020, sì che tutti i dati personali trattati devono essere cancellati o resi definitivamente anonimi (art. 6, comma 6, del d.l. n. 28 del 2020).

5. Dall'impiego della tecnologia analizzata derivano molti rischi. Quello principale è, sicuramente, la violazione della riservatezza. Per certi aspetti, non meno problematica, vista la pericolosità di tale sistema di controllo, è l'inefficacia dell'operazione. Nelle stesse linee guida del garante europeo si avverte che l'efficacia dei sistemi di tracciamento tecnologico del contagio possono risultare efficaci soltanto se siano impiegati da un numero percentualmente apprezzabile

di utenti, così da essere in grado di fissare con precisione i contatti in termini di "prossimità e durata" (Linee-guida 04/2020, cit., § 1, punto 6).

Non meno trascurabile è il rischio di non assumere piena consapevolezza che il tracciamento eseguito mediante applicazioni mobili sia diverso dal tracciamento manuale. Il primo non è sostitutivo del tracciamento tradizionale. Anzi, il monitoraggio tecnologico ha lo scopo di coadiuvare il secondo. Come precisato dall'EDPB "tali applicazioni devono far parte di una strategia globale in materia di sanità pubblica per combattere la pandemia, compresi, tra l'altro, la sperimentazione e il successivo tracciamento manuale dei contatti ai fini dell'eliminazione di casi dubbi" (Linee-guida 04/2020, cit., § 1, punto 6). Al riguardo l'art. 6, comma 1, del d.l. n. 28 del 2020 stabilisce che le modalità operative del sistema di allerta tramite la piattaforma informatica unica nazionale sono complementari alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale.

Il ricorso alla tecnica dell'anonimizzazione (come pure previsto dall'art. 6, comma 2, lett. c, del d.l. n. 28 del 2020) deve fare, necessariamente, i conti con gli elementi di contesto nel quale vegano raccolti e trattati i dati (Resta, G.: "Anonimato, responsabilità, identificazione: prospettive di diritto comparato", in *Dir. inf.*, 2014, p. 171 ss.). In un ambiente metropolitano gli spostamenti, anche di piccola percorrenza, determinano un'elevata possibilità di contatto non routinario e non identificabile. Le persone che, ad esempio, utilizzano mezzi pubblici per raggiungere il posto di lavoro incontrano, casualmente, persone sconosciute. In contesti urbani periferici, invece, gli spostamenti espongono a una relazionalità limitata e routinaria determinando un potenziale disvelamento dell'anonimato. Dunque, si tratta di valutare, secondo ragionevolezza, se la misura di anonimizzazione risulti efficace. Lo stesso Garante europeo ricorda che l'anonimizzazione fa riferimento all'uso di una serie di tecniche finalizzate a eliminare la possibilità di collegare i dati a una persona fisica identificata o identificabile con uno sforzo "ragionevole". Questo "test di ragionevolezza" deve tenere conto "sia degli aspetti oggettivi (tempi, mezzi tecnici) sia di elementi di contesto che possono variare caso per caso (rarità di un fenomeno, la densità di popolazione, la natura e il volume dei dati). Se i dati non superano tale test, non sono anonimizzati e pertanto rientrano nel campo di applicazione del regolamento generale sulla protezione dei dati".

Del resto, la valutazione della robustezza della tecnica di anonimizzazione adottata dipende da tre fattori: 1) individuabilità o *singling out* (possibilità di isolare una persona all'interno di un gruppo sulla base dei dati); 2) correlabilità (possibilità di correlare due *record* riguardanti la stessa persona); 3) inferenza (possibilità di dedurre, con probabilità significativa, informazioni sconosciute relative a una persona) (Linee-guida 04/2020, cit., § 2.2, punto 15 s.). Considerando che solo i dati anonimi possono essere utilizzati senza restrizioni, a differenza di quelli

pseudonimizzati (che, invece, rientrano nell'ambito di applicazione della disciplina generale sul trattamento dei dati personali), è evidente che i dati non possono essere resi anonimi, isolatamente, ma necessitano di essere anonimizzati solo in una serie di informazioni. Ogni intervento su singolo dato equivarrebbe a una forma di pseudonimizzazione. È stato, già, dimostrato che spesso le informazioni ritenute anonime non lo solo di fatto a causa delle tracce della mobilità. Si evoca una polvere di frammenti di dati che correlati rendono possibile la re-identificazione (Pyrgelis, A., Troncoso, C., De Cristofaro, E.: "Knock Knock, Who's There? Membership Inference on Aggregate Location Data", 2017). È bene segnalare che l'art. 6, comma 3, del d.l. n. 28 del 2020 prevede la possibilità di utilizzo dei dati in forma aggregata o, comunque, anonima per fini di sanità pubblica, profilassi, statistici o di ricerca scientifica (ai sensi degli articoli 5, par. 1, lett. a e 9, par. 2, lettere i e j, del GDPR), generando il rischio, concreto, della formazione di c.dd. "identità collettive". Dovrà, pertanto, essere operata, al riguardo, un'attenta valutazione.

Un ulteriore rischio, infine, è quello di trattare dati relativi a casi di falsi positivi. Il Garante europeo ricorda che "vi sarà sempre, in una certa misura, la possibilità del verificarsi di falsi positivi". In vista di ciò, atteso che l'identificazione di un pericolo di infezione può avere un forte impatto sui singoli individui, imponendo forme di isolamento fino a negativizzazione del test, è indispensabile poter effettuare la correzione dei dati. Naturalmente, ciò vale solo "in presenza di situazioni o implementazioni in cui il trattamento e la conservazione dei dati sono configurati in modo da permettere tecnicamente di apportare le correzioni suddette, e ove sia probabile il verificarsi degli effetti negativi di cui sopra" (art. 6, comma 2, lett. f, del d.l. n. 28 del 2020).

6. Un ruolo fondamentale nel tracciamento tecnologico del contagio, dunque, è giocato dalla capacità di elaborare uno strumento *software* sicuro nella fase di progettazione, nel rispetto dei concetti di *privacy by design* e *privacy by default* (Principato, A.: "Verso nuovi approcci alla tutela della *privacy*: *privacy by design* e *privacy by default settings*", in *Contr. impr./Eur.*, 2015, p. 197 ss.; D'Acquisto, G., Naldi, M.: *Big data e privacy by design. Anonimizzazione Pseudonimizzazione Sicurezza*, Torino, 2016, p. 33 ss.). In questo senso, l'applicazione non dovrebbe permettere di tracciare la posizione dei singoli utenti, ma fornire soltanto le informazioni di prossimità (art. 6, comma 2, lett. c, del d.l. n. 28 del 2020), avvalendosi di sistemi di anonimizzazione che rendano difficile da re-identificazione e conservando i dati sulle apparecchiature degli utenti (Linee-guida 04/2020, cit., § 3.1, punto 27).

Dal quadro delineato, la tecnologia da seguire potrà essere sia quella che vede i dati custodi in modo decentralizzato sui dispositivi degli utenti sia una diversa

soluzione con gestione accentrata delle informazioni. Di certo, la seconda opzione desta maggiori perplessità in tema di sicurezza delle informazioni. Ciò non toglie che ove si rispettino le indicazioni normative vigenti e si impieghino adeguati strumenti di crittografia, anche una gestione accentrata dei dati risulterebbe pienamente armonizzabile con il sistema ordinamentale. A ogni modo, l'impiego di tecnologia BLE eviterebbe di raccogliere dati di geolocalizzazione, atteso che l'obiettivo delle applicazioni non è controllare gli spostamenti delle persone per far rispettare le prescrizioni, ma tracciare i contatti di prossimità tra gli utenti (in tal senso, pure, Comunicazione della Commissione europea Orientamenti sulle *app*, cit.). L'introduzione delle tecnologie di *contact-tracing* richiede, comunque, per i rischi che esse sottendono, una valutazione d'impatto sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR (Mantelero, A.: "Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. valutazione d'impatto e consultazione preventiva (artt. 32-39)", in AA.VV.: *Il nuovo Regolamento europeo sulla* privacy, cit., p. 305 ss.). In tal senso, l'art. 6, comma 2, del d.l. n. 28 del 2020, stabilisce che le misure da introdursi devono essere precedute da siffatta valutazione, costantemente aggiornata (sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 36, paragrafo 5, del GDPR e dell'articolo 2 *quinquiesdecies* del Codice della *privacy*), al fine di garantire un livello di sicurezza adeguato ai rischi per i diritti e le libertà degli interessati (Parere sulla proposta normativa, cit.).

In questo senso, un tema determinante è quello della verificabilità dell'algoritmo impiegato, il cui codice sorgente, come raccomandato, dovrebbe essere reso pubblico e sottoposto a esame periodico da parte di esperti indipendenti (Linee-guida 04/2020, cit., § 3.1, punto 37). Allo scopo di rispondere a tale esigenza, l'art. 6, comma 5, del d.l. n. 28 del 2020, prevede che i programmi informatici di titolarità pubblica sviluppati per la realizzazione della piattaforma e l'utilizzo dell'applicazione di tracciamento siano resi disponibili e rilasciati sotto licenza aperta (determinante sarà comprendere il ruolo della piattaforma di interoperabilità Apple-Google e verificare se le *Application Programming Interface* Apple-Google rispetteranno gli *standard* di pseudonimizzazione stabiliti dall'ENISA, agenzia UE per la *cybersecurity*).

Non deve essere trascurato, altresì, che un sistema di tracciamento in ambito sanitario non può prescindere, per un efficace funzionamento, dalla pronta gestione sanitaria delle segnalazioni, le quali, altrimenti, risulterebbero sterili o addirittura dannose. Come rilevato, il *contact-tracing* richiede la possibilità di integrazione del momento tecnologico con quello manuale (art. 6, commi 1 e 2, lett. b, del d.l. n. 28 del 2020), ad esempio nella gestione dei falsi positivi e, quindi, nella correzione delle informazioni che costringerebbero l'utente a restrizioni della libertà personale o, eventualmente, a responsabilità. La segnalazione nell'*app* di utenti infetti deve essere effettuata, dunque, secondo una procedura che preveda

l'impiego di codici monouso, correlati a identità pseudonime delle persone infette, collegati a un laboratorio o a un operatore sanitario. Se la conferma non può essere ottenuta in modo sicuro, non dovrebbe aversi alcun trattamento di dati sulla base di una presunzione di validità dello *status* relativo all'utente (Linee-guida 04/2020, cit., § 3.2, punto 46).

In conclusione, di fronte alla necessità di interrompere il *lockdown* delle attività sociali, si potrebbe essere tentati di affermare che non vi sia altra scelta che accettare l'idea del tracciamento tecnologico del contagio. Costruita in questi termini, la questione è, di certo, mal posta. Non si tratta di prendere atto di una decisione ineludibile, gravida di conseguenze irreparabili. Piuttosto, è necessario assumere che la tecnologia, alle condizioni esposte, è utile a gestire un attento bilanciamento tra valori alla base dell'ordinamento. Le applicazioni mobili possono aiutare le autorità sanitarie, a livello nazionale ed europeo, a monitorare e contenere l'attuale pandemia, divenendo efficaci presidi in fase di revoca delle misure di contenimento (come rilevato nella Comunicazione della Commissione europea Orientamenti sulle *app*, cit.). Del resto, com'è stato ricordato dal Garante europeo, "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". Tuttavia, è necessario sottolineare che qualunque sforzo venga messa in atto, anche dal punto di vista tecnologico, non potrà risultare davvero efficace senza un'opera di responsabilizzazione dei titolari del trattamento (D'Ambrosio, M.: "Progresso tecnologico", cit., p. 110 ss.) e, soprattutto, di educazione degli utenti (sul punto sarà fondamentale assicurare il rispetto della previsione di cui all'art. 6, comma, 2 lett. a, del d.l. n. 28 del 2020) in grado di incidere sul "disciplinamento sociale" della collettività (come delineato, seppure per altri versi, da Oestreich, G.: "Strukturprobleme des europäischen Absolutismus", in *VSWG*, 55, 1968, p. 329 ss.).