cepAdhoc

No 4 | 2020 21 aprile 2020

Applicazioni per il tracciamento di contatti ai sensi della legislazione dell'UE sulla protezione dei dati personali

Il "libero consenso" dei singoli è un prerequisito per la fase successiva nella lotta contro il COVID-19

Martina Anzini


© shutterstock

Le applicazioni (app) per il tracciamento di contatti dovrebbero svolgere un ruolo importante nella lotta contro il Coronavirus. Il quadro normativo dell'UE in materia di protezione della privacy e dei dati personali, tuttavia, stabilisce dei vincoli giuridici per tali applicazioni.

- Le app per la registrazione di prossimità - che registrano solo i contatti epidemiologicamente rilevanti - sono un'alternativa più rispettosa della protezione dei dati personali rispetto alle applicazioni per la registrazione dei dati di localizzazione. Proprio per questo motivo, la legittimità di queste ultime può essere esclusa.
- Le app di registrazione di prossimità possono funzionare senza dati personali, facendo così cadere il relativo trattamento dei dati fuori dall'ambito di applicazione del Regolamento Generale sulla Protezione dei Dati (GDPR).
- Si applica tuttavia la Direttiva sulla Privacy Elettronica (E-Privacy). Essa stabilisce un divieto generale per le app di memorizzare informazioni su Smartphone e di accedere alle informazioni già memorizzate su Smartphone. Questo divieto può essere superato tramite consenso. Pertanto, le app per la ricerca di contatti possono funzionare legalmente solo con il consenso degli utenti.
- Questo consenso deve essere "fornito liberamente". Pertanto, esso non può essere ottenuto dagli Stati membri subordinando il diritto alla circolazione delle persone all'utilizzo dell'app.
- Gli Stati membri non sono nemmeno autorizzati a imporre legalmente l'uso di un'applicazione di registrazione di prossimità, in quanto mancano le basi giuridiche per derogare al divieto di cui sopra ai sensi della Direttiva E-Privacy.

Indice

1 Tracciamento digitale dei contatti

L'Organizzazione Mondiale della Sanità (OMS) definisce il tracciamento dei contatti come un processo di monitoraggio che comporta l'identificazione e la gestione dei contatti di casi d'infezione probabili o confermati. Ciò consente alle autorità sanitarie (i) di trattare rapidamente le persone infettate da una malattia contagiosa e (ii) di identificare rapidamente i casi secondari che possono insorgere dopo la trasmissione del contagio dai casi primari noti, con lo scopo di interrompere ulteriori contagi. Il tracciamento dei contatti viene effettuato mediante i seguenti passaggi:

1. identificare i contatti della persona che è risultata infetta;

2. informare tali contatti in merito a: i) lo stato dei loro contatti, ii) cosa significa lo stato dei loro contatti, (iii) le azioni che dovrebbero intraprendere in quanto persone potenzialmente infette e (iv) l'importanza di ricevere cure tempestive in caso di sviluppo di sintomi; la quarantena o l'isolamento potrebbero essere necessari per contatti ad alto rischio;

3. un regolare follow-up dei contatti per monitorare i sintomi e verificare la presenza di segni d'infezione[1].

Secondo il Centro europeo per la Prevenzione e il Controllo delle Malattie (ECDC), "il tracciamento dei contatti è una misura essenziale per combattere l'epidemia in corso di COVID-19, in combinazione con la ricerca di casi attivi ed i test, e in sinergia con altre misure come il distanziamento fisico".[2] L'ECDC riferisce che questa valutazione si basa, tra l'altro, sulle prove emergenti rispetto all'evoluzione della pandemia in Cina e a Singapore. In questi Paesi, l'efficiente tracciamento dei contatti ha ridotto al minimo l'intervallo dii tempo tra l'insorgenza dei sintomi e l'isolamento, e si ritiene che abbia contribuito notevolmente ad una lotta efficace contro il virus.[3]

La forma più tradizionale di ricerca dei contatti consiste nel chiedere alla persona infetta informazioni sui suoi movimenti e sulle persone con cui è stata in contatto nei tempi previsti ("i contatti"). La tecnologia digitale, tuttavia, consente alle autorità sanitarie di utilizzare strategie alternative e più efficienti, vale a dire strategie che riducono al minimo i costi di ricerca dei contatti in termini di tempo ed il bisogno di risorse umane. A questo riguardo, sono disponibili le seguenti opzioni:

- registrazione dei dati relativi all'ubicazione per rintracciare rapidamente i luoghi visitati dalla persona infetta entro i tempi previsti e controllare le persone che hanno visitato contemporaneamente anche questi luoghi; oppure

- registrazione solo di eventi epidemiologicamente rilevanti di prossimità della persona infetta ad altri soggetti, in modo che questi ultimi possano essere rapidamente identificati.

Qualunque sia l'opzione selezionata, le app per Smartphone sembrano essere lo strumento migliore per implementarla, dato che (i) gran parte della popolazione possiede uno Smartphone, (ii) le persone lo portano continuamente con sé e (iii) gli utenti esercitano un controllo esclusivo su di esso (il che significa che le persone generalmente non "prestano" il proprio Smartphone ad altri)[4].

---

1 https://www.who.int/news-room/q-a-detail/contact-tracing

2 ECDC, Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, p. 2.

3 ECDC, Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update, p. 2.

4 Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, p. 7.

Entrambe le opzioni sollevano, almeno potenzialmente, questioni di compatibilità con il quadro normativo dell'UE in materia di tutela della vita privata e di protezione dei dati personali. Dal momento che la loro configurazione finale avrà un'enorme influenza sull'esistenza e sulla natura delle problematiche relative alla protezione dei dati, sembra opportuno esaminare la legislazione applicabile in materia di protezione dei dati personali. Questo sarà l'oggetto del presente lavoro.

2 Possibilità di tracciamento digitale dei contatti ai sensi della normativa UE sulla protezione dei dati

2.1 Strumenti rilevanti per la protezione dei dati personali ai sensi del diritto dell'UE

La legalità del tracciamento digitale dei contatti, per quanto riguarda il trattamento dei dati e le restrizioni alla privacy, deve essere valutata con riferimento al Regolamento Generale sulla Protezione dei Dati (GDPR) e alla direttiva E-Privacy.

- Il GDPR[5] stabilisce norme riguardanti (i) la protezione delle persone fisiche per quanto riguarda il trattamento dei dati personali e (ii) la libera circolazione di tali dati nel mercato interno[6].

- La Direttiva E-Privacy[7][8] (i) armonizza le disposizioni nazionali che tutelano il diritto alla privacy e alla riservatezza con riferimento al trattamento dei dati personali nel settore delle comunicazioni elettroniche e (ii) garantisce la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica in tutta l'UE[9].

Il suo obiettivo dichiarato è quello di evidenziare e completare il GDPR[10] ai fini della protezione dei dati personali e della libera circolazione dei dati personali nel settore delle telecomunicazioni[11].

2.2 Opzione I – Un'app per la registrazione dei dati di localizzazione

Gli Smartphone consentono di monitorare costantemente i dati di localizzazione affidandosi a diverse infrastrutture tecnologiche. Tra queste, in particolare, il *Global Positioning System* (GPS), le stazioni di base GSM[12] ed il WiFi[13].

Un'app di tracciamento dei contatti potrebbe registrare e memorizzare tutti i dati di localizzazione di tutti gli utenti dell'app per consentire il tracciamento dei movimenti di ogni individuo. Se un soggetto

---

5 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati), GUUE L 119, 4.5.2016, p. 1.

6 Art. 1 (1) GDPR.

7 Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GUUE L 201, 31.7.2002, p. 37.

8 Sulla proposta COM(2017) 10 del 10.01.2017 di Regolamento del Parlamento Europeo e del Consiglio riguardante il rispetto della vita privata e la protezione dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla privacy e le comunicazioni elettroniche), v. Eckhardt P. e Hoffman A., https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2017_10_E-Privacy/cepPolicyBrief_COM_2017_10_Privacy_and_electronic_communications.pdf.

9 Art. 1 (1) Direttiva 2002/58/EC.

10 I riferimenti alla vecchia direttiva sulla protezione dei dati personali (direttiva 95/46/CE) nella Direttiva E-Privacy devono essere ora intesi come riferimenti alla GDPR (cfr. Art. 94 comma 2 GDPR).

11 Art. 1 (2) Direttiva 2002/58/EC.

12 Global System for Mobile Communications, in italiano Sistema Globale per Comunicazioni Mobili.

13 V. Art. 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 16 maggio 2011.

risulta infetto, tutti gli utenti dell'app che sono stati in contatto con lui saranno individuati incrociando i loro dati di localizzazione con quelli del caso contagiato da COVID-19. Essi riceveranno di conseguenza un messaggio di avvertimento.

I dati relativi all'ubicazione sono protetti dal GDPR perché si qualificano come "dati personali". Infatti, qualsiasi trattamento di informazioni relative a una persona fisica identificata o identificabile rientra nell'ambito di applicazione del GDPR[14]. Inoltre, il trattamento dei dati relativi all'ubicazione - ossia i dati trattati in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica, con l'indicazione della posizione geografica delle apparecchiature terminali dell'utente - è soggetto a severe limitazioni ai sensi della direttiva E-Privacy.[15]

In un documento recentemente indirizzato alla Commissione, il Comitato Europeo per la Protezione dei Dati (EDPB) ha espresso critiche su un'app per la registrazione dei dati di localizzazione. In particolare, secondo l'EDPB, l'elaborazione dei dati di localizzazione non è strettamente necessaria per raggiungere lo scopo di un efficace tracciamento dei contatti, perché esiste un'opzione diversa e meno invadente, cioè la registrazione di prossimità.[16] Ciò ha indotto l'EDPB a concludere che, oltre a creare rischi per la sicurezza e la privacy, "registrare i movimenti di un individuo attraverso le applicazioni di tracciamento dei contatti violerebbe il principio della minimizzazione dei dati".[17][18] Nella sua recente Guida, la Commissione UE ha condiviso la posizione dell'EDBP.[19]

2.3 Opzione II - Un'app per la registrazione di prossimità

L'alternativa a un'app per la registrazione della localizzazione dei dati è un'app che registra e memorizza solo i contatti epidemiologicamente rilevanti. Secondo la Commissione, l'app dovrebbe basarsi sulla tecnologia Bluetooth e potrebbe funzionare come segue[20].

1. L'app genererà degli identificatori temporanei dello Smartphone[21], e raccoglierà via *Bluetooth* gli identificatori temporanei che vengono prodotti dalle applicazioni che operano nei dispositivi vicini.

2. Tali rilevazioni ("*handshake*") saranno registrate in modo decentralizzato sul telefono o centralmente su un server[22] solo quando il contatto è epidemiologicamente rilevante, cioè quando comporta un effettivo rischio di infezione.[23] Ciò significa che il contatto deve durare abbastanza a lungo ed essere caratterizzato da un livello di vicinanza fisica sufficiente per la trasmissione del virus.

3. Infine, il meccanismo di allarme che avverte gli utenti dell'app che hanno avuto un contatto epidemiologicamente rilevante con un caso di COVID-19 sarà diverso a seconda che la registrazione sia centralizzata o meno. Nel primo caso, ossia quando la cronologia dei contatti del soggetto infetto viene

---

14 Art. 4(1) GDPR.
15 Art. 5(1), 6 e 9 Direttiva E-Privacy.
16 "Le applicazioni per il tracciamento dei contatti non richiedono il tracciamento della posizione dei singoli utenti. Il loro obiettivo non è quello di seguire i movimenti degli individui o di far rispettare le prescrizioni. " (https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodivappguidance_final.pdf).
17 https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf
18 Il principio di minimizzazione dei dati, sancito dall'art. 5 (1) (c) del GDPR, prevede che i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati".
19 Communication from the Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, C(2020) 2523, Brussels, 16.4.2020 (Commission Guidance).
20 Commission Guidance, p. 9.
21 Composto da sequenze di numeri e lettere che cambiano nel tempo.
22 La soluzione decentrata è più in linea con il principio di minimizzazione. Le autorità sanitarie dovrebbero avere accesso solo a dati di prossimità del dispositivo di una persona infetta, in modo che sia in grado di contattare le persone a rischio d'infezione (Commission Guidance, pag. 10).
23 Commission Guidance, p. 9.

caricata in una banca dati centrale, gli utenti dell'app con gli identificatori corrispondenti saranno automaticamente avvisati che potrebbero essere stati esposti (*server backend solution*). Nel secondo caso, quando cioè la cronologia dei contatti è memorizzata sul dispositivo, l'utente dell'app trovato contagiato dal COVID-19 può inviare un avviso agli altri utenti dell'app i cui identificatori sono elencati nella sua storia dei contatti (elaborazione decentralizzata).

2.3.1 La necessità del consenso dell'utente dell'app

Secondo la Commissione, i codici temporanei che l'app genera e raccoglie attivano solo i contatti per ricevere un avviso sul proprio Smartphone.[24] Non consentono l'identificazione degli Smartphone o il suo proprietario. Pertanto, i codici di cui sopra non si qualificano come dati personali e il loro trattamento non rientra nel campo di applicazione del GDPR.[25]

La memorizzazione delle informazioni sul dispositivo dell'utente o l'accesso alle informazioni già memorizzate è tuttavia ancora disciplinata dal quadro normativo dell'UE in materia di protezione dei dati personali, in quanto si applica l'art. 5 della Direttiva E-Privacy. Ai sensi della Direttiva, tali attività sono consentite soltanto:

- se intrinsecamente necessarie per fornire il servizio della società dell'informazione (*information society service*); o

- con il consenso dell'abbonato/utente.

La Commissione ritiene che una parte dei dati necessari per la ricerca dei contatti sia superiore a quanto è strettamente necessario per far funzionare l'app, ad esempio i codici temporanei di altri utenti. L'archiviazione e l'accesso alle attività non sono quindi intrinsecamente necessari. La loro legittimità è, pertanto, condizionata al previo consenso dell'utente.[26]

Secondo la direttiva E-Privacy, il consenso deve essere fornito in modo chiaro e completo con riferimento, tra l'altro, alle finalità del trattamento. Il concetto è analogo a quello di consenso ai sensi dell'art. 6 (1) (a) del GDPR.[27] Questo riferimento al GDPR è particolarmente rilevante, poiché impedisce agli Stati membri di porre per legge l'uso dell'app di ricerca di contatti come condizione per poter usufruire della libertà di movimento.

In effetti, l'interpretazione del consenso ai sensi dell'art. 6 (1) (a) GDPR deve essere in linea con l'approccio orientato ai diritti fondamentali della legislazione sulla protezione dei dati personali. Ciò significa che, poiché l'importanza del controllo dell'interessato sui suoi dati è espressamente riconosciuta dall'attuale legislazione vigente in materia di protezione dei dati personali. il requisito deve essere interpretato in modo da conferire all'interessato un sostanziale - e non solo formale - controllo sui propri dati.[28] Questo approccio all'interpretazione del consenso dovrebbe guidare anche la comprensione delle caratteristiche che il consenso deve possedere, ai sensi dell'articolo 4 (1) (11) GDPR, per essere valido ai fini del trattamento dei dati. In base a questa disposizione, per "consenso del soggetto titolare dei dati s'intende qualsiasi indicazione libera, specifica, informata e inequivocabile della

[24] "Se le autorità sanitarie desiderano contattare gli utenti che sono stati a stretto contatto con una persona infetta anche attraverso telefono o SMS, hanno bisogno del consenso di tali utenti per fornire i loro numeri di telefono" (Commission Guidance, pag. 9).
[25] Considerandum 26 GDPR.
[26] Commission Guidance, p. 6.
[27] Art. 5 (3) Direttiva E-Privacy.
[28] Art. 29 Working Party (Gruppo dell'articolo 29 per la tutela dei dati) (2017), p. 9.

volontà dell'interessato con la quale egli [...] esprime il consenso al trattamento dei dati personali a lui o lei riferiti".[29]

Il requisito della "libera prestazione del consenso"[30] esige quindi che l'interessato debba avere una reale possibilità di scelta tra l'accettazione e il rifiuto. Ciò sarebbe difficilmente possibile se all'interessato fosse posta l'alternativa tra utilizzare l'app o subire gravi limitazioni della sua libertà di movimento. In altre parole, gli Stati membri non possono far dipendere il diritto delle persone di circolare liberamente dal loro utilizzo dell'app. Tale condizionalità significherebbe che il consenso fornito dalle persone non è stato espressamente liberamente e sarebbe quindi privo di validità.

2.3.2 L'uso di un'app per la ricerca di contatti può essere imposto dalla legislazione nazionale?

Mentre il divieto generale di archiviazione e di accesso ai dati, di cui all'art. 5 della Direttiva E-Privacy, non lascia spazio all'obbligo nazionale di utilizzare le applicazioni di ricerca di contatti, l'art. 15 della stessa Direttiva E-Privacy potrebbe fornire una base giuridica adeguata per l'introduzione di tale obbligo da parte degli Stati membri. In base a questa disposizione, gli Stati membri possono superare le garanzie fornite dalla disciplina UE sulla protezione dei dati personali agli utenti dei servizi informatici, a condizione che

- lo facciano per via legislativa;

- ciò sia giustificato dalla necessità di salvaguardare la sicurezza nazionale (cioè la sicurezza dello Stato), la difesa, la sicurezza pubblica e la prevenzione, le indagini, l'accertamento e il perseguimento dei reati o dell'uso non autorizzato del sistema di comunicazione elettronica;

- si tratti di una misura necessaria, appropriata e proporzionata all'interno di una società democratica per salvaguardare gli obiettivi di cui sopra;

- ciò sia conforme ai principi generali del diritto comunitario, compresi i diritti, le libertà e i principi enunciati nella Carta dei Diritti Fondamentali dell'Unione Europea.

È interessante notare come l'art. 15 non elenchi la sanità pubblica tra i motivi che consentono agli Stati membri di limitare le garanzie concesse agli utenti dei servizi della società dell'informazione - in questo caso delle app - dalla Direttiva E-Privacy. Inoltre, ci sono buone ragioni per non permettere che si faccia affidamento su obiettivi di legge diversi da quelli espressamente elencati per limitare le garanzie offerte dalla Direttiva E-Privacy, e per non interpretare le motivazioni giuridiche in essa indicate (quali la "pubblica sicurezza") in modo tale da includervi la "sanità pubblica" nel significato inteso dall'art. 15.

Infatti, secondo la CGUE, l'elenco degli obiettivi stabilito dall'art. 15 è esaustivo[31] e soggetto a una rigorosa interpretazione.[32] In primo luogo, l'art. 15 deve essere inteso come una clausola che consente agli Stati membri di derogare a un obbligo generale del diritto dell'UE a cui sono soggetti, ad es. per garantire il rispetto per le garanzie contenute nella Direttiva E-Privacy. Di conseguenza, questa deve essere interpretata in modo rigoroso. In particolare, "tale disposizione non può giustificare che la

[29] Art. 4(11) GDPR.
[30] Art. 4 (1) e (11) GDPR.
[31] Sentenza del 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, EU:C:2016:970, par. 90; Conclusioni dell'Avvocato Generale M. Campo Sánchez-Bordona del 15 gennaio 2020, Ordre des barreaux francophones and germanophone and Others, C520/18, EU:C:2020:7, par. 34.
[32] Sentenza del 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, par. 89.

deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati, previsto dall'articolo 5 della medesima Direttiva [2002/58, Direttiva E-Privacy], divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata."[33] In secondo luogo, la stessa formulazione letterale dell'art. 15 chiarisce che le misure legislative devono essere giustificate sulla base di uno dei motivi di cui all'art. 15 (1), escludendo così che possano essere legittimamente invocati motivi supplementari.[34]

3 Conclusioni

Le app per la ricerca di contatti non sono di per sé incompatibili con il quadro normativo dell'UE in materia di privacy e protezione dei dati. Tuttavia, sulla base della nostra analisi della legge applicabile, è possibile individuare alcuni limiti giuridici.

In primo luogo, la legittimità di un'app per la registrazione dei dati di localizzazione, che l'EDPB e la Commissione hanno fortemente contestato, può essere esclusa. Ciò è dovuto all'esistenza di un'alternativa più rispettosa della protezione dei dati personali, ovvero le applicazioni di registrazione di prossimità.

In secondo luogo, un'app per la registrazione di prossimità può funzionare senza dati personali, ponendo così l'elaborazione dei dati relativi al di fuori del campo d'applicazione del GDPR. La Direttiva E-Privacy, invece, trova applicazione, e richiede il previo consenso dell'utente a che l'app possa memorizzare informazioni sul suo Smartphone, o accedere ad informazioni già memorizzate su quest'ultimo. Questo consenso deve essere "fornito liberamente" dall'utente dell'app, e quindi non può essere ottenuto dagli Stati membri facendo dipendere il diritto alla circolazione delle persone dall'uso dell'app.

Infine, la necessità del libero consenso dell'utente per il pieno funzionamento dell'app esclude che gli Stati membri possano imporne l'uso, né la Direttiva E-Privacy suggerisce che gli Stati siano autorizzati a farlo per ragioni di interesse pubblico.

[33] Sentenza del 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, par. 89.
[34] Sentenza del 21 dicembre 2016, Tele2 Sverige AB, cause riunite C-203/15 e C-698/15, par. 90.