CORONAVIRUS
OVERCOMING THE DIFFICULTIES

LO SVILUPPO E L'USO DI APP DI CONTACT TRACING NELLA LOTTA ALLA DIFFUSIONE DI COVID-19: IN EQUILIBRIO TRA DIRITTO ALLA SALUTE E PROTEZIONE DEI DATI PERSONALI

DE BERTI JACCHIA FRANCHINI FORLANI
STUDIO LEGALE

Le app di contact tracing quali strumento di contrasto alla diffusione di Coid-19 e la tutela della privacy

Fin dall'inizio di questa fase emergenziale ci si era da più parti interrogati su come la tecnologia potesse essere messa a servizio della comunità, come strumento di supporto alle già esistenti misure di contrasto e contenimento della diffusione della pandemia in atto. Una delle tematiche più ricorrenti e discusse è stata quella dell'implementazione e adozione di applicazioni di *contact tracing,* in grado di allertare i cittadini della possibile esposizione al virus, tramite analisi dei contatti avuti con soggetti poi risultati positivi, e di ricostruire quindi la potenziale catena di contagi.

Naturalmente c'era la consapevolezza che le app di *contact tracing* avrebbero potuto dare un contributo determinante a fini di valutazione dell'andamento della pandemia e monitoraggio dei focolai. Il maggior pregio di queste tecnologie, specialmente se confrontate con i metodi di monitoraggio tradizionali, è legato a due macro fattori: il primo risiede nella maggior rapidità e precisione di analisi che queste app offrono, mentre il secondo, di carattere economico e operativo, consiste nel minor impiego di risorse, umane ed economiche, richiesto per il loro funzionamento.

Di fronte alla indubbia utilità di simili tecnologie, ci si è interrogati però anche su quali debbano essere i loro limiti, visto che queste app costituiscono uno strumento dall'intrinseco e alto potenziale invasivo nei confronti dei diritti di libertà dei cittadini, specie se esse non dovessero essere adeguatamente regolamentate e realizzate secondo criteri trasparenti e condivisi a livello nazionale e comunitario. Tra tutte le domande che questo tipo di strumenti solleva, basti pensarne a una: è lecito, ad esempio, utilizzare app di *contact tracing* per monitorare l'osservanza della quarantena da parte degli individui contagiati?

Nel nostro precedente articolo sulla geolocalizzazione e utilizzo dei big data per combattere la pandemia, avevamo evidenziato il parere, in parte sfavorevole, con cui il Garante per la Protezione dei Dati Personali si era espresso nei confronti di app di *contact tracing* che consentissero il monitoraggio sistematico e costante dell'ubicazione degli individui (sulla falsariga del modello cinese e, in parte, coreano): tale monitoraggio appariva, e appare, soluzione

sproporzionata e, in definitiva, non utile al conseguimento della finalità di contenimento del contagio[1].

Lungi dal condannare aprioristicamente l'utilizzo di app nella lotta al Covid-19*,* il Garante, peraltro, aveva sottolineato l'esigenza che le soluzioni tecnologiche adottate dal Governo risultassero adeguate a garantire la tutela dei diritti dei soggetti interessati, non da ultimo il diritto alla protezione dei dati personali.

Le Linee Guida dell'EDPB

L'importanza delle garanzie che simili app di tracciamento devono apprestare è stata ribadita anche a livello comunitario: il Garante Europeo per la Protezione dei Dati Personali (EDPB) ha sancito che le soluzioni tecnologiche adottate dovranno essere sviluppate cooperando con le autorità sanitarie nazionali, potranno essere installate solo su base volontaria (quindi, le app saranno liberamente scaricabili dagli individui), non saranno basate sull'individuazione della posizione degli individui (no, quindi, alla geolocalizzazione per seguire i movimenti dei singoli o imporre divieti di accesso a determinate zone) e dovranno essere programmate per garantire una conservazione sicura dei dati che risulti proporzionale alla finalità per cui gli stessi sono stati raccolti: verosimilmente, la fine dell'emergenza segnerà il momento ultimo in cui tutti i dati acquisiti andranno necessariamente cancellati. Le app inoltre dovranno garantire il più possibile l'anonimato (o, almeno, la riservatezza) delle persone coinvolte, e questo sarà possibile mediante l'adozione di appropriate misure tecniche e organizzative, quali ad esempio la criptazione dei dati, la pseudonimizzazione o, quando sia possibile, l'anonimizzazione totale e irreversibile degli stessi. Tematica fondamentale, infine, è quella dell'interoperabilità delle diverse soluzioni adottate a livello europeo: l'UE tenta, così, di assicurare la cooperazione e collaborazione degli stati membri nel seguire l'evolversi della pandemia e nel trovare possibili soluzioni per avviarsi verso l'uscita dalla grave crisi sanitaria. Un progetto, in questo senso, esiste già: è il cosiddetto Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), organizzazione no profit che coinvolge 130 individui provenienti da 8 stati membri dell'UE, che ha lavorato su sistemi di monitoraggio basati sulla tecnologia *bluetooth*.

L'EDPB ha poi precisato ulteriormente i requisiti tecnologici di tali soluzioni pubblicando, il 21 aprile 2020, le Linee Guida sulle app di *contact tracing.* Nelle Linee Guida 4/2020 il Garante europeo ha ribadito che, ai fini del principio di minimizzazione, le app non dovranno far uso dei dati di geolocalizzazione relativi agli individui, ma potranno acquisire solo i dati di prossimità (vale a dire, i contatti avuti tra diversi dispositivi mobili via *bluetooth*, rilevabili senza registrare l'ubicazione delle persone fisiche). Inoltre, l'EDPB ha specificato l'importanza del fatto che le app funzionino riducendo al minimo il rischio di identificazione degli individui (utilizzando quindi codici casuali al posto di nomi), evidenziando che dovranno essere adottate appropriate misure anche ai fini di prevenzione della possibile re-identificazione dell'individuo (implementando misure atte a impedire di poter risalire dal codice pseudonimo all'identità effettiva della persona). Per raggiungere tale risultato, l'EDPB ha indicato che i codici che vengono associati ai dispositivi dovrebbero essere generati da processi che riflettano lo stato dell'arte delle tecniche di crittografia e cambiare periodicamente: con tali accorgimenti, si potrà evitare che un codice univoco risulti associato a un individuo e, con ciò, prevenire anche eventuali tentativi di tracciamento abusivo dello stesso. I dati acquisiti dalle app di *contact tracing,* inoltre, dovranno essere conservati, sempre secondo quelle che sono le direttive del Garante europeo, sui dispositivi mobili degli individui, e potranno essere trasmessi esternamente solo nei casi e nella misura in cui ciò si riveli necessario, sempre che vi sia la positiva volontà dell'individuo infettato di consentirlo. Ciò comporta che le app non abbiano, né possano avere, accesso ai dati già presenti sui nostri dispositivi mobili (ad es. messaggi,

[1] Per saperne di più, https://www.dejalex.com/wp-content/uploads/2020/03/Articolo_Geolocalizzazione.pdf

rubrica, foto, ecc…) se tale accesso non abbia effettivamente una qualche utilità ai fini del corretto funzionamento dell'app, né che possano tantomeno trasmetterli a terze parti. Le segnalazioni di soggetti infetti dovranno avvenire – sempre tramite codice pseudonimo - solo dopo aver verificato, attraverso personale sanitario, l'effettivo contagio dell'individuo, al fine di ridurre il rischio di falsi positivi e, in ogni caso, previo consenso della persona interessata: per manifestare la volontà del soggetto infetto di condividere i dati raccolti sul suo dispositivo, il Garante europeo ha parlato di una manifestazione di volontà mediante, ad esempio, generazione di una *OTP* (*one time password*) inviata dalle autorità sanitarie al dispositivo della persona positiva, che autorizzerà la condivisione mediante inserimento di questa *OTP* nell'app. L'EDPB ha puntualizzato che il fatto che le app saranno installate volontariamente, poi, non implica che la base giuridica del trattamento sarà sempre e necessariamente il consenso degli interessati, in quanto la situazione emergenziale giustifica il trattamento dei dati sulla base del prevalente interesse pubblico, che dovrà essere però "definito" dalle autorità nazionali mediante apposita normativa che stabilisca i casi e i confini di liceità del trattamento.

L'individuazione dell'app "Immuni"

Proprio dalla falsariga di quanto prodotto a livello comunitario, nasce quella che sarà adottata come l'app italiana anti-Covid-19. Il Governo italiano ha riunito un comitato di esperti (la cosiddetta *task force*) che ha avuto il compito di vagliare, nelle scorse settimane, i numerosi progetti che le sono stati sottoposti. La *task force*, dopo una selezione operata su un campione di circa 300 potenziali app candidate, si è espressa favorevolmente nei confronti di un'app basata sul principale utilizzo della tecnologia *bluetooth* e, in via secondaria, della geolocalizzazione (solo in forma aggregata, non riconducibile cioè al posizionamento dei singoli individui).

In particolare, con l'Ordinanza n. 10/2020 del 16 aprile, firmata dal Commissario Straordinario per l'emergenza Covid-19 Domenico Arcuri, è stata ufficialmente individuata l'app anti-contagio che aiuterà il sistema Italia nella fase di uscita dal *lockdown*, la c.d. Fase 2.

L'app, al momento ancora in fase di sviluppo e collaudo, risponde al nome di "Immuni", ed è stata sviluppata dalla società Bending Spoons, in collaborazione con il Centro Diagnostico Sant'Agostino e Jakala. La licenza del software sarà concessa gratuitamente al Governo, così come il codice sorgente, affinché si realizzino uno studio e un controllo del suo regolare funzionamento.

L'app, come detto, sfrutta la tecnologia *bluetooth* e permette di ricostruire la linea dei contatti e delle interazioni tenuti tra gli individui, e questo avviene sfruttando le celle *bluetooth* dei nostri dispositivi mobili che interagiscono tra di loro: rispetto alle interazioni dei segnali tra celle telefoniche, il vantaggio legato all'utilizzo del *bluetooth* sta nella maggior precisione e accuratezza che tale strumento assicura, visto che i dispositivi interagiscono tra loro tramite *bluetooth* quando si trovano a distanze molto più strette (1-10 m) di quelle individuabili tramite le celle telefoniche (nell'ordine anche di centinaia di metri).

Nell'audizione informale dell'8 aprile dinanzi al Presidente del Garante Privacy, è stato evidenziato che la soluzione di interazione *bluetooth* parrebbe "la migliore nel selezionare i possibili contagiati all'interno di un campione più attendibile perché, appunto, limitato ai contatti significativi". La tecnologia utilizzata consentirebbe un approccio conforme ai principi di minimizzazione e proporzionalità sanciti nel Regolamento UE 679/2016.

In pratica, ad ogni dispositivo mobile che avrà scaricato l'app, sarà associato un codice *bluetooth*, per garantire la tutela della riservatezza degli interessati, vale a dire gli utilizzatori del dispositivo. Quando l'individuo si sposterà e verrà in contatto con altri soggetti, dotati anch'essi di app, il suo dispositivo registrerà – in locale, per tutto il periodo di potenziale incubazione del virus – tutti i

codici *bluetooth* che si sono trovati, per un certo periodo di tempo, a una distanza tale (circa un metro dal soggetto) da rappresentare una possibile minaccia di contrazione del virus.

Una volta che un individuo risulti positivo al Covid-19, l'operatore sanitario che ha effettuato il test, utilizzando una diversa app, genererà un codice tramite cui il soggetto contagiato potrà caricare su un server i codici *bluetooth* registrati sul proprio dispositivo. Il server calcolerà, sulla base dei parametri precedentemente enunciati (tempo di esposizione e vicinanza al soggetto contagiato) il rischio a cui gli individui che sono entrati in contatto con il contagiato sono esposti, quindi invierà una notifica al loro dispositivo allertandoli della potenziale contrazione del virus e prescrivendo il comportamento da adottare (se contattare numeri di emergenza, rimanere in isolamento, ecc.).

Gli esperti hanno stimato che, per essere efficace, l'app dovrebbe essere scaricata almeno dal 60% della popolazione italiana. Questo pone non pochi problemi – si veda il noto caso del crash dell'INPS, i cui server subissati di domande sono collassati – relativi all'effettivo funzionamento dell'app in caso di sovraccarico e congestionamento dei server.

L'applicazione selezionata avrà anche un'altra utile funzione, che dovrebbe permettere, dietro richiesta degli stessi cittadini che si presentino ai controlli, una diagnosi del rischio contagio più accurata e personalizzata: difatti essa consentirà agli utenti di tenere un vero e proprio diario clinico, che riporti, oltre all'età e al sesso, le principali patologie contratte in passato, eventuali medicinali assunti – regolarmente o recentemente – e l'evoluzione o comparsa di sintomatologie sospette. Non è chiaro quali saranno le misure di sicurezza a protezione di questi dati e se gli stessi saranno conservati nella memoria locale oppure se saranno visibili in automatico a operatori sanitari e/o al gestore dell'applicazione. Verosimilmente, i dati dovrebbero essere quantomeno pseudonimizzati (non contenere, cioè, riferimenti immediati all'individuo a cui appartengono) e conservati in un formato criptato, onde assicurare il rispetto della riservatezza degli interessati.

Modalità di utilizzo dell'app Immuni e profili di tutela della privacy

Sullo sfruttamento dei dati raccolti tramite geolocalizzazione GPS, al momento, parrebbero non esserci spiragli circa un loro utilizzo, se non in forma aggregata: ciò è pienamente conforme alle direttive espresse in sede comunitaria e nazionale. Il Garante Privacy ha chiarito infatti come sia ben diverso effettuare la "verifica della posizione del soggetto sottoposto ad obbligo di permanenza domiciliare perché positivo, utilizzando dunque la geolocalizzazione del telefono (che si presuppone, ma non è detto, segua passo passo il soggetto) per accertare l'effettivo rispetto del divieto di allontanamento dal domicilio", sfruttando il GPS come una sorta di braccialetto elettronico, rispetto alla necessità di ricostruire a ritroso i "dati sull'interazione del soggetto poi risultato positivo con altri soggetti, per verificarne, nel periodo in cui aveva capacità virale, gli eventuali contatti".

Al fine di introdurre l'app, lo Stato (o comunque il soggetto da esso individuato per gestire l'app), in qualità di titolare del trattamento, ai sensi dell'art 35 del GDPR, dovrà effettuare una valutazione dell'impatto che l'app stessa avrà sulla privacy degli utenti, analizzando i rischi cui questi ultimi sono esposti e correlando tali rischi alle misure di sicurezza adottate per mitigarli. L'introduzione dell'app, inoltre, come auspicato dal Garante Privacy e dall'EDPB, dovrebbe essere preceduta da norme di rango primario che ne andranno a disciplinare il funzionamento, circoscrivendo le finalità del trattamento, i tempi di conservazione dei dati ed i soggetti autorizzati al loro trattamento, tenuto conto dell'interesse collettivo alla tutela della salute dei cittadini. Allo stesso tempo, tali norme dovrebbero prevedere misure di garanzia dei diritti dei cittadini e cristallizzare le conseguenze per chi dovesse violarle. In tal senso, deve registrarsi la decisione dei maggiori partiti politici di avviare un dibattito parlamentare sul punto.

Per assicurare il funzionamento dell'app, come detto, è necessario il contributo attivo dei cittadini: se infatti gli stessi non scaricheranno l'app, o non porteranno con sé il loro dispositivo negli spostamenti, l'utilità della soluzione individuata dal Governo svanirebbe. L'installazione dell'applicazione, almeno per il momento e secondo le indicazioni date dell'EDPB, è su base volontaria.

Per questo si è enfatizzata la duplice necessità di avere, da un lato, il codice sorgente del software disponibile *open source*, in maniera che possa essere analizzato e studiato, mentre, dall'altro, affidare la gestione dell'app a soggetti pubblici, per generare – auspicabilmente – fiducia nei cittadini circa il rispetto delle finalità di trattamento per cui i loro dati sono stati raccolti e trattati, la trasparenza delle operazioni effettuate e l'assicurazione di veder cancellati i dati non appena sia terminato il periodo di possibile esposizione alla minaccia. Come sottolineato dalla Presidente dell'EDPB, tale fiducia e il massimo utilizzo possibile dell'app da parte dei cittadini in ogni settore della popolazione potrebbero anche essere promossi con un'efficace campagna di comunicazione, anche in relazione alle misure di tutela della privacy insite nell'app.

Scongiurato, per il momento, il pericolo di sconfinamento nei modelli di controllo e monitoraggio sistematico adottati in altre realtà, non resta che attendere la data di *go live* di Immuni per verificare la reale efficacia di tale soluzione e quanto i cittadini saranno disposti a collaborare nell'utilizzo di questo strumento per favorire un miglior contrasto alla diffusione di Covid-19.

23 aprile 2020

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Ulitsa Bolshaya Ordynka 37/4 · 119017, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com