GRUPPO DI LAVORO 8 – PROFILI GIURIDICI

RELAZIONE PROPOSTA n. 71

Nome soluzione

CovidApp - Covid Community Alert.

Soggetto proponente

L'app viene proposta dal team denominato "Coronavirus Outbreak Control", che non risulta possedere personalità giuridica.

Tipologia di dati trattati dall'app

In base alla descrizione fornita, il funzionamento dell'app garantirebbe il trattamento di dati in forma anonima o comunque il trattamento di informazioni con una ridottissima capacità identificativa, peraltro solo eventuale e indiretta nell'ipotesi in cui si verifichino eventi patologici. In due soli frangenti sembrerebbe ravvisabile un trattamento di dati personali, pur con limitate possibilità di re-identificazione: anzitutto, in relazione all'indirizzo IP dell'utente al momento della trasmissione delle informazioni registrate in locale al server; in secondo luogo, in riferimento alla attività di sblocco del diario clinico di un paziente da parte del personale medico, che implica necessariamente (e inevitabilmente) l'associazione tra l'ID randomico attribuito al paziente che utilizza l'app e l'identità del paziente medesimo, nota all'operatore sanitario che lo ha precedentemente visitato (e derivante da una precedente, autonoma e separata attività di trattamento di dati relativi alla salute).
Sotto il primo profilo, tuttavia, i dati inerenti agli indirizzi IP non formano comunque oggetto di memorizzazione e sono comunque proposte misure idonee di mitigazione.
Quanto al secondo versante, il rischio connesso alla inevitabile cognizione dell'associazione tra paziente visitato e ID inserito nel sistema potrebbe parimenti essere contenuto imponendo l'immediata cancellazione delle informazioni all'operatore sanitario.
Al di fuori di queste circostanze, le informazioni immagazzinate riguardano le interazioni spaziali anonime registrate mediante tecnologia Bluetooth con altri dispositivi nel periodo antecedente e la relativa durata temporale (funzionali a rivelare il rischio di esposizione con il dispositivo appartenente di un paziente riscontrato clinicamente positivo).
L'installazione dell'app non richiede il trattamento del numero telefonico del dispositivo. All'utente, all'atto del login, è infatti assegnato un ID generato pseudo-randomicamente e soggetto su base costante a un processo di *shuffling* volto a ridurre qualsiasi rischio di tracciamento dei dispositivi sulla base del segnale Bluetooth.
Se l'utente lo desidera, su base volontaria, è consentita l'attivazione del segnale GPS, che comunque non comporta un tracciamento generalizzato dell'utente e si limita a registrare

esclusivamente le interazioni con altri dispositivi (non operando, cioè, quando il dispositivo risulta in stato di "isolamento").

Modalità del trattamento

L'app procede alla generazione di codici identificativi anonimi correlati ai device (smartphone) su cui è installata al fine di verificarne l'interazione spaziale con altri dispositivi che potrebbero successivamente risultare appartenenti a individui di cui sia riscontrata la positività al virus. In caso di disinstallazione e successiva reinstallazione dell'app il codice randomico è generato *ex novo*. L'app è in grado di riscontrare l'associazione tra l'ID randomico originale e quelli successivamente assegnati all'esito del processo di *shuffling* conservando i dati per finestre di tempo limitate. La comunicazione dei dati relativi alle interazioni registrate da ciascun dispositivo su cui l'app sia stata installata comporta in ogni caso il trattamento dell'indirizzo IP, che può tuttavia essere accompagnato da idonee misure di mitigazione del rischio come segnalato in relazione generale.
Su base periodica, i dati registrati mediante tecnologia Bluetooth e salvati in locale, relativi all'interazione con altri dispositivi e indicativi degli spostamenti effettuati dai rispettivi proprietari, sono trasmessi al server e archiviati in modalità *cloud*.
Al contempo, in caso di visita, mediante un'apposita interfaccia dedicata (CoviDoc), gli operatori sanitari, con il consenso dell'utente *in loco*, provvedono, tramite la scansione del QR code associato al dispositivo in essere ai pazienti, ad aggiornare il diario clinico, segnalando eventuali casi di contagio. Si precisa che l'attività di trattamento dei dati relativi alla salute effettuata dal personale medico che successivamente adoperi l'app risale invece a una autonoma e separata fase diagnostica e a un trattamento separato e autonomo dei dati (pare in ogni caso opportuno che l'operatore sanitario proceda all'immediata cancellazione dell'identificativo, prevenendone così la conservazione, onde minimizzare ogni rischio di re-indentificazione collegato alla sua personale conoscenza del paziente cui si riferisce il codice randomico anonimo utilizzato).
Una volta aggiornato lo status clinico di un utente, l'app è in condizione di individuare all'interno del database i dispositivi (identificati da ID anonimo) con i quali il dispositivo appartenente al paziente dichiarato positivo (o sospetto positivo) si sia trovato in una rilevante prossimità spaziale (tale da rendere apprezzabile il rischio di contagio) nell'arco dei quattordici giorni antecedenti così da inviare loro notifiche push (con misure tecniche e organizzative atte a impedirne la identificazione) contenenti l'informazione circa l'esposizione a rischio e possibili istruzioni sul comportamento da adottare.
Il funzionamento dell'app presuppone una previa definizione della distanza e della durata della interazione spaziale tra dispositivi rilevanti al fine di ritenere apprezzabile il rischio di contagio.
Il processo di continua memorizzazione su base periodica delle interazioni registrate tra dispositivi consente di rimediare a un *gap* tecnico dovuto alla impossibilità dei dispositivi iOS di trasmettere segnali Bluetooth in modalità *background*. Con questa soluzione tecnica, l'interazione tra dispositivi Android e dispositivi iOS consente di rimediare alla limitazione

tecnica dei dispositivi Apple che ricevono il segnale ma non lo trasmettono e garantire una percentuale di copertura del 98,9%, che sarebbe altrimenti limitata al 71,5%.

Uso di soluzioni di terze parti

L'app utilizza la tecnologia di tracciamento contatti basata sul Bluetooth Low Energy (LE). La componente server del progetto utilizza invece i servizi *cloud* della piattaforma Amazon AWS, così come progettata, ma può essere dispiegata su strutture autonome e proprietarie del titolare del trattamento.

Privacy by design - Privacy by default

Dall'esame della documentazione, la soluzione tecnologica appare fortemente improntata al rispetto dei principi di *privacy by design* e *privacy by default*. Nella definizione delle caratteristiche e delle modalità operative dell'app, si è tenuto conto dello stato dell'arte, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per i diritti e le libertà delle persone fisiche. Questa certosina attenzione emerge nella dettagliata presentazione tecnica dell'app, ove si documenta l'implementazione delle misure tecniche e organizzative adeguate, tra cui la minimizzazione del trattamento di dati e la pseudonimizzazione.

Misure di sicurezza

Sotto il profilo tecnico, la documentazione non è corredata da report che dimostrino l'esecuzione di test di sicurezza sulle app e sui server utilizzati. Non è quindi dato formulare una compiuta valutazione in relazione agli aspetti di sicurezza informatica e di resistenza a possibili attacchi informatici. Si segnala tuttavia l'impegno a una continua implementazione dell'applicazione grazie a un team di sviluppatori del codice *open source*. I proponenti dichiarano altresì di aver dato corso ad attività quali *penetration test e reverse engineering* di cui non hanno ancora prodotto la relativa documentazione, come sopra specificato.
Nella descrizione, si segnala che tutte le comunicazioni tra app e server utilizzano protocolli HTTP su Transport Layer Security (HTTPS), avvalendosi pertanto di cifratura mediante crittografia asimmetrica. I relativi certificati sono gestiti da Amazon AWS, che fornisce la piattaforma di *cloud*.
Non è precisata la localizzazione dei *data center* di archiviazione delle informazioni, tuttavia la documentazione dichiara la conformità dell'app alla legislazione applicabile nell'Unione europea.

Analisi dei rischi per le libertà e i diritti degli interessati

Non si ravvisano, sulla base delle informazioni rappresentate dal proponente, particolari rischi per le libertà e i diritti degli interessati legati al fisiologico funzionamento dell'app.

L'obiettivo perseguito dall'app non è quello di permettere l'individuazione di un paziente infetto, bensì di notiziare ai suoi utenti le possibili interazioni spaziali entro l'arco temporale dei 14 giorni antecedenti con dispositivi appartenenti a utenti le cui connotazioni cliniche siano state esaminate dal personale medico, con conseguente riscontro di positività al Coronavirus e aggiornamento del diario sanitario. Si potrebbero tuttavia registrare, in condizioni "patologiche" che prescindono dalla normale operatività dell'app e dal suo fisiologico funzionamento, attacchi informatici in grado di comportare il rischio di una re-identificazione degli utenti precedentemente "anonimizzati" con annessa, possibile, esposizione dei dati relativi alla salute (quali l'aggiornamento dello stato clinico del paziente all'esito dell'effettuazione di un tampo, positivo o negativo che sia).
La ricerca di modalità volte ad assicurare in ogni fase l'anonimato, frutto di una adesione apprezzabile ai principi di *privacy by design* e *privacy by default*, costituisce senza dubbio un punto di forza della soluzione proposta, le cui modalità tecniche appaiono congegnate in modo da limitare al massimo il rischio di identificazione dei titolari dei dispositivi. L'app presenta inoltre una possibile implementazione legata all'utilizzo della tecnologia GPS, la cui attivazione sarebbe eventualmente rimessa all'utente, e dunque previo consenso, ma che si consiglia in ogni caso di valutare in relazione al suo possibile impatto sui diritti e le libertà degli individui. In ogni caso, il tracciamento è circoscritto all'evenienza in cui il dispositivo dell'utente interagisca con lo spazio, non attivandosi invece in fasi di "isolamento".
Non sono precisate le misure volte a consentire la distruzione automatica delle informazioni, sebbene il riferimento cronologico appaia legato alle interazioni occorse nei quattordici giorni antecedenti lo sblocco del diario clinico del paziente.
La presentazione dell'app non è corredata da una valutazione di impatto, ma dà conto dell'*endorsement* di un team di esperti in materie giuridiche, informatiche e ingegneristiche.
Il proponente dichiara che è comunque in fase di finalizzazione e di revisione legale il "documento privacy".