CORONAVIRUS E TRACCIAMENTO TECNOLOGICO: ALCUNE RIFLESSIONI SULL'APPLICAZIONE E SUI RELATIVI SISTEMI DI INTEROPERABILITÀ DEI DISPOSITIVI

CORONAVIRUS AND TECHNOLOGICAL TRACKING: SOME CONSIDERATIONS ON THE APPLICATION AND THE RELATED INTEROPERABILITY SYSTEMS OF THE DEVICES

Actualidad Jurídica Iberoamericana Nº 12 bis, mayo 2020, ISSN: 2386-4567, pp. 836-847

Carolina
PERLINGIERI

ARTÍCULO RECIBIDO: 9 de mayo de 2020
ARTÍCULO APROBADO: 10 de mayo de 2020

RESUMEN: Il saggio analizza il tema del tracciamento dei contagi nello stato di emergenza sanitaria. Particolare attenzione è rivolta alla disamina degli aspetti giuridici dell'applicazione scelta per monitorare l'epidemia rispetto alla quale centrale appare la questione relativa alla qualificazione del rapporto Governo italiano con le due aziende, Apple e Google, alle quali è stato chiesto di sviluppare sistemi di interoperabilità.

PALABRAS CLAVE: Coronavirus; tracciamento; dati personali; pseudonimizzazione; interoperabilità.

ABSTRACT: *The essay analyses the issue of tracking infections in the state of health emergency. Particular attention is paid to the examination of the legal aspects of the application chosen to monitor the epidemic in relation to which central is the question of qualification of the relationship between the Italian government and Apple and Google companies who have been asked to develop interoperability systems.*

KEY WORDS: *Coronavirus; tracking; personal data; pseudonymization; interoperability.*

1. La dichiarazione dello stato di emergenza sanitaria – deliberata dal Consiglio dei Ministri il 31 gennaio 2020 ai sensi dell'art. 7, comma 1, lett. c), d.lgs. n. 1 del 2018 per la durata di 6 mesi dovuta alla diffusione del COVID-19 – ha sollevato una molteplicità di questioni giuridiche che richiedono un'adeguata e urgente riflessione. Un aspetto particolarmente rilevante attiene al delicato tema dei sistemi di tracciamento dei contagiati. Le tecnologie e il trattamento dei dati digitali possono acquisire un ruolo di ausilio al problema epidemiologico in quanto strumenti utili soprattutto per monitorare e prevenire il contagio.

Il tema si presenta particolarmente dibattuto non soltanto in merito alle diverse modalità operative sul trattamento dei dati dipendente dalle scelte effettuate da chi le ha progettate e/o ne ha richiesto la progettazione, ma anche con riguardo alla differente raccolta e gestione dei dati e alla modalità di interazione delle *App* tra dispositivo utente, eventuale server centrale e terzi potenziali contagiati.

Con riguardo al primo aspetto, occorre sottolineare che l'insieme delle regole tecniche di struttura dei diversi sistemi create dai programmatori informatici costituiscono gli strumenti di controllo dell'architettura e quindi ne stabiliscono i vari modi d'uso sia in relazione al compimento delle attività, sia per le modalità di trasmissione dei flussi informativi. Pertanto, la tecnologia con le sue regole di funzionamento non può essere considerata neutrale (con specifico riferimento all'ambito giuridico del dibattito in corso sulla neutralità della tecnica, cfr. Irti, N.-Severino, E.: *Dialogo su diritto e tecnica*, Roma-Bari, 2001) dal momento che costituisce il risultato di una scelta, tra diverse soluzioni, demandata all'esecuzione di algoritmi da parte di una macchina (sul punto da ultimo cfr. Gitti, G.: "Dall'autonomia regolamentare e autoritativa alla automazione della decisione robotica", in *Tecnologie e diritto*, 2020, in corso di pubblicazione) sì da determinare differenti conseguenze giuridiche. Se il diritto è veicolato mediante il mezzo tecnologico, talvolta tradotto in un algoritmo o comunque in grado di incidere sui rapporti privati, non si può condividere l'idea che la tecnica sia giuridicamente neutra. Si può affermare che la tecnica può costituire un'ulteriore fonte del diritto, un nuovo *soft law*; trattasi di una serie di atti, non omogenei quanto a origine e natura, che, benché privi di effetti giuridici vincolanti, risultano comunque, in vario modo, giuridicamente rilevanti. Pertanto, in questa direzione, con riguardo al tema in oggetto, occorre indagare sul rapporto tra i predetti sistemi e il diritto al fine di consentire la valutazione delle differenti conseguenze collegate all'uso della tecnologia adottata.

• Carolina Perlingieri
Ordinario di diritto privato Napoli "Federico II". Correo electrónico: carolina.perlingieri@unina.it

Con riguardo al secondo aspetto, particolarmente delicata è la questione relativa alla gestione dei dati raccolti e all'inoltro a un server centrale o ai possibili contagiati direttamente dall'*App* del dispositivo. Trattasi di due modelli alternativi – l'uno centralizzato, l'altro decentralizzato – nella gestione dei codici identificativi dei possibili contagiati che incide altresì sui sistemi di notifica dell'esposizione al possibile contagio.

Il tema in oggetto rappresenta un aspetto della più ampia questione relativa alla governance delle novità tecnologiche e dell'incidenza delle loro diverse modalità operative sui rapporti civilistici da affrontare a partire dalla considerazione del ruolo di supporto e servizio della tecnica al diritto. Come evidenziato anche di recente dal Presidente del Garante per la protezione dei dati personali "il diritto è l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza. Sarebbe per altro auspicabile un'alleanza tra tecnologia e diritto che può rappresentare l'architrave di una risposta democratica e lungimirante alle nuove minacce del digitale, minacce fortunatamente controbilanciate dalle straordinarie potenzialità di questi mezzi. Questo presuppone anzitutto il massimo equilibrio tra le discipline deputate a governare il rapporto tra le libertà e il lato oscuro della tecnica, ovvero quella di protezione dati e quella a tutela della sicurezza cibernetica" (intervista del Presidente dell'Autorità garante per la protezione dei dati personali Soro, A.: "Tecnologia e diritto devono allearsi per una corretta governance digitale", 16 aprile 2020, in www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9317569).

2. Se le misure tecnologiche devono essere di ausilio al contenimento e al controllo del virus, gli algoritmi che ne consentono il funzionamento si alimentano soltanto mediante la raccolta dei dati. È l'inscindibilità del binomio tecnologia-dati che consente il trattamento algoritmico dei dati personali raccolti al fine di costituire un supporto alla strategia di risposta alla pandemia causata dal COVID-19, ma al tempo stesso continua ad alimentare il dibattito in merito alle implicazioni relative ai diritti fondamentali della persona e in particolare di tutela della vita privata.

A tal proposito il Comitato europeo per la protezione dei dati (European Data Protection Board-EDPB), in questo contesto di emergenza legata al COVID-19, non soltanto ha sottolineato che il quadro giuridico in materia di protezione dei dati personali, essendo flessibile, è in grado di conseguire una risposta efficace per limitare la pandemia e proteggere i diritti umani e le libertà fondamentali, ma ha anche fornito delle Linee-guida sul trattamento dei dati relativi alla salute a fini di ricerca scientifica (03/2020 del 21.04.2020) e sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti (04/2020 del 21.04.2020) evidenziando che il binomio tecnologia-dati nel contesto attuale debba servire quale strumento

di protezione delle persone nel rispetto di un uso dei dati adeguato, necessario e proporzionato.

3. Dal punto di vista della normativa sul trattamento dei dati, il Regolamento generale sulla protezione dei dati 2016/679 (GDPR) consente alle autorità competenti in materia di salute pubblica di trattare dati personali purchè nel rispetto dei principi generali (art. 5 GDPR) e delle condizioni contenute nel testo di legge sia nazionale che europeo. Il Considerando 46 GDPR prevede espressamente che, tra i trattamenti legittimi per motivi di interesse pubblico e per la tutela degli interessi vitali dell'interessato, rientrano in particolare quelli "a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione".

In particolare, l'art. 23 GDPR nonché anche l'art. 15 direttiva relativa alla vita privata e alle comunicazioni elettroniche cd. direttiva e-*privacy* 2002/58/CE e l'art. 52 Carta dei diritti fondamentali dell'Unione europea consentono di introdurre, con una norma di legge, una limitazione ai diritti degli interessati la quale, rispettando l'essenza dei diritti e delle libertà fondamentali, deve costituire una misura necessaria e proporzionata per la salvaguardia esclusivamente di obiettivi di pubblico interesse generale.

Dunque il tema deve essere affrontato tenendo presente queste condizioni alle limitazioni dei diritti degli interessati da introdurre necessariamente con una norma di legge nel rispetto dell'essenza di tali diritti qualora le misure siano necessarie e proporzionate al fine di perseguire obiettivi quali quello dell'emergenza sanitaria (sul punto, con riguardo alla necessaria 'gradualità' e proporzionalità delle misure, v. l'intervista del Presidente dell'Autorità garante per la protezione dei dati personali Soro, A.: "Privacy e democrazia ai tempi della pandemia", 24 marzo 2020, in *https://fondazioneleonardo-cdm.com/it/news/privacy-e-democrazia-ai-tempi-della-pandemia-intervista-ad-antonello-soro/*).

L'eventuale utilizzazione di dati di localizzazione è ammissibile esclusivamente a supporto del contenimento della pandemia per disporre misure di isolamento e quarantena. Come è noto due sono le principali fonti di dati relativi all'ubicazione: i dati raccolti da fornitori di servizi di comunicazione elettronica (si pensi agli operatori di telecomunicazioni mobili) nel corso della prestazione del loro servizio e i dati raccolti da fornitori di servizi della società dell'informazione, la cui funzionalità richiede l'uso di tali dati (ad esempio, navigazione, servizi di trasporto, ecc.). Il trattamento di questi dati di ubicazione è diverso a seconda che la raccolta sia effettuata dal fornitore di servizi di comunicazione elettronica o dal fornitore di servizi della società dell'informazione. Nella prima ipotesi, i dati possono essere

trattati soltanto entro i limiti di cui agli artt. 6 e 9 della direttiva e-*privacy* e quindi possono essere trasmessi alle autorità o a terzi soltanto se sono stati resi anonimi dal fornitore oppure, per i dati indicanti la posizione geografica dell'apparecchiatura terminale di un utente che non sono dati relativi al traffico, con il previo consenso degli utenti. Nella seconda ipotesi, ai dati raccolti si applica l'art. 5 della direttiva e-*privacy* nonché gli artt. 6 e 9 GDPR sì che l'archiviazione di informazioni sul dispositivo dell'utente o l'accesso alle informazioni già archiviate sono consentiti soltanto se l'utente ha prestato il consenso o se la memorizzazione e/o l'accesso siano autorizzati legalmente a norma dell'art. 15 della direttiva e-*privacy* nonché degli artt. 6, paragrafo 1, lett. d, e, e 9, paragrafo 2, lett. i GDPR, quale misura necessaria e proporzionata.

Qualora, invece, l'uso sia finalizzato al tracciamento dei contatti, tale uso deve essere rivolto esclusivamente al fine di informare le persone che probabilmente sono entrate in contatto ravvicinato con soggetti successivamente confermati positivi, al fine di interrompere tempestivamente la trasmissione del contagio.

Sulla base della normativa nazionale ed europea sul trattamento dei dati personali, il ricorso all'uso di un'*App* di tracciamento dei contatti deve essere volontario, anonimo o quanto meno pseudonimizzato, non basarsi sulla tracciabilità dei movimenti individuali, bensì soltanto sulle informazioni di prossimità relative agli utenti, necessariamente limitato alla fase dell'emergenza sanitaria.

Se dunque da un lato è confermata la centralità del ruolo del consenso quale criterio principale di legittimazione al trattamento, dall'altro le misure tecniche di tracciamento per essere conformi alla normativa in materia di dati personali devono utilizzare dati anonimi o meglio pseudonimizzati. Infatti, a tal proposito, se vero è che il singolo dato può sempre essere collegato a una persona identificata o identificabile sì da consentirne soltanto una pseudonimizzazione mediante cifratura o altre trasformazioni matematiche, è anche vero che per insiemi di dati è, di regola, realizzabile l'anonimizzazione anche se occorre considerare che in presenza di certe correlazioni e univocità è pur sempre possibile la re-identificazione.

4. Alla luce di questo quadro, la Presidenza del Consiglio dei Ministri ha richiesto il parere del Garante per la protezione dei dati personali su una proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19 (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", 29 aprile 2020, in www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9328050) con la quale il tracciamento di dati di prossimità dei dispostivi – resi anonimi o comunque pseudonimizzati, con esclusione di

ogni forma di geolocalizzazione – è effettuato tramite l'utilizzo di un'applicazione installata su base volontaria, destinata alla registrazione dei soli contatti tra soggetti che abbiano parimenti scaricato tale *App* al fine di analizzare l'andamento epidemiologico o per ricostruire la catena dei contagi, salvo trattamento in forma aggregata o anonima per finalità scientifiche o statistiche.

Il Garante ha espresso parere favorevole su questa proposta normativa, seguita dal Decreto legge n. 28 del 30.04.20, mettendo in evidenza in particolare che il sistema di *contact tracking* prefigurato non appare in contrasto con i principi di protezione dei dati personali in quanto non soltanto è previsto da una norma di legge sufficientemente dettagliata (si pensi all'articolazione del trattamento, alla tipologia di dati raccolti, alle garanzie accordate agli interessati, alla temporaneità della misura), ma soprattutto si fonda sull'adesione volontaria dell'interessato; esclude ogni forma di condizionamento della determinazione individuale e di disparità di trattamento basate sulla scelta di consentire o meno il tracciamento; è preordinato al perseguimento di fini di interesse pubblico indicati con sufficiente determinatezza; esclude il trattamento secondario dei dati così raccolti per fini diversi, salva la possibilità (nei termini generali previsti dal Regolamento) di utilizzo, in forma anonima o aggregata, a fini statistici o di ricerca scientifica.

La misura di *contact tracking* predisposta, inoltre, appare conforme ai principi di minimizzazione e ai criteri di *privacy by design* e *by default* dal momento che prevede la raccolta dei soli dati di prossimità dei dispositivi, il loro trattamento in forma quantomeno pseudonimizzata escludendo il ricorso a dati di geolocalizzazione e limitandone la conservazione al tempo strettamente necessario ai fini del perseguimento dello scopo indicato, con cancellazione automatica alla scadenza del termine dell'emergenza sanitaria.

In particolare l'applicazione di tracciamento dei contatti essendo collegata alla SIM del dispositivo, può garantire soltanto una pseudonimizzazione la quale avviene – utilizzando la tecnologia *Bluetooth-Low-Energy* – mediante il rilascio ogni 15 minuti di un codice alfanumerico sì da determinare una sequenza di codici che resta immagazzinata sul dispositivo. Questa sequenza è decodificata soltanto quando è accertata la positività e quindi, in questa circostanza, occorre ricostruire a ritroso la catena epidemiologica dei contatti. L'opzione adottata dal Governo prevede che il contagiato – tramite un codice fornito dall'autorità sanitaria – trasmette a un server centrale, pubblico e collocato nel territorio nazionale, la lista dei codici, presenti nel dispositivo, identificativi e anonimi con i quali è entrato in contatto nell'ultimo periodo. Successivamente sull'*App* del possibile contagiato, identificato da un codice alfanumerico, comparirà l'avviso di rischio e il protocollo da seguire.

Questo sistema di rinvio a una piattaforma centralizzata secondo il quale sono le autorità sanitarie ad accedere ai dati trasmessi dal dispositivo della persona positiva e ad inviare l'*alert* ai possibili contagiati, è l'alternativa a un sistema decentralizzato in virtù del quale il segnale anonimo di rischio è inviato automaticamente dall'App ai possibili contagiati invitati a rivolgersi al personale sanitario per le opportune valutazioni (cfr. Resta, G.: "La protezione dei dati personali nel diritto dell'emergenza COVID-19", in *Giustiziacivile.com*, n. 5/2020, p. 15, secondo il quale "L'alternativa tra un sistema di archiviazione delle informazioni centralizzato ed uno decentralizzato è evidentemente cruciale per definire le caratteristiche operative e le implicazioni giuridiche della specifica architettura tecnologica").

Questi due diversi sistemi di archiviazione delle informazioni sono l'espressione di due contrapposti approcci non soltanto tecnologici, ma anche metodologici. Conseguentemente appare confermata la necessità di riaffermare il primato del diritto sulla tecnica quale utile strumento al servizio di esigenze fondamentali dell'uomo, in primo luogo, la salvaguardia della salute e della vita.

Nonostante sia le linee guida del Comitato europeo per la protezione dei dati si siano espresse in senso favorevole alla conservazione dei dati esclusivamente sul terminale dell'utente (Comitato europeo per la protezione dei dati-EDPB, 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 21-4-2020, punto 27) sia la Risoluzione del Parlamento europeo sull'azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze (del 17.04.2020 n. 2020/2616) abbia sottolineato l'opportunità "che la memorizzazione dei dati sia completamente decentralizzata" (punto 41) per ridurre i rischi di uso improprio dei dati, il Governo italiano ha optato per una soluzione diversa che appare condivisibile. In particolare se è vero che il sistema centralizzato rappresenta una forma meno garantista della *privacy*, tuttavia rappresenta la soluzione maggiormente efficace per conseguire il controllo dei soggetti a rischio secondo una prospettiva solidaristica diretta al contrasto dell'epidemia e alla tutela della salute pubblica. Altresì occorre evidenziare che la condivisione di una simile scelta presuppone il carattere pubblico della gestione del sistema centralizzato e l'ubicazione del server sul territorio nazionale nonchè l'attribuzione della qualità di titolare del trattamento al Ministero della Salute, nonché quella di responsabili del trattamento alla Protezione Civile, all'Istituto Superiore di Sanità, alle Strutture pubbliche e private accreditate del SSN.

5. L'adesione alla predetta soluzione presuppone, altresì, che si faccia chiarezza su un'altra questione: quella relativa alla qualificazione giuridica del rapporto

Governo italiano con le due aziende Apple-Google alle quali è stato chiesto di realizzare sistemi di interoperabilità *Application Programming Interface* (API) che consentano non soltanto lo scambio di segnali via *Bluetooth Low Energy* tra i dispositivi degli utenti che hanno scaricato l'*App* di *contact tracking*, bensì soprattutto al Servizio Sanitario Nazionale di interfacciarsi con i dispositivi mobili *Android* e *iOS* di utenti positivi e di coloro con i quali sono entrati in contatto. Infatti se alcune questioni legate alla cybersecurity e alla protezione dei dati personali sono state affrontate adeguatamente in linea anche con gli *standard* sulla *data protection* dell'Agenzia dell'Unione europea per la *cybersecurity*-ENISA (cfr. diversi sono i rapporti pubblicati dall'ENISA con riguardo alle tecniche di pseudonimizzazione e migliori pratiche in *www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices*; le raccomandazioni sulla modellatura della tecnologia secondo le disposizioni del GDPR – Esplorazione del concetto di protezione dei dati per impostazione predefinita in https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2; il *tracking online* e meccanismi di protezione dell'utente, in www.enisa.europa.eu/publications/online-tracking-and-user-protection-mechanisms; il manuale sulla sicurezza del trattamento dei dati personali in www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing; *Privacy* e protezione dei dati nelle applicazioni mobili in www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications), è anche vero che vi sono ancora alcuni aspetti opachi di tale rapporto.

Se una delle principali fonti di rischio per la protezione dei dati personali è l'introduzione di identificatori di dispositivi permanenti, la scelta di un sistema che genera gli ID utente in maniera causale sostituendoli in modo coordinato e sincronico al trascorrere di un breve intervallo di tempo, accantona questo rischio in quanto assicura la pseudonimizzazione. Tuttavia, al tempo stesso, è anche vero che i registi dell'ambiente da pseudonimizzare sono i due fornitori, costruttori e gestori dei sistemi di interoperabilità e non il titolare del trattamento sì da dover evidenziare l'ulteriore rischio relativo a un condizionamento delle API pur sempre modificabili.

In questa direzione appare necessario l'impegno di *Apple* e *Google* di non modificare, se non di comune accordo, le API. L'eventuale modifica inciderebbe sulla raccolta dei dati (si pensi all'estensione ad altri dati quali quelli di ubicazione), consentendo il trattamento per finalità diverse da quella di cui all'art. 6, comma 1 (ad esempio per il controllo dell'isolamento o della quarantena) sì da determinare una scelta tecnica in contrasto con quanto stabilito dal predetto art. 6, comma 3 del Decreto legge n. 28 del 30.04.20 secondo il quale "i dati raccolti attraverso l'applicazione di cui al comma 1 non possono essere trattati per finalità diverse da quella di cui al medesimo comma 1, salva la possibilità di utilizzo 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".

Al riguardo si può ipotizzare una configurazione del rapporto tra il Ministero della Salute e le due aziende americane sulla base dell'art. 28 GDPR. In particolare tale norma al paragrafo 1 riconduce la figura del responsabile del trattamento in colui che effettua un trattamento "per conto del titolare del trattamento" qualora presenti "garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato" con la previsione che se il responsabile del trattamento "viola il presente regolamento determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento".

Altresì l'art. 28, paragrafo 3 GDPR richiede che "i trattamenti da parte di un responsabile del trattamento" siano "disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento" e la previsione di tale contratto o altro atto giuridico può basarsi anche, "in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43" (art. 28, paragrafo 6 GDPR).

In questo modo un simile rapporto contrattuale può essere configurato nel richiamo anche nella sola certificazione concessa al titolare del trattamento, il Ministero della Salute, di "clausole contrattuali tipo" di cui al paragrafo 7 dell'art. 28 GDPR e, in particolare, al paragrafo 3, lett. c dell'art. 3 GDPR in forza del quale il responsabile del trattamento è colui che adotta tutte le misure richieste ai sensi dell'art. 32 GDPR in materia di sicurezza del trattamento.

Pertanto l'affidamento di un segmento del trattamento non richiede a soggetti privati di elevata competenza tecnologica soltanto requisiti di affidabilità e trasparenza ma anche la responsabilità e la controllabilità.

Il tema del controllo, anche in quest'ambito, acquista un ruolo centrale e decisivo qualora si intenda porsi in una prospettiva diretta a creare un clima di fiducia nelle istituzioni.

6. Se dunque, appare condivisibile la scelta di un sistema centralizzato mediante il ricorso a un server pubblico collocato sul territorio nazionale, occorreva sollevare la questione nevralgica collegata alla qualificazione giuridica del rapporto tra il Governo italiano e le due aziende *High tech* quale presupposto per intraprendere percorso trasparente nella raccolta e nella gestione dei dati personali necessari per la gestione della Fase 2 dell'emergenza sanitaria. Problema che potrebbe ugualmente ripresentarsi qualora il rapporto riguardi gli enti locali, in particolare le regioni, e le società programmatrici dei sistemi operativi delle *App* che possono configurare autonome e differenti iniziative le quali – in quanto spesso non coordinate – rischiano di indebolire l'efficacia complessiva della strategia di contrasto. Al contrario, l'effettività del contrasto alla diffusione del contagio richiede un indirizzo uniforme che coinvolga non soltanto il nostro Paese bensì tutti i Paesi membri dell'Unione europea e che potrebbe concretizzarsi con l'adozione di un unico progetto di data tracking.

In conclusione, al fine di creare un clima di fiducia istituzionale che stimoli la popolazione a un uso consapevole della tecnologia per il perseguimento di finalità solidaristiche in questa "Fase 2" occorre non soltanto introdurre strumenti adeguati, necessari, proporzionati e temporanei ma soprattutto fare chiarezza sui rapporti, ancora troppo opachi, con coloro che creano e gestiscono le diverse tecnologie impiegate nel perseguimento di interessi pubblici.