Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

OSSERVATORIO SU COMMERCIO INTERNAZIONALE E DIRITTI UMANI N. 3/2020

1. ALCUNE CONSIDERAZIONI IN MERITO AL TRATTAMENTO DEI DATI DA PARTE DELLE APP DI TRACCIAMENTO DEI CONTAGI NEL CONTESTO EUROPEO: COME CONFINARE UN VIRUS SENZA CONFINI

1. L'applicazione "Immuni", approvata dal Governo italiano al fine di controllare la diffusione del contagio da Covid-19 attraverso una piattaforma digitale che traccia i contatti tra le persone, può essere scaricata in modo volontario e gratuito dai principali *store* di software per smartphone e, una volta installata, genera in modo continuativo codici casuali e temporanei che identificano il dispositivo in cui l'app è contenuta, senza tuttavia riferirsi in alcun modo ai dati personali del proprietario.

L'app utilizza la tecnologia *Bluetooth Low Energy* (BLE) per comunicare con gli smartphone entrati nel suo raggio di azione, inviando il codice in quel momento generato e recependo al contempo i codici generati dagli smartphone degli altri utilizzatori dell'app.

La tecnologia BLE garantisce l'anonimato e al contempo evita la necessità di individuare la posizione del proprietario dello smartphone, in quanto ha il solo scopo di scambiare dati con i dispositivi circostanti senza permettere il tracciamento satellitare a fini di geolocalizzazione (GPS).

La lista di codici così generati viene archiviata in locale, sul telefono, dall'applicazione stessa insieme alla lista di codici ricevuti dagli smartphone degli utilizzatori con cui si è entrati in contatto.

Nel caso in cui un utilizzatore dell'app risulti positivo al virus Covid-19, potrà allertare un operatore sanitario, che provvederà a scaricare tutti i codici generati dall'app su un server centrale, al quale l'applicazione si connette quotidianamente. Di conseguenza, gli smartphone degli utilizzatori entrati in contatto con il soggetto positivo effettueranno un abbinamento tra i codici ricevuti e i codici indicati dal server centrale come codici "a rischio", notificando esclusivamente l'avvenuto contatto e consigliando di rivolgersi ad una struttura sanitaria per accertamenti.

Tutti i codici, generati e ricevuti dagli utilizzatori, sono del tutto anonimi e, per espressa disposizione normativa, saranno soggetti a cancellazione al termine della pandemia e comunque entro il 31 dicembre 2020.

2. L'utilizzo della piattaforma "Immuni" ha, soprattutto in fase di avvio, sollevato dubbi e perplessità in merito alle modalità di bilanciamento tra il diritto alla tutela della *privacy* e ad

un corretto trattamento dei dati personali e l'interesse pubblico alla tutela della salute, anche in applicazione di norme internazionali ed europee.

Va detto che, nonostante la pandemia di Covid-19 abbia rappresentato un evento assolutamente imprevedibile, non è stato necessario elaborare nuove regole, risultando quelle esistenti perfettamente adatte a gestire le nuove esigenze (come qui chiarito dallo *European data protection board*, EDPB).

Ricordiamo come il diritto alla tutela della *privacy*, tutelato nel Patto internazionale sui diritti civili e politici (art. 17), nella Convenzione europea dei diritti dell'uomo (art. 8), nella Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, nel Regolamento generale per la protezione dei dati personali dell'UE (GDPR), nella direttiva ePrivacy del 2002, non abbia natura assoluta, dal momento che queste fonti permettono di derogarvi al fine di tutelare interessi superiori, come nel caso in cui occorra perseguire l'interesse generale della tutela della salute, contemplato, ad esempio nel considerando 46 o nell'art. 9, par. 2, lett. i), del GDPR (qui il testo integrale).

E parimenti le limitazioni al diritto alla tutela dei dati personali (che, nato nel contesto della privacy, se ne è progressivamente affrancato) devono rispettare alcuni principi sanciti a livello internazionale, sovranazionale e nazionale.

In particolar modo, la possibilità di limitare tale diritto trova fondamento nella sua natuura di diritto fondamentale relativo (sul punto v. G. FINOCCHIARO, *Il punto sull'app Immuni: bilanciamento tra diritti*) che, quindi, in caso di perseguimento di interessi pubblici superiori, può essere soggetto a deroga, purché siano rispettati i principi di *necessità* (e cioè uno stretto rapporto tra gli obiettivi che si intendono perseguire e l'individuazione delle opzioni meno invasive tra quelle adottabili; cfr. anche il c.d. *principio di minimizzazione*) e *proporzionalità* (e cioè l'idoneità della misura a perseguire l'obiettivo rilevante, il bilanciamento tra obiettivo e interferenza nella tutela dei dati personali; per una disamina si veda G. DELLA MORTE, *La tempesta perfetta COVID-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*).

I dati a tal fine raccolti, peraltro, devono rispettare determinati requisiti per poter essere processati alla luce di un corretto bilanciamento tra la tutela della *privacy* e la tutela del diritto alla salute.

Occorre, infatti, che le inferenze siano previste da una norma giuridica (categoria che, va detto, può essere variamente intesa; c.d. *formalità*), risultino necessarie nel quadro di una società democratica (*indispensabilità*), perseguano lo scopo di tutela della salute (*finalità*), siano specificamente individuate (*tassatività*), indichino il loro periodo di vigenza (*temporalità*), siano contestabili (*impugnabilità*) e non risultino eccessive rispetto allo scopo perseguito (*proporzionalità*).

Il perseguimento della tutela della salute pubblica risulta quindi uno degli obiettivi idonei a legittimare la limitazione della tutela dei dati personali.

In merito ad Immuni, si è infatti in più occasioni chiarito che, anche se il *download* dell'app è volontario e non vi sono ripercussioni in caso di mancata installazione della piattaforma sul proprio dispositivo (a differenza di quanto previsto in altri Paesi, come si vedrà *infra*), ciò che legittima il funzionamento dell'applicazione non è il mero consenso dell'avente diritto, bensì la necessità di tutelare la salute, nel rispetto del principio di limitazione delle finalità, volto appunto ad evitare utilizzi ultronei dei dati rispetto a quelli ammessi per le finalità sinora viste(*ex multis* v. E. CIRONE, *L'App italiana di contact tracing alla prova del GDPR: dall'habeas data al ratchet effect il passo è breve?*).

3. La progettazione dell'app nel rispetto del principio della *privacy by design* sancito dall'art. 25, par. 1 GDPR ha risolto molti dei problemi che erano stati in precedenza paventati, che intendiamo riassumere qui brevemente.

I principali dubbi riguardavano i profili di rischio connessi alla geolocalizzazione degli utenti, all'anonimizzazione, e alla conservazione dei dati, sia con riferimento alle modalità di raccolta che alla durata.

Tutti questi aspetti sono stati, in più occasioni, messi in luce dalle istituzioni UE e dai competenti organi di settore: la Commissione europea, ad esempio, in una *Comunicazione sugli Orientamenti sulle app a sostegno della lotta alla pandemia di covid-19 relativamente alla protezione dei dati personali* dell'aprile 2020, aveva richiesto che il *download* della app avvenisse su base volontaria e che la stessa non comportasse la geolocalizzazione; parimenti il Parlamento europeo, in una *risoluzione relativa alla Azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze* aveva ribadito la necessità della natura non obbligatoria dell'applicazione e ha manifestato una posizione contraria alla conservazione dei dati in forma centralizzata; infine, il *Comitato europeo per la protezione dei dati personali*, richiamando la posizione della Commissione, esplicitava, nelle sue *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* la necessità di mantenere l'applicazione su base volontaria e di evitare il tracciamento GPS dei fruitori.

In particolare, per quanto riguarda l'Italia, con riferimento al problema della conservazione dei dati personali, considerata la necessità di garantire la trasparenza della loro modalità di gestione (come espresso qui dal EDPB), il decreto legge 30 aprile 2020 n. 28 ha stabilito che i dati potranno essere conservati solo fino al termine della pandemia e comunque non oltre il 31 dicembre 2020.

Come dicevamo, un altro aspetto da chiarire concerneva le modalità di conservazione dei dati, in considerazione della possibilità alternativa, da un lato, di una loro centralizzazione tramite un server in cui i codici generati dagli smartphone sarebbero stati archiviati e, dall'altro lato, di una loro conservazione decentralizzata, tale per cui ogni smartphone avrebbe conservato al proprio interno la lista di codici generati e la lista di codici ricevuti dai soggetti con cui si era entrati in contatto, connettendosi al server centrale solo una volta al giorno per aggiornamenti.

Si è ritenuto che, in considerazione dei succitati orientamenti europei, la decentralizzazione dei dati fosse meglio rispettosa del diritto al trattamento dei dati e alla riservatezza, essendo la stessa comunque idonea a soddisfare l'interesse generale della tutela della salute: si è quindi stabilito, come dicevamo in apertura, che i dati raccolti siano conservati all'interno del singolo smartphone e che il collegamento con il server centrale serva solo a raffrontare gli stessi con quelli contrassegnati come appartenenti ad un soggetto positivo al Covid-19.

Va, inoltre, osservato come la decentralizzazione della conservazione dei dati meglio garantisca anche l'anonimizzazione degli stessi.

Con riferimento a quest'ultimo requisito, si è poi posto il problema di distinguere l'effettiva anonimizzazione dalla figura della pseudonimizzazione, non altrettanto garantista.

L'EDPB ha, nelle proprie linee guida, ribadito e chiarito ancora una volta questa differenza, evidenziando, al contempo, come, nel caso di specie, l'anonimizzazione dei dati fosse un'assoluta priorità: ebbene, come noto, la differenza tra le due figure risiede sostanzialmente nel fatto che, mentre la pseudonimizzazione impedisce solo *ictu oculi* di

identificare un soggetto, ricollegandolo ad uno pseudonimo che tuttavia non preclude in assoluto la possibilità di risalire alla sua identità, l'anonimizzazione rende anonimo in modo assoluto e definitivo il dato, e quindi, nel caso di specie, l'identità dell'utilizzatore dell'app.

Va pure osservato che distinguere i meccanismi di pseudonimizzazione da quelli di anonimizzazione può risultare in alcuni casi complesso; dalle linee guida del *Comitato europeo per la protezione dei dati personali* si evincono comunque criteri utili per stabilire se i dati siano effettivamente anonimi: ciò avviene qualora dai dati sia impossibile risalire all'identità di un soggetto anche solo partendo da un gruppo ristretto di individui; qualora, invece, risulti possibile ricollegare tra loro più scambi reciproci di codici avvenuti in momenti diversi o qualora risulti possibile comunque dedurre informazioni non conosciute su un determinato individuo, si rientra nell'ipotesi della pseudonimizzazione. In buona sostanza, afferma l'EDPB, per poter essere considerati anonimi, i dati raccolti devono garantire l'*effettiva* impossibilità di risalire, *con ogni strumento*, all'identità del soggetto al quale si riferiscono.

Si è ritenuto, pertanto, che la decentralizzazione della conservazione dei dati, insieme ai principi di minimizzazione e di limitazione delle finalità, permetta una migliore anonimizzazione degli stessi.

A completare questo processo si è optato, poi, come pure accennavamo in apertura, per uno scambio di dati basato sulla prossimità invece che sul tracciamento.

La tecnologia BLE, utilizzata dall'applicazione, permette difatti agli smartphone di rilevare i dispositivi nelle vicinanze e interagire con essi, pur impedendo ogni localizzazione GPS. In sostanza, l'applicazione riconosce la presenza di altre app nelle vicinanze, ma non è in grado di indicare *dove* si trovino geograficamente queste ultime.

In virtù del principio di *minimizzazione* e di *anonimizzazione* dei dati si è ritenuto che questo sistema sia il più adatto (pur non essendo esente da problemi, come si vedrà *infra*), rilevando solo l'interazione tra due dispositivi e non già il luogo in cui la stessa è avvenuta; si tenga inoltre presente che il tracciamento della posizione potrebbe essere usato per risalire all'identità degli utilizzatori.

La tecnologia BLE, oltre ad essere preferita al tracciamento GPS, è stata privilegiata anche rispetto alla localizzazione basata sul traffico telefonico in quanto tale meccanismo, pur permettendo più immediate comunicazioni in caso di urgenza, non avrebbe garantito l'anonimizzazione assoluta, richiesta a livello sovranazionale.

4. L'applicazione italiana "Immuni" non è naturalmente l'unica utilizzata per fronteggiare la pandemia di Covid-19, ma senza dubbio risulta essere tra le più garantiste predisposte dai vari Stati.

In tutto il mondo ci sono esempi di applicazioni alternative, anch'esse su base nazionale, che non paiono garantire, però, specie quelle adottate al di fuori del contesto UE, un livello di tutela e un bilanciamento dei diritti analogo a quanto previsto nell'ordinamento italiano ed europeo.

Per citare alcuni tra gli esempi più lontani dal funzionamento di "Immuni", si pensi alla Russia, che ha introdotto un sistema di tracciamento GPS finalizzato a creare un "recinto virtuale" per controllare il rispetto della quarantena da parte dei contagiati, oppure alla Cina, in cui l'applicazione di lotta al contagio assegna addirittura al proprietario dello smartphone un codice-colore (verde se si è sani, giallo se si è a rischio e rosso se si è contagiati) che può in qualunque momento essere soggetto a controllo da parte delle forze dell'ordine, con la precisazione che uscire di casa senza lo smartphone o senza aver installato l'app equivale ad avere un codice rosso; o ancora a Israele, in cui il tracciamento

dei contagi era previsto attraverso il controllo incrociato e costante di tabulati telefonici e transazioni tramite carta di credito (questo fino alla dichiarazione di illegittimità da parte della Alta Corte di Giustizia di Israele, per mancanza di una legge di copertura).

Il funzionamento dell'app "Immuni" ha fatto discutere anche con riguardo all'applicazione di norme dell'Organizzazione Mondiale del Commercio in merito al "se" il servizio fornito dall'applicazione rientrasse nella figura dello scambio di merci (dal momento che per alcuni Stati qualsiasi scambio di beni digitali è riconducibile a tale categoria) o nella figura dei servizi. La dottrina ha ritenuto al riguardo che si tratti di scambio di servizi, con la conseguente necessità di ricondurla alla disciplina prevista dall'Accordo generale sugli scambi di servizi (GATS), pur ritenendo applicabili eccezioni all'esclusione dagli obblighi di liberalizzazione, giustificate dalla necessità di evitare una discriminazione arbitraria tra i Paesi (per una disamina approfondita e completa, e l'analisi della procedura di adozione nel contesto commerciale multi-plurilaterale, si veda G.M. RUOTOLO, *Alcune osservazioni sulle app di tracciamento dei contatti e dei contagi alla luce del diritto dell'Organizzazione Mondiale del Commercio*).

5. L'app "Immuni" non risulta, però, essere esente da criticità relative al suo funzionamento.

In primis, è evidente come la sua efficacia sia direttamente proporzionale alla sua diffusione, in quanto la stessa necessita di raccogliere il maggior numero possibile di dati dagli altri smartphone per poter essere accurata; la scelta di mantenere il suo *download* su base puramente volontaria, seppur giustificata alla luce del bilanciamento di interessi e dei principi nazionali e sovranazionali di cui si è detto, costituisce indubbiamente un ostacolo al suo più efficace funzionamento.

Allo stesso tempo, l'utilizzo della tecnologia BLE comporta l'alto rischio di falsi positivi e falsi negativi. Infatti, le onde utilizzate dal Bluetooth sono in grado di attraversare gli oggetti solidi, come pareti o divisori; pertanto l'essere in prossimità di un altro soggetto, anche se isolati (si pensi a due auto accostate al semaforo o a due persone separate da una parete) sarà registrato dall'applicazione come contatto tra i due utilizzatori (anche se in casi siffatti, evidentemente, non c'è alcun rischio di contagio) e l'assenza di tracciamento GPS impedirà di risalire all'esatta posizione in cui tale contatto è avvenuto.

L'applicazione, pertanto, pur risultando efficace sulla carta, necessita di un impegno attivo e di un uso accorto da parte dell'utilizzatore per poter risultare efficiente.

DAVIDE VAIRA