Relazione[1] per la Commissione Giustizia al Senato nell'ambito dell'audizione informale del 14 maggio 2020 e in relazione al DDL S.1786, sulla conversione in legge del decreto-legge 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, nonché 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.

FRANCESCO PAOLO MICOZZI – AVVOCATO E PROFESSORE A CONTRATTO DI INFORMATICA GIURIDICA, UNIVERSITÀ DEGLI STUDI DI PERUGIA

Premessa

Nel periodo a cavallo tra il 2019 e il 2020 ha iniziato a diffondersi, a livello mondiale, la pandemia di COVID-19 (causata dal virus SARS-CoV-2). La pandemia in questione, la cui diffusione avrebbe avuto origine nella città cinese di Wuhan, arriva in Italia verso la fine del mese di gennaio 2020 con una tale viralità da imporre al Governo l'adozione, con decreti-legge e decreti ministeriali, una serie di misure emergenziali.

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

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

Tuttavia, il *contact tracing* rimesso alle semplici interviste fatte dal personale sanitario sconta la "debolezza" di essere rimesso alla memoria del paziente e alla sua capacità di indicare soggetti determinati. Per questo motivo in alcuni paesi, tra cui la Corea del Sud, già da qualche anno sono stati approntati sistemi tecnologici per eseguire il *contact tracing*. Impiegare le tecnologie per sopperire all'intrinseca debolezza della memoria del paziente può comportare, di converso, l'insorgere di ulteriori problematiche (sotto svariati profili) dovute all'impiego di una sorveglianza tecno-sanitaria su larga scala.

Le soluzioni di contact tracing tecnologico

---

[1] Alcune parti della presente relazione sono tratti da un documento, a firma dello scrivente, attualmente in fase di pubblicazione, in forma più estesa, nella *Special Issue* dedicata alla gestione dell'emergenza CoViD-19 di BioLaw Journal - Rivista di Biodiritto, rivista giuridica di fascia A, online e peer-reviewed, che approfondisce i rapporti tra diritto e scienza in prospettiva comparata.

Allo stato l'orientamento del Governo italiano sembrerebbe quello di adottare una soluzione di *contact tracing* basata sulla tecnologia bluetooth, e in particolare la *bluetooth low energy*, o BLE (particolare tipo di tecnologia bluetooth a basso consumo energetico). La tecnologia BLE, infatti, consentirebbe ai diversi dispositivi (ad esempio smartphone) di comunicare (tra dispositivi e/o con un server centrale) informazioni relative all'eventuale "contatto" tra diversi soggetti, all'intensità del segnale (dal quale può inferirsi la distanza alla quale i dispositivi si sono trovati) e la "durata" del contatto.

Scendendo maggiormente nel dettaglio, occorre precisare che, a seconda dello schema logico di implementazione della tecnologia BLE per il *contact tracing* impiegato, possono aversi, sotto il profilo del trattamento di dati personali, differenti modelli applicativi. Le valutazioni sulla capacità di maggiore o minore aderenza ai principi generali sul trattamento dei dati personali, previsti dall'art. 5 del GDPR, pertanto, andranno fatte non tanto sul "modello" quanto sull'applicazione pratica dello stesso. Due "modelli" di *contact tracing* tramite BLE si contendono, infatti, la primazia: uno che si appoggia a un sistema centralizzato di memorizzazione delle informazioni e un altro che, invece, non concentra le informazioni di "contatto" in un server centrale ma le memorizza all'interno del singolo dispositivo (sistema decentrato). La modalità di conservazione delle informazioni di tracciamento non è di poco momento, per quanto riguarda la disciplina sulla protezione dei dati personali, posto che nelle succitate linee-guida 4/2020 EDPB si precisa che sebbene entrambe le soluzioni siano praticabili, "*entrambe comportano una serie di vantaggi e svantaggi*" e che dovrebbero ponderarsi attentamente "*gli effetti in termini di protezione dei dati e privacy nonché i possibili impatti sui diritti delle persone*", comunque, in via generale, la soluzione decentrata sarebbe maggiormente rispettosa del principio di minimizzazione[2]. Due sono i protocolli attualmente allo studio e in via di adozione nelle diverse soluzioni applicative proposte a livello europeo: PEPP-PT[3] (*Pan-European Privacy-Preserving Proximity Tracing*) che segue il modello centralizzato e; DP-3T[4] (*Decentralized Privacy-Preserving Proximity Tracing*) che, come intuibile, impiega lo schema decentralizzato.

In particolare il protocollo DP-3T

È interessante, a questo punto, esaminare meglio la logica di funzionamento del modello DP-3T[5] che, con tutta probabilità, sarà impiegato nella soluzione tecnologica di *contact tracing* favorita dal Governo italiano. Il protocollo DP-3T prevede, come già visto, l'impiego della tecnologia BLE e un sistema decentralizzato per la memorizzazione delle informazioni. Una volta che la App venga installata nel dispositivo dell'utente, essa prenderebbe a generare gli EphID (*ephemeral identifiers*[6]), ossia codici alfanumerici anonimi (in quanto non contenenti informazioni riconducibili al dispositivo che li ha generati) ad intervalli temporali regolari e prefissati (un nuovo EphID sarebbe generato ogni 15 minuti). Gli EphID generati (dal dispositivo sul quale sia installata la App di

---

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

contact tracing) sono memorizzati all'interno dell'App (in un registro che potremmo definire "registro dei codici generati") e, contemporaneamente, trasmessi tramite segnali radio (BLE) a tutti i dispositivi che si trovino ad una certa distanza (massimo 50 metri, circa). La stessa App memorizza, allo stesso modo, tutti gli EphID ricevuti tramite BLE dalle App dei soggetti che si trovino nelle vicinanze, all'interno di un altro registro che potremmo chiamare, ipoteticamente, "registro dei codici ricevuti" – gli analoghi codici, ricevuti dalle altre App. In tal modo la medesima App memorizzerà al suo interno sia un registro dei codici (EphID) generati e trasmessi, sia un registro dei codici (EphID) ricevuti dagli altri dispositivi.

Nel momento in cui dovesse accertarsi il contagio da SARS-CoV-2, i sanitari chiederebbero al paziente se ha installato la App e se vuole mettere a disposizione gli EphID generati dal suo dispositivo. In caso affermativo il sanitario genererebbe un codice di autorizzazione che verrebbe, poi, mostrato sotto forma di QR-Code (ossia un codice a barre bidimensionale impiegato tipicamente per memorizzare informazioni destinate a essere lette tramite la telecamera dello smartphone) e che consente all'utente di inviare al server di backend il suo "registro dei codici generati" che viene, così, messo a disposizione di tutti gli altri soggetti che abbiano installato la App. Questi ultimi potranno, una volta ricevuti tali codici, verificare (confrontandoli) se taluno dei codici ricevuti dal server corrisponda a uno dei codici memorizzati nel "registro dei codici ricevuti". In un sistema decentrato, quindi, qualsiasi utilizzatore della App potrà essere informato del fatto che è entrato in contatto, per un certo periodo e a una certa distanza, con un soggetto al quale sia stata diagnosticata la patologia. Tuttavia, nessuno è in grado di sapere quale sia il dispositivo che abbia generato i codici ricevuti né potrà essere individuato e contattato, nemmeno dal servizio sanitario: il fatto che egli si ponga in quarantena o decida di recarsi presso un centro medico per eseguire i controlli diagnostici, è rimesso, quindi, al suo "buon senso".

L'art. 6 del DL 28/2020

Il procedimento normativo della tecnologia di contact tracing trova la sua conclusione (almeno sino a questo momento) nell'art. 6 del DL 30 aprile 2020, n. 28, rubricato "Sistema di allerta Covid-19". L'attuale versione è frutto anche dell'intervento del Garante per la protezione dei dati personali che ha offerto al Governo una serie di suggerimenti, con il parere del 29 aprile[7], che sono stati recepiti nella versione definitiva della norma in questione.

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

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

ogni trattamento di dati personali ai sensi del medesimo articolo dovrà cessare alla cessazione dell'emergenza e, comunque, entro il 31 dicembre 2020.

Considerazioni finali

Considerazione 1

La prima considerazione prende spunto da quanto correttamente rilevato nella nota di lettura n. 147 del Servizio del Bilancio nel punto in cui si prevede che "*l'implementazione della piattaforma potrebbe implicare anche la necessità di un potenziamento del sistema di individuazione dei contagiati e di rilevamento della loro evoluzione sanitaria (con tamponi ed, eventualmente, test sierologici) proprio al fine di rendere efficace il sistema di tracciamento, altrimenti destinato, per quanto ben congegnato tecnologicamente, a rivelarsi poco utile*". Ciò significa che qualsiasi sistema di tracciamento dei contatti si rivelerebbe assolutamente inutile se non vi sia la disponibilità e possibilità di somministrare i test diagnostici (tamponi faringei o test sierologici o altra misura individuata utile, dal punto di vista sanitario, all'accertamento del contagio) ai soggetti eventualmente allertati per il tramite dell'Applicazione di contact tracing che si rechino presso le strutture sanitarie.

Considerazione 2

Sebbene le previsioni normative contemplate dall'art. 6 del DL 28/2020 siano state in larga parte adeguate alle indicazioni sia delle linee-guida 4/2020 EDPB che del parere del Garante per la protezione dei dati personali, residuano margini di ambiguità. Innanzitutto, non è stato chiarito, come auspicato dal Garante nel suo parere, se il sistema di contact tracing sarà centralizzato ovvero decentrato nella memorizzazione e gestione delle informazioni di tracciamento. In particolare, l'art. 6, comma 2, lett. e), si prevede che i dati relativi ai contatti siano conservati "anche" nei dispositivi mobili degli utenti.

Si suggerisce di rimuovere l'inciso "anche" dall'art. 6, co. 2, lett. e), in modo da rendere maggiormente garantito il processo di trattamento e protezione dei dati personali assicurando che sia implementato un sistema decentralizzato di conservazione dei dati sia pure anonimi/pseudonimizzati.

Considerazione 3

Il comma 2, lett. a) prevede che gli utenti debbano ricevere specifiche informazioni ai sensi degli artt. 13 e 14 del GDPR. Tra queste informazioni si indicano, in particolare, finalità e operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati.

Il comma 6 prevede la cosiddetta *sunset clause*, in cui si definiscono i tempi di operatività del sistema di allerta. Si prevede, in particolare, che comunque entro la data del 31 dicembre 2020 "tutti i dati trattati devono essere cancellati o resi definitivamente anonimi".

Si suggerisce di aggiungere al comma 2, lett. a), tra le informazioni da sottoporre agli interessati, anche le "tecniche di anonimizzazione" che saranno impiegate ai sensi del successivo comma 6 del medesimo articolo.

Si suggerisce, inoltre, che le medesime misure di cancellazione o anonimizzazione previste dal comma 6 siano applicabili, a richiesta dell'utente/interessato, anche nell'ipotesi in cui lo stesso, prima ancora del termine del 31 dicembre 2020, decida di disinstallare l'applicazione dal proprio dispositivo di telefonia mobile.

Considerazione 4

Il Garante per la protezione dei dati personali, nell'audizione dell'8 aprile 2020 in Commissione IX (Trasporti, Poste e Telecomunicazioni) della Camera dei Deputati, aveva suggerito, come qualcosa di essenziale, "sancire (con il presidio di sanzioni adeguate) l'obbligo di cancellazione dei dati decorso il periodo di potenziale utilizzo (salva la conservazione in forma aggregata o comunque anonima per soli fini statistici o di ricerca) e l'illiceità di qualsiasi riutilizzo dei dati per fini diversi da quelli di tracciamento dei contatti, nei termini suindicati."

Si suggerisce di introdurre, nel codice della privacy – d.lgs. 196/2003 - una norma penale incriminatrice che sanzioni le ipotesi di utilizzo illecito o omessa anonimizzazione o cancellazione delle informazioni personali eventualmente acquisite attraverso il sistema di allerta COVID-19 oltre il termine individuato nel 31 dicembre 2020.

Considerazione 5

In base a quanto previsto dal comma 5 dell'art. 6 non è chiaro se anche l'applicazione dovrà essere rilasciata sotto licenza aperta ai sensi dell'art. 69 del Codice dell'amministrazione digitale (d.lgs. 82/2005) posto che si prevede che con tale licenza – che garantirebbe maggiore trasparenza di funzionamento al sistema di tracciamento dei contatti – siano rilasciati esclusivamente "*i programmi sviluppati per realizzare la piattaforma e utilizzare l'applicazione*". In un'ottica di maggiore trasparenza dovrebbe estendersi il rilascio con licenza aperta dell'applicazione e del codice sorgente della stessa. Ciò consentirebbe di "compilare" l'applicazione partendo dal codice sorgente e di verificare appieno il funzionamento dell'applicazione reperibile presso gli app store (Google Play e Apple Store) che sarà confrontabile – con gli algoritmi di hash – con la medesima versione della app compilata.

Si suggerisce di modificare il comma 5 dell'art. 6 in modo che sia chiaro che anche l'App che gli utenti/interessati andranno ad installare sul loro dispositivo di telefonia mobile debba essere rilasciata con codice sorgente aperto e con licenza aperta ai sensi dell'art. 69 del D.Lgs. 82/2005.